ACTIVITEITENVERSLAG 2020
RAPPORT D'ACTIVITÉS 2020

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.

ACTIVITEITENVERSLAG 2020

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

Vast Comité van Toezicht op de
inlichtingen- en veiligheidsdiensten

Voorliggend *Activiteitenverslag 2020* werd door het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten goedgekeurd op de vergadering van 12 juli 2021.

(*getekend.*)
Serge Lipszyc, voorzitter
Pieter-Alexander De Brock, raadsheer
Thibaut Vandamme, raadsheer
Wauter Van Laethem, dienstdoend griffier

Activiteitenverslag 2020
Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

Alle rechten voorbehouden. Behoudens uitdrukkelijk bij wet bepaalde uitzonderingen mag niets uit deze uitgave worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt, op welke wijze ook, zonder de uitdrukkelijke voorafgaande toestemming van de uitgevers.

Ondanks alle aan de samenstelling van de tekst bestede zorg, kunnen noch de auteurs noch de uitgever aansprakelijkheid aanvaarden voor eventuele schade die zou kunnen voortvloeien uit enige fout die in deze uitgave zou kunnen voorkomen.

INHOUD

LIJST MET AFKORTINGEN

ADCC	Algemene Directie Crisiscentrum
ADIV	Algemene Dienst Inlichting en Veiligheid
AG	Administrateur-generaal (VSSE)
AGA	adjunct-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*
BPR	*Business Process Re-engineering*
BP&V	Brussel Preventie & Veiligheid
BS	Belgisch Staatsblad
BSS	*British Security Service* (ook gekend als MI5)
BTA	Bevoegde toezichthoudende autoriteit
CCB	Centrum voor Cybersecurity Belgium
CCIRM	*Collection Coordination Information Requirement Management* (ADIV)
CCIV	Coördinatiecomité Inlichtingen en Veiligheid
CHOD	*Chief of Defence*
CI	*Counterintelligence*
CNCTR	*Commission nationale de contrôle des techniques de renseignement*
CIA-model	Confidentiality, Integrity & Availability-model
COC	Controleorgaan voor politionele informatie
CRAB	Compte Rendu Analytique – Beknopt Verslag
CRIV	Compte Rendu Intégral – Integraal Verslag
CTG	*Counter Terrorism Group*
CTIVD	Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten
DA	Directeur Analyse (VSSE)

DIA	*Defence Intelligence Agency*
DISCC	*Defense Intelligence and Security Coordination Centre* (ADIV)
DoD	*US Department of Defense*
DPA	*Data Protection Authority*
DPO	*Data Protection Officer*
DRP	*Disaster recovery plan*
DVZ	Dienst Vreemdelingenzaken
EEAS	*European External Action Service*
EU INTCEN	*EU Intelligence and Analyses Centre*
EUMS	*European Union Military Staff*
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)
GCHQ	*General Communications Headquarters*
GGB	Gemeenschappelijke gegevensbank
GRU	Russische militaire inlichtingendienst
HTF	*Homegrown terrorist fighters*
Hand.	Handelingen
HP	Haatpropagandisten
HUMINT	*Human intelligence*
ICP	*Intelligence collection plan*
ICT	Informatie- en communicatietechnologie
IMINT	*Image intelligence*
ION	Instelling van openbaar nut
IPCO	*Investigatory Powers Commissioner's Office*
ISTAR-bataljon	*Intelligence, surveillance, target acquisition and reconnaissance*-bataljon
ITIL	*Information Technology Infrastructure Library*
IVS	Inlichtingen- en veiligheidsschool
JDR	*Joint Detection Reports*
JITF	*Joint Intelligence Task Force*
K.B.	Koninklijk besluit
KB C&VM	Koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen

KB FTF	Koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank 'Foreign Terrorist Fighters' en tot uitvoering van sommige bepalingen van de afdeling 1*bis* 'Het informatiebeheer' van hoofdstuk IV van de Wet op het politieambt
KB TF	Koninklijk besluit van 23 april 2018 tot wijziging van het Koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank 'Foreign Terrorist Fighters' en tot uitvoering van sommige bepalingen van de afdeling 1*bis* 'Het informatiebeheer' van hoofdstuk IV van de Wet op het politieambt en tot omvorming van de gemeenschappelijke gegevensbank 'Foreign Terrorist Fighters' naar de gemeenschappelijke gegevensbank 'Terrorist Fighters'
KB HP	Koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 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	Lokale integrale veiligheidscel
LTF	*Local task force*
M.B.	Ministerieel besluit
MEDINT/MEDINTEL	*Medical intelligence*
MoU	*Memorandum of Understanding*
MPG	Materie, problematiek, geografie
NA	*Note aux autorités*
NAVO	Noord-Atlantische Verdragsorganisatie
NISS	Rwandese inlichtingendienst
NOS	*Nato Office of Security*
NSIP	Nationaal Strategisch Inlichtingenplan
NSO	*NATO Standardization Office*
NVO	Nationale Veiligheidsoverheid
NVR	Nationale Veiligheidsraad
OCAD	Coördinatieorgaan voor de dreigingsanalyse
OSINT	*Open sources intelligence*
OTIR	*Operational Travel Inteligence Room*
Parl. St.	Parlementaire Stukken van Kamer en Senaat
PGE	Potentieel gewelddadige extremisten
Plan R	Actieplan Radicalisme
PNR-Wet	Wet van 25 december 2016 betreffende de verwerking van passagiersgegevens

PROTEUS	Gegevensbank OCAD
RFI	*Request for information*
RVVR	Ruimte voor Vrijheid, Veiligheid en Recht
SIDIS Suite	Penitentiaire gegevensbank
SIGINT	*Signals intelligence*
SIS	*Secret Intelligence Service* (ook gekend als MI6)
SITRAN	*Signalétique transversal* (gegevensbank FOD Financiën)
SOP	*Standard Operating Procedures*
SQL	*Structured query language*
TCEI	*Transatlantic Commission on Election Integrity*
TF	*Terrorist fighters*
TV	Terrorisme-veroordeelden
Vast Comité I	Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten
Vast Comité P	Vast Comité van Toezicht op de politiediensten
Vr. en Antw.	Schriftelijke vragen en antwoorden (Kamer of Senaat)
VSSE	Veiligheid van de Staat
W.Beroepsorgaan	Wet van 11 december 1998 houdende oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen
W.C&VM	Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen
W.I&V	Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst
W.OCAD	Wet van 10 juli 2006 betreffende de analyse van de dreiging
WPA	Wet van 5 augustus 1992 op het politieambt
W.Toezicht	Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse

WOORD VOORAF

2020 startte voor het Vast Comité I met de organisatie van een internationaal colloquium naar aanleiding van het tienjarig bestaan van de zgn. 'BIM-Wet'. Gastsprekers waren onder meer de voorzitter van de Kamer van Volksvertegenwoordigers, de vice-premier en minister van Justitie, de '*special rapporteur*' van de Verenigde Naties, de diensthoofden van de inlichtingen- en veiligheidsdiensten, de federale procureur, maar ook vertegenwoordigers van de orde van advocaten, van de pers en van het maatschappelijk middenveld. Ze hadden het in het bijzonder over de verdiensten van de inzet van bijzondere inlichtingenmethoden in België. In hun discours werd een evenwicht gezocht tussen enerzijds de bescherming van de veiligheid van de Staat en anderzijds de individuele rechten en vrijheden. Collega-vertegenwoordigers van onafhankelijke toezichthoudende autoriteiten uit Frankrijk, Nederland en Zwitserland namen eveneens deel aan deze reflectie.

Amper enkele weken later werden we geconfronteerd met het coronavirus (COVID-19). Deze pandemie deed niet alleen vragen rijzen – en doet dat nog steeds – over de bescherming van de burger en de eerbiediging van zijn individuele rechten en vrijheden, maar heeft ook de plaag van de desinformatie, '*fake news*' en pogingen om onze democratieën te destabiliseren, nieuw leven ingeblazen.

Onze samenleving werd geraakt door de impact van deze pandemie op onze bevolking en op de instellingen. Het dagelijkse leven werd grondig verstoord.

Dit onder meer door de invoering van 'telewerk' dat gedurende een lange periode verplicht werd voor zowel werknemers uit de particuliere als uit de openbare sector. Desondanks hebben de veiligheidsactoren moeten vaststellen dat zowel voor de inlichtingen- en veiligheidsdiensten als voor het Vast Comité I, het schier onmogelijk was om het concept 'thuiswerk' te implementeren. Deze onmogelijkheid is ongetwijfeld te wijten aan de aard van de functie en, zoals de geijkte uitdrukking luidt, aan de noodzaak van 'continuïteit van de dienstverlening'. Maar de voornaamste reden van de verplichting om in onze beveiligde werkomgeving te moeten blijven, is ingegeven door het ontbreken van een beveiligde, externe communicatie- en werkomgeving in België.

Het is inderdaad in de 21ste eeuw nog steeds onmogelijk om thuis of ergens anders dan binnen de muren van onze instellingen aan een geclassificeerd document te werken, of om op een veilige manier te communiceren over een 'GEHEIM' of 'ZEER GEHEIM'-item. Het aanhoudende gebrek aan investeringen door de Staat in dit soevereine domein, zou uiteindelijk kunnen laten uitschijnen dat de overheid onverschillig staat tegenover de inlichtingenwereld.

Niettegenstaande deze vaststelling, wil het Vast Comité I benadrukken en toejuichen dat de activiteiten van zowel de inlichtingen- en veiligheidsdiensten als deze van het toezichtorgaan tijdens de hele pandemie onverdroten werden verdergezet, vaak onder druk om de individuele gezondheidsvoorschriften nauwgezet na te leven. En dit ondanks het feit dat er geen enkel vaccinatieplan was voor de medewerkers die in deze periode voor de veiligheidsinstellingen werkten.

Het democratisch toezicht op de diensten werd versterkt. Het Comité heeft aan de Kamer van volksvertegenwoordigers zijn methodologie van voortdurende verificatie voorgelegd om te garanderen dat de tussenkomst van de inlichtingendiensten wat betreft de werkzaamheden van politieke mandatarissen, niet het voorwerp vormde van toezicht of controle buiten het wettelijk kader.

De evolutie van extreemrechts in Europa en in vele andere democratieën heeft ons ertoe gebracht om, voor het eerst in de geschiedenis, te analyseren hoe de inlichtingen- en veiligheidsdiensten met deze dreiging omgaan.

Verder werd de aandacht ook gevestigd op de wijze waarop de relaties tussen de twee inlichtingendiensten met buitenlandse partners worden verwezenlijkt. Het Vast Comité I maakte van deze gelegenheid gebruik om te benadrukken dat controle door de regering de hoeksteen moet blijven van het 'internationale beleid' van de inlichtingen- en veiligheidsdiensten.

In het streven naar een betere werking van het administratief rechtscollege inzake veiligheidsmachtigingen, -attesten en -adviezen, werd het Parlement een tekst voorgelegd waarin de werking van deze jurisdictie wordt aangepast. Het is niet alleen de bedoeling dat zij de 'natuurlijke rechter' wordt op het gebied van veiligheid, maar ook dat de toegang voor de rechtzoekende wordt vergemakkelijkt. Daarom werd tevens een afzonderlijke website voor het beroepsorgaan gecreëerd (www.beroepsorgaan.be).

Onze dagelijkse werkzaamheden omvatten ook de behandeling van klachten van burgers. Deze klachten worden beantwoord door het Vast Comité I alleen, hetzij in overleg met andere bevoegde instanties zoals het Vast Comité P, het Controleorgaan op de politionele informatie (COC), de Gegevensbeschermingsautoriteit (GBA) of de Federale Ombudsmannen. Vast staat dat de burgers worden geconfronteerd met een lawine van instellingen op het gebied van gegevensbescherming. Het Vast Comité I dringt aan op vereenvoudiging op dit gebied in het kader van de geplande herziening van de Gegevensbeschermingswet (GBW).

Het bovenstaande is slechts een weerspiegeling van de veelzijdige activiteiten die het Comité onder vele verschillende petten uitvoert: toezichthouder/auditor in het kader van de toezichtonderzoeken, juridische adviseur in verband met verschillende belangrijke adviezen op parlementair niveau, een luisterend oor in het debat over het sociaal statuut van de agenten van de inlichtingendienst, hervormer in verband met de managementverandering in de schoot van de ADIV, initiatiefnemer van wetgevingsprojecten, (mede)auteur van alle activiteitenverslagen die door de wetgever worden opgelegd (bijv. in het kader van BELPIU, de gemeen-

schappelijke gegevensbanken, de gegevensbeschermingsautoriteit, het gebruik van bijzondere inlichtingenmethoden), boekhouder wanneer het gaat om bijzondere fondsen, en rechter met meer dan 200 beslissingen van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen. En zoals Aristoteles schreef: "*het geheel is meer dan de som der delen*".

Aangezien het takenpakket steeds wordt uitgebreid, is het Comité de mening toegedaan dat op het moment dat de Kamer een debat op gang heeft gebracht over de synergiën tussen bepaalde instellingen of over het statuut van hun personeel, de vraag van het Vast Comité I om bijkomende budgettaire middelen voor de uitbouw van haar beveiligd computernetwerk, niet langer meer uit de weg kan worden gegaan. Het Comité moet worden versterkt, en wel snel: de personeelsleden maken zich zorgen en die zorgen openen de deur voor een gebrek aan motivatie, terwijl net die motivatie in deze woelige tijden goed kan worden gebruikt. De administratieve inertie *sensu lato*, de onzekerheid over de toekomst van onze instelling en de broosheid van de door de wet geboden rechtspositie lag trouwens aan de basis van het ontslag van één van de drie raadsheren van het Vast Comité I. Maar veel meer dan het lot van onze instelling en onze personeelsleden, staat de toekomst van de democratie op het spel.

Het gegeven dat het Comité niet de middelen krijgt die het nodig heeft om zijn wettelijke taken te vervullen, legt een zware verantwoordelijkheid op de schouders van de politieke wereld. Het Vast Comité I is het Argos-baken van onze Staat: we kunnen natuurlijk wel zonder baken de zee opgaan, maar als het schip in de storm terechtkomt, is het het enige dat ons in staat stelt hulp bij te sturen naar waar dat nodig is.

De aanslagen in Zaventem en Brussel zijn de duidelijkste voorbeelden van de noodzaak om te investeren in de strijd tegen de verschillende vormen van dreiging die ons meer ooit te wachten staan. We weten vandaag dat niemand veilig is. Samen met de inlichtingen- en veiligheidsdiensten, is het Vast Comité I betrokken bij de dagelijkse strijd tegen deze levensgevaarlijke dreigingen, gekend onder de noemers 'terrorisme', 'extremisme', 'spionage', 'inmenging, 'proliferatie', 'criminele organisatie', 'sektarische organisaties, 'cyberaanval'...

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

28 juni 2021

HOOFDSTUK I
DE TOEZICHTONDERZOEKEN

In 2020 finaliseerde het Vast Comité I acht toezichtonderzoeken, waarvan één gezamenlijk met het Vast Comité van Toezicht op de politiediensten (I.1 tot I.8). Het zijn diverse instanties of personen die het Comité kunnen 'vatten' met een toezichtonderzoek: de parlementaire Begeleidingscommissie, de voogdijministers, elke (rechts)persoon die klacht of aangifte wenst te doen… Het Comité kan ook zelf het voortouw nemen: zeven van de acht in 2020 gefinaliseerde onderzoeken werden ambtshalve opgestart. Slechts één onderzoek werd uitgevoerd op verzoek van de parlementaire Begeleidingscommissie. Verder opende het Comité in 2020 zeven nieuwe onderzoeken. Een korte omschrijving van de nog lopende en/of opgestarte onderzoeken, volgt in I.11. De naar aanleiding van de toezichtonderzoeken geformuleerde aanbevelingen werden gebundeld in Hoofdstuk XII.

In totaal ontving het Comité in 2020 62 klachten of aangiften.[1] Na een kort vooronderzoek en de verificatie van een aantal objectieve gegevens, wees het Comité 55 klachten of aangiften af omdat ze kennelijk niet gegrond waren[2] (art. 34 W.Toezicht) en in een geval was het Comité onbevoegd om de opgeworpen vraag te behandelen. In dat laatste geval werd de klager doorverwezen naar de bevoegde instantie (de Brusselse procureur des Konings). Van de zes behandelde klachten konden er drie worden afgerond in 2020, twee klachten zijn nog lopende en één klacht werd gehercategoriseerd als DPA-klacht (cf. Hoofdstuk V).

Naast toezichtonderzoeken opent het Vast Comité I ook zogenaamde 'informatiedossiers' die moeten toelaten om een respons te bieden op vragen met betrekking tot de werking van de inlichtingendiensten en het OCAD.[3] Indien dergelijke dossiers aanwijzingen van disfuncties aan het licht brengen of van aspecten van de werking van inlichtingendiensten die nader onderzoek behoeven, kan het Comité overgaan tot het opstarten van een toezichtonderzoek. Indien echter duidelijk is dat een dergelijk onderzoek geen meerwaarde ressorteert vanuit de doelstellingen

---

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 De aanleiding voor het opstarten van informatiedossiers is zeer divers: de directie van een inlichtingendienst maakt melding van een incident en het Comité wil nagaan hoe het werd afgehandeld; de media melden een voorval en het Comité wil weten of dit strookt met de realiteit en of er een meer algemene problematiek achter schuilgaat…

van het Vast Comité I, krijgt het informatiedossier geen verder gevolg. In 2020 werden onder meer informatiedossiers geopend over het disfunctioneren (meer bepaald een gebrek aan informatiedoorstroming) van de administraties en openbare overheden, waarbij het 'vakjesdenken' verhinderde om de veiligheid van de burger te kunnen garanderen[4] en werd er gereflecteerd over de ontwikkeling van een Kruispuntbank Veiligheid. Drie van deze informatiedossiers (over de coronakwestie en de bevoegdheid van de inlichtingendiensten, het sociaal overleg in de schoot van de Veiligheid van de Staat en incidenten in een buitenlandse operatiezone) vormden het onderwerp van bespreking met de parlementaire Begeleidingscommissie en maken onderdeel uit van voorliggend hoofdstuk.

I.1. DE ONDERSTEUNENDE DIENSTEN VAN HET OCAD

Het Vast Comité I heeft, gezamenlijk met het Vast Comité P, een toezichtonderzoek verricht naar de ondersteunende diensten van het Coördinatieorgaan voor de dreigingsanalyse (OCAD).[5] Dit onderzoek had in het bijzonder 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). 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. De inlichtingendiensten (VSSE en ADIV) en de politiediensten (Federale Politie en lokale politiezones) maakten geen voorwerp uit van dit onderzoek.[6] Ook de in 2018 bijkomend aangewezen ondersteunende diensten (het Crisiscentrum van de FOD Binnenlandse Zaken, de Thesaurie van de FOD Financiën, het Gevangeniswezen en de dienst Erediensten en Vrijzinnigheid bij de FOD Justitie) maakten geen voorwerp uit van voorliggend onderzoek.[7]

---

4 Het Comité wees de Regering ook op de recurrentie van dit probleem, dat al werd onderstreept tijdens de werkzaamheden van de Parlementaire Onderzoekscommissie naar de 'terroristische aanslagen' van 22 maart 2016.

5 Het onderzoek werd opgestart halfweg januari 2018 en afgesloten halfweg juni 2020.

6 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').

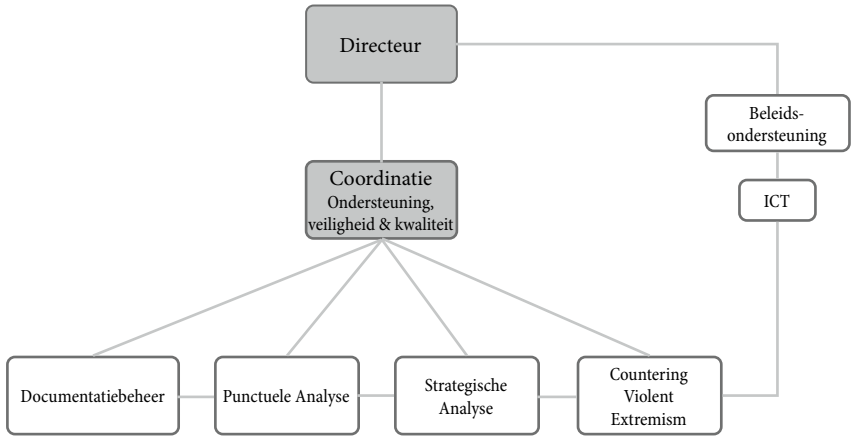
7 Bij KB van 17 augustus 2018 werd de lijst van ondersteunende diensten van het OCAD uitgebreid met deze vier diensten. Deze diensten maakten geen deel uit van het voorwerp van dit onderzoek omdat het te vroeg was om de informatiestroom en de in dat kader geïmplementeerde processen te kunnen analyseren (cf. I.11.9.).

I.1.1. ALGEMEEN KADER

I.1.1.1. Het OCAD: bevoegdheden, structuur en informatiebeheer

De kerntaak van het OCAD bestaat erin op eigen initiatief of op verzoek van bepaalde overheden punctuele of strategische evaluaties te maken over dreigingen inzake terrorisme en extremisme.[8] Daarnaast heeft het Coördinatieorgaan nog andere opdrachten: de samenwerking met gelijkaardige buitenlandse en internationale diensten, de coördinatie van het Actieplan Radicalisme (Plan R) van de federale regering, de functie van operationeel verantwoordelijke van de gemeenschappelijke gegevensbank *Terrorist Fighters* en Haatpropagandisten (GGB TF&HP), de strategische evaluaties van de dreiging voor kritieke infrastructuren, de evaluaties bij de bevriezing van tegoeden en de adviesverlening bij de intrekking van identiteitskaarten.

Organisatorisch bestaat het OCAD in principe, naast een directeur en adjunct-directeur, uit vier operationele departementen (dossier- en documentatiebeheer, punctuele analyse, strategische analyse en *countering violent extremism*), een coördinatiedienst en twee ondersteunende afdelingen (strategische ondersteuning en informatietechnologie).



8 Deze opdrachten staan omschreven in de Wet van 10 juli 2006 houdende analyse van de dreiging (W.OCAD) en in het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 houdende analyse van de dreiging (KB OCAD).

Het departement Dossier- en documentatiebeheer, samengesteld uit administratieve personeelsleden[9], is belast met het actualiseren van de OCAD-gegevensbank en de gemeenschappelijke gegevensbank. Deze afdeling, die tegelijkertijd *front office* (beheer van inkomende documenten en van de wachtdienst[10]) en *back office* (voor het beheer van dossiers) is, vormt het zenuwcentrum voor het informatiebeheer van het OCAD. Daarnaast behoort het verzamelen en verwerken van informatie via sociale media en *open source intelligence* tot het takenpakket.

Het departement Punctuele Analyse bestaat uit personeelsleden gedetacheerd uit de ondersteunende diensten (de zgn. deskundigen).[11] Deze afdeling is belast met het opstellen van de punctuele dreigingsevaluaties en staat in voor de verbinding met de ondersteunende diensten van het OCAD. Ze staat ook in voor de daadwerkelijke behandeling van de documenten die op het OCAD toekomen vanuit de ondersteunende diensten en voor het opmaken van verzoeken om informatie (*Request for information*, RFI) naar deze diensten. De deskundigen nemen ook deel aan werkgroepen van het Plan R, aan lokale *taskforces* (LTF)[12] en voorzien in de opvolging van een aantal *terrorist fighters* en/of haatpropagandisten. Buiten de kantooruren oefenen ze de functie van wachtdienstofficier uit.

Het departement Strategische Analyse bestaat uit personeelsleden met een specifiek personeelsstatuut dat exclusief verbonden is met het OCAD (de zgn. analisten). De afdeling heeft als voornaamste opdracht om op periodieke basis de belangrijkste dreigingen ten opzichte van ons land en de Belgische belangen in het buitenland te identificeren en hun verwachte evolutie te schetsen in strategische analyses en nota's.

Het departement Countering Violent Extremism is samengesteld uit personeelsleden die door de FOD Binnenlandse Zaken aan het OCAD ter beschikking werden gesteld of die door bepaalde ondersteunende diensten werden gedetacheerd. Het departement is in de eerste plaats belast met het beheer en de

---

9 De personeelsleden van het OCAD hebben verschillende statuten. Elke gedetacheerde deskundige en gedetacheerd administratief personeelslid behoudt het personeelsstatuut van zijn oorspronkelijke dienst. Daarnaast zijn er analisten en administratieve medewerkers die met eigen middelen van het OCAD zijn aangeworven. Die verschillende statuten veroorzaken problemen binnen het OCAD: ze kunnen frustraties veroorzaken (in het bijzonder het verschil met betrekking tot de wachtdiensten waarvoor sommigen betaald worden en anderen inhaalrust krijgen en het verschil in statuut tussen de gedetacheerde deskundigen en de analisten (statuut A3)).

10 Het OCAD garandeert namelijk 24 uur per dag en zeven dagen per week een wachtdienst.

11 De van de ondersteunende diensten afkomstige deskundigen worden gedetacheerd voor een hernieuwbare periode van vijf jaar. Ze vormen niet het voorwerp van een specifieke evaluatie in het kader van hun functie bij het OCAD. Hun statuut is gebaseerd op hun statuut in hun oorspronkelijke dienst. Volgens de directie van het OCAD is het aanbevolen om een zekere continuïteit te hebben bij de deskundigen omdat ze door het OCAD worden opgeleid wat betreft terrorisme en extremisme, wat niet gebeurt binnen hun oorspronkelijke dienst.

12 Lokale *taskforce* (LTF): een "*overlegplatform, ingericht op gedeconcentreerd niveau, waarbinnen informatie en inlichtingen over gewelddadige radicalisering worden uitgewisseld en coördinatie-afspraken gemaakt worden over het inwinnen van deze informatie*" in: Derde tussentijds verslag over het onderdeel 'Veiligheidsarchitectuur' van de Parlementaire onderzoekscommissie, *Parl. St.* Kamer 2017-18, 54K1752/008, 162.

coördinatie van het Plan R. Daarnaast nemen ook deze personeelsleden deel aan lokale *taskforces*, en worden ze ingeschakeld in de opvolging van een aantal *terrorist fighters* en/of haatpropagandisten.

De Coördinatiedienst tot slot is belast met het operationeel vertalen naar de verschillende departementen van de beslissingen van de OCAD-directie. Ze is eveneens verantwoordelijk voor de betrokken werklastverdeling en samenwerking.

Het OCAD beheert en verwerkt een grote hoeveelheid informatie en documenten. Om het beheer ervan te organiseren beschikt het over een gegevensbank, PROTEUS genaamd, waarvan uitsluitend het OCAD-personeel een toegangsrecht heeft. Elk personeelslid heeft de mogelijkheid om gegevens in te voeren in deze gegevensbank.

I.1.1.2. De ondersteunende diensten: meldingsplicht, middelen en procedures

De wetgever en de Koning hebben verschillende instrumenten en middelen ingesteld om de informatie-uitwisseling tussen het OCAD en de ondersteunende diensten te organiseren. Vooreerst voorziet de W.OCAD in een meldingsplicht. Krachtens artikel 6 W.OCAD zijn overheidsinstanties die aangewezen zijn als ondersteunende dienst van het OCAD namelijk verplicht om ambtshalve of op vraag van de OCAD-directeur alle inlichtingen waarover zij in het kader van hun opdrachten beschikken en die relevant zijn voor de evaluatieopdrachten van het OCAD, aan laatstgenoemde over te maken. Het niet naleven van deze meldingsplicht door de ambtenaren van de ondersteunende diensten wordt strafrechtelijk gesanctioneerd.[13]

Artikel 11 § 1 KB OCAD bepaalt vervolgens dat iedere ondersteunende dienst in zijn schoot een 'centraal contactpunt' moet aanstellen dat belast is met: (1) de uitwisseling van inlichtingen met het OCAD, (2) de efficiënte verspreiding van deze inlichtingen binnen de ondersteunende dienst waarvan het afhangt, en (3) het waken over de ambtshalve mededeling aan het OCAD, binnen de kortste termijn, van alle voor de evaluatieopdrachten van het OCAD relevante inlichtingen waarover de betrokken ondersteunende dienst beschikt. Het KB OCAD verduidelijkt echter niet wat het bedoelt met een 'centraal contactpunt'. Het kan zodoende gaan om een personeelslid dat daarvoor wordt aangesteld of om een dienst die bestaat uit meerdere personen. Er wordt in het KB ook niet verduidelijkt dat de aanstelling van een centraal contactpunt de mogelijkheid van andere contactpunten binnen de ondersteunende dienst uitsluit.[14] De toepassing van het KB veronderstelt wel dat een lid van het personeel (of een dienst) duidelijk wordt geïdentificeerd als centraal contactpunt en specifiek wordt belast met de aan dit contactpunt toegekende opdrachten.

---

13 Artikel 14 W.OCAD.

14 In deze zin is het beter om het te hebben over het voornaamste contactpunt.

Artikel 7 § 1 W.OCAD stelt dat het OCAD samengesteld moet worden uit, onder meer, deskundigen die worden gedetacheerd uit de ondersteunende diensten. Het koninklijk besluit van 23 januari 2007 betreffende het personeel van het Coördinatieorgaan voor de dreigingsanalyse bepaalt verder dat de gedetacheerde deskundigen fungeren als verbindingsofficier naar hun dienst van oorsprong.[15] Een aspect binnen de taakstelling van deze categorie van personeelsleden bestaat bijgevolg uit het verzorgen van de band met hun oorspronkelijke dienst en zodoende uit het bevorderen van de informatiestroom met de ondersteunende dienst. De deskundigen vormen echter niet de enige contactpunten voor hun diensten van oorsprong. Er kunnen ook rechtstreekse contacten bestaan tussen andere leden van het OCAD en het personeel van de ondersteunende diensten. Voor de directie van het OCAD schaadt een dergelijke werkwijze de informatie-uitwisseling niet, aangezien alle relevante informatie wordt ingevoerd in de PROTEUS-gegevensbank.

De concrete informatiestroom tussen het OCAD en zijn ondersteunende diensten wordt georganiseerd naargelang de documenten al dan niet geclassificeerd zijn. De informatiestroom wordt zodoende georganiseerd overeenkomstig de Classificatiewet van 11 december 1998[16] en het uitvoeringsbesluit van 24 maart 2000.[17] Beide rechtsnormen bevatten strenge regels voor de bewaring, raadpleging, reproductie, overmaking en vernietiging van geclassificeerde informatie. Geclassificeerde documenten kunnen tussen het OCAD en de ondersteunende diensten uitgewisseld worden via het BINII-systeem.[18] Beschikt een ondersteunende dienst niet over een dergelijk systeem, dan worden geclassificeerde documenten verzonden per koerier. Via de installatie van dit BINII-systeem, dat functioneel beheerd wordt door de ADIV, werd tegemoet gekomen aan artikel 11 § 7 KB OCAD dat bepaalt dat een beveiligd en gecodeerd communicatie- en informatiesysteem dient te worden ingevoerd ten einde de communicatiesnelheid tussen het OCAD en de ondersteunende diensten te vergemakkelijken. De ondersteunende diensten dienen te voldoen aan bepaalde beveiligingsvereisten, waaronder infrastructurele veiligheidsmaatregelen en het beschikken over een veiligheidsofficier.

Centraal bij de uitwisseling en het beheer van alle niet-geclassificeerde *in*- en *out*-documenten staat de functionele mailbox van het OCAD. Tijdens de kantooruren wordt deze mailbox opgevolgd door het departement Dossier- en documentatiebeheer. Buiten de kantooruren ligt de kennisname van de informatie en de verdere verwerking bij de aangeduide wachtdienstofficier, m.a.w. bij een gedetacheerde deskundige (departement Punctuele Analyse).[19]

---

15 Bijlage 3.B. Profielbeschrijving voor gedetacheerd expert bij OCAD van niveau A bij het KB van 23 januari 2007.

16 Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

17 KB van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

18 BINII staat voor *Belgian Intelligence Network Information Infrastructure*.

19 De gedetacheerde deskundigen worden via een beurtrol aangewezen als wachtdienstofficier.

I.1.2. DE INFORMATIESTROOM TUSSEN HET OCAD EN DE VIER ONDERZOCHTE ONDERSTEUNENDE DIENSTEN

I.1.2.1. FOD Binnenlandse Zaken – Dienst Vreemdelingenzaken[20]

Binnen de Dienst Vreemdelingenzaken (DVZ) zijn er hoofdzakelijk twee diensten die in contact staan met het OCAD: de cel Radicalisme en de cel Opsporingen. De cel Radicalisme werd opgericht in mei 2016 en bestond bij afsluiting van het toezichtonderzoek uit acht personeelsleden.[21] Ze valt onder de afdeling Beleidsondersteuning, die rechtstreeks afhangt van de directeur-generaal van de Dienst Vreemdelingenzaken. De cel Opsporingen valt onder de directie Controle Binnenland en Grenzen, en bestaat uit een twintigtal personen. Deze cel wordt beschouwd als het contactpunt van de Dienst Vreemdelingenzaken voor alle partnerdiensten.[22] Voor wat betreft de rechtstreekse contacten met het OCAD vormt echter de cel Radicalisme het voornaamste contactpunt.

Er zijn twee deskundigen gedetacheerd uit de Dienst Vreemdelingenzaken naar het OCAD, waarvan één de functie van leidinggevende van het departement Punctuele Analyse uitoefent. Het is voornamelijk de tweede gedetacheerde die de rol van verbindingsofficier met de Dienst Vreemdelingenzaken op zich neemt. De twee deskundigen hebben geen rechtstreekse toegang tot de DVZ-gegevensbanken Evibel en VisaNet.[23]

De informatie-uitwisseling van het OCAD met de Dienst Vreemdelingenzaken is, na deze met de politie- en inlichtingendiensten, de meest omvangrijke van alle ondersteunende diensten. De geïmplementeerde procedures beperken daarenboven sterk de mogelijkheid dat informatie verloren gaat.[24] Bovendien neemt de Dienst Vreemdelingenzaken deel aan de lokale *taskforces*, waardoor een regelmatige samenwerking met het OCAD verzekerd is.

De aanzienlijke informatiestroom tussen het OCAD en de DVZ is grotendeels te wijten aan de grote toename van het aantal veiligheidsscreenings[25] van asielzoekers die aan het OCAD werden gevraagd na de aanslagen in Parijs en Brussel (via de cel Radicalisme). Ook de installatie van een tweede gedetacheerde deskundige in 2016 en de actieve rol van de DVZ in het kader van de gemeenschappelijke gegevensbank (waarvoor het OCAD de operationele verantwoordelijkheid

---

20 De Dienst Vreemdelingenzaken is een algemene directie van de FOD Binnenlandse Zaken, die onder leiding staat van een directeur-generaal.

21 In juni 2019 bestond de cel Radicalisme nog uit slechts zes personen.

22 De verantwoordelijke van de cel Opsporingen is tevens de veiligheidsofficier van de Dienst Vreemdelingenzaken.

23 Ze hebben ook geen toegang tot de penitentiaire gegevensbank Sidis Suite.

24 Functionele mailboxen staan in kopie.

25 Om na te gaan of personen al dan niet gekend zijn of om bijgewerkte informatie te bekomen over reeds gekende personen.

draagt) dragen bij aan de omvang van de informatiestroom.[26] Met betrekking tot de verzoeken tot veiligheidsscreening rijst wel de vraag hoe gepast die is. De Dienst Vreemdelingenzaken bevraagt hiervoor immers reeds andere diensten (zoals de VSSE en de politiediensten). Ook rijst de vraag in hoeverre het OCAD bevoegd is om te antwoorden, aangezien het OCAD niet de originele houder van de informatie is (regel van de derde dienst[27]).

De veiligheidsmaatregelen met betrekking tot geclassificeerde documenten worden nageleefd en toegepast door de veiligheidsofficier (systeem van dubbele omslagen, koffertje voor het transport van geclassificeerde documenten, beveiligde kamer met kluis, veiligheidsmachtigingen, aangepaste inhoud vreemdelingendossiers[28]...). De veiligheidsofficier heeft in het gebouw waarnaar de Dienst Vreemdelingenzaken is verhuisd, alle veiligheidsmaatregelen getroffen.

I.1.2.2. FOD Buitenlandse Zaken

Binnen de FOD Buitenlandse Zaken vormt de dienst M1.3 het voornaamste contactpunt voor het OCAD. Deze dienst is belast met de strijd tegen het terrorisme en heeft binnen zijn takenpakket de coördinatie van het Plan R binnen de FOD.[29] Vanuit deze hoedanigheid neemt de dienst deel aan diverse werkgroepen binnen het actieplan en geeft in dat kader de relevantie informatie door binnen de FOD. Het geeft ook de informatie van de diplomatieke posten door aan andere overheidsdiensten.[30] De dienst M1.3 behandelt echter geen individuele gevallen. Het OCAD heeft eveneens rechtstreekse contacten met andere diensten van de FOD Buitenlandse Zaken, voornamelijk de dienst C1.2 (internationale gerechtelijke samenwerking[31]), de dienst C2.3 (monitoring van reis- en identiteitsdocumenten[32]),

---

26 Alle leden van de cel Radicalisme hebben toegang tot de gemeenschappelijke gegevensbank.

27 De regel van de derde dienst bepaalt dat uitsluitend de houder van de informatie, dat wil zeggen degene die aan de oorsprong van de informatie ligt, mag beslissen aan wie de informatie wordt bekendgemaakt.

28 Geclassificeerde informatie of informatie met beperkte verspreiding is niet zichtbaar in het individuele dossier van de asielzoeker of, meer algemeen, van de migrant. Elk lid van de DVZ dat dit soort dossiers behandelt kan wel zien dat er dergelijke informatie beschikbaar is bij de cel Radicalisme of de veiligheidsofficier.

29 De dienst Strijd tegen het terrorisme (M1.3) valt onder de directie Veiligheidspolitiek (M1) van de directie-generaal Multilaterale Zaken en Mondialisering (DGM).

30 Naast het OCAD gaat het bijvoorbeeld om de VSSE, de ADIV, de politie, de DVZ…

31 De dienst Internationale gerechtelijke samenwerking (C1.2) valt onder de directie Noodbijstand en gerechtelijke zaken (C1) van de directie-generaal Consulaire Zaken (DGC). De dienst is het unieke contactpunt terrorisme voor de diplomatieke posten in het buitenland. Het ontvangt informatie van die posten en geeft die door aan, met name, het OCAD (met de dienst M1.3 in kopie). Het gaat hier om dossiers voor de internationale gerechtelijke samenwerking met betrekking tot terrorisme, individuele gevallen die gekend zijn voor terrorisme/radicalisme en Belgen in buitenlandse gevangenissen.

32 De dienst Monitoring (C2.3) valt onder de directie Reis- en identiteitsdocumenten (C2) van de directie-generaal Consulaire Zaken (DGC). De dienst is belast met het beheer van de PASSBAN-procedure, de procedure voor de intrekking van reisdocumenten (paspoorten).

de directie S1 (security[33]) en de directie P (protocol en veiligheid[34]). Ook de directie-generaal Bilaterale Zaken staat in contact met het OCAD voor de uitwerking van algemene analyses van (geo)politieke situaties, met het doel om de politieke situatie van België te verduidelijken.[35] Er werd door de FOD Buitenlandse Zaken één deskundige gedetacheerd naar het OCAD.

Volgens zowel het OCAD als de FOD Buitenlandse Zaken verhindert de veelheid aan contactpunten niet dat de informatie goed circuleert. De Comités merkten daarentegen in hun onderzoek wel op dat er informatie verloren zou kunnen gaan bij de FOD Buitenlandse Zaken vanwege de talrijke rechtstreekse contacten met het OCAD. Om dit te vermijden, moet men binnen de FOD Buitenlandse Zaken eraan denken de dienst M1.3 op de hoogte te brengen (bijv. via de functionele mailbox) van informatie-uitwisselingen.

Wat betreft beveiliging, is de FOD Buitenlandse Zaken de enige van de vier onderzochte ondersteunende diensten die over het BINII-systeem beschikt.[36] Ook de procedures voor geclassificeerde documenten werden nageleefd. De FOD Buitenlandse Zaken beschikt over diverse veiligheidsofficieren.

I.1.2.3. FOD Mobiliteit en Vervoer

Binnen de FOD Mobiliteit en Vervoer verzorgt de in 2015 opgerichte Crisiscel[37] het voornaamste contact met het OCAD.[38] De cel vormt eveneens het contactpunt met het Nationaal Crisiscentrum (NCCN), de Nationale Veiligheidsoverheid (NVO),

---

33 De directie Security (S1) hangt rechtstreeks af van de voorzitter van het directiecomité van de FOD. Ze is, onder meer, samengesteld uit de dienst Crisiscentrum (S1.1) die het beheer van de crisisdossiers van de diplomatieke posten en van het crisiscentrum tot het takenpakket heeft, en de dienst Veiligheid (S1.2) hoofdzakelijk belast met de veiligheid van de personeelsleden en van de gebouwen zowel op het Hoofdbestuur als op de diplomatieke en consulaire posten in het buitenland. Ze is zodoende belast met de interne veiligheid van de FOD Buitenlandse Zaken.

34 De directie Protocol en Veiligheid (P) valt rechtstreeks onder de voorzitter van het directiecomité van de FOD. De directie is onder meer verantwoordelijk voor de bescherming van personen en goederen die deel uitmaken van de diplomatieke zendingen in België. Het Protocol merkte gedurende het toezichtonderzoek op dat het de logica achter de analyse van het OCAD niet altijd begrijpt. Soms zijn er VIP-bezoeken die omwille van de persoon of de banden met ons land een indeling in niveau 2 zouden verdienen, maar niveau 1 krijgen, en andere waarvan men zou verwachten dat ze niveau 1 krijgen, die niveau 2 krijgen. De dienst zou ook graag op de hoogte worden gebracht van niveauwijzigingen wanneer bepaalde VIP's overgaan naar niveau 3.

35 Er worden interdepartementale vergaderingen georganiseerd waaraan het departement Strategische Analyse van het OCAD deelneemt.

36 Op het moment dat het toezichtonderzoek werd uitgevoerd (midden 2018). De Dienst Vreemdelingenzaken en de FOD Mobiliteit en Vervoer hadden aangegeven dat ze eveneens zouden beschikken over het systeem.

37 Op het ogenblik van het toezichtonderzoek bestond deze cel uit drie personen, die samen twee voltijdse equivalenten vormden.

38 Voor 2015 verzorgde het Bureau voor Burgerlijke Verdedigingsplannen (BBVP) binnen de FOD het contact met het OCAD. Er was ook binnen elk directoraat-generaal een persoon die belast was met alles m.b.t. terrorisme. Deze personen waren duidelijk geïdentificeerd, maar er was geen gestructureerd systeem.

het Centrum voor Cybersecurity Belgium (CCB) en de NAVO. De Crisiscel is ook belast met het beheer van de wachtdienst van de FOD.[39] De cel, of de persoon van wacht, staat in voor de verspreiding van de OCAD-evaluaties naar de betrokken directoraten-generaal, beleidscellen en andere belanghebbenden (bijv. Infrabel, Belgocontrol). De FOD Mobiliteit en Vervoer heeft één deskundige gedetacheerd naar het OCAD.

De Crisiscel heeft sinds haar oprichting een reeks doeltreffende maatregelen genomen die zorgen voor zeer goede omstandigheden voor de informatie-uitwisseling met het OCAD (o.m. een programma en procedure voor het beheer van de informatie-uitwisseling, een beveiligde kamer voor de bewaring en raadpleging van geclassificeerde documenten[40]). Op het terrein is de informatiestroom echter zeer beperkt, wat kan worden verklaard door het gebruik van andere communicatiekanalen (bijv. via de luchtvaartpolitie), maar ook door het gebrek aan kennis van de personeelsleden van de FOD over de opdrachten van het OCAD en de functie van de Crisiscel als contactpunt voor het OCAD. Het is bovendien niet uitgesloten dat er rechtstreekse contacten worden ondernomen tussen de FOD Mobiliteit en Vervoer en het OCAD die niet langs de Crisiscel gaan. Om informatieverlies te vermijden, moet het personeel van de FOD Mobiliteit en Vervoer eraan worden herinnerd om de Crisiscel van deze informatie-uitwisselingen op de hoogte te brengen.

I.1.2.4. FOD Financiën – Douane en Accijnzen[41]

Het contactpunt van het OCAD binnen de Algemene Administratie Douane en Accijnzen van de FOD Financiën is de Administratie Opsporing.[42] Deze administratie bestaat uit een centrale cel en elf externe diensten die belast zijn met de gerechtelijke opsporing op fiscaal, maar ook op niet-fiscaal vlak (bijv. drugshandel).[43] Er zijn drie onderzoeksdomeinen: douanefraude, accijnsfraude en gemeenrechtelijke fraude. Voor elk domein bestaat binnen de centrale cel van de Administratie Opsporing een aparte dienst.

Van de vier ondersteunende diensten die het voorwerp van dit toezichtonderzoek uitmaakten, is de informatiestroom tussen het OCAD en de Algemene Administratie Douane en Accijnzen het kleinst. De Administratie Opsporing

---

39 De wachtdienst van de FOD bestaat uit acht personen uit de vier directoraten-generaal (Wegvervoer en Verkeersveiligheid, Duurzame Mobiliteit en Spoorbeleid, Scheepvaart en Luchtvaart).

40 De veiligheidsofficier en zijn plaatsvervanger maken daarenboven integraal deel uit van de Crisiscel.

41 De Douane en Accijnzen is een algemene administratie van de FOD Financiën, die onder leiding staat van een administrateur-generaal.

42 De Algemene Administratie Douane en Accijnzen bestaat uit 3.800 personen in totaal, waarvan 250 personen behoren tot de Administratie Opsporingen.

43 Naast gerechtelijke onderzoeken verricht de Administratie Opsporingen ook activiteiten wat 'rapportering' wordt genoemd. Dit komt neer op het opstellen van een verslag met informatie die (nog) niet het voorwerp van een gerechtelijke procedure vormt.

toont geen interesse in de samenwerking met het OCAD: de verantwoordelijke ziet deze eerder als een verlies aan middelen dan als een meerwaarde in het kader van het beheer van de dossiers van douane en accijnzen. Deze houding is enigszins begrijpelijk gezien de zeer beperkte informatiestroom met het OCAD en het feit dat de dienst paradoxaal genoeg de meeste gedetacheerde personen levert (drie).[44] De verantwoordelijke ziet daarenboven niet in welke bij de Administratie Opsporing beschikbare informatie nuttig zou kunnen zijn voor het OCAD en omgekeerd.[45] Dat roept de vraag op of er geen andere afdelingen binnen de Algemene Administratie Douane en Accijnzen zijn die beschikken over relevante informatie voor het OCAD.

Er vinden daarenboven rechtstreekse contacten plaats tussen het OCAD – meer bepaald door een uit de Douane gedetacheerde deskundige – met andere diensten van de FOD Financiën zonder dat de Administratie Opsporingen hiervan op de hoogte is. Deze situatie kan tot een verlies van informatie leiden aangezien er weinig garanties zijn dat de informatie correct wordt opgeslagen.

De FOD Financiën beschikt over een veiligheidsofficier. De beveiligingsregels voor de bewaring van geclassificeerde documenten worden desondanks binnen de Administratie Opsporingen niet nageleefd: de documenten worden gewoon bewaard in een afgesloten kast in een open ruimte waartoe het schoonmaakpersoneel toegang heeft. De verantwoordelijke is zich daarvan bewust en heeft het probleem al aangehaald, maar legt uit dat het zeer moeilijk is om materiaal te verkrijgen van de dienst logistiek.

I.1.3. BESLUIT

Er is binnen elk van de vier ondersteunende diensten een duidelijk identificeerbaar, voornaamste contactpunt van het OCAD. Om gemakkelijker en efficiënter te werken bestaan er naast het (de) officiële contactpunt(en) ook andere contactpunten van het OCAD. Dat is op zich geen probleem als er procedures voor de doorgifte en uitwisseling van informatie bestaan, zoals het in kopie zetten van de functionele mailboxen van het OCAD (beheerd door het departement Dossier- en documentatiebeheer) en van de voornaamste contactpunten van de ondersteunende diensten. Via deze werkwijze wordt informatie gecentraliseerd en verlies van informatie vermeden.

De informatiestromen met de Dienst Vreemdelingenzaken en de FOD Buitenlandse Zaken zijn zeer uitgebreid. Deze met de FOD Mobiliteit en Vervoer

---

44 Twee deskundigen (Punctuele Analyse) en één administratief personeelslid (Dossier- en documentatiebeheer).

45 De gedetacheerde deskundigen en het gedetacheerd administratief personeelslid hebben wel een rechtstreekse toegang tot de gegevensbank van de FOD Financiën, SITRAN (SIgnalétique TRANsversal).

en de Administratie Douane en Accijnzen zijn daarentegen veel beperkter. Als verklaring werd door laatstgenoemden aangehaald dat bepaalde informatie al via andere kanalen wordt doorgegeven (onder meer via de politie) en dat ze minder relevante informatie voor het OCAD hebben. Een goede informatie-uitwisseling ontstaat echter niet alleen door de geïmplementeerde structuren en procedures, maar ook door een goede informatie-uitwisselingscultuur binnen de ondersteunende diensten en het feit dat het personeel van deze diensten weet dat er binnen hun organisatie een contactpunt is met het OCAD en de opdrachten ervan kent. Bij de Dienst Vreemdelingenzaken en de FOD Buitenlandse Zaken zaten laatstgenoemde aspecten goed. Bij de FOD Mobiliteit en Vervoer en de Administratie Douane en Accijnzen was de situatie twijfelachtiger.

Wat betreft de minimale beveiligingsnormen voor de bewaring van geclassificeerde documenten werd er alleen een probleem bij de Administratie Douane en Accijnzen vastgesteld, waar die normen niet werden nageleefd.

Binnen het OCAD vormt het departement Dossier- en documentatiebeheer het zenuwcentrum voor het informatiebeheer van het OCAD. Daarnaast spelen de gedetacheerde deskundigen van het departement Punctuele Analyse een centrale rol binnen de informatie-uitwisseling tussen het OCAD en de ondersteunende diensten. De Comités stelden in hun onderzoek wel vast dat er verbetering mogelijk is binnen de communicatie tussen de verschillende departementen. Meer in het bijzonder kan de interne communicatie rond de bevoegdheden van de deskundigen (die regelmatig kunnen variëren) uitgebreider worden georganiseerd.

I.2. DE WERKING VAN DE DIRECTIE COUNTERINTELLIGENCE (CI) VAN DE ADIV: OPVOLGING VAN DE AANBEVELINGEN (BIS)

I.2.1. CONTEXTUALISERING EN OPZET

Eind december 2016 verzocht de toenmalige minister van Defensie het Vast Comité I een onderzoek te voeren naar de werking van de Directie Counterintelligence (CI) van de ADIV. Dit onderzoek[46] gaf een inkijk in de ernst, de complexiteit en de pluriformiteit van de tekortkomingen. Het Comité was ervan overtuigd dat de Directie CI belang had bij een organisatie en sturing die beantwoordt aan de standaarden van een doelmatige (effectieve) en doeltreffende (efficiente) overheidsdienst. Aan deze standaarden was niet voldaan. Het onderzoek gaf

[46] VAST COMITÉ I, *Activiteitenverslag 2018*, 2-17 ('I.1. De werking van de Directie Counterintelligence (CI) van de ADIV').

aanleiding tot omstandige aanbevelingen.[47] Wat de uitvoeringsdata betreft, werden prioriteiten aangegeven van 'zeer hoog' (te realiseren tegen eind 2018), over 'hoog' (te realiseren tegen eind juni 2019) tot 'gemiddeld' (te realiseren tegen eind december 2019). Een opvolgingsonderzoek naar de mate van uitvoering van het geheel van de aanbevelingen werd uitgevoerd.[48] In maart 2020 startte een tweede opvolgingsonderzoek, dat in juni 2020 werd afgerond.[49]

I.2.2. EEN NIEUWE STRUCTUUR BIJ ADIV

Als reactie op de audit van de Directie CI en om de aanbevelingen van de Parlementaire Commissie 'Aanslagen' te realiseren, werd in juni 2018 bij de ADIV beslist een *Business Process Re-engineering* (BPR) op te starten. Vanaf januari 2020 werd de Directie Counterintelligence – net zoals trouwens de Directie Intelligence – opgenomen in een nieuwe structuur. Dit betekende vanzelfsprekend niet dat er daardoor CI-opdrachten van de ADIV verdwenen. Wel werden personeelsleden van de (voormalige) Directie CI die zich op terrorisme richtten, overgeheveld naar het 'Gemeenschappelijk CounterTerro Platform VSSE-ADIV'. Door deze wijzigingen waren bepaalde aanbevelingen niet meer of minder relevant, of dienden ze minstens in een ander licht te worden bekeken.

I.2.3. DE UITVOERING VAN DE AANBEVELINGEN VAN AUDIT 2018: STAND VAN ZAKEN (BIS)

Het Comité trachtte zich – opnieuw op basis van documentair onderzoek en interviews – een beeld te vormen in hoeverre er inzake de aanbevelingen een significante vooruitgang werd gerealiseerd.

In de eerste helft van 2019 boekte de ADIV inzake counterintelligence, ondanks de problemen die zich in het verleden voordeden, vooruitgang. De rol en taak van Directie Counterintelligence binnen de ADIV en in relatie tot de VSSE, werd verduidelijkt (door totstandkoming van een 'Gemeenschappelijk CounterTerro

---

47 VAST COMITÉ I, *Activiteitenverslag 2018*, 130-134 ('XII.2.1. Diverse aanbevelingen voor de ADIV naar aanleiding van het toezichtonderzoek naar de werking van de Directie Counterintelligence').

48 VAST COMITÉ I, *Activiteitenverslag 2019*, 28-31 ('I.6. De werking van de Directie Counterintelligence (CI) van de ADIV: opvolging van de aanbevelingen').

49 Na de bespreking van zijn verslag (3 juni 2020) werd op verzoek van de Begeleidingscommissie een stand van zaken meegedeeld betreffende de gerechtelijke en/of administratieve dossiers van de betrokken ADIV-medewerkers. Het doel daarvan was om de leden van de Begeleidingscommissie in staat te stellen te beoordelen of het raadzaam was om betrokken te horen. In: VAST COMITÉ I, *Stand van zaken van verschillende dossiers waarin de leden van de ADIV betrokken zijn*, 10 juli 2020 (Ref. 2019/268/2).

platform' met de VSSE), er kwam een nieuwe strategische aanpak, er werd gewerkt aan interne richtlijnen (*standing operating procedures*, SOP) en de infrastructuurproblemen werden grondig aangepakt.

De nieuwe structuur opende perspectieven: een meer gestroomlijnde planning over de verschillende materies heen werd gerealiseerd, een betere afstemming tussen collecte en analyse werd mogelijk gemaakt en oude 'culturele' tegenstellingen inzake *tradecraft* werden aangepakt.

Het Vast Comité I was van mening dat de ADIV belangrijke inspanningen had verricht om de vele disfuncties weg te werken en de counterintelligence-functie beter te ontwikkelen. Weliswaar bleven een aantal items aandacht opeisen. Er bleef onder andere een achterstand bestaan inzake de *input* van gegevens in de databank. De interne controle moest nog worden versterkt en de beheersinformatie nodig om de dienst *hands-on* te kunnen sturen, moet verder worden uitgebouwd. Ook diende de aansturing van de provinciale diensten, die ondertussen weliswaar beter bemand zijn, nog op punt worden gesteld. Er bleven dus nog een aantal werven open. Het Vast Comité I nam zich voor de uitvoering van de aanbevelingen verder nauwgezet op te volgen.

I.3. BREXIT EN DE RELATIE TUSSEN DE BELGISCHE EN BRITSE INLICHTINGENDIENSTEN

In juni 2016 werd in het Verenigd Koninkrijk een referendum georganiseerd[50] waarbij werd gestemd voor de uittreding uit de Europese Unie. Enige tijd later startten aanslepende uittredingsonderhandelingen. Uiteindelijk trad het Verenigd Koninkrijk uit de Europese Unie op 31 januari 2020.

Dit proces, dat gemeenzaam bekend geraakte als de 'Brexit', wierp zekere vragen op over de mogelijke gevolgen van de Britse terugtrekking uit de Europese Unie op het vlak van de samenwerking tussen de twee Belgische (en andere Europese) inlichtingendiensten en de drie Britse (burgerlijke) inlichtingendiensten, te weten de *British Security Service* (BSS, ook gekend als MI5), de *Secret Intelligence Service* (SIS, ook gekend als MI6) en het *Government Communications Headquarters* (GCHQ).

Het Vast Comité I opende in mei 2019 een toezichtonderzoek naar de effecten van de Brexit voor de samenwerking tussen de Belgische (VSSE en ADIV) en de Britste inlichtingendiensten. In het bijzonder wenste het Comité na te gaan of er

[50] In maart 2017 stelde de Britse regering – met instemming van het Parlement – artikel 50 van het Verdrag betreffende de werking van de Europese Unie in werking, dat het mogelijk maakt voor een lidstaat om uit de EU te treden (Verdrag van Lissabon tot wijziging van het Verdrag betreffende een Europese Unie en het Verdrag tot oprichting van de Europese Gemeenschap, ondertekend te Lissabon, 13 december 2007, *Publicatieblad van de Europese Unie*, 17 december 2007, C306, ISSN 1725-2474).

een risico bestond dat de Brexit deze samenwerking in het gedrang zou kunnen brengen. Ook de wijze waarop de Belgische inlichtingendiensten zich hierop voorbereidden was aan de orde.[51]

I.3.1. 'INLICHTINGENMATERIE' IS GEEN BEVOEGDHEID VAN DE EUROPESE UNIE

I.3.1.1. Verdrag betreffende de werking van de Europese Unie van 2007

De Europese Unie mag alleen optreden in materies waarvoor de EU-landen haar, via de EU-verdragen, uitdrukkelijk de bevoegdheid hebben gegeven. Deze verdragen bepalen wie op welk gebied wetgeving mag vaststellen: de EU, de nationale overheid, of allebei (de zgn. gedeelde bevoegdheden). *In casu* valt de werking van de inlichtingendiensten niet onder de bevoegdheid van de EU noch zijn het gedeelde bevoegdheden. Het onderwerp behoort integendeel tot de exclusieve bevoegdheid van de lidstaten. Dit blijkt uit het Verdrag betreffende de werking van de Europese Unie van 2007.

Wel dient vermeld te worden dat de EU toch een bepaalde 'eigen inlichtingen-capaciteit' heeft. Teneinde hun functies uit te oefenen en om de informatie te verzamelen die ze nodig hebben om hun taken te kunnen uitvoeren, houden een aantal EU-departementen zich bezig met het verzamelen van inlichtingen, met informatiebeveiliging en contraspionage tegen mogelijk spionage tegen de Europese Instellingen (bijv. EU INTCEN).

I.3.1.2. De Politieke Verklaring in het kader van de Brexit tussen de EU en het VK

De uitsluitend nationale bevoegdheid voor nationale veiligheid blijkt ook uit de Politieke Verklaring, opgesteld om het kader te schetsen voor de (toekomstige) betrekkingen tussen de Europese Unie en het Verenigd Koninkrijk. Deze Politieke Verklaring dateert van oktober 2019 en is een niet-bindende verklaring die samengaat met het eigenlijke Brexit-akkoord.[52]

In diezelfde Politieke Verklaring wordt ook een specifiek deel gewijd aan het 'veiligheidspartnerschap'. Met dit begrip wou men aantonen dat veiligheid zowel

---

51 Op het tijdstip van het voeren van het toezichtonderzoek (oktober – november 2019) was er – omwille van de conflictueuze en onduidelijke situatie in het Verenigd Koninkrijk – geen zekerheid over de *timing* noch over de precieze omstandigheden van de uittreding. Het rapport werd gefinaliseerd in de eerste trimester van 2020.

52 In deel IV. Institutionele en andere horizontale regelingen, artikel 133 van de Politieke Verklaring wordt gesteld: *"De toekomstige betrekkingen (nvdr : tussen het VK en de EU) moeten voorzien in passende uitzonderingen met betrekking tot veiligheid: nationale veiligheid behoort tot de exclusieve bevoegdheid van respectievelijk de Unielidstaten en het Verenigd Koninkrijk."*

voor de EU, voor haar lidstaten als voor het Verenigd Koninkrijk een belangrijk domein is en blijft op het vlak van samenwerking.

I.3.2. DE HUIDIGE SAMENWERKING VAN DE BELGISCHE DIENSTEN MET DE BRITSE INLICHTINGENDIENSTEN

I.3.2.1. Wettelijke basis voor de internationale samenwerking

Het Verdrag betreffende de werking van de Europese Unie laat alle ruimte voor de internationale samenwerking tussen EU-lidstaten, zowel onderling als met derden. Artikel 73 bepaalt in die optiek het volgende: *"Het staat de lidstaten vrij onderling en onder hun verantwoordelijkheid vormen van samenwerking en coördinatie te organiseren zoals zij het passend achten tussen hun bevoegde overheidsdiensten die verantwoordelijk zijn voor het verzekeren van de nationale veiligheid."*

De wettelijke basis voor de samenwerking vanuit de Belgische inlichtingendiensten met hun buitenlandse partners vinden we terug in artikel 20 W.I&V.

Wat de samenwerking betreft met buitenlandse diensten, wordt verwezen naar een richtlijn uitgevaardigd door de Nationale Veiligheidsraad (NVR). Op 26 september 2016 werd door de ministers van Justitie en Landsverdediging in een nota aan de NVR de als 'Vertrouwelijk Wet 11.12.1998' geclassificeerde 'Richtlijn aangaande de relaties van Belgische inlichtingendiensten met buitenlandse inlichtingendiensten' voorgelegd. Deze richtlijn streeft ernaar een inschatting te maken van buitenlandse inlichtingendiensten met als doel de aard van de relatie met elke dienst te bepalen. Het vormt een beleidsondersteunend instrument voor de bilaterale samenwerking.

I.3.2.2. De Veiligheid van de Staat

Er bestaan in het Verenigd Koninkrijk drie burgerlijke inlichtingendiensten. De VSSE werkt op bilateraal vlak samen met twee van deze diensten, meer in het bijzonder met de *British Security Service* (BSS ofte MI5) en de *Secret Intelligence Service* (SIS ofte MI6). Beide diensten vormen een belangrijke partner voor de VSSE. De BSS verzamelt en analyseert inlichtingen met betrekking tot binnenlandse dreigingen, de SIS verzamelt zijn inlichtingen in het buitenland. De samenwerking tussen deze twee Britse inlichtingendiensten met de VSSE situeert zich op de bevoegdheidsdomeinen die alledrie de diensten gemeenschappelijk hebben, namelijk terrorisme, spionage en proliferatie van massavernietigingswapens. Met de derde inlichtingendienst, het *Government Communications Headquarters* (GCHQ), die verantwoordelijk is voor *signal intelligence* (SIGINT), is er geen rechtstreekse samenwerking. Er is evenmin, van de kant van de VSSE, een samenwerking met Britse militaire inlichtingendiensten.

Naast bilaterale contacten vinden er ook contacten en uitwisseling van inlichtingen plaats tussen de VSSE en de Britse inlichtingendiensten via multilaterale fora, zoals de Club van Bern en de *Counter Terrorism Group* (CTG). Het is belangrijk te benadrukken dat zowel de Club van Bern als de CTG informele, intergouvernementele samenwerkingsverbanden zijn die los staan van de structuren van de Europese Unie. De Britse dienst, die deel uitmaakt van de Club van Bern en de CTG, drukte reeds eerder de wens uit om deel te kunnen blijven uitmaken van beide multilaterale fora ná de uittreding van het Verenigd Koninkrijk uit de Europese Unie (zoals bijv. ook Noorwegen en Zwitserland).

I.3.2.3. De Algemene Dienst Inlichting en Veiligheid

Ook bij de militaire inlichtingendienst ADIV speelt de bilaterale en multilaterale samenwerking met hun Britse partners zich af buiten de EU-structuren. De bilaterale contacten zijn ook hier tussenstatelijk en van dienst tot dienst. De multilaterale contacten spelen zich voornamelijk af binnen NAVO-verband.

Op bilateraal vlak wordt door de ADIV samengewerkt met de SIS (MI6), BSS (MI5) en de GCHQ, waarbij de dienst de GCHQ beschouwt als zijn belangrijkste Britse partner. De diensten werken onder meer samen aangaande het delen van expertise op het vlak van SIGINT, het counteren van cyberdreigingen alsook de uitwisseling van inlichtingen over (spionage)dreiging. Het Verenigd Koninkrijk beschikt ook over een militaire inlichtingendienst, genaamd *Defence Intelligence*, die deel uitmaakt van het Britse ministerie van Defensie. De opdracht van *Defence Intelligence* is om te fungeren als leverancier van strategische, militaire inlichtingen aan het ministerie en de strijdkrachten. Een opvallend gegeven was dat de ADIV in het kader van dit onderzoek verklaarde geen rechtstreekse, bilaterale samenwerking te onderhouden met de *Defence Intelligence*.

Er is ook samenwerking tussen de ADIV en onder meer de Britse diensten binnen een multilateraal kader. Binnen de EU-structuren is er de *European Union Military Staff* (EUMS) die deel uitmaakt van de *European External Action Service* (EEAS). De EUMS bevat een *Intelligence Directorate* dat verantwoordelijk is voor het opstellen van strategische analyses die kunnen bijdragen tot de planning in het kader van crisisrespons en militaire operaties van de EU. Het *Intelligence Directorate* bestaat uit militaire analisten die gedetacheerd worden vanuit de militaire inlichtingendiensten van de EU-lidstaten. Ook de ADIV beschikt over een analist bij de EUMS.

I.3.3. MOGELIJKE GEVOLGEN VAN DE 'BREXIT' VOOR DE INLICHTINGENDIENSTEN

I.3.3.1. Hypotheses over de impact van Brexit voor de Britse inlichtingendiensten

Kort na de Brexit, bleef moeilijk in te schatten welke de reële gevolgen ervan zouden zijn voor de inlichtingendiensten. Doorgaans worden in de – hoofdzakelijk Angelsaksische – literatuur drie hypotheses (*schools of thought*) opgeworpen.[53]

De *'optimistic school'* stelt dat de Brexit een positieve ontwikkeling is en dat deze op geen enkele manier de interne en uitwendige veiligheid van het Verenigd Koninkrijk zal schaden of ondermijnen. Deze visie legt een grotere nadruk op de relatie van de Britse inlichtingendiensten met hun Amerikaanse partners dan de relatie met de EU-partners. De Brexit zorgt er immers voor dat het Verenigd Koninkrijk geen deel zal uitmaken van een toekomstige federale, Europese staat die ook bevoegd zal worden voor veiligheidsmateries, wat ertoe had kunnen leiden dat de huidige, goede werking van de Britse inlichtingendiensten zou worden gewijzigd en verstoord. Er wordt gesteld dat het Verenigd Koninkrijk de overige EU-lidstaten (die te weinig investeren in hun inlichtingendiensten) niet nodig heeft op inlichtingenvlak, omdat het naar eigen zeggen over het meest competente, efficiëntste en best gefinancierde inlichtingenapparaat beschikt. De huidige relatie tussen de Britse inlichtingendiensten en deze van de overige EU-lidstaten wordt beschouwd als onevenwichtig, waarbij de Britse diensten 'meer geven dan ze terugkrijgen'. Daarenboven vindt de meeste uitwisseling van inlichtingen plaats op bilateraal en niet op multilateraal vlak. Deze bilaterale samenwerking, vooral op het vlak van contraterrorisme, met andere landen zal na de Brexit gewoon worden verdergezet.

De *'pessimistic school'* daarentegen beweert dat de Brexit zal zorgen voor een ernstige ondermijning van de Britse nationale veiligheid. Er wordt geargumenteerd dat het Verenigd Koninkrijk zijn plaats en rol zal verliezen in de ontwikkeling van een nu embryonaal Europees inlichtingenapparaat en Europese databanken. De Brexit zou kunnen leiden tot een verzwakking van de positie van de Britse inlichtingendiensten ten aanzien van andere landen, in eerste instantie de Verenigde Staten. Volgens deze zienswijze zorgden de Britse diensten – net omwille van hun brugfunctie naar diensten van andere EU-landen – voor een meerwaarde voor de Amerikanen. Na de Brexit zouden de Verenigde Staten het Verenigd Koninkrijk kunnen gaan zien als een tweederangsland en op zoek kunnen gaan naar een andere bevoorrechte partner binnen de EU (bijv. Duitsland).

De derde of 'pragmatische' stroming houdt het midden tussen de twee voorgaande. Volgens deze visie zal de Brexit geen significant effect hebben op de Europese en Britse veiligheid in het algemeen, noch op inlichtingenvlak in het

---

53 I.L. KONSTANTOPOULOS en J.M. NOMIKOS, *Journal of Intelligence History*, 'Brexit and intelligence: connecting the dots', 2017, Vol. 16, NO. 2, 100-107.

bijzonder. Men meent dat de samenwerking op inlichtingenvlak zal worden verdergezet door het Verenigd Koninkrijk en zijn Europese partners, hetzij op bilaterale basis, hetzij in een multilaterale bijzondere relatie om de internationale uitdagingen en dreigingen aan te gaan en de gemeenschappelijke doelstelling van veiligheid te bereiken. De reden voor deze bewuste keuze is rationaliteit en wederzijds belang. Deze denkwijze leek de meest gangbare te zijn binnen de inlichtingengemeenschap zelf, tenminste wanneer men zich baseert op een aantal uitspraken die door (ex-) leidinggevenden in het openbaar werden gedaan.

I.3.3.2. Inschatting door de Belgische diensten over de gevolgen van de Brexit

Belangrijk om op te merken is dat aan de VSSE noch aan de ADIV werd gevraagd (en ze evenmin zelf verzochten) om betrokken te worden bij enig overleg met een Belgische autoriteit, bijvoorbeeld met de voogdijminister of op het niveau van de Nationale Veiligheidsraad (NVR) over een mogelijke impact van de Brexit. Er werden ter zake vragen, instructies noch richtlijnen ontvangen door de diensten.

Het weze vermeld dat er op het niveau van de federale regering in maart 2019 een thematische ministerraad werd gehouden over de Brexit. Tijdens deze ministerraad werden heel wat onderwerpen besproken, maar geen ervan had betrekking op de inlichtingendiensten (maar bijvoorbeeld wel op de politiediensten).

Verder bleek dat zowel de VSSE als de ADIV *a priori* zelf geen formeel gestructureerde (risico)analyse opstelden over de mogelijke impact van de Brexit op hun samenwerking met de Britten. De twee diensten maakten wel een denkoefening met betrekking tot mogelijke gevolgen van de Brexit voor de relatie met de Britse inlichtingendiensten ná het opstarten van het toezichtonderzoek.

Op basis van deze denkoefening, meende de VSSE dat de impact van de Brexit op haar samenwerking met de Britse diensten wellicht beperkt zal zijn, omdat deze samenwerking zich op een tussenstatelijk niveau afspeelt, buiten de EU-structuren. De dienst ging ervan uit dat de samenwerking met haar Britse partners niet of nauwelijks effecten zal ondervinden van de uittreding. Naar de inschatting van de VSSE, zou de Brexit ook geen directe juridische gevolgen hebben voor de samenwerking. Er kunnen echter wel bepaalde bijkomende aspecten opduiken, bijvoorbeeld inzake privacy, of inzake de toegang van de Britse diensten tot datasets en gegevens die vallen onder EU-regelingen. De VSSE besliste wel de vraag over de mogelijke gevolgen van de Brexit voor de toekomstige Belgisch-Britse samenwerking op inlichtingenvlak voor te leggen aan de Britse partnerdiensten.[54]

Net als de VSSE is ook de ADIV van mening dat de uittreding van het Verenigd Koninkrijk geen gevolgen zal hebben voor de samenwerking van de dienst met zijn

[54] Het antwoord werd, met goedkeuring van de Britse diensten, door de VSSE aan het Vast Comité I meegedeeld. Vermits het een als GEHEIM Wet 11.12.1998 geclassificeerd document betreft, kan over de inhoud – behoudens de daarin vervatte oproep tot verdere samenwerking – geen nadere informatie worden verstrekt.

Britse partners. De dienst verklaarde geen specifieke gesprekken te hebben gevoerd met zijn Britse partners over mogelijke gevolgen van de Brexit, en herhaalde dat hij geen instructies of richtlijnen had ontvangen van Belgische overheden in dit verband.

I.3.4. BIJKOMENDE ASPECTEN

I.3.4.1. De bescherming van (persoons)gegevens

Het feit dat de Europese regelgeving na de Brexit niet meer van toepassing is in het Verenigd Koninkrijk, meer bepaald de regelgeving op het vlak van de bescherming van (persoons)gegevens, werd door de Belgische inlichtingendiensten aangehaald als een mogelijk heikel punt voor de informatieuitwisseling met hun Britse partners.[55]

Aangezien het VK geen lid meer zal zijn van de EU, gelden specifieke – lees: strengere – regels voor de doorgifte van persoonsgegevens. Deze regels liggen vervat in de artikelen 93 en 94 van de Gegevensbeschermingswet (GBW).

Ook het Akkoord inzake de terugtrekking van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland uit de Europese Unie en de Europese Gemeenschap voor Atoomenergie en de bijgaande Politieke Verklaring, bevat een aantal bepalingen in verband met de regelingen voor de bescherming van de verwerking van persoonsgegevens en informatie.[56]

Hoe dan ook betreft het hier een materie die niet enkel specifiek de inlichtingenmaterie betreft, maar veel algemener is. In voorkomend geval moet dit wellicht opgevolgd worden door de verschillende nationale bevoegde instanties (in België de bevoegde ministers en de verschillende data-beschermingsautoriteiten). Het Comité stelde dan ook dat het aangewezen is dat deze ook oog hebben voor mogelijke repercussies op het vlak van de inlichtingenmaterie en desnoods de inlichtingendiensten te betrekken bij eventuele discussies.

---

55 Ook in het *"Rapport relatif de la délégation parlementaire au renseignement pour l'année 2018"* boog het Franse toezichtsorgaan zich over de vraag wat de mogelijke gevolgen van de Brexit kunnen zijn voor het Europese inlichtingenbestel. Het thema van de bescherming van persoonsgegevens werd geïdentificeerd als een mogelijk probleem voor de toekomstige samenwerking tussen de Europese (Franse) en Britse inlichtingendiensten. Volgens de auteurs van dit rapport is het noodzakelijk dat *"het Verenigd Koninkrijk zal moeten aantonen dat het een voldoende niveau van bescherming van persoonsgegevens garandeert en zal het ook de bevoegdheid van het Hof van Justitie van de Europese Unie moeten erkennen om klachten over de verwerking van persoonsgegevens te behandelen* (vrije vertaling)." (Yaël BRAUN-PIVET, "*Rapport rélatif de la délégation parlementaire au renseignement pour l'année 2018*", Délegation Parlementaire au Renseignement, Assemblée Nationale / Sénat, 11 avril 2019, 88).

56 Het weze vermeld dat de Politieke Verklaring geen bindende kracht heeft, zodat niet voorzien kan worden op welke manier en wanneer de erin opgenomen engagementen in de praktijk zullen worden omgezet.

I.3.4.2. Toegang van het VK tot Europese (politionele) databanken

Een belangrijk gevolg van de terugtrekking van het Verenigd Koninkrijk uit de EU is dat het VK niet langer toegang heeft tot Europese databanken. Hierbij dient in de eerste plaats te worden gedacht aan gegevens die worden beheerd door Europol en aan de toegang tot het Schengen Informatiesysteem (SIS-II).[57] Aangezien het hier echter om politionele databanken gaat, ging het Vast Comité I hier niet verder op in. Zoals reeds vermeld, is de EU niet bevoegd voor de inlichtingenmaterie *sensu stricto*, en zijn er op het niveau van de EU geen 'inlichtingendatabanken' zodat ter zake geen probleem kan opduiken.

I.3.4.3. Een toenemende Europese integratie op inlichtingenvlak na de Brexit?

Zoals vermeld, is er vanuit de lidstaten steeds een grote terughoudendheid geweest ten aanzien van het afstaan van bevoegdheden inzake nationale veiligheid aan het intergouvernementele niveau, *in casu* de Europese Unie. Het Verenigd Koninkrijk is sinds zijn toetreding tot de EU, steeds één van de lidstaten geweest die een beperkte en beperkende benadering heeft voorgestaan van de Europese integratie, en al helemaal op het vlak van nationale veiligheid en inlichtingendiensten.

Eén van de verworvenheden van het Verdrag van Lissabon was de verwezenlijking van een ruimte van vrijheid, veiligheid en recht (RVVR). In dit Verdrag is vooral het Derde Deel, Titel V (artikelen 67 tot en met 89) gewijd aan de RVVR. In het kader van de RVVR werden 133 maatregelen voorgesteld, waarvan door het Verenigd Koninkrijk slechts 35 werden aangenomen na een expliciete *'opt in'*.

Anderzijds hebben vooral de voorbije vijftien à twintig jaar aangetoond dat er nood is aan een toenemende Europese samenwerking op veiligheidsgebied en dat deze samenwerking zich ook heeft ontwikkeld, vooral op het vlak van de bestrijding van transnationale criminaliteit, van contraterrorisme en van cyberveiligheid.

Eén van de mogelijke gevolgen van de uittreding van het Verenigd Koninkrijk zou kunnen zijn dat er zich een toenemende structurele samenwerking zal manifesteren tussen de inlichtingendiensten van de overgebleven lidstaten van de Europese Unie. Het *EU Intelligence and Analysis Centre* (EU INTCEN) en het *Intelligence Directorate* van de *EU Military Staff* die deel uitmaken van de *European External Action Service* zijn momenteel de enige inlichtingenstructuren binnen de Europese instellingen. Deze organen stellen strategische analyses op, op basis van open bronneninformatie en inlichtingenanalyses die worden aangeleverd door de

---

57 In het Brexit-akkoord (Deel 1, artikel 8) werd het volgende vermeld: *"Tenzij in dit akkoord anders is bepaald, zal het Verenigd Koninkrijk aan het eind van de overgangsperiode niet langer recht hebben op toegang tot enig netwerk, enig informatiesysteem en enige databank dat of die op grond van het recht van de Unie is opgericht. Het Verenigd Koninkrijk zal passende maatregelen nemen om te waarborgen dat het zich geen toegang verschaft tot netwerken, informatiesystemen of databanken ten aanzien waarvan het geen recht op toegang meer heeft."*

inlichtingendiensten van de lidstaten. Een mogelijke ontwikkeling zou kunnen zijn dat, naast het INTCEN, binnen EU-verband een structuur zou worden opgezet voor de uitwisseling van operationele inlichtingen, bijvoorbeeld op het vlak van contraterrorisme, inmengingactiviteiten door derde staten of cyberdreigingen.

In november 2018 werd ook reeds door de EU-ministers van Defensie en Buitenlandse Zaken beslist om een *Joint EU Intelligence School* op te richten. Dit project zal worden gecoördineerd door de Griekse overheid.

I.3.5. CONCLUSIE

Het Vast Comité I vond geen aanwijzingen dat de terugtrekking van het Verenigd Koninkrijk uit de Europese Unie negatieve gevolgen zou hebben voor de Belgische en Britse inlichtingendiensten. Eenzelfde stem klonk vanuit het Verenigd Koninkrijk. Er waren vooralsnog geen redenen om te twijfelen aan hetgeen de Britse instanties ter zake officieel hebben verklaard, onder andere in de tekst van de Politieke verklaring die samengaat met het Brexit-akkoord tussen het VK en de EU.

I.4. DE MOGELIJKE INMENGING DOOR BUITENLANDSE DIENSTEN/STATEN BIJ BELGISCHE VERKIEZINGEN

Hoewel in de Verenigde Staten de resultaten van het onderzoek daaromtrent niet volledig publiek werden gemaakt, rezen er sterke vermoedens dat buitenlandse diensten/Staten (meer bepaald de Russische) tijdens de Amerikaanse presidentsverkiezingen van 2016 gepoogd hebben deze verkiezingen te beïnvloeden via cybermiddelen. Ook in Europa, en dus in België, is dit denkbaar.

De *online* cyberbeïnvloeding van verkiezingen vanuit het buitenland kan diverse vormen aannemen. Het kan gaan om *hacking,* infiltratie en manipulatie van kiestechnologie via toegang tot kiescomputers; om *hacking* en infiltratie van computersystemen, om partijstrategieën of gevoelige informatie over politici te bekomen, en deze dan te lekken via de pers of de sociale media; of nog, de *online* verspreiding van *fake news* en desinformatie via sociale mediaplatformen en websites van mediabedrijven.

Met het zicht op de verkiezingen van mei 2019[58] was dit thema bijzonder actueel. Het houden van open en faire verkiezingen behoort immers tot de kern van de democratie. Het is de taak van de inlichtingendiensten om bepaalde bedreigingen tegen de Belgische instellingen in kaart te brengen en de bevoegde

[58] Het betrof de verkiezingen van het Europees Parlement, van de Kamer van Volksvertegenwoordigers en van de Gewest- en Gemeenschapsparlementen van 26 mei 2019.

autoriteiten hiervan in kennis te stellen. Het Comité besloot dan ook begin 2019 een toezichtonderzoek[59] te openen naar de wijze waarop de Belgische inlichtingendiensten reageren (inlichtingen verzamelen, waarschuwingen uitzenden, internationaal samenwerken, eventueel verstoren…) op de mogelijke inmenging door buitenlandse diensten/Staten bij Belgische verkiezingen.

I.4.1. EEN TOENEMENDE BEWUSTWORDING

Ook in België was er sprake van een toenemende bewustwording rond het thema van kwaadwillige beïnvloeding van politieke processen en verkiezingen.

Er werd een interdepartementale cel gecreëerd die *roadmaps* ontwikkelde om concrete acties te ondernemen. De Regering was overigens van mening dat een nationale aanpak niet kon volstaan. België werkte dan ook op de opeenvolgende Europese Raden mee aan het verhogen van de weerbaarheid van de EU tegen desinformatiecampagnes. Een belangrijk onderdeel van de Belgische tegenstrategie was in dit kader de internationale samenwerking via de EU en de NAVO, via onder andere het *NATO Cooperative Cyber Defence Centre of Excellence* (Talinn). Ook ontwikkelde België een samenwerking met het *Kenniscentrum voor de bestrijding van hybride dreigingen* (Helsinki).

Mogelijke coördinatie van het detecteren van cyberaanvallen werden dan weer toevertrouwd aan het Centrum voor Cybersecurity België (CCB), waaraan ook de ADIV deelnam. Het Crisiscentrum voorzag in de oprichting van een samenwerkingsplatform inzake desinformatie en strategische communicatie. Op nationaal vlak was er ook nog het project *stopfakenews.be* van de minister van Digitale Agenda.

Ook werd de problematiek van digitale desinformatie verschillende malen door het CCB en de inlichtingendiensten besproken in de schoot van het Coördinatiecomité Inlichtingen en Veiligheid (CCIV). Het CCB werkte ook samen met de FOD Binnenlandse Zaken rond de beveiliging van het elektronisch stemsysteem.

De Regering wees ook op de oprichting, binnen de ADIV, van een *Cyber Security Operations Center*. Deze dienst werd verantwoordelijk voor de detectie en bestrijding van cyberincidenten en diende zich te concentreren op de bescherming van netwerken en wapensystemen van Defensie, maar diende ook technische bijstand te verlenen aan onderzoeken van het CCB of het federaal parket (*infra*).

---

[59] Voluit 'Toezichtonderzoek naar de wijze waarop de inlichtingendiensten een mogelijke inmenging van buitenlandse diensten in Belgische verkiezingen opvolgen, de eventuele bedreigingen tegen trachten te gaan, erover rapporteren aan de autoriteiten, en in het bijzonder wat betreft het gevaar van cyberinmenging of cyberaanvallen op dit vlak'. Het rapport werd begin 2020 gefinaliseerd.

I.4.2. DE ROL TOEGEKEND AAN DE VSSE

Op basis van de artikelen 7, 1° en 8 W.I&V is de VSSE bevoegd om inlichtingen in te winnen over mogelijke beïnvloeding van verkiezingen via cybermiddelen, vermits dergelijke mogelijke beïnvloeding valt onder de begrippen 'spionage' en 'inmenging'.[60] Aangezien desinformatie en *fake news* vaak deel uitmaken van operaties die gestuurd worden door offensieve, buitenlandse inlichtingendiensten, zag de VSSE zichzelf als een *'natuurlijke partner in de strijd tegen deze problematiek'*.

De VSSE zag haar rol als het inwinnen en analyseren van inlichtingen met betrekking tot deze problematiek, en vervolgens het sensibiliseren van overheden, administraties, bedrijven en andere instellingen. De VSSE stelde evenwel dat het geen actief beleid ontwikkelde met betrekking tot het informeren van burgers om nepnieuws van echt nieuws te onderscheiden. Evenmin zag de dienst het als zijn taak om sociale media en technologiebedrijven op te volgen om te beoordelen hoe effectief hun aanpak van nepnieuws was, evenmin als het opstellen van een definitie ervan.

Het Comité kon vaststellen dat de dienst in augustus 2018 reeds interne instructies uitvaardigde rond de verkiezingen van 2019, en de opvolging ervan toebedeelde aan drie van zijn afdelingen. De focus kwam daarbij te liggen op dreigingen vanuit Rusland. Twee grote sociale media-actoren werden van nabij gevolgd en er werd ook een taakverdeling hieromtrent met de ADIV afgesproken. De bedoeling was niet om feiten op hun waarachtigheid te controleren of om *fake news* te detecteren, maar wel om trachten te bepalen welke specifieke profielen actief waren. Hierbij werd geen gebruik gemaakt van geautomatiseerde monitoring. In november 2018 ging de VSSE een stap verder en richtte een interne, transversale *Groupe de Travail – Élections* op. Deze werkgroep werkte een actieplan uit om nader te bekijken wat de bijdrage van de dienst kon zijn aan de gezamenlijke *Joint Intelligence Task Force (JITF) (infra)* die werd opgericht met de ADIV.

I.4.3. DE ROL TOEGEKEND AAN DE ADIV

De bevoegdheid van de ADIV leek op het eerste zicht ter zake minder evident dan deze van de VSSE. De ADIV is immers in de eerste plaats een militaire inlichtingendienst die zich op militaire materies moet richten. Toch boog de ADIV zich over het fenomeen van cyberinmenging in verkiezingen, nu clandestiene beinvloeding van politieke processen veelal een militaire oorsprong kent. Zo is het gemeengoed dat bijvoorbeeld de Russische militaire inlichtingendienst GRU een

---

60 Volledigheidshalve dient te worden vermeld dat de VSSE eveneens bevoegd is om de materie op te volgen via artikel 7, 3° W.I&V waarbij de VSSE de taak heeft tot "*het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgische grondgebied.*"

strategie van *hybrid warfare* hanteert. In die zin sluit dit aan bij de bevoegdheid van de ADIV, ook al is de bedreiging niet (louter) gericht tegen militaire ICT-systemen. Een tweede belangrijk aanknopingspunt is te vinden in het artikel 9 W.I&V: *"Op verzoek van de Veiligheid van de Staat verleent de Algemene Dienst Inlichting en Veiligheid zijn medewerking aan de Veiligheid van de Staat bij het inwinnen van inlichtingen wanneer militairen betrokken zijn bij activiteiten bedoeld in artikel 7, 1°en 3°."* Aangezien er belangrijke vermoedens bestonden dat de bedreiging vaak tot stand kwam door toedoen van buitenlandse militaire diensten, was het gewettigd dat de ADIV de VSSE ter zake bijstond.

De ADIV stelde over de mogelijke cyberbedreigingen tijdens de gemeenteraadsverkiezingen in 2018 en de federale verkiezingen in 2019 al in november 2017 een sensibiliseringsnota op voor zijn voogdijminister.[61] Ook werd beslist om een tijdelijk 'Projectteam Élections *2019*' (PTE19) op te richten, bestaande uit reservisten en medewerkers vanuit vier verschillende directies. Hun opdracht liep tot en met de dag van de verkiezingen, spitste zich enkel toe op de Russische Federatie en volgde enkel 'externe beïnvloeding' en/of 'manipulatie'. De werking van dit tijdelijke team stond los van de structuur van de bestaande directies binnen de ADIV. Wel werd in samenspraak met deze directies een collecteplan opgesteld. Tevens werd het initiatief genomen om een studie op te starten met betrekking tot de mogelijke dreiging.

I.4.4. DE SAMENWERKING BINNEN DE JOINT INTELLIGENCE TASK FORCE (JITF)

Eind 2018 werd door de VSSE en de ADIV[62] een *Joint Intelligence Task Force* (JITF) opgericht. Deze had als specifieke *scope* de *online* beïnvloeding van de federale en regionale verkiezingen in België door Russische Staatsactoren. De *taskforce* was actief op vier verschillende terreinen, te weten (1) sensibilisering en *resilience building*, (2) strategische (fenomeen)analyse, (3) detectie van risico's en incidenten en (4) crisisbeheer in de vorm van o.a. communicatie en vroege waarschuwing.

Op het vlak van sensibilisering en het verhogen van de weerbaarheid nam de *taskforce* verschillende initiatieven.[63] Er werden ook twaalf detectieprojecten ontwikkeld, met als doel om pogingen tot beïnvloeding te detecteren. De JITF werkte overigens ook samen met diverse internationale partners, waaronder de *East StratCom Task Force* van de *European External Action Service*[64], die over een

---

61 *Parl. St.* Kamer, 2017-18, 54K3267/1, 13 september 2018, 9.

62 De ADIV beperkte zich daarbij tot de inzet van zijn collectiecapaciteiten als detectoren en tot een vorm van *primary assessment*.

63 Zoals bijv. de briefing van de minister van Justitie en van vertegenwoordigers van de Belgische media eind januari 2019.

64 De *EEAS East StratCom Task Force* werd door de Europese Raad in het leven geroepen in maart 2015 met als specifiek doel om de verspreiding van Russische desinformatie tegen te gaan.

databank beschikt met verspreiders van desinformatie over de EU. Er werd ook een samenwerking opgezet met de *Transatlantic Commission on Election Integrity*.

Op basis van vernoemde projecten en de gedetecteerde risico's en incidenten werkte de JITF operationele analyses uit die uitmondden in zogenaamde *Joint Detection Reports* (JDR) waarin onder andere melding werd gemaakt van verslaggeving in Russische media over situaties in België, waarin gepeild werd naar de oorsprong van Twitteraccounts, over welbepaalde verspreide desinformatie over België of nog, over de eerste bevindingen van aanwezige grote internetbedrijven.

Naast de operationele analyse werden ook strategische analyses (*Joint Thematic Reports* (JTR)) opgesteld op basis van de informatiecollecte van beide diensten.

De laatste pijler van de aanpak van de JITF situeerde zich op het vlak van nationale en internationale samenwerking op het gebied van *cybersecurity*. Hierbij lag het initiatief niet bij de inlichtingendiensten zelf, maar bij andere instanties, met name het Crisiscentrum en het Centrum voor Cybersecurity België.

I.4.5. SAMENWERKING VAN DE INLICHTINGENDIENSTEN MET ANDERE ACTOREN

Uiteraard werkten de inlichtingendiensten in deze niet op een eiland.

Zo konden onder meer diverse initiatieven worden opgetekend met andere Belgische overheidsinstellingen. Er vond overleg plaats tussen de VSSE en de Directie-generaal Instellingen en Bevolking van de FOD Binnenlandse Zaken bedoeld om te anticiperen op mogelijke dreigingen gericht tegen de verkiezingen. Ook werd overleg georganiseerd tussen de twee inlichtingendiensten en het Centrum voor Cybersecurity België.[65] Het CCB stelde, in samenwerking met beide inlichtingendiensten, een sensibiliseringsgids samen voor politici en politieke partijen.[66] Later greep ook overleg plaats met het Crisiscentrum. Er werden afspraken gemaakt over de communicatiestrategie en er werd bepaald dat de rol van de inlichtingendiensten zich vooral situeerde in het in kaart brengen van de mogelijke verspreiding van desinformatie met als doel de verkiezingsresultaten te beïnvloeden.

In de eerste maanden van 2019 werd door de VSSE ook de buitenlandse aanpak in verschillende Europese landen bestudeerd en werden partnerdiensten bevraagd.

De VSSE legde ook contacten met *Facebook* waarin onder meer werd toegelicht dat omwille van negatieve ervaringen naar aanleiding van verkiezingen in het verleden – onder meer in de Verenigde Staten – door het bedrijf een actieplan werd

---

65 Het CCB van de FOD Kanselarij van de Eerste Minister stond in eerste instantie in voor het counteren van eventuele externe, technische dreigingen.

66 "Veilig online tijdens de verkiezingscampagne – Aanbevelingen voor een cyberveilige en digitaal veilige campagne.", CCB, VSSE, ADIV, februari 2019, 9p. Deze brochure is sinds februari 2019 consulteerbaar op de website van de VSSE (www.vsse.be).

ontwikkeld. Er werd tevens vernomen hoe het bedrijf omgaat met valse informatie bedoeld om de publieke opinie te beïnvloeden en *Facebook* zette zijn vaststellingen uiteen aangaande de Europese verkiezingen.

Het 'Projectteam Élections 2019' (PTE19) van de ADIV kon voor de ondersteuning van zijn analyses een beroep doen op al eerder opgebouwde goede contacten met het NATO Strategic *Communications Centre of Excellence* (NATO StratCom COE).[67] Deze expertise heeft het PTE19 toegelaten een goed inzicht te verkrijgen in de technieken die door Russische of door Rusland gesponsorde actoren werden gebruikt om buitenlandse doelpublieken te beïnvloeden. De JTIF nam eveneens contact op met de *Transatlantic Commission on Election Integrity* (TCEI), een project van de *Alliance of Democracies*, een non-profitorganisatie die werd opgericht door onder andere voormalig NAVO-Secretaris-generaal Rasmussen. De TCEI hanteerde daarbij een speciaal hiervoor ontwikkelde *software* om abnormaal Twittergedrag te detecteren en paste dit reeds toe tijdens verschillende verkiezingscampagnes. Ten slotte namen vertegenwoordigers van de VSSE en/of de ADIV deel aan een aantal overlegfora, seminaries en conferenties over de thematiek.

I.4.6. CONCLUSIES

Na onderzoek was het Vast Comité I de mening toegedaan dat de twee inlichtingendiensten de nodige stappen hadden ondernomen om mogelijke bedreigingen ten aanzien van de Belgische en Europese verkiezingen van mei 2019 tegen te gaan. De diensten hadden:

- tijdig de problematiek herkend en opgenomen;
- de risico's en bedreigingen onderzocht en in kaart gebracht;
- zich naar behoren georganiseerd;
- de nodige samenwerking met elkaar en met andere actoren tot stand gebracht;
- de Regering en andere *stakeholders* gesensibiliseerd en regelmatig op de hoogte gehouden zodat zo nodig maatregelen hadden kunnen worden genomen.

Volgens de diensten bleven gevreesde grootschalige acties uit, terwijl werd vastgesteld dat desinformatietactieken steeds meer werden verfijnd.

---

[67] Het NATO StratCom COE (https://www.stratcomcoe.org), dat gevestigd is in Riga (Letland), werd operationeel in januari 2014 met de ondertekening van een memorandum door zeven NAVO-lidstaten. Het is een door de NAVO geaccrediteerde internationale, militaire organisatie die internationale deskundigen samenbrengt.

I.5. HET MEMORANDUM OF UNDERSTANDING (MOU) TUSSEN ADIV EN DE RWANDESE INLICHTINGENDIENSTEN

Het Vast Comité I besliste om in het bijzonder de draagwijdte te onderzoeken van het MoU dat in oktober 2016 werd afgesloten tussen de Algemene Dienst Inlichting en Veiligheid (ADIV) en de Rwandese inlichtingendiensten en, algemener, de afsluiting van een samenwerking tussen een Belgische inlichtingendienst en een van zijn buitenlandse partners.[68]

I.5.1. WETGEVEND KADER

I.5.1.1. De Wet houdende regeling van de inlichtingen- en veiligheidsdiensten

De wetgever moedigt sinds 1998 de samenwerking aan van de inlichtingendiensten met de Belgische politiediensten en de administratieve en gerechtelijke overheden enerzijds en met buitenlandse inlichtingen- en veiligheidsdiensten anderzijds. Artikel 20 W.I&V geeft de VSSE en de ADIV de algemene bevoegdheid om samenwerkingsverbanden aan te gaan met de inlichtingen- en veiligheidsdiensten van andere landen.

De wet preciseert de aard van de samenwerking noch de praktische modaliteiten ervan, maar belast de Nationale Veiligheidsraad (NVR) met de taak om de voorwaarden ervan te bepalen.

I.5.1.2. De toepassing van de wet en de ministeriële richtlijn

In september 2016 werd door de ministers van Justitie en Landsverdediging de als 'Vertrouwelijk Wet 11.12.1998' geclassificeerde 'Richtlijn aangaande de relaties van Belgische inlichtingendiensten met buitenlandse inlichtingendiensten' voorgelegd aan de NVR.[69] De richtlijn streeft ernaar om een inschatting te maken van buitenlandse diensten met als doel de aard van de relatie te bepalen. Het is een beleidsondersteunend instrument voor de bilaterale/multilaterale samenwerking.

De richtlijn omschrijft de mechanismen die de VSSE en de ADIV hanteren om op gestructureerde wijze de keuze van de internationale partners te objectiveren,

---

68 Het onderzoek werd geïnitieerd door de Begeleidingscommissie. Zie *Parl. St.*, Kamer, 2019-20, 55-888/001, 11.

69 MIT 16-007498 van 26.09.2016. De NVR heeft die richtlijn goedgekeurd op 30 september 2016. Het Comité had hier al langer en herhaaldelijk op aangedrongen. In VAST COMITÉ I, *Activiteitenverslag 2012* ('I.1.2. Nadere regels voor de samenwerking met buitenlandse diensten'), *Activiteitenverslag 2013* ('IX.1.1. Uitvoering van de artikelen 19 en 20 W.I&V') en *Activiteitenverslag 2014* ('IX.1.2. Richtlijnen inzake de samenwerking met buitenlandse diensten').

om de mate van samenwerking te bepalen en om de samenwerking op regelmatige basis te evalueren.[70]

De richtlijn bepaalt echter niet eenduidig of de VSSE en de ADIV al dan niet een voorafgaande ministeriële toestemming of de toestemming van een andere instantie moeten verkrijgen.[71] Het Comité was echter al in 2014 van oordeel "*dat er vanuit de inlichtingendiensten een grotere openheid moet zijn over bestaande bi- of multilaterale samenwerkingsverbanden en dit in de eerste plaats ten aanzien van de bevoegde ministers. In dergelijke samenwerkingsverbanden kunnen immers engagementen worden genomen of keuzes gemaakt die een politieke aftoetsing en dekking behoeven. Anders gezegd, dienen de bevoegde ministers afdoende te worden geïnformeerd opdat zij steeds in de mogelijkheid zouden zijn om hun politieke verantwoordelijkheid op te nemen. Daarbij moet opgemerkt worden dat wat 'politiek relevant' is of niet, kan evolueren in de tijd*".[72] In 2017 kwam er opnieuw een aanbeveling door het Comité omtrent de nood aan een politieke dekking.[73]

I.5.1.3. Een Memorandum of Understanding van de ADIV met de Rwandese inlichtingendiensten

Een memorandum van overeenstemming (*Memorandum of Understanding*[74]) is een document dat een overeenkomst of een bilateraal of multilateraal akkoord tussen de partijen beschrijft. Het geeft een toenadering van de intenties van de verschillende partijen aan, wat wijst op een gemeenschappelijke actielijn. Het wordt vaak gebruikt in gevallen waarin de partijen geen juridische verbintenis zijn aangegaan of in situaties waarin de partijen geen uitvoerbare overeenkomst kunnen sluiten. Het is een formeler alternatief voor een *gentlemen's agreement*. In het internationaal publiekrecht vallen de memoranda van overeenstemming onder de algemene categorie van verdragen. Juridisch gezien vooronderstellen ze geen bindend karakter, maar drukken ze een beleidsintentie van de ondertekenaars uit.

Wat betreft het sluiten van een MoU of elke andere vorm van samenwerking met een buitenlandse partner, meent het Comité dat dit onmiskenbaar een politiek

---

70 De Richtlijn beantwoordde echter slechts gedeeltelijk aan de aanbevelingen van het Comité: *"Evenwel wordt daarin het doorgeven van informatie/persoonsgegevens aan buitenlandse diensten slechts zeer summier behandeld. Het Comité houdt wat dit betreft dan ook vast aan zijn eerdere aanbevelingen en acht een initiatief prioritair. Hierbij moet alleszins aandacht zijn voor het beginsel dat de inlichtingendiensten bij de informatie-uitwisseling zorgvuldig tewerk moeten gaan*." VAST COMITÉ I, *Activiteitenverslag 2016*, 166.

71 Zie in die zin: Wetsvoorstel tot wijziging van de wet van 30 november 1998 houdende regeling van inlichtingen- en veiligheidsdiensten met het oog op het invoeren van wegingsnotities voor de samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten, *Parl. St.* Kamer 2019-20, nr. 55-956/001 (23 januari 2020).

72 VAST COMITÉ I, *Activiteitenverslag 2014*, 113.

73 VAST COMITÉ I, *Activiteitenverslag 2017*, 107 ('XII. Politieke dekking voor samenwerkings-verbanden').

74 Foreign and Commonwealth Office, Legal directorate, Treaty section, *Treaties and memoranda of understanding (mou's) guidance on practice and procedures*, Bijgewerkt maart 2014.

karakter heeft, ook al is een dergelijke overeenkomst volgens de ADIV niet juridisch bindend. De partner-inlichtingendienst kan die overeenkomst immers vrijwillig of onvrijwillig gebruiken om zijn persoonlijke belangen te verdedigen en de diplomatieke relaties van België schade toebrengen.[75] Op het ogenblik van het onderzoek had de ADIV samenwerkingsverbanden[76] met diverse buitenlandse partners ontwikkeld, waarvan slechts 15% het voorwerp uitmaakten van een MoU, waaronder deze die op 14 oktober 2016 werd afgesloten met de Rwandese diensten.

Dit MoU werd ondertekend door het toenmalig hoofd van de ADIV, en de secretaris-generaal van de Rwandese Inlichtingendienst (NISS). Het betrof een niet-geclassificeerd document[77] met als voorwerp: *"to regulate the terms and conditions of exchange of national classified information, to define areas of bilateral cooperation in the field of intelligence and to formalize the procedure regarding the meetings between the two Participants"*.[78] Er wordt daarbij ingegaan op drie partnerschapsdomeinen, maar er wordt niet gepreciseerd op welke wijze dit in de praktijk moet worden gerealiseerd.

Ondanks de verplichting opgelegd door artikel 33 W.Toezicht om "*uit eigen beweging aan het Vast Comité I de interne reglementen en richtlijnen over, alsook alle documenten die de handelwijze van de leden van die diensten regelen*"[79] te zenden en de herhaalde aanbevelingen van het Comité, diende opnieuw te worden vastgesteld dat de ADIV hiertoe het met Rwanda afgesloten MoU niet uit eigen beweging had aangeleverd.

I.5.2. ANALYSE

I.5.2.1. Wat betreft de evaluatie van de partner en de ondertekening van het MOU

In de loop van het onderzoek preciseerde de ADIV dat de overeenkomsten die de dienst met een partner aangaat niet juridisch bindend zijn en weinig intenties

---

75 Het Comité had in zijn rapporten over de zaak Edward Snowden en de klacht van een medewerker van de ADIV al op dat risico gewezen. VAST COMITE I, *Activiteitenverslag 2014* (II.1. De Snowden-onthullingen en de informatiepositie van de Belgische inlichtingendiensten') en VAST COMITÉ I, *Activiteitenverslag 2017* ('II.1. Een klacht over drie operaties van de ADIV').

76 Het Comité constateerde dat er geen verband bestaat tussen deze vorm van samenwerking en het door de ADIV ontwikkelde en door de minister van Defensie ondertekende Inlichtingenstuurplan.

77 Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (W.C&VM).

78 "*de voorwaarden voor de uitwisseling van geclassificeerde nationale informatie regelen en definieren, de domeinen van een bilaterale samenwerking voor inlichtingen definiëren en de procedure voor vergaderingen tussen de deelnemers formaliseren*" (vrije vertaling).

79 VAST COMITÉ I, *Activiteitenverslag 2014*, 125 ('IX.3. Aanbeveling in verband met de doeltreffendheid van het toezicht: strikte toepassing van artikel 33 § 2 W.Toezicht'). *"Deze verplichting geldt ook voor afspraken, Memorandums of Understanding (MoU's)* (door ons onderlijnd) *of overeenkomsten gesloten op internationaal vlak, weze het bi- of multilateraal*".

inhouden. De dienst preciseerde ook dat zijn acties worden ontwikkeld in overeenstemming met de activiteiten en de politieke positie van België.

De ADIV stelde dat er, gezien de zeer beperkte impact van deze overeenkomst voorafgaand aan de ondertekening ervan, niet werd gevraagd om de toestemming van de minister van Defensie.

Het Comité kon vaststellen dat er voorafgaand aan het afsluiten van het MoU geen evaluatie plaatsvond van de Rwandese partner overeenkomstig de ministeriele richtlijn van 26 september 2016. De ADIV vermeldde die beoordeling pas later te hebben uitgevoerd, meer bepaald in de tweede helft van 2018.

De ADIV heeft na analyse de Rwandese dienst gecategoriseerd. Het Comité stelde na onderzoek vast dat deze analyse niet gedateerd, te beknopt en onvoldoende gedocumenteerd was. Verder was er geen sprake van een globale beoordeling van ADIV, maar vormde deze het resultaat van de analyse van twee van zijn directies. Bovendien maakte een van deze directies geen gebruik van de beoordelingscriteria van voormelde richtlijn. Ten slotte werd geen melding gemaakt van bepaalde incidenten.

I.5.2.2. Wat betreft de technische inhoud van het MOU

Het Comité kon vaststellen dat het MoU bepalingen voor beide partijen bevatte met betrekking tot:

- de uitvoering van het MoU dewelke altijd zal plaatsvinden in overeenstemming met de nationale en internationale normen van de respectievelijke landen;
- de regel van de derde dienst die moet worden nageleefd;
- de overeenstemming en de classificatieniveaus;
- de maatregelen voor de bewaring en beveiliging van geclassificeerde documenten;
- de procedures in het geval van incidenten of compromittering;
- de procedures voor het organiseren van vergaderingen.

Het MoU bevatte geen bepalingen over de samenwerkingsdomeinen of over het beheer en de doorgifte van persoonsgegevens.

I.5.3. BESLUITEN

Het Comité blijft ervan overtuigd dat de Belgische inlichtingendiensten moeten blijven investeren in een samenwerking met de buitenlandse diensten, zowel bilateraal als multilateraal.[80] Die samenwerking moet echter volledig transparant en traceerbaar zijn, gezien deze een onmiskenbaar politiek karakter heeft.

Ondanks de verplichting opgelegd door artikel 33 W.Toezicht om "*uit eigen beweging aan het Vast Comité I de interne reglementen en richtlijnen over, alsook alle documenten die de handelwijze van de leden van die diensten regelen*" te zenden en de herhaalde aanbevelingen van het Comité, stuurde de ADIV de bovengenoemde documenten, waaronder de MoU's, nog steeds niet door naar het Vast Comité I.

Wat de samenwerking met een buitenlandse partner betreft, herhaalde het Comité zijn vaststelling dat zijn aanbevelingen met betrekking tot de noodzaak van een politieke toestemming voorafgaand aan het sluiten van bilaterale/internationale overeenkomsten niet werden opgevolgd. De ministeriële richtlijn blijkt geen ondubbelzinnige bepaling te bevatten volgens dewelke de inlichtingendiensten de goedkeuring van de minister moeten verkrijgen alvorens een formele of informele overeenkomst voor samenwerking met een buitenlandse dienst te sluiten, ook al kan hij daarvoor politiek verantwoordelijk zijn.

Wat meer bepaald het partnerschap met de Rwandese diensten betreft, was het Comité van mening dat de ADIV de ministeriële richtlijn niet heeft nageleefd, zowel bij het afsluiten van de overeenkomst als bij de uitvoering ervan.

Het Comité stelde opnieuw vast dat de ADIV onvoorzichtig was, aangezien dit soort documenten niet uniform wordt geclassificeerd.

Ondanks het bestaan van de richtlijn stelde het Comité vast:

- dat de partner laattijdig werd geëvalueerd (twee jaar na de ondertekening van het MoU);
- dat de evaluatie niet gedateerd, te beknopt en onvoldoende gedocumenteerd was;
- dat de in de richtlijn bepaalde evaluatiecriteria niet uniform werden toegepast[81];
- dat incidenten niet werden gemeld;
- dat er geen tweejaarlijkse evaluatie werd uitgevoerd.

Ondanks de eerdere aanbevelingen van het Vast Comité I, stelde het vast dat de standpunten van de verschillende directies aangaande deze thematiek binnen de ADIV uiteenliepen en dat er geen gezamenlijk standpunt bestond.

---

80 Zie ook: VAST COMITÉ I, *Activiteitenverslag 2013* ('IX.1.1. Uitvoering van de artikelen 19 en 20 W.I&V').

81 De voormalige directies 'Intelligence' (I) en 'Counter Intelligence' (CI) gebruiken niet dezelfde evaluatiecriteria.

I.6. INFORMATIE- EN COMMUNICATIETECHNOLOGIE IN HET INLICHTINGENPROCES BIJ DE ADIV

I.6.1. 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. Informatie kan afkomstig zijn van menselijke bronnen (HUMINT), digitale bronnen zoals '*open sources*' (OSINT), afluisteroperaties (SIGINT), beeldmateriaal (GEOINT)... De constante groei van de gegevensstromen vereist passende systemen die geschikt zijn om die stromen te absorberen en om een correcte, snelle en doeltreffende analyse mogelijk 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 ICT-praktijken, en moet tegelijk rekening houden met technologische ontwikkelingen[82], zoals bijv. '*big data*'.[83]

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.[84] [85]

Daarop startte het Vast Comité I in mei 2019 een '*Toezichtonderzoek betreffende de informaticamiddelen die de Belgische inlichtingendiensten gebruiken om informatie te verzamelen, te analyseren en te communiceren in het kader van de inlichtingencyclus*'. Het onderzoek spitste zich toe op de informaticamiddelen die

---

82 De toezichtsorganen vervullen in dit verband ook een belangrijke rol. Zie in dit verband: K. VIETH en T. WETZLING, *Data-driven Intelligence Oversight. Recommendations for a System Update*, StiftungNeueVerantwortung, november 2019, 63 p.

83 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.

84 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').

85 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.

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.[86] 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[87] te identificeren waarmee de diensten te maken kregen en die risico's te verminderen door gepaste aanbevelingen te formuleren.

De ADIV maakte het eerst voorwerp uit van onderzoek, en dit omwille van de impact van de herstructurering van deze dienst op het vlak van ICT-tools en werkmethoden.[88] De onderzoeksvragen luidden als volgt:

- Welke technologieën en tools op het vlak van ICT gebruikt de ADIV 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')[89] toegepast (meer bepaald: *'change management'*, *'inventory management'*, *'business continuity'*, *'incident management'*, *'problem management'* …)?
- 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?[90]

Het onderzoek had dus tot doel de risico's te identificeren waarmee de ADIV te maken kreeg en aanbevelingen te formuleren om die risico's te verminderen.

---

86 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'*).

87 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.

88 Het onderzoek werd – voor wat betreft de ADIV – afgerond in mei 2020. Het onderzoeksluik 'ICT-VSSE' liep door in 2020-2021.

89 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).

90 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).

Daarbij was het zogenaamde 'CIA-model'[91] 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.

Er werd daarbij geen analyse gemaakt van de ICT-instrumenten die specifiek worden gebruikt voor SIGINT.[92] Ook de ICT-middelen die de Directie Cyber gebruikt, werden enkel geanalyseerd voor zover ze betrekking hebben op de inlichtingencyclus. De bevoegdheden van die directie omvatten immers ook (en overigens hoofdzakelijk) activiteiten die geen (of niet rechtstreeks) betrekking hadden op de inlichtingencyclus (artikel 11, § 1, 1° en 5° W.I&V), maar veeleer slaan op cyberdefensie en, desgevallend, cyberaanvallen (artikel 11, § 1, 2° W.I&V).[93]

I.6.2. CONTEXT

I.6.2.1. Team, personeel en netwerken

De informatica van de ADIV wordt voornamelijk beheerd door de Stafafdeling J6 van de dienst. Deze afdeling is opgedeeld in twee pijlers: de eerste beheert de *software* (analisten, ontwikkelaars, databankbeheerders), terwijl de tweede vooral actief is op vlak van het beheer van de *hardware* zoals het netwerk, de servers, het magazijn en de helpdesk. De Stafafdeling J6 beheert meerdere netwerken (in functie van de aard van de informatie die er circuleert) en ook de gebruikers. Elke medewerker kan meerdere gebruikersaccounts hebben in functie van zijn bevoegdheden, opdrachten en *need-to-know*. Deze netwerken kunnen zowel op Belgisch grondgebied als in het buitenland beschikbaar zijn.

---

91 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).

92 Het gaat immers om een materie met het classificatieniveau 'ZEER GEHEIM'. Dit maakt het voorwerp uit van een lopend toezichtonderzoek.

93 Dit betekent "*zorgen voor het behoud van de militaire veiligheid (…) en, in het kader van de cyberaanvallen op wapensystemen, militaire informatica- en verbindingssystemen of systemen die de Minister van Landsverdediging beheerst, 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*".

I.6.2.2. Databanken

Wat betreft de databanken en hun beheersystemen, kon er bij de ADIV een onderscheid worden gemaakt tussen zogenaamde:
- 'grote' databanken: er bestaan bij de ADIV meerdere types databanken. De meeste daarvan zijn relationele SQL-databanken (*Structured Query Language*). De meeste databanken draaien op de MS-SQL-technologie van Microsoft, al blijven er nog wel andere types over. Twee databanken zijn van het type 'no-SQL'. De vroegere Directie I beschikte over een systeem van 'groepssoftware' (*groupware*). Dat systeem laat toe documenten in een bibliotheek te plaatsen ('referentiesysteem' of '*repository*') waar ze worden 'gepubliceerd' (via een portaal) zodat ze toegankelijk zijn voor meerdere personen of groepen.
- 'kleine' databanken: naast de databanken voor de belangrijkste applicaties bestaan er ook kleine individuele databanken of databanken per dienst.

Daar waar het belang van de databanken evident is, bleek dikwijls dat ze in de loop van de jaren zodanig in omvang toenamen dat het quasi-onmogelijk werd om in de gigantische hoeveelheden gegevens die ze bevatten, nog op efficiënte wijze de relevante gegevens terug te vinden. Het Vast Comité I suggereerde daarbij een aantal oplossingen[94]:
- een consolidatie en reorganisatie van de databanken van het type SQL met de toevoeging van zoekindexen. Deze methode is goedkoop en levert resultaten voor de courantste verrichtingen;
- het gebruik van '*data warehouses*' ('*big data*'), waarin alle gegevens van de verschillende databanken worden gedupliceerd zodat het mogelijk wordt om grootschalige analyses uit te voeren die toelaten tendensen vast te stellen of om informatie te ontdekken die aanvankelijk niet voor de hand liggend is wanneer men enkel elke databank afzonderlijk bekijkt. Deze methode vereist een grote rekenkracht en een groot opslagvermogen alsook een grondige kennis van het te behandelen onderwerp, met als doel een correct datamodel op te stellen;
- het gebruik van nieuwe types databanken die niet langer gebaseerd zijn op gestructureerde relaties (SQL) maar veeleer op de aanwezigheid van elementen (gegevens, tags) die toelaten een relevantiescore van de informatie te bepalen. Het gaat om zogenaamde 'no-sql'-databanken die een veel eenvoudigere structuur hebben en de mogelijkheid bieden te zoeken naar de inhoud van bestanden of naar *tags*.

---

94 Naar analogie zou een SQL-databank bijvoorbeeld het klantenbestand van een winkel zijn. Het '*data warehouse*' zou dan de consolidatie van de klantenbestanden en de aankopen van alle winkels in België zijn. Een databank van het type 'no-sql' zou dan bijvoorbeeld een zoekmotor zijn (bijv. Google).

Het Comité heeft ook een aantal vaststellingen gedaan met betrekking tot de veiligheid van het fysieke materiaal of van de ICT-communicatie. Het is een dienst van de Directie Cyber die de veiligheidstests uitvoert voordat een applicatie in gebruik wordt genomen binnen Defensie en de ADIV.

I.6.3. EVALUATIE VAN DE RISICO'S

Voor elk onderdeel van de ICT-organisatie van de ADIV werden een aantal aandachtspunten opgesomd. Tijdens dit onderzoek heeft het Comité de aandacht gevestigd op bepaalde risico's, hun waarschijnlijkheid en beperkingspistes (*mitigation*) om die risico's te verminderen. Daarbij werd een overzicht van de bij de ADIV vastgestelde problemen, ingedeeld volgens categorie.[95] Bij de grootste risico's voor de dienst, werd de aandacht gevestigd op:

- de snelheid van het netwerk, aangezien dat wordt gebruikt voor alle applicaties en dus belangrijk is voor de goede uitvoering van de opdrachten van de dienst;
- de monitoring van het netwerk, maar ook van de volledige digitale infrastructuur, met als doel proactief op zoek te gaan naar voortekenen van storingen of trage werking;
- de registratie (logging) van de activiteiten om zich te beschermen tegen misbruik, maar ook met als doel bewijzen in rechte te kunnen overleggen in verband met de activiteiten van de gebruikers;
- het beheer van de '*Active Directory*' om de mogelijkheid van '*privilege creeping*'[96] te beperken (wanneer bij elke functiewijziging meer toegangsrechten worden verworven, zonder dat vroegere rechten worden geschrapt);
- *change management*, opdat elke wijziging (update, nieuwe installatie) verloopt volgens een strikte procedure die een methode omvat die toelaat terug te keren naar de vorige situatie.

Ten slotte werd het probleem van het gebrek aan ICT-personeel aangekaart. Het bleef belangrijk om dit dringend aan te pakken en de aanwervingsprocedure onverwijld te lanceren, aangezien het om een vrij lange procedure gaat. Als het tekort aan ICT-personeel aanhield of nog groter werd, bestond/bestaat immers de kans dat alle onderliggende opdrachten werden verstoord in het geval van een storing of eenvoudigweg voor het onderhoud van de *hard-* of *software*-infrastructuur.

---

95 Omwille van het vertrouwelijke karakter, kan in dit publiek activiteitenverslag niet worden ingegaan op de details van deze risico-analyse.

96 Een geleidelijke opeenstapeling (vaak bij functiewijzigingen) van toegangsrechten die verder gaan dan wat een individu nodig heeft om zijn of haar job te doen. In de ICT is een '*privilige*' een bepaald toegangsrecht dat een eindgebruiker heeft op een bestand of een virtuele machine.

I.7. DE OPVOLGING VAN EXTREEMRECHTS DOOR DE BELGISCHE INLICHTINGENDIENSTEN

I.7.1. ONDERZOEKSOPZET: INLICHTINGENCYCLUS EN RISICOANALYSE

Door het toenemend aantal internationale, terroristische incidenten die in verband werden gebracht met individuen met een extreemrechts gedachtengoed, door de opkomst van identitaire bewegingen alsook omwille van de spraakmakende reportage over Schild & Vrienden[97], achtte het Vast Comité I het opportuun om een toezichtonderzoek te openen naar de wijze waarop de inlichtingendiensten de bedreiging die uitgaat van (het fenomeen) extreemrechts in België opvolgen en erover rapporteren aan de autoriteiten.

Het Comité wenste te onderzoeken of en hoe de inlichtingendiensten werk maken van hun wettelijke opdracht om het extremisme, en meer bepaald het extreemrechts extremisme in België, op te volgen. Hiertoe werd de 'risico-aanpak' geïntegreerd in de inlichtingencyclus. Dat vertaalde zich als volgt:

Fase van de inlichtingencyclus	Risico	Onderzoeksvragen
Inlichtingendoelen afbakenen (strategisch op beleidsniveau)	Het fenomeen wordt niet herkend of het trekt onvoldoende de aandacht; Het wordt niet goed (juridisch of strategisch) omschreven (kwalitatieve afbakening); Het wordt niet gekwantificeerd zodat men niet kan inschatten wat het in de realiteit betekent (kwantitatieve afbakening)	Wie moet de afbakening doen en wat is de juridische en strategische context? Welke zijn de instructies van de bevoegde ministers, de Nationale Veiligheidsraad of andere instanties? Wordt er door de Belgische inlichtingen- en veiligheidsdiensten een gemeenschappelijke definitie gehanteerd in het kader van het Plan Radicalisme? Is het fenomeen gekwantificeerd?

97 https://www.vrt.be/vrtnws/nl/2018/09/05/pano-wie-is-schild-vrienden-echt/

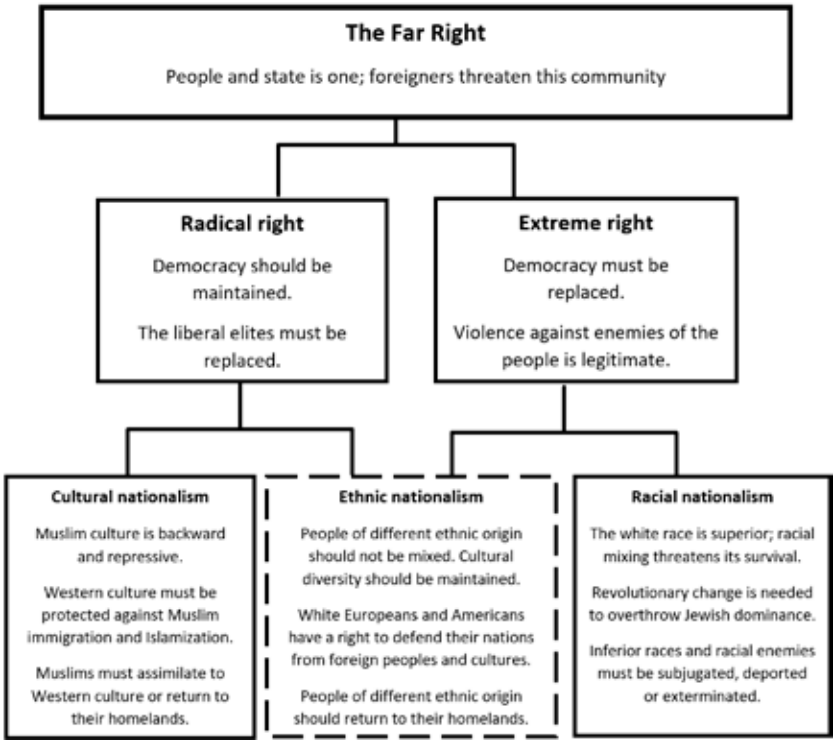
Inlichtingendoelen afbakenen, plannen opstellen en zich organiseren (operationeel en tactisch, op niveau van de diensten)	Het fenomeen is herkend, maar is onvoldoende vertaald in de organisatie en de interne planning (niet proportioneel).	Hoe nemen de inlichtingendiensten zelf het fenomeen 'extreemrechts' op in hun organisatie en planning? Hoe wordt bepaald welke groeperingen en situaties het voorwerp uitmaken van actieve opvolging? Hoe zijn de diensten georganiseerd om deze opvolging uit te voeren? Welke prioriteiten werden er gelegd? Is de inzet van de middelen (personeel, methoden…) proportioneel ten aanzien van het beoogde doel?
Collecte en verwerking	Er is onvoldoende collecte: Te weinig bronnen om het fenomeen op te volgen; De bronnen en instrumenten worden niet goed in stelling gebracht; De verwerking van de gegevens stelt problemen.	Welke methoden werden gebruikt (gewone methoden (bijv. HUMINT), bijzondere inlichtingenmethoden …)? Hoe wordt de informatie verwerkt?
Analyse en verspreiding / samenwerking	Er is geen of onvoldoende analyse. De inlichtingen worden niet verspreid zodat het fenomeen geen beleidsaandacht krijgt. Er is onvoldoende samenwerking.	Welke inschattingen werden er gedaan (analyse) en hoe werd daarover gerapporteerd naar de autoriteiten? Hoe werkt men samen met welke partners?
Feedback	Het beleidsniveau geeft geen *feedback* zodat het niet mogelijk is de inlichtingendoelen te verfijnen of bij te sturen	Welke *feedback* ontvingen de diensten van de gebruikers?

I.7.2. EXTREEMRECHTS: BEGRIPPENKADER EN BEELDVORMING

I.7.2.1. Vanuit een academische invalshoek

De opvattingen omtrent de precieze invulling van het begrip 'extreemrechts' en 'rechtsextremisme' blijken erg verschillend; er is duidelijk geen consensus omtrent de exacte definitie van deze concepten. Toch vormde een artikel van de Nederlandse politoloog Mudde (1995) de basis voor een conceptualisering van

extreemrechts in Europa.[98] Mudde maakte binnen het rechtse politieke spectrum een onderscheid tussen gematigd rechts en extreemrechts. Binnen extreemrechts werd dan vervolgens een opsplitsing gemaakt tussen radicaal rechts, dat opereert binnen een democratisch kader, en rechts-extremisme, dat voorstander is van het gebruik van geweld of andere onconventionele middelen om politieke verandering te bewerkstelligen. De Noren Bjørgo en Ravndal[99] (2019) werkten een aantal van deze concepten verder uit en ontwikkelden een conceptueel model, waarin drie 'families' van hedendaags extreemrechts te vinden zijn:[100]



98 C. MUDDE, 'Right-Wing Extremism Analyzed. A Comparative Analysis of the Ideologies of Three Alleged Right-Wing Extremist Parties (NPD, NDP, CP'86)', European Journal of Political Research, 1995, Vol. 27, Issue 2, pp. 203-224.

99 T. BJØRGO & J.A. RAVNDAL, *Extreme-Right Violence and Terrorism: Concepts, Patterns, and Responses*, International Centre for Counter-Terrorism, September 2019, 22 p.

100 Deze indeling is niet enkel van academisch, maar ook van praktisch belang. Het onderscheid tussen drie extreemrechtse families maakt duidelijk welke de groepen en individuen zijn die het meest waarschijnlijk geweld zullen gebruiken (rechts-extremisme). In deze stroming wordt geweld beschouwd als een legitieme, noodzakelijke en vaak lovenswaardige manier van handelen. Aanhangers van raciaal nationalisme (bijv. neonazi's, fascisten en blanke supremacisten), scoren hoog onder daders van extreemrechts geweld.

Wat cijfermateriaal betreft, bleek uit een dataset[101] betreffende incidenten van extreemrechts geweld en/of terrorisme met dodelijke slachtoffers in West Europa en de Verenigde Staten, dat er in West-Europa een piek was in dodelijk extreemrechts geweld en terrorisme in het begin van de jaren 1990 en aan het begin van het millennium. Sindsdien is er een neerwaartse trend, met een kleinere piek in 2016, mogelijk te wijten aan de Europese vluchtelingencrisis. Uit cijfermateriaal verzameld door de Duitse inlichtingendienst *Bundesamt für Verfassungsschutz* (BfV), blijkt dat in Duitsland het aantal rechts-extremisten sinds 2013 gestaag is toegenomen, terwijl ook het aantal door rechts-extremisten gepleegde gewelddaden toenam van 2014 tot 2018, met een piek in 2015-2016.[102]

I.7.2.2. Beeldvorming over extreemrechts door de Belgische diensten

a) Het Coördinatieorgaan voor de dreiginsanalyse (OCAD)[103]

In een nota schetst het OCAD een algemeen beeld van het fenomeen 'rechts-extremisme'.[104] Het OCAD stelt dat het proces van gewelddadige rechtsextremistische radicalisering erg gelijklopend is met andere radicaliseringsprocessen (bijv. islamistisch jihadisme). De dienst verwijst daarbij naar Bjørgo, die stelt dat ideologie een ondergeschikte rol speelt in de radicalisering van extreemrechtse jongeren. Diffuse, vijandige gevoelens spelen daarentegen wel een grote rol.

Het OCAD ziet drie voorname voedingsbodems voor extreemrechts: bepaalde *trigger events*, de specifieke maatschappelijke context en (socio)psychologische motieven. Internet blijkt een alsmaar belangrijkere factor in het verspreiden van radicale en gewelddadige ideologieën en propaganda: het is goedkoop en wordt massaal gebruikt, het laat toe om wereldwijde netwerken te creëren, door de (relatieve) anonimiteit zijn verkondigde meningen vaak radicaler dan wanneer de identiteit van de auteur bekend is, en radicale propaganda kan zich razendsnel verspreiden of 'viraal gaan' door gebruik te maken van geautomatiseerde profielen of zogenaamde *bots*. Rechts-extremisten, aldus het OCAD, trachten een 'wij-zij' gevoel te creëren, van waaruit de aanhangers ofwel een superioriteitsgevoel dan wel een slachtofferrol aannemen, die impliceert dat men vanuit een bepaalde hoek 'bedreigd' wordt. Vaak gaat dit alles ook samen met complottheorieën, waarbij

---

101 J.A. RAVNDAL, 'Right-wing terrorism and violence in Western Europe', *Perspectives on Terrorism*, 2016, Vol.X, Issue 3. De cijfers werden geupdated in J.A. RAVNDAL, S. LYGREN, A.R. JUPSKAS en T. BORGJO, RTV *Trend Report. Right wing terrorism and violence in Western Europe (1990-2019)*. Hierin : *"To sum up the year 2019, we may conclude that right-wing terrorism and violence still constitute significant problems in Western Europe"*.

102 EUROPOL, 'Terrorism Situation and Trend Report 2019 (TE-SAT)', 27 June 2019, p. 61.

103 Hoewel de opvolging van extreemrechts door het OCAD geen voorwerp uitmaakt van onderzoek, werd vooralsnog contact opgenomen met deze dienst, niet in het minst omdat hij fungeert als pilootdienst van de Werkgroep Extreemrechts in het kader van het Actieplan Radicalisme (Plan R).

104 COÖRDINATIEORGAAN VOOR DE DREIGINGSANALYSE, *Nota beeldvorming rechts-extremisme*, 14 februari 2020, 39 p.

wordt beweerd dat een samenzwering van de overheid en de *mainstreammedia* 'de waarheid' tracht te verbergen en te manipuleren. Een andere tactiek waartoe door rechts-extremistische bewegingen wordt opgeroepen is, nog volgens het OCAD, een zogenaamde 'mars door de instellingen'. Deze strategie bestaat erin om via participatie in sociale bewegingen en via deelname aan democratische, politieke processen aan invloed te winnen met als doel om op termijn de eigen ondemocratische ideologie te kunnen doordrukken.

b) De VSSE en de ADIV

De VSSE stelt vast dat het extreemrechtse milieu in België de voorbije jaren een 'fundamentele transformatie' heeft ondergaan. Traditionele verschijningsvormen zoals neonazisme en de skinheadcultuur zijn op hun retour, terwijl het anti-islam en anti-migratieactivisme – vooral sinds de vluchtelingencrisis van 2015-2016 – de *main topics* werden. Waar in het verleden extreemrechtse groeperingen eerder de nationalistische gevoelens van hun aanhangers aanspraken, is de focus verschoven naar xenofobe standpunten. Dit geldt zowel voor 'oudere' extreemrechtse groeperingen, als voor nieuwe bewegingen. De VSSE stelt ook een verhoogde interesse vast bij rechts-extremisten voor wapens en wapentrainingen. De dienst is van oordeel dat de grootste concrete dreiging uitgaat van zogenaamde '*lone actors*', die op eigen houtje radicaliseren en gewelddadige acties beramen.[105]

De opvolging van extremistische activiteiten werd door de wetgever expliciet toegewezen aan de VSSE (artt. 7 en 8, 1°, c° W.I&V). Dat verhindert echter niet dat de ADIV op legitieme wijze extremisme bij militairen of burgerpersoneel van Defensie zou opvolgen, althans voor zover zij een mogelijke dreiging vormen voor het departement of zijn werking.[106] Evenwel heeft de ADIV omtrent deze materie geen eigen visie ontwikkeld.[107] De dienst baseert zich hiervoor op het werk van de VSSE en het OCAD.

---

105 VEILIGHEID VAN DE STAAT, *Jaarrapport 2019*, 20 (https://www.vsse.be/nl/jaarrapport-2019).

106 Bovendien schrijven bepalingen betreffende het statuut van het militair en burgerlijk personeel voor dat zij de Grondwet en de wetten moeten naleven en de morele en materiële belangen van de Staat moeten verdedigen. Bepaalde daden of uitingen van een extremistisch gedachtegoed, zowel binnen als buiten de professionele context, kunnen worden bestraft omdat ze in tegenspraak zijn met het tuchtstatuut, de deontologie en de militaire reglementen.

107 In 2012 startte het Vast Comité I reeds een toezichtonderzoek naar de opsporing en opvolging van extremistische elementen (extreemrechts, extreemlinks, als radicaal islamisme) bij het personeel van Defensie. Binnen Defensie bleek een vrij beperkt aantal individuen betrokken bij extremistische activiteiten. In de loop van het onderzoek stelde de ADIV dat het aantal militairen die de aandacht trekken omwille van mogelijke betrokkenheid bij extremistische activiteiten, beperkt is.

I.7.3. EERSTE STAP IN DE INLICHTINGENCYCLUS: AFBAKENING VAN HET INLICHTINGENDOEL EXTREEMRECHTS

I.7.3.1. Kwalitatieve afbakening: definiëring van het fenomeen

Bij het organiseren van de inlichtingenfunctie en het bepalen waar een inlichtingendienst de aandacht op moet richten, is het eerst en vooral van belang om de fenomenen duidelijk te definiëren en vervolgens in beeld te brengen.

De VSSE verwijst naar artikel 8 van de Wet op de inlichtingen- en veiligheidsdiensten (W.I&V) om te bepalen of een individu of groepering als rechtsextremistisch dient te worden beschouwd. De wet vermeldt echter niet uitdrukkelijk wat onder 'extreemrechts' of 'rechts-extremisme' dient te worden begrepen.[108] De dienst verwijst verder ook naar het conceptueel model van Bjørgo (*supra)* en baseert zich op de definitie zoals die wordt gehanteerd door de Nederlandse Algemene Inlichtingen- en Veiligheidsdienst (AIVD).

Op de vraag van het Comité naar definities en concepten van de militaire inlichtingendienst, kwam geen antwoord dat afwijkt van dat van andere actoren. In de praktijk gaat de aandacht van de dienst uit naar militairen die zich eventueel schuldig maken aan racistische, negationistische of discriminatoire uitlatingen of gedrag, of die deel uitmaken van groeperingen die dergelijke uitlatingen of gedrag tentoonspreiden. Door het feit dat de ADIV zich richt op de vrijwaring van de militaire belangen, is hun opvolging van extreemrechts minder uitgebreid dan bij de VSSE. De ADIV baseert zich dan ook op de analyses van de VSSE voor het ruimer in kaart brengen van de problematiek en richt zich naar de door de VSSE gehanteerde definities en concepten.

Maar aan wie komt het toe de afbakening te doen? Eerst en vooral dient de wetgever te bepalen waar de inlichtingendiensten zich op moeten richten en het werkingsveld af te bakenen (cf. de Wet op de inlichtingen- en veiligheidsdiensten). In tweede orde zijn er de bevoegde ministers: de artikelen 4 en 10 W.I&V bepalen dat de VSSE en de ADIV hun opdrachten vervullen door tussenkomst van respectievelijk de ministers van Justitie en Landsverdediging. Parallel daarmee komt de Nationale Veiligheidsraad (NVR) tussen die het algemeen inlichtingen- en

---

[108] Een aantal van deze begrippen werden uitgewerkt door: J. SEGERS en D. PEETERS, 'Inlichtingendiensten en extremisme', in M. COOLS, K. DASSEN, R. LIBERT, P. PONSAERS (eds.), *De Staatsveiligheid – Essays over 175 jaar Veiligheid van de Staat*, Politeia, 2005, pp. 281-302). Vooral het voorkomen van de term 'nationalisme' in de wettelijke definitie van extremisme vraagt om enige toelichting: *"Nationalisme is voor de dienst (VSSE) als fenomeen in relatie tot extremisme enkel van belang, in zoverre het aansluit bij de eerder aangehaalde begrippen van racisme en/of xenofobie. Met andere woorden, bewegingen die op democratische wijze een grotere mate van autonomie nastreven van een bepaalde (volks)gemeenschap, of die een zekere voorliefde voor het eigen volk centraal stellen met respect voor de mensenrechten, dienen niet als extremistisch te worden beschouwd"*.

veiligheidsbeleid vastlegt en de prioriteiten stelt. Het operationaliseren van de opdrachten komt toe aan de inlichtingendiensten zelf, zo nodig in coördinatie met andere veiligheidsdiensten (bijv. het OCAD).

a) De Inlichtingenwet (1998)

In de Inlichtingenwet maar ook in de W. OCAD worden de termen 'extreemrechts' of 'rechtsextremisme' niet expliciet gedefinieerd. Art. 8, 1°, c) W.I&V vermeldt enkel volgende definitie van 'extremisme': *"racistische, xenofobe, anarchistische, nationalistische, autoritaire of totalitaire opvattingen of bedoelingen, ongeacht of ze van politieke, ideologische, confessionele of filosofische aard zijn, die theoretisch of in de praktijk strijdig zijn met de beginselen van de democratie of de mensenrechten, met de goede werking van de democratische instellingen of andere grondslagen van de rechtsstaat"*. Met de Wet van 30 maart 2017 werd aan deze definitie toegevoegd: "*Hieronder wordt ook het radicaliseringsproces begrepen*".[109]

Een voorbehoud is hier op zijn plaats, in de zin dat de wetgever zelf te kennen gaf dat de zaken hoe dan ook relatief vaag blijven. De leden van de wetgevende macht stelden in de bespreking voorafgaand aan de invoering van de W.I&V dat de definities '*niet zo nauwkeurig zijn als strafdefinities*' of hanteerden de term '*zogenaamde*' extremistische dreiging' (W.OCAD).

b) De Nationale Veiligheidsraad (NVR) en de voogdijministers

De Nationale Veiligheidsraad of de voogdijministers hebben geen elementen of specificeringen toegevoegd aan de terminologie die door de wetgever is gebruikt, noch wat betreft het algemene concept van extremisme, noch wat betreft de specifieke begrippen extreemrechts of rechtsextremisme.

c) De inlichtingendiensten en het Actieplan Radicalisme (Plan R)

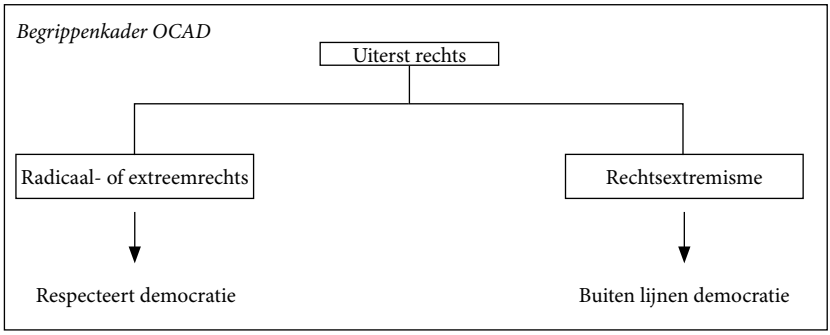
De VSSE noch de ADIV hebben een 'eigen' terminologie ontwikkeld met betrekking tot extreemrechts. Dit lijkt niet onlogisch: indien ze dit zouden hebben gedaan, zou het risico hebben bestaan dat ze buiten of boven de vigerende normen (in de eerste plaats de W.I&V) zouden zijn gegaan. Wel moet de aandacht gevestigd

[109] In art. 3, 15° W.I&V wordt het begrip 'radicaliseringsproces' gedefinieerd: *"een proces waarbij een individu of een groep van individuen op een dusdanige wijze wordt beïnvloed dat dit individu of deze groep van individuen mentaal gevormd wordt of bereid is tot het plegen van terroristische handelingen*". Ook in de memorie van toelichting bij de BIM-uitbreiding werd de term toegelicht: "*[…] een proces van de evolutie van een individu in een welbepaalde context, te weten een radicale. Op punt 0 van het proces begint het individu met het delen van radicale ideeën die haaks staan op de democratische waarden van onze samenleving. Dit stemt overeen met het extremisme, in de zin van de wet houdende regeling van de inlichtingen- en veiligheidsdiensten. Het individu is nog niet in het stadium van het stellen van terroristische handelingen, en zal dit misschien ook nooit bereiken. Het radicaliseringsproces dekt in feite de twee fenomenen van extremisme en terrorisme*".

worden op een belangrijk initiatief waarin 'extreemrechts' ook ter sprake komt: het Actieplan Radicalisme (Plan R)[110] dat in 2006 tot stand kwam en in 2015 werd geactualiseerd. Het Plan R biedt via de *National Task Force* en verschillende werkgroepen, platformen voor de verschillende partners om informatie en expertise uit te wisselen en aldus tot een zo correct mogelijke beeldvorming te komen van bedreigende fenomenen, om zo de impact van deze fenomenen te reduceren.

Binnen de 'Werkgroep Extreemrechts' van het Plan R werd gewerkt aan een studie waarvan de eerste doelstelling was om duidelijkheid trachten te scheppen in het begrippenkader.[111] Een tweede doelstelling was om duidelijkheid te verschaffen over wat nu precies de 'scope' zou moeten zijn van de diensten met betrekking tot de opvolging van extreemrechts of rechts-extremisme. Er wordt gewezen op de vaststelling dat de gebruikte terminologie met betrekking tot het fenomeen niet homogeen is en dat diverse concepten door elkaar worden gebruikt.

Het OCAD deed een voorstel om de termen 'radicaal rechts' of 'extreemrechts' te gebruiken voor actoren die de democratie respecteren, en de term 'rechts-extremistisch' voor zij wiens acties en opvattingen de democratische grenzen overschrijden.



De VSSE gaf echter aan het Comité te kennen dat de dienst het niet eens is met de door het OCAD voorgestelde terminologie, met name het onderscheid tussen extreemrechts en rechts-extremisme.

I.7.3.2. Kwantitatieve afbakening: de omvang van het fenomeen

Eens het voor de inlichtingendiensten duidelijk wordt dat een fenomeen zich manifesteert, is het van belang de grootte daarvan in te schatten. Op deze manier kan immers bepaald worden hoeveel middelen tegenover de dreiging in stelling moeten worden gebracht en met welke prioriteit.

110 https://www.besafe.be/sites/default/files/2019-06/plan_r_nl.pdf

111 COÖRDINATIEORGAAN VOOR DE DREIGINGSANALYSE, *'Beeldvorming rechts-extremisme'*, 14 februari 2020, 39 p. Het OCAD formuleert daarin vijf categorieën van beleidsaanbevelingen om de strijd tegen rechts-extremisme effectiever te maken.

Niettegenstaande er heel wat internationale gegevens beschikbaar zijn over gebeurtenissen en incidenten die met extreemrechts in verband worden gebracht, diende het Comité vast te stellen dat er in België een manifest gebrek is aan kwantitatieve gegevens over hoe groot de dreiging is die uitgaat van extreemrechts. Het Comité kreeg hierover geen duidelijke cijfers van beide inlichtingendiensten.

Het OCAD[112] liet optekenen dat er een grote mate van onderrapportering is van haatmisdrijven en rechts-extremistisch geïnspireerde incidenten. Deze worden niet altijd als dusdanig (h)erkend en geregistreerd door de veiligheidsdiensten. In tegenstelling tot in onder meer Duitsland, is het in België niet de gewoonte om bij PV's een speciale melding te maken van ideologische motieven bij bijv. geweldpleging. Dat maakt het moeilijk om het fenomeen te kwantificeren en *mutatis mutandis* om de volledige (juiste) informatie bij de inlichtingendiensten te krijgen. De effectieve omvang en evolutie van het fenomeen blijft hierdoor moeilijk in te schatten, waardoor het ook moeilijk wordt om te bepalen welke middelen dienen ingezet te worden.[113] [114]

I.7.4. DE DIENSTEN REORGANISEREN EN PLANNEN

I.7.4.1. Reorganisatie

In 2016 voerde de VSSE een interne hervorming door waarbij voor een aantal materies de secties van respectievelijk de binnen- (analyse) en buitendiensten werden samengevoegd tot één sectie. Zo ook voor de secties die werkten op ideologisch extremisme (extreemrechts en extreemlinks). In 2020 werd deze sectie versterkt met bijkomende medewerkers.

In januari 2020 trad er ook bij de ADIV een nieuwe structuur in voege. Als gevolg van deze reorganisatie werd een analyseplatform 'Non-Religious Ideological Threats' gecreëerd. Net zoals bij de VSSE, volgt dit platform zowel extreemrechts als extreemlinks op, terwijl er ook aan criminele motorbendes aandacht wordt

112 *Ibid.*

113 Ook in Frankrijk stelde een parlementaire commissie hetzelfde probleem van gebrek aan kwantificering vast : « La commisson ne dispose pas d'éléments permettant de chiffrer l'évolution des diverses infractions commises par les groupuscules (…) L'État n'effectue aucun suivi des infractions en fonction des motivations idéologiques de leurs auteurs. », « Rapport fait au nom de la commission d'enquête sur la lutte contre les groupuscules d'extrême droite en France », Assemblée Nationale, n°2006, 6 juin 2019.

114 Het is zaak om de vroege signalen op te pikken door onder andere politiediensten, parketten, lokale autoriteiten, hulpverleners. Een beter begrip van bepaalde symbolen, logo's en andere specifieke elementen van de rechtsextremistische cultuur door lokale autoriteiten, politie, sociale diensten … kan, aldus het OCAD, helpen om de problematiek in kaart te brengen. Ook deelnemers aan LTF's en LIVC's (Plan R) die tot nu toe voornamelijk gefocust waren op het islamistisch extremisme, hebben niet altijd voldoende kennis van het rechts-extremisme. Hiertoe blijkt bijkomende sensibilisering evenwel genoodzaakt.

besteed. Na de invoering van de nieuwe structuur werd het team dat ideologische extremisme behandelt, versterkt met een aantal medewerkers. Het ging hierbij wel grotendeels om stagiair-analisten die een zekere inlooptijd nodig hadden.

I.7.4.2. Planning en sturing

In het *Actieplan 2019-20* van de VSSE worden de strategische doelstellingen vertaald naar operationele doelstellingen. In dit plan worden 'extremisme en terrorisme' benoemd als één van de prioritaire materies. De klemtoon ligt daarbij op het detecteren van individuen en groepen die extremistisch gedrag steunen en/of verspreiden en op het minimaliseren van de impact van dergelijk gedrag. Daarbij gaat bijzondere aandacht naar propaganda die gewelddadige acties en het 'overgaan tot de daad' looft. Bijzondere aandacht wordt ook besteed aan individuen met rechtsextremistische opvattingen die tegelijkertijd een fascinatie voor wapens tentoonspreiden en/of hebben deelgenomen aan paramilitaire trainingen.

Het *Veiligheidsinlichtingen Stuurplan* bepaalt dan weer de elementen van het inlichtingen- en veiligheidsbeleid van de ADIV. Dit plan is bedoeld voor een periode van vijf jaar en heeft als doel de primaire en secundaire objectieven aan te duiden voor de *(counter)intelligence*-activiteiten van de ADIV. Het collecteren en analyseren van dreigingen uitgaande van extremistische, radicale en subversieve organisaties aangaande de belangen van Defensie, behoren tot de prioriteiten die zijn beschreven in dit stuurplan. Het *Intelligence Collection Plan (ICP)* vormt op zijn beurt de concrete uitwerking van de inlichtingenprioriteiten uit het stuurplan. Het gaat in essentie om indicatoren die behulpzaam zijn bij het beoordelen van gedragingen en uitingsvormen die in verband kunnen worden gebracht met rechts-extremisme. Dit ICP, dat de leidraad vormt voor de collectediensten, moet de ADIV toelaten om informatie te verzamelen over wie een uitgesproken extreemrechts gedachtengoed heeft, welke extreemrechtse groeperingen actief zijn binnen Defensie, of er actief wordt gerekruteerd binnen Defensie, of er een dreiging uitgaat vanuit extreemrechts tegen Defensie of zijn medewerkers, en of er incidenten vanuit een extreemrechts kader hebben plaatsgevonden.

I.7.5. GEGEVENS VERZAMELEN (COLLECTE) EN VERWERKEN

I.7.5.1. HUMINT

De exploitatie van menselijke bronnen (HUMINT) neemt voor de VSSE een zeer belangrijke plaats in met betrekking tot de collecte van informatie betreffende extreemrechts. In 2019 en 2020 werd een aanzienlijke inspanning geleverd met betrekking tot de rekrutering van menselijke bronnen. In de periode 2016-2018 lag de focus van de VSSE vooral op de bestrijding van (islamistisch) terrorisme. De

VSSE is van oordeel dat de informatiepositie van de dienst binnen het extreemrechtse milieu goed te noemen is, en dat de dienst daardoor in staat is om een correcte inschatting te kunnen maken van de dreiging. In de loop van 2019 en 2020 werden de collectediensten die de opvolging verzekeren van ideologisch extremisme versterkt, wat resulteerde in een aanzienlijke toename van het aantal informatierapporten.

In de loop van het onderzoek kon worden vastgesteld dat het aantal menselijke bronnen dat de ADIV informatie kan verschaffen over het rechts-extremistische milieu, zeer beperkt is. Ook het relatief beperkte aantal collecterapporten wees op een gebrek: er was maar een beperkte 'onafhankelijke' informatiepositie met betrekking tot extreemrechts, onafhankelijk van de traditionele militaire rapportering. De dienst kan moeilijk zelf gevallen van rechtsextremistische infiltratie binnen de strijdmacht detecteren.

I.7.5.2. SOCMINT

Met betrekking tot de concrete dreiging die uitgaat van rechts-extremisme, wordt de rol van individuen en zogenaamde '*lone actors*' alsmaar belangwekkender. Dergelijke individuen zijn echter moeilijk te detecteren omwille van hun isolatie en hun afwezigheid in de activiteiten van groeperingen. Vaak halen zij hun extremistische inspiratie op het Internet en zijn zij enkel via dit medium actief. De inzet van bijkomende *sociale media intelligence* (SOCMINT)-middelen om de online-activiteiten van (rechts-)extremisten op te volgen, wordt door de VSSE als zeer belangrijk aanzien.

Hoewel SOCMINT bij de ADIV een almaar groter belang krijgt bij de collecte, vormden de informatierapporten op basis van HUMINT de belangrijkste informatiebron. Het aantal rapporten dat de analysedienst bevoegd voor rechts-extremisme in 2019 ontving van de Cel SOCMINT, was niet veel. Deze cel stelt zijn rapporten steeds op na een bevraging door de analysediensten in de vorm van een *Request for Collect* (RFC) en gaat niet proactief te werk. De situatie op vlak van SOCMINT verbeterde in het najaar van 2020 gevoelig. In september 2020 werden een tiental rapporten opgesteld in verband met extreemrechts. De cel bevond zich op het ogenblik van de bevraging nog wel op slechts 50% van de voorziene capaciteit, en het ontbrak haar aan performante *software*.

I.7.5.3. Bijzondere inlichtingenmethoden (BIM)

Er werden in 2017, 2018 en 2019 respectievelijk 82, 52 en 62 bijzondere inlichtingenmethoden toegepast door de VSSE bij de opvolging van extreemrechts. De bijdrage van HUMINT voor de collecte van informatie over ideologisch extremisme was volgens de VSSE groter dan bij sommige andere door de dienst opgevolgde

dreigingen, waardoor het aantal BIM's relatief beperkter is dan in de context van andere dreigingen.

Door de ADIV werd er in de periode 2015-2019 slechts één bijzondere inlichtingenmethode toegepast bij de opvolging van extreemrechts (op een totaal van 216 methoden). Ook met betrekking tot de inzet van BIM's is er een stijging vast te stellen: in 2020 werden (tot september) vijf BIM's ingezet in verband met de problematiek van extreemrechts.

I.7.5.4. Verwerking van informatie

De gegevens over extreemrechts worden, net zoals deze over alle andere materies, door de VSSE in een centrale databank opgenomen.[115] In de loop van het onderzoek bleek het niet mogelijk om op een geautomatiseerde manier cijfergegevens op te vragen over de gevolgde materies. De dienst verklaarde dat de gegevens "*manueel uit de databank gefilterd*" moesten worden.

Bij de ADIV kon er (opnieuw) worden vastgesteld dat het tijdsverloop tussen het opstellen van een collecterapport en de exploitatie ervan door de analysedienst, gemiddeld zeer lang is. Dit was te wijten aan zowel de onderbemanning van de collectediensten, als aan de gebrekkige informatiedoorstroming binnen de ADIV. Bovendien kon ook worden vastgesteld dat de tijdige inbreng van informatie in de databanken een probleem vormt. Dit was het gevolg van een onvoldoende aantal documentalisten, waardoor ook analisten werden genoodzaakt zich te wijden aan het invoeren en ter beschikking stellen van de informatie in de databanken, wat ten koste ging van hun eigenlijke kerntaken.

I.7.6. ANALYSEREN EN VERSPREIDEN - SAMENWERKEN

I.7.6.1. Analyse door de inlichtingendiensten

In 2019 stelde de VSSE in vergelijking met de twee voorgaande jaren een gevoelige toename vast van het aantal inkomende en uitgaande berichten met betrekking tot extreemrechts. Deze toename gold voor de communicatie met zowel binnen- als buitenlandse partners. De VSSE beperkte zich de voorbije jaren grotendeels tot punctuele analyses betreffende bepaalde groeperingen en stromingen binnen de extreemrechtse scène, maar heeft geen algemene fenomeenanalyses op gesteld. Wel werden briefings gegeven aan bepaalde autoriteiten. Eerder stelde het Comité dat het produceren van voorspellende inlichtingen, scenario's en hypotheses tot de essentie van een inlichtingendienst behoort. De VSSE verklaarde echter niet

[115] De VSSE heeft op het ogenblik van het onderzoek een project lopende om deze centrale databank te vervangen door een nieuwe databank die meer mogelijkheden moet bieden.

over het nodige personeel te beschikken om voorspellende inlichtingen te kunnen produceren.

De VSSE maakt gebruik van een analysetool met een vijftigtal indicatoren op basis waarvan kan worden beoordeeld wat de mate van radicalisering is van een individu, of wat de mate van risico is dat dit individu zou kunnen overgaan tot extremistische geweldpleging. Dit instrument moet toelaten om meer gericht informatie te collecteren en beter de grootste dreigingen op te sporen. Het instrument werd in de loop van het onderzoek enkel toegepast op individuen die het voorwerp uitmaakten van onderzoekdossiers die gerelateerd waren aan islamistisch terrorisme en extremisme, en niet met betrekking tot ideologisch extremisme. Ontoereikende personeelscapaciteit maakte het niet mogelijk om het gebruik van dit instrument uit te rollen op bredere schaal.

De ADIV leverde een aantal cijfers voor 2019 over de werklast van het analyseplatform 'niet-religieuze ideologische dreigingen', en meer bepaald de analisten die extreemrechts behandelen. Het meest opvallende aan deze cijfers is het lage aantal *Requests for Collection* (RFC) dewelke de collecte van informatie aansturen. Volgens de medewerkers van het platform is de huidige personeelsbezetting ontoereikend om een voldoende opvolging van de materie te verzekeren. De analisten worden met te veel bijkomende taken belast (geven van briefings, bijwonen van vergaderingen, behandeling van veiligheidsverificaties…), waardoor zij te weinig tijd overhouden voor hun '*core business*', het analyseren van de hun toegewezen problematiek. Ze dienen zich wegens tijdsgebrek noodgedwongen reactief te richten op *ad hoc* dossiers van rechtsextremistische militairen die zij doorgespeeld krijgen van interne of externe partners. Het Comité kon vaststellen dat men niet toekwam aan het maken van eigen analyses over de eventuele evolutie van het fenomeen, specifiek binnen Defensie.

Het OCAD, pilootdienst van de Werkgroep Extreemrechts in het kader van het Plan R, maakt daarentegen wel algemene analyses op. Deze zijn, hun opdracht indachtig, in principe vooral 'dreigingsanalyses', maar kunnen ook als algemene fenomeenanalyses worden gecatalogeerd.[116] In die zin wordt de mogelijke lacune inzake fenomeenanalyses bij de beide inlichtingendiensten toch (gedeeltelijk) opgevuld.

I.7.6.2. Verspreiding en samenwerking

De VSSE deelt haar inlichtingen over extreemrechts met diverse partners. Op nationaal niveau is er samenwerking in de Werkgroep Extreemrechts (Plan Radicalisme). Sinds 2018 worden door de dienst ook bijkomende inspanningen geleverd op het vlak van sensibilisering en werden briefings gegeven aan journalisten, academici…

116 In uitvoering van artikel 8, 1° W. OCAD: "*een gemeenschappelijke evaluatie die moet toelaten te oordelen of de dreiging, bedoeld in artikel 3, zich kunnen voordoen of, indien ze al vastgesteld werden, hoe deze evolueren (…)*".

Ten slotte is er ook de *outreach* naar de samenleving in de vorm van sensibilisering van de verschillende maatschappelijke actoren. Met betrekking tot extreemrechts verklaart de dienst dat het tot op heden minder initiatieven heeft ontplooid op het vlak van sensibilisering dan in verband met bijv. islamisme.[117] Inzake internationale samenwerking is er, naast bilaterale samenwerking met vooral Europese partners, ook de samenwerking in het multilaterale platform Club van Bern.

Het analyseplatform van de ADIV stelde de voorbije jaren enkele strategische nota's op met betrekking tot extreemrechts die gericht waren aan de minister van Defensie. Uit het onderzoek blijkt dat de dienst zich echter vooral richt op punctuele inlichtingen die van operationele aard zijn. Er worden ook regelmatig briefings gegeven, onder andere in de Koninklijke Militaire School (KMS) voor de korpschefs van de eenheden en in de Inlichtingen- en Veiligheidsschool (IVS) voor S2-officieren van de verschillende operationele eenheden van de Krijgsmacht. Inzake internationale samenwerking kent de ADIV in verband met extreemrechts enkel een bilaterale samenwerking. Er bestaan rond deze materie geen multilaterale samenwerkingsplatformen. In 2019 had overleg over extreemrechts plaats met een viertal Europese partnerdiensten.

I.7.7. FEEDBACK

De VSSE krijgt zelden of nooit *feedback*, tenzij – wat de internationale partners betreft – eventueel een bijkomende vraag om inlichtingen, waaruit kan afgeleid worden dat de inlichtingen inderdaad interesse wekken. Hoewel er weinig informatie beschikbaar is over de specifieke *feedback* van externe partners over de opvolging door de dienst van extreemrechts, verwijst het Vast Comité I naar de algemene behoeftenbevraging dewelke de dienst uitvoerde tussen maart en juni 2019. Uit de bevraging kwam naar voor dat het werk van de VSSE door de externe partners van de dienst als overwegend positief wordt ervaren: veruit de meeste respondenten zijn van mening dat de medewerkers van de dienst professioneel en transparant (in de mate van het mogelijke) zijn, en dat er veel expertise aanwezig is binnen de dienst. Meestal is de indruk die verkregen wordt bij rechtstreeks contact met de dienst positiever dan het beeld dat vaak van de dienst wordt opgehangen in de media. De inhoud van de producten van de VSSE worden over het algemeen gewaardeerd, en de verstrekte inlichtingen worden als bruikbaar bestempeld. Hoewel veel klanten aangeven dat zij het moeilijk vinden om te bepalen of de VSSE dreigingen

---

117 Bijvoorbeeld salafisme, een thema waarover de VSSE een brochure publiceerde, dat breed verspreid werd bij het maatschappelijk middenveld en allerlei organisaties die met het fenomeen in aanraking komen. De VSSE wijst er zelf op dat bijvoorbeeld de Duitse inlichtingendienst BfV regelmatig communiceert over de dreiging van extreemrechts naar verschillende geledingen in de samenleving. Ook de Nederlandse dienst AIVD publiceerde in oktober 2018 een brochure getiteld *"Rechts-extremisme in Nederland, een fenomeen in beweging."*

tijdig detecteert, geven de meesten aan dat zij erin vertrouwen dat de dienst hier toe in staat is.

Vóór de invoering van de nieuwe structuur van de ADIV in januari 2020 werd enkel bij de producten van de vroegere Directie I *feedback* gevraagd. Vanaf de invoering van de nieuwe organisatiestructuur worden ook bijkomende inspanningen geleverd op dit vlak. Aan elk uitgaand product wordt een vraag om *feedback* van de partners toegevoegd. Er werd ook een dienst voor *quality control* in het leven geroepen die tot taak heeft – naast de kwaliteitscontrole van alle inlichtingenproducten – om een dialoog aan te gaan met de diverse partners met als doel de producten beter af te stemmen op de behoeften.

I.7.8. BESLUITEN

Bij de aanvang van het onderzoek onderscheidde het Comité een aantal risico's en bracht deze in verband met de inlichtingencyclus.

Het Vast Comité I deelt de mening van het OCAD dat de gebruikte terminologie met betrekking tot de bedreiging die uitgaat van extreemrechts niet homogeen gedefinieerd is en dat diverse concepten door elkaar worden gebruikt. Zelfs indien men kan stellen dat de wetgever wel degelijk een omschrijving heeft gegeven van het begrip 'extremisme', dan toch blijven de termen 'extreemrechts' of 'rechts-extremisme' (en derhalve ook 'linksextremisme') onbepaald. Ook de Nationale Veiligheidsraad of de bevoegde ministers geven ter zake geen richting aan.

Een tweede – desnoods parallelle stap – bestaat erin om de bedreiging kwantitatief af te bakenen en beleids- en beheersinformatie te verzamelen. Dergelijke gegevens laten toe om de evolutie van een bedreiging in te schatten, maar bieden de inlichtingendiensten ook de mogelijkheid om te bepalen waar zij welke middelen dienen in te zetten. Dergelijke informatie bij de uitvoering van het onderzoek niet in België of bij de twee diensten.

Wat de VSSE betreft, kon het Comité vaststellen dat de dienst na een terugval tijdens de terroristische crisis van 2015-2016, opnieuw heeft geïnvesteerd in het opvolgen van het ideologisch extremisme, waaronder extreemrechts valt. Er werd personeel toegewezen en er werden operationele en tactische doelstellingen bepaald. Het aantal bronnen (HUMINT) die informatie over extreemrechts aanbrachten, is in 2019-2020 verhoogd en er was sprake van een inhaalbeweging nadat deze materie tijdens de periode 2015-2016 (terroristische aanslagen) minder aandacht kreeg. Het gebrek aan een duidelijke omschrijving van de dreiging en van de hoegrootheid ervan, maakt het echter moeilijk om uit te maken of de ingezette middelen proportioneel zijn. Het Comité stelde ook vast dat de VSSE analyses uitvoert, maar dat deze vooral gericht zijn op het opsporen van mogelijke dreigingen van geweld door extreemrechtse middens. Algemene fenomeenanalyses, die tot hypotheses en scenario's en 'voorspellende inlichtingen' leiden, komen daardoor

ook zelden aan bod. Het Comité meent dat dit niettemin tot de essentie van een inlichtingendienst behoort.

Wat de ADIV betreft, is na een reorganisatie van begin 2020, een nieuw gemengd platform tot stand gekomen dat tot doel heeft om het (rechts)extremisme in de Krijgsmacht op te volgen. Er werd personeel toegekend en er werden objectieven gesteld. Er zijn echter wel aanwijzingen dat de (logistieke) ondersteuning onvoldoende is; dit blijkt uit de relatief lange doorlooptijd van sommige rapporten en een probleem bij het invoeren van gegevens in de databank. Daarenboven stelde het Comité vast dat de informatiepositie beperkt is. Bij de ADIV richten de analisten zich wegens tijdsgebrek reactief op *ad hoc* dossiers van rechts-extremistische militairen die zij krijgen van interne of externe partners. Zij voeren geen algemene fenomeenanalyses uit over extreemrechts bij Defensie. Niettemin lijkt dit noodzakelijk.

Het Vast Comité I acht het noodzakelijk dat de VSSE en de ADIV nauw samenwerken met betrekking tot de bedreiging van extreemrechts, en dat op regelmatige basis overleg en uitwisseling van inlichtingen zou plaatsvinden.

Tot slot stelde het Comité een gebrek aan *feedback* vast van de bestemmelingen van de inlichtingen van beide inlichtingendiensten. Dit gold evenzeer voor het beleidsniveau, waardoor het moeilijk wordt om de inlichtingendoelen te verfijnen of bij te sturen.

I.8. HET CORONAVIRUS EN DE BEVOEGDHEIDSKWESTIE VAN DE BELGISCHE INLICHTINGENDIENSTEN

I.8.1. AANZET

De enorme impact van het coronavirus en van de bestrijding ervan op het maatschappelijk, socio-economisch en persoonlijk leven zorg(d)en voor ongeziene tijden. De aard van de crisis had tot gevolg dat 'corona' geruime tijd de nationale en internationale agenda overheerste.

Bij elke crisis rijst de legitieme vraag of de gebeurtenissen vermeden hadden kunnen worden. Ook vragen naar de wijze van reactie op de crisis, meer bepaald naar het zorgvuldig karakter van het beheer ervan, vormen een vast onderdeel van de afhandeling van de gebeurtenissen.

In de nationale en internationale media verschenen diverse berichten over de (mogelijke) rol van inlichtingendiensten bij het voorkomen en bestrijden van pandemieën en van bepaalde aspecten en gevolgen van de coronacrisis in het bijzonder. Zo werd duidelijk gemaakt dat in sommige landen de inlichtingengemeenschap reeds jaren waarschuwen voor de dreiging die uitgaat van pandemieën. Dergelijke waarschuwingen gebeuren in de strategische toekomstverkenningen die

inlichtingendiensten ten dienste van hun regering maken en waar een antwoord wordt geformuleerd op de vraag welke trends op middellange en lange termijn een gevaar kunnen vormen voor de nationale veiligheid. Zo werd bijvoorbeeld in de VS reeds in 2004 gewaarschuwd voor het globale gevaar dat uitgaat van pandemieën.[118] Met betrekking tot de coronacrisis bleek uit de internationale berichtgeving ook dat sommige inlichtingendiensten belast worden met bepaalde aspecten van het ziektebeheer van de coronacrisis. In Israël bijvoorbeeld worden de digitale onderzoekers van de militaire inlichtingendienst, ter ondersteuning van de artsen en onderzoekers van het ministerie van Volksgezondheid, ingeschakeld om alle beschikbare informatie over het virus te verzamelen en ter beschikking te stellen van de regering, de gezondheidsautoriteiten en de defensieleiding. In andere landen verstrekken de inlichtingendiensten geen concrete medische informatie maar wel kennis en ervaring over het beheer van crisissen en nationale veiligheidsdreigingen. Zo werd in het Verenigd Koninkrijk een senior contra-terrorisme-functionaris tijdelijk aan het hoofd gezet van het net opgerichte *Joint Biosecurity Centre*, bevoegd voor het bepalen van het dreigingsniveau uitgaande van het coronavirus en voor de coördinatie van de aanpak ervan. Tot slot maken diverse nationale en internationale persartikels duidelijk dat inlichtingendiensten wereldwijd zich bezighouden met veiligheidsdreigingen die voortvloeien uit de gezondheidsdreiging 'coronavirus' (terrorisme, extremisme, propaganda en desinformatie, e.d.m.). Zo waarschuwde bijvoorbeeld de EU-contra-terrorismecoördinator bij de Europese Raad voor een globale veiligheidscrisis ten gevolge van de coronacrisis en de gevolgen ervan voor de werkzaamheden van de veiligheidsinstanties.[119]

I.8.2. HET CORONAVIRUS ALS BEDREIGING

Het sars-cov-2 is een virus behorende tot de familie van de coronavirussen. Bij de mens creëert dit een ziekte, genaamd covid-19. De hoge besmettelijkheidsgraad van dit coronavirus, het ontbreken van antistoffen bij de mens, de afwezigheid van een vaccin en het gedrag van de mens (hoge mobiliteit, sociale contacten, de helft van de wereldbevolking leeft en woont in steden) zou voor een snelle en omvangrijke verspreiding van het virus zorgen. De Wereldgezondheidsorganisatie kwalificeerde deze epidemie als een pandemie.

Het coronavirus vormt een duidelijke bedreiging voor de volksgezondheid, zowel op nationaal als op mondiaal niveau. Het schadelijk karakter doet zich niet

---

118 National Intelligence Council (NIC), *Mapping the Global Future. Report of the National Intelligence Council's 2020 Project*, December 2004. In de twee daaropvolgende toekomstverkenningen, nl. NIC Global Trends 2025 (publ.2008) en NIC Global Trends 2030 (publ.2012), werd een stijgende aandacht gegeven aan het gevaar dat uitgaat van een pandemie.

119 https://www.zeit.de/gesellschaft/zeitgeschehen/2020-05/terrorismus-coronavirus-extremismus-sicherheit-krise-eu

louter voor op gezondheidsvlak, maar ook op economisch, sociaal en psychologisch vlak.

I.8.3. DE VRAAG NAAR DE WERKZAAMHEDEN VAN DE BURGERLIJKE INLICHTINGENDIENST IN HET KADER VAN HET CORONAVIRUS

I.8.3.1. Het bevoegdheidsvraagstuk

Overeenkomstig de artikelen 7 en 8 W.I&V laat de bevoegdheid van de VSSE binnen de inlichtingenopdracht zich bepalen door de te beschermen belangen in combinatie met de te beheersen dreigingen. De vraag of de burgerlijke inlichtingendienst bevoegd is in een concreet geval, moet m.a.w. beantwoord worden door na te gaan of in dit concreet geval een aanknopingspunt te vinden is met minstens één belang[120] alsook met minstens één dreiging.[121] De dienst kan m.a.w. slechts gebeurtenissen, groeperingen of personen onderzoeken die mogelijks een gevaar uitmaken voor de vernoemde fundamentele belangen, wanneer dit onderzoek de detectie en opvolging beoogt van de wettelijke opgesomde dreigingen.[122] Dit zogenaamde doelbindingsprincipe is vastgelegd in artikel 13 W.I&V en artikel 75, 2° GBW.

De keuze van de wetgever voor een vaste lijst van veiligheidsdreigingen heeft tot gevolg dat de VSSE niet verantwoordelijk gesteld kan worden voor het niet, al dan niet ambtshalve, informeren van andere overheidsinstanties over gevaren die niet tot deze wettelijke lijst behoren. Het doelbindingsprincipe binnen de inlichtingenverstrekking verwoord in artikel 19, eerste lid W.I&V laat hierover geen twijfel

---

120 De te beschermen 'belangen' zijn: (a) de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, (b) de uitwendige veiligheid van de Staat en de internationale betrekkingen en (c) het wetenschappelijk en economisch potentieel van het land. Enkel deze belangen mogen door de VSSE beschermd worden. Belangrijk is dat de wetgever de regering wel de bevoegdheid heeft gegeven deze lijst via koninklijk besluit uit te breiden. Tot op heden werd hier geen gebruik van gemaakt. Gelet op de ruime wettelijke omschrijving van vernoemde belangen verbaast dit niet.

121 De te beheersen 'dreigingen' zijn: spionage, inmenging, extremisme, terrorisme, proliferatie, schadelijke sektarische organisaties en ten slotte criminele organisaties. Enkel deze gevaren mogen door de VSSE gedetecteerd en opgevolgd worden.

122 De memorie van toelichting bij de Wet van 30 maart 2017 verduidelijkt dat *"de finaliteit van de inlichtingenopdracht bestaat uit het identificeren en beheersen van fenomenen, groeperingen en personen die een bepaalde veiligheidsdreiging betekenen of zouden kunnen betekenen. Het gaat met andere woorden zowel over het detecteren, opvolgen en beheersen van potentiële dreigingen (of risico's), alsook over het opvolgen en beheersen van reeds gedetecteerde dreigingen (of gevaren)*." (*Parl. St.* Kamer 2015-2016, nr. 54-2043/001, 59). Bij de verwezenlijking van deze zgn. 'inlichtingenfinaliteit' dient de VSSE zich te bewegen binnen de wettelijke grenzen van de inlichtingenopdracht (art. 7, 1° W.I&V) en heeft de dienst uitsluitend de (onderzoeks)bevoegdheden ter beschikking die door de wetgever werden vastgelegd in de Inlichtingenwet van 30 november 1998.

bestaan. De VSSE heeft enkel de bevoegdheid om inlichtingen aan derden te verstrekken overeenkomstig de doelstelling van haar opdrachten. Lees: het detecteren, opvolgen en beheersen van de wettelijk opgesomde veiligheidsdreigingen.

Tot slot voorziet de Inlichtingenwet, in tegenstelling tot bij de fundamentele belangen, geen mogelijkheid om de lijst van de op te volgen dreigingen via koninklijk besluit uit te breiden. Indien de opdracht van de VSSE door het beleid niet als afdoende wordt ervaren, zal de Inlichtingenwet aangepast moeten worden.

I.8.3.2. Detectie en opvolging in het kader van het coronavirus

Op de door het Vast Comité I aan de VSSE gestelde vraag naar de eventuele bevoegdheden in het kader van het coronavirus antwoordde de administrateur-generaal van de VSSE:

> *"dat de enige juridische grondslag voor de werking van de VSSE i.h.k.v. de "Covid-19-pandemie" zich bevindt in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. Daarin staat immers vermeld dat het onze primaire opdracht is om inlichtingen in te winnen, te analyseren en te verwerken die betrekking hebben op elke activiteit die de inwendige veiligheid van de staat en het voortbestaan van de democratische orde, de uitwendige veiligheid van de staat en de internationale betrekkingen, het wetenschappelijk en economisch potentieel of elk ander fundamenteel belang van het land bedreigt of zou kunnen bedreigen. Wij dienen deze drie domeinen te beschermen tegen diverse bedreigingen (spionage, inmenging, terrorisme, extremisme, proliferatie, schadelijke sektarische organisaties en criminele organisaties). Dit is dan ook wat wij onverkort doen d.m.v. de nota's die wij overmaken aan de bevoegde politieke en administratieve overheden (…)".*

De VSSE staat in voor de bescherming van de *'inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde'*. Dit belang wordt, onder meer, omschreven als *'de veiligheid en de fysieke en morele vrijwaring van personen'* (art. 8, 2°, b W.I&V). Als landelijke epidemie brengt het coronavirus duidelijk de fysieke vrijwaring van de Belgen en de in België verblijvende vreemdelingen in gevaar.

Desondanks behoort de detectie en bestrijding van de gezondheidsdreiging 'coronavirus' niet tot de bevoegdheden van de VSSE. De burgerlijke inlichtingendienst is namelijk uitsluitend bevoegd voor de detectie van en het onderzoek naar de vernoemde zeven veiligheidsdreigingen. *Medical intelligence* (MEDINT), oftewel het inwinnen, analyseren en verspreiden van medische informatie die van belang is voor o.m. de politieke besluitvorming (meer diepgaande definitie, *infra*), valt buiten het bevoegdheidsbereik van de VSSE. De veiligheidsdreigingen waarvoor de VSSE bevoegd is, zijn overigens dreigingen met de mens als dreigingsbron.

Gezondheidsverschijnselen en, meer algemeen, natuurverschijnselen die een dreigingsbron vormen voor de vernoemde fundamentele belangen van het land, vallen als dreiging op zich niet binnen de wettelijke interessesfeer van de VSSE.

Anderzijds kan het inwinnen en analyseren van medische informatie wel tot de wettelijke interessesfeer van de VSSE behoren, doch slechts wanneer een onderzoek hiernaar gebeurt in het kader van de detectie van de wettelijke opgesomde veiligheidsdreigingen. De centrale vraag hier is dan in welke mate het medisch verschijnsel 'coronavirus' leidt tot extremisme, inmenging, e.d.m. Een folder[123], gezamenlijk uitgebracht door de VSSE en de ADIV, situeert zich binnen deze context. Ze focust zich op rechtsextremisme, linksextremisme, (potentiële) inmenging via pro-Russische berichtgeving en via desinformatie door buitenlandse mogendheden, en WEP-materies.

Tot slot dient vermeld te worden dat er binnen de medische gemeenschap consensus bestond dat er bij de verspreiding van het coronavirus geen schade verwekkend oogmerk in het geding was. Indien de VSSE evenwel, via open of gesloten bronnen, ernstige aanwijzingen had bekomen waaruit bleek dat het coronavirus wel als biologisch wapen wordt of werd aangewend, dan moest de verspreiding ervan gekwalificeerd worden als de proliferatie van CBRN-materiaal.[124] Dergelijke informatie zou de VSSE vatten tot een meer diepgaand onderzoek.

I.8.4. DE VRAAG NAAR DE WERKZAAMHEDEN VAN DE MILITAIRE INLICHTINGENDIENST IN HET KADER VAN HET CORONAVIRUS

I.8.4.1. Het bevoegdheidsvraagstuk

De inlichtingenopdracht van de ADIV wordt omschreven in artikel 11, §1, 1° W.I&V. Op grond van deze bepaling heeft de ADIV als taakstelling:

(1) het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die volgende belangen bedreigen of zou kunnen bedreigen:
   a. de onschendbaarheid van het nationaal grondgebied of de bevolking,
   b. de militaire defensieplannen,
   c. het WEP m.b.t. de actoren verbonden met defensie,
   d. de vervulling van de opdrachten van de strijdkrachten,
   e. de veiligheid van de Belgische onderdanen in het buitenland,
   en er de bevoegde ministers onverwijld over in te lichten.

---

123 Beide inlichtingendiensten brachten op 21 april 2020 de folder "Het verborgen gevaar achter covid-19"uit (https://vsse.be/nl/het-verborgen-gevaar-achter-covid-19).

124 CBRN-materiaal staat voor chemische, biologische, radiologische en nucleaire goederen en instrumenten.

Net zoals bij de VSSE laat het bevoegdheidsbereik van de ADIV binnen dit onderdeel van de inlichtingenopdracht zich bepalen door de te beschermen belangen in combinatie met de te beheersen dreigingen. De vraag of de militaire inlichtingendienst bevoegd is in een concreet geval moet m.a.w. ook hier beantwoord worden door na te gaan of er een aanknopingspunt te vinden is met minstens één belang alsook met minstens één dreiging.

Er bestaan echter ook verschillen met de bevoegdheidsomschrijving van de VSSE. Het belangrijkste verschil bestaat in de vereiste aanwezigheid van een militair aspect, 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.

Van betekenis voor voorliggende aangelegenheid is dat de dreigingen die tot de bevoegdheid van de ADIV behoren, net zoals bij de VSSE, de mens als dreigingsbron moeten hebben.[125] Dreigingsbronnen andere dan menselijke activiteiten, bijv. natuurverschijnselen, vallen slechts onder het bevoegdheidsbereik in de mate dat de opvolging hiervan leidt of kan leiden tot een dreiging voor bovenvermelde fundamentele belangen.

(2) 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, en er de bevoegde ministers onverwijld over in te lichten.

Dit onderdeel van de inlichtingenopdracht wordt aangeduid als de 'inlichtingensteun aan militaire operaties'. Het opzet ervan bestaat in het beschermen van de troepen en in het ondersteunen van de eigenlijke operaties via het verzamelen en verwerken van gegevens over vreemde mogendheden, vijandige of potentieel vijandige (elementen van) reguliere strijdkrachten, irregulier strijdende partijen en over gebieden en omstandigheden waarin wordt opgetreden of in de toekomst mogelijk moet worden opgetreden.

Het gaat over het identificeren en opvolgen van factoren die een veiligheidsrisico kunnen vormen voor lopende of (eventueel) toekomstige militaire operaties in het binnen- of buitenland en, desgevallend, de relevante informatie doorgeven aan de bevoegde militaire overheden en diensten. Hierbij kunnen de factoren die de (inter)nationale veiligheid (potentieel) beïnvloeden zowel menselijke activiteiten als niet-menselijke verschijnselen zijn. De ADIV heeft in dit kader echter geen taakstelling om ieder denkbaar risico actief op te sporen en te bestrijden. Zoals gezegd, bestaat het uiteindelijk doel van dit militair inlichtingenwerk in het beschermen van de troepen en in het ondersteunen van de eigenlijke operatie. Slechts

125 De artikelen 11, §2, 1° tot 4° W.I&V bevat telkenmale de zin "*elke uiting van het voornemen om*". Een dergelijk wilsuiting is enkel mogelijk bij de mens.

vanaf het ogenblik dat een activiteit, verschijnsel of geïdentificeerd risico mogelijks een gevaar kan inhouden voor een bepaalde militaire operatie of de erbij betrokken troepen, behoort het inwinnen en verwerken van relevante informatie tot de bevoegdheid van de ADIV.

De inlichtingensteun aan militaire operaties is geen exclusieve bevoegdheid van de ADIV. Binnen de Krijgsmacht oefenen ook de S2-instanties, de zgn. personen en diensten belast met het militaire functiegebied 'inlichtingen en veiligheid', eveneens een belangrijke rol binnen het ter zake vergaren en verwerken van relevante militaire inlichtingen. Daarnaast zijn er eveneens diverse overheidsinstanties binnen en buiten de Krijgsmacht belast met het actief verzamelen en bestuderen van specifieke informatie en risico's die, desgevallend, van betekenis kunnen zijn voor lopende of (eventueel) toekomstige militaire operaties.

I.8.4.2. De ruimere context: medical intelligence

De vraag stelde zich in welke mate *medical intelligence* (MEDINT of MEDINTEL) binnen het bevoegdheidsbereik van de ADIV valt. Om hierop een afdoende antwoord te kunnen formuleren, diende vooreerst de vraag beantwoord te worden wat exact onder deze activiteit valt.

De term *medical intelligence* is zowel in de Belgische inlichtingengemeenschap als in de Belgische defensie weinig gekend. Een internationale blik leert dat deze term (o.m.) omschreven wordt in de 'Glossary of terms and definitions' van het *NATO Standardization Office* (NSO):

> *"medical intelligence'* is *'(i)ntelligence derived from medical, bio-scientific, epidemiological, environmental and other information related to human or animal health. Note: This intelligence, being of a specific technical nature, requires medical expertise throughout its direction and processing within the intelligence cycle"*.[126]

Voor de NAVO-lidstaten vormt de MEDINT-functie m.a.w. een defensiefunctie.[127]

In sommige landen wordt de MEDINT-functie ingericht binnen een (de) militaire inlichtingen- en veiligheidsdienst. Een voorbeeld hiervan vormt de Verenigde

126 AAP-06, ed. 2019, NATO Glossary of terms and definitions.

127 Eveneens van betekenis is dat de NAVO hierover een specifieke cursus organiseert, zijnde de "M4-87 NATO Medical Intelligence Course (MEDINTEL)". De NAVO stelt hierover: *'(m)edical intelligence is a crucial element of medical support and has undergone considerable changes. NATO's concept of joint and multinational missions and NATO's ability to respond outside of traditional areas of operation (whenever and wherever) has added to a growing importance attached to (medical) force protection. This has led to increased demands for comprehensive, integrated, timely, and cohesive medical intelligence.'*

Staten waar deze activiteit wordt uitgeoefend door het *National Center for Medical Intelligence* (NCMI), onderdeel van het *Defense Intelligence Agency* (DIA).[128]

Wat voorligt is de vraag of *medical intelligence*, in het bijzonder of de detectie en opvolging van de gezondheidsdreiging 'coronavirus' en het vervolgens informeren van de bevoegde militaire overheden en diensten, binnen het bevoegdheidsbereik van de ADIV valt. Dit is een antwoord op een juridische vraag, zijnde of de ADIV wettelijk bevoegd is om dergelijke inlichtingenactiviteiten uit te oefenen.

Hiermee samenhangend is de vraag of andere onderdelen binnen de Belgische krijgsmacht belast kunnen worden met (een onderdeel van) de MEDINT-functie. Daarbij kan in de eerste plaats aan de medische component worden gedacht.

Het bevoegdheidsvraagstuk of *medical intelligence* daadwerkelijk ingericht 'kan' worden als ADIV-activiteit moet ook onderscheiden worden van de beleidsmatige vraag of het militaire functiegebied 'inlichtingen en veiligheid' ingericht moet worden binnen de medische component van defensie, of als dit beter – zoals bij de US DIA – een onderdeel vormt van een militaire inlichtingen- en veiligheidsdienst. Het Comité beperkte zich tot de studie van de bevoegdheidsreikwijdte van de ADIV.

I.8.4.3. Detectie en opvolging in het kader van het coronavirus

Op de door het Vast Comité I aan de ADIV gestelde vraag naar de eventuele bevoegdheden in het kader van het coronavirus, antwoordde de chef van de ADIV:

> *"(…) je peux vous dire que le SGRS n'est pas compétent pour « la détection et/ou le suivi de la pandémie proprement dite ».*
> *Si le SGRS est bien compétent pour faire du renseignement relatif à toute activité qui menace ou pourrait menacer les intérêts visés à l'article 11 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, il est néanmoins évident qu'il n'a pas de compétence en matière médicale et qu'il appartient à d'autres autorités publiques belges de détecter des pandémies et de suivre les conséquences directes des maladies sur la santé des citoyens.*
> *Dès lors, la compétence du SGRS se limite aux conséquences « indirectes » de la pandémie et du contexte qui l'entoure sur le potentiel économique et scientifique dans le secteur de la Défense, sur la sécurité des systèmes informatiques de la Défense, sur les plans et missions de la Défense, sur la sécurité des ressortissants*

---

128 De US Department of Defense (DoD) omschrijft medical intelligence als *'that category of* intelligence *resulting from collection, evaluation, analysis, and interpretation of foreign* medical, *bio-scientific, and* environmental *information that is of interest to* strategic planning *and to military medical planning and operations for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both* military *and* civilian *sectors.*' Zie: U.S. Department of Defense, feb. 15, 2013, Joint Publication 1-02, Department of Defense Dictionary of Military and Associates Terms.

belges à l'étranger, … et est orientée essentiellement sur les menaces de type espionnage, ingérence, extrémisme, … ".[129]

Zoals gesteld, richtte het Vast Comité I zich op het bevoegdheidsbereik van de inlichtingenopdracht van de ADIV, en dus niet op de beheersmatige inrichting van de inlichtingenactiviteiten, noch op de beleidsmatige prioriteiten erbinnen.

Net zoals de VSSE, heeft de ADIV geen bevoegdheid tot het actief opsporen en bestrijden van medische risico's die mogelijks een gevaar vormen voor de volksgezondheid. De ADIV is een militaire inlichtingen- en veiligheidsdienst, en heeft geen bevoegdheden binnen de ziektepreventie en -bestrijding. Net zoals de VSSE, heeft de ADIV wel een bevoegdheid binnen de beheersing van de gevolgen van het gezondheidsrisico, in de mate dat deze gevolgen zich situeren binnen het wettelijk bevoegdheidsdomein. De gezamenlijk met de VSSE uitgebrachte folder vormt hiervan een duidelijke illustratie.[130]

Covid-19 vormt niet enkel een bedreiging voor de volksgezondheid in België. Ook vormt het een bedreiging voor de volksgezondheid in het buitenland, waaronder in (potentiële) militaire conflictzones. *Medical intelligence* vindt in hoofdzaak haar bestaansreden in het inwinnen van informatie over het ziektebeeld bij de bevolking in een bestaand of potentieel toekomstig operatiegebied. Het gaat o.m. over het zoeken naar mogelijke ziekten en epidemieën die een invloed hebben of kunnen hebben op de aanwezige militairen, op de relatie van de militairen met de aanwezige bevolking, en op factoren die een invloed kunnen hebben op de buitenlandse missie. Vanuit wettelijk oogpunt valt *medical intelligence* niet binnen het bevoegdheidsbereik van de ADIV. De vraag in welke mate *medical intelligence* als volwaardig aandachtsgebied binnen de Krijgsmacht is ingericht of zou moeten worden ingericht, behoort niet tot de bevoegdheid van het Vast Comité I.

Tot slot dient ook bij een bespreking van de bevoegdheden van de ADIV vermeld te worden dat de verspreiding van het coronavirus niet wordt aanzien als een doelbewuste menselijke handeling. Ook hier geldt de opmerking dat indien de ADIV, via open of gesloten bronnen, ernstige aanwijzingen zou bekomen waaruit

---

129 *"(…) ik kan u zeggen dat de ADIV niet bevoegd is voor « de detectie en/of de opvolging van de eigenlijke pandemie ».*
Hoewel de ADIV bevoegd is voor de informatiegaring met betrekking tot elke activiteit die de belangen bedoeld in artikel 11 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten bedreigt of zou kunnen bedreigen, is het niettemin logisch dat de dienst geen bevoegdheid heeft binnen medische aangelegenheden en dat het detecteren van pandemieën en het opvolgen van de directe ziektegevolgen op de volksgezondheid toebehoort aan andere Belgische publieke autoriteiten.
Dientengevolge beperkt de bevoegdheid van de ADIV zich tot de indirecte gevolgen van de pandemie en omgevingscontext op het economisch en wetenschappelijk potentieel in de Defensiesector, op de veiligheid van informaticasystemen van Defensie, op de plannen en opdrachten van Defensie, op de veiligheid van Belgische onderdanen in het buitenland, … en is gericht op bedreigingen van het type spionage, inmenging, extremisme …". (vrije vertaling)

130 Zie in de zin ook de recente oprichting van het Information Warfare Platform door ADIV (i.s.m. de VSSE) dat de strijd wil aangaan tegen de verspreiding van desinformatie, ook rond covid-19.

blijkt dat het coronavirus als biologisch wapen wordt of werd ingezet, dit dus binnen het bevoegdheidsdomein van de ADIV zou vallen.

I.8.5. CONCLUSIE

Diverse en uiteenlopende maatregelen beogen de coronacrisis in al haar aspecten te beheersen. Ook inlichtingendiensten wereldwijd worden door hun regeringen ingeschakeld binnen het beheer van deze crisis. Traditioneel zijn deze categorie van overheidsinstanties actief binnen het opsporen en bestrijden van nationale veiligheidsdreigingen. De concrete invulling hiervan verschilt echter van land tot land. Internationale berichtgeving over de rol van inlichtingendiensten binnen de coronacrisis maakt duidelijk dat de taken van diverse inlichtingendiensten ter zake soms ruim uit elkaar liggen.

Op Belgisch niveau vormen de activiteiten van de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid een schakel binnen de indijking van en de strijd tegen bepaalde veiligheidsdreigingen die voortvloeien uit de huidige crisis. De Belgische inlichtingen- en veiligheidsdiensten worden hierbij gestuurd door de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

Krachtens de wet hebben de VSSE noch de ADIV een bevoegdheid binnen het actief opsporen en bestrijden van medische risico's die mogelijks een gevaar vormen voor de volksgezondheid. Het zijn inlichtingendiensten en ze hebben wettelijk geen rol te vervullen binnen de ziektepreventie en -bestrijding. *Medical intelligence* behoort niet tot het takenpakket van beide diensten.

Beide inlichtingendiensten hebben wel een taak te vervullen binnen de beheersing van bepaalde gevolgen van het gezondheidsrisico wanneer deze gevolgen zich situeren binnen het bevoegdheidsdomein van de diensten. De folder "Het verborgen gevaar achter covid-19" toonde duidelijk aan dat beide diensten hun wettelijk te vervullen rol zorgvuldig en proactief hebben ingevuld. Daarnaast toonde het aan dat de wet in dit kader voldoende duidelijk is en geen aanpassingen behoeft.

I.9. SOCIAAL OVERLEG IN DE SCHOOT VAN DE VEILIGHEID VAN DE STAAT

De Veiligheid van de Staat is samengesteld uit personeel van binnen- en buitendiensten. Historisch gezien bestaan er twee personeelsstatuten. Het koninklijk besluit van 2 oktober 1937 houdende het statuut van het rijkspersoneel regelt het statuut van het personeel van de binnendienst (*in casu* het personeel behorende tot de Directie van de Analyse, de Stafdirectie, de Staf van de Directie-generaal en de Directie van de Operaties). De agenten van de buitendiensten (*in casu* deze die

behoren tot de Directie van de Operaties, de Stafdirectie en de Staf van de Directiegeneraal) hebben een specifiek statuut dat wordt geregeld door het koninklijk besluit van 13 december 2006 betreffende het statuut van de ambtenaren van de buitendiensten van de Veiligheid van de Staat. Dit KB voorziet in een 'bijzonder' financieel statuut en in een systeem van toelagen, vergoedingen en bonussen.

De Regering, die het statuut van het personeel van de medewerkers van de Veiligheid van de Staat wenste aan te passen, legde daartoe een ontwerp van koninklijk besluit tot wijziging van het KB van 13 december 2006 voor sociaal overleg voor. Het voorstel (het zgn. KB 'kleine integratie') strekte tot de totstandbrenging van een convergentie van de personeelsstatuten van toepassing binnen de VSSE, meer in het bijzonder tot een gedeeltelijke integratie van de medewerkers van de binnendiensten in het administratief en geldelijk statuut van de medewerkers van de buitendiensten. Het betrof een eerste maatregel in het kader van een meer algemene hervorming binnen de VSSE en bij uitbreiding van de totstandkoming van een 'uniek statuut' zoals aanbevolen door de parlementaire onderzoekscommissie 'terroristische aanslagen'.[131]

Vakbondsafgevaardigden konden zich evenwel niet vinden in het voorstel en brachten daarvan de parlementaire Begeleidingscommissie alsook het Vast Comité I op de hoogte.

In overeenstemming met zijn organieke wet, bleef het Comité alert voor dit dossier in de mate waarin een sociaal conflict raakt aan de efficiëntie van de werking van de Veiligheid van de Staat. Het Comité zag zich evenwel niet bevoegd inzake sociale conflicten en was de mening toegedaan dat eventuele geschillen moeten worden beslecht in de onderhandelings- en overlegcomités en, indien nodig, door een sociaal bemiddelaar.[132]

Toch vond in augustus 2020 een vergadering plaats tussen het Vast Comité I en twee vertegenwoordigers van een vakbondsorganisatie, beiden lid van de buitendiensten van de Veiligheid van de Staat. Het Comité herinnerde hen aan de grenzen van zijn bevoegdheid op sociaal vlak, aan de geest van de Wet van 2004, en aan de noodzaak om de sociale dialoog te behouden met de autoriteiten, en, ten slotte, aan het belang om de goede werking van de Veiligheid van de Staat en de garantie van het welzijn van de werknemers. De Administrateur-generaal van de Veiligheid van de Staat werd, met de instemming van de vakorganisatie, op de hoogte gebracht van de ontmoeting.

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

---

131 Daartoe vond in augustus 2020 een vergadering plaats van het Onderhandelingscomité, waarbij de buitendiensten van de Veiligheid van de Staat, het OCAD en de kabinetten van Justitie en Defensie met elkaar in contact zijn om te werken aan een ontwerp van een uniek statuut.

132 Het is de Wet van 17 maart 2004 tot regeling van de betrekkingen tussen de overheid en de vakbonden van het personeel van de buitendiensten van de Veiligheid van de Staat die de regels voor de onderhandelingen en het overleg met de buitendiensten regelt. *B.S.* 2 april 2004, in voege getreden op 12 april 2004.

buitendiensten van de Veiligheid van de Staat, verscheen in het Belgisch Staatsblad op 1 oktober 2020. Het besluit trad in werking op 1 januari 2021.

I.10. INCIDENTEN IN EEN BUITENLANDSE OPERATIEZONE

Een belangrijk deel van het werk van de ADIV is gericht op de productie van inlichtingen over de politiek-militaire situatie in het buitenland. In 2018 bestudeerde het Comité de ontplooiing van de ADIV in een bepaalde[133] operatiezone.[134] De ADIV levert er steun aan de Belgische militaire commandanten ter plaatse en staat in voor de *force protection* van de Belgische militairen. De dienst voert eveneens ondersteunende opdrachten uit voor de Belgische ambassade en draagt bij tot de veiligheid van de expats. Tijdens zijn onderzoek detecteerde het Comité enkele kwetsbaarheden die een mogelijk risico inhielden voor de veiligheid van de operaties of het personeel.

Sedertdien ontving het Comité opnieuw informatie over een reeks ernstige incidenten die plaatsvonden en dewelke een risico betekenden op vlak van de veiligheid. Een geclassificeerd rapport werd geadresseerd aan de Chef ADIV, met de CHOD en minister van Defensie in kopie. Daarin werd de ADIV dringend uitgenodigd om maatregelen te nemen teneinde de ingezette manschappen te beschermen.

Het Comité betreurde te moeten vaststellen dat de veiligheidsincidenten enkel hadden geleid tot een procedure tot intrekking van een veiligheidsmachtiging en dat de dienst niet de minste tuchtprocedure inleidde. Verder moest het Comité vaststellen dat wanneer de ADIV geconfronteerd werd met een overtreding of een misdrijf van zijn medewerkers, artikel 29 Sv. niet werd toegepast en de strafbare feiten niet bij de gerechtelijke autoriteiten werden aangegeven. Er werd ten slotte opnieuw[135] herinnerd aan de noodzaak tot uitvoerige verslaggeving door de ADIV bij veiligheidsincidenten waarbij alle dimensies (niet alleen technisch, maar ook op vlak van het gedrag) moeten worden onderzocht en geanalyseerd.

---

133 Om veiligheidsredenen besloot het Comité om de locatie niet te vermelden.

134 VAST COMITÉ I, *Activiteitenrapport 2018*, 17-20 ('I.2. De activiteiten van de ADIV in een buitenlandse operatiezone').

135 VAST COMITÉ I, *Activiteitenrapport 2015*, 109 ('IX.2.8. Een uitvoerige verslaggeving bij veiligheidsincidenten').

I.11. TOEZICHTONDERZOEKEN WAAR IN DE LOOP VAN 2020 ONDERZOEKSDADEN WERDEN GESTELD EN ONDERZOEKEN DIE IN 2020 WERDEN OPGESTART

I.11.1. DE TOEPASSING VAN NIEUWE (BIJZONDERE) INLICHTINGENMETHODEN

Al in 2010 werden de mogelijkheden voor de ADIV en de VSSE om informatie te verzamelen, aanzienlijk uitgebreid. Sindsdien kunnen de diensten een beroep doen op gewone, specifieke en uitzonderlijke methoden, die een weerspiegeling zou zijn van de mate van intrusiviteit van de maatregelen.[136] Gelet op de tussengekomen wetswijzigingen, werd ondertussen de draagwijdte van een aantal methoden gewijzigd – lees verruimd –, werden sommige 'bijzondere' methoden 'gewone' methoden en werden nieuwe gewone methoden toegevoegd.

Derhalve kreeg ook het Comité een aantal controlemogelijkheden bij voor wat betreft sommige 'gewone' methoden, weliswaar voor omzeggens elke methode verschillend geregeld. Het betreft onder meer het toezicht op de identificatie van de gebruiker van telecommunicatie (art. 16/2 W.I&V), de toegang tot PNR-gegevens (art. 16/3 W.I&V), de toegang tot politionele camerabeelden (art. 16/4 W.I&V), of nog, de controle voorafgaand aan intercepties, intrusies in een informaticasysteem en de opname van bewegende beelden (art. 44/3 W.I&V).

Het Comité besliste om deze thematiek te bestuderen in zijn in 2019 geopende '*toezichtonderzoek naar de toepassing en de interne controle door de inlichtingendiensten naar de methoden en instrumenten de recent door de wetgever zijn ingevoerd of aangepast en waarbij het Vast Comité I een bijzondere toezichtsrol werd toebedeeld*'.

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). 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. Bij gebrek aan een uitvoeringsbesluit[137] kon de laatste nieuwe gewone observatiemethode, te weten het gebruik laten maken door inlichtingendiensten van politionele camerabeelden (art. 16/4 W.I&V), nog niet in werking treden.

---

136 Het Comité organiseerde naar aanleiding van het tienjarige bestaan van de zgn. BIM-Wet van 2010 een colloquium in de Kamer (*infra*). Hierover: J. VANDERBORGHT, (ed.), *Bijzondere inlichtingenmethoden in de schijnwerpers*, Antwerpen, Intersentia, 2020, 70 e.v..

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

I.11.2. INFORMATIE- EN COMMUNICATIETECHNOLOGIE IN HET inlichtingenproces bij de VSSE

In mei 2019 deelde het Vast Comité I aan de Kamervoorzitter de opstart van het 'Toezichtonderzoek betreffende de informaticamiddelen die de Belgische inlichtingendiensten gebruiken om informatie te verzamelen, te analyseren en te communiceren in het kader van de inlichtingencyclus' mee. De draagwijdte van het onderzoek werd bij de start duidelijk afgebakend. Het onderzoek spitst zich toe op de informaticamiddelen die specifiek worden gebruikt ter ondersteuning van de elementen van de inlichtingencyclus. Het onderzoek heeft tot doel de risico's te identificeren waarmee de diensten te maken krijgen en die risico's te verminderen door gepaste aanbevelingen te formuleren.

Een eerste module (ADIV) werd halfweg 2020 afgewerkt.[138] De resultaten van het onderzoek bij de VSSE worden ingewacht begin 2021.

I.11.3 DE OPVOLGING VAN VRIJGELATEN TERRO-VEROORDEELDEN DOOR DE VSSE

Belgische rechtbanken spraken de afgelopen vijf jaar (2015-2020) in totaal 464 veroordelingen uit voor feiten die verband hielden met terroristische activiteiten.[139] 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 uitgezeten of werden, na beslissing van de strafuitvoeringsrechtbank, voorwaardelijk vrijgelaten.

Gezien het 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. OCAD, het Directoraat-generaal Penitentiaire Inrichtingen, de Justitiehuizen, de lokale en de

---

138 Zie hierover 'I.6. Informatie- en communicatietechnologie in het inlichtingenproces bij de ADIV' (*supra*).

139 M. VANDERSMISSEN, *Knack*, 19 januari 2021 ('Belgische rechtbanken veroordeelden de voorbije vijf jaar 464 terroristen'). Bij de bijna 500 veroordelingen zijn er ook 200 jihadisten die zich nog in Syrië of Irak bevinden of bevonden. Het is niet duidelijk hoeveel van hen nog in leven zijn.

federale politie…) en binnen welke structuren (*Local Task Forces, Joint Intelligence and Decision Committees*…). Ten slotte wordt via *benchmarking* de Franse en Engelse manier van aanpak bestudeerd. Het onderzoek wordt gefinaliseerd in het eerste semester van 2021.

I.11.4. HET RISICO OP INFILTRATIE BIJ DE TWEE INLICHTINGENDIENSTEN

Afgelopen jaren werd de internationale inlichtingenwereld opgeschrikt door een aantal cases van infiltratie (en *insider threat*). Het Comité nam in 2019 het initiatief een toezichtonderzoek op te starten naar de wijze waarop de twee inlichtingendiensten met het risico op infiltratie omgaan: welke risico's worden onderkend, welke tegenmaatregelen worden genomen om ze te beheersen en om er op te reageren indien ze zich voordoen?

Er vonden diverse werkvergaderingen met de ADIV en de VSSE plaats over de thematiek 'cartografie en risico-evaluatie van infiltratie in de schoot van de inlichtingendiensten'. Het proces van risicomanagement zoals hernomen in de ISO 31000-norm vormde daarbij de vertrekbasis.[140] Het onderzoek wordt in de loop van 2021 gefinaliseerd.

I.11.5. MOGELIJKE DREIGINGEN VOOR HET BELGISCHE WETENSCHAPPELIJK EN ECONOMISCH POTENTIEEL: OPVOLGONDERZOEK

In 2016 werd een toezichtonderzoek afgerond naar de bescherming van het wetenschappelijk en economisch potentieel naar aanleiding van de zgn. 'Snowden-onthullingen'.[141] Deze onthullingen gaven een inkijk in onder meer het bestaan van het PRISM-programma waarbij de Amerikaanse 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

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

141 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'.

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.

I.11.6. SPIONAGE VIA GEMANIPULEERDE CODEERAPPARATRUUR: DE OPERATIE RUBICON

De 'Operatie Rubicon'[142] 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.[143] 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.

Een dag na de bekendmaking (12 februari 2020) reageerde de ADIV in een Belga-persbericht: *"De ADIV is op de hoogte van de Rubicon-affaire en onderzoekt momenteel de mogelijke omvang van de gemelde afluisterpraktijken", zo reageert de inlichtingendienst een dag later in een korte mededeling aan Belga. Daarin wordt niet expliciet aangegeven of België al dan niet geviseerd zou geweest zijn door de operatie, die eerst "Thesaurus" en later "Rubicon" werd genoemd. "Meer in het algemeen is de ADIV zich ten volle bewust van de vooruitgang, maar ook van de gevaren en/of potentiële misbruiken in verband met het gebruik van crypto hardware*", zo vervolgt de mededeling. De ADIV "*doet er alles aan om zich tegen hen te wapenen en maakt*

142 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'.

143 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')).

er vooral een erezaak van om enerzijds het wettelijk kader op dit gebied te respecteren en anderzijds een morele "code" te hanteren ten opzichte van zijn partners/bondgenoten in een wereld waar, zonder naïef te zijn, vertrouwen vaak met voorzichtigheid gepaard gaat".

Daarop besloot het Comité een toezichtonderzoek te openen, waarmee een antwoord werd gezocht naar vragen als[144]: in welke mate waren de Belgische inlichtingendiensten op de hoogte (of in welke mate dienden ze er – gezien hun wettelijke opdrachten – van op de hoogte te zijn? 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.11.5).

I.11.7. OFFENSIEVE INLICHTINGENMIDDELEN VOOR DE INLICHTINGENDIENSTEN?

Gelet op de door de wetgever omschreven inlichtingenopdracht bevinden de voor de inlichtingendiensten relevante informaties zich zowel in het binnen- als in het buitenland. In september 2019 werd daarom een toezichtonderzoek geopend 'naar de behoefte voor (bijkomende) inlichtingenmiddelen bij de Belgische inlichtingendiensten'. 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 mogelijkheden waaronder juridische mogelijkheden (m.a.w. onderzoeksbevoegdheden) om in het buitenland informatie te kunnen inwinnen.

Omwille van andere prioriteiten konden in 2020 nog geen concrete onderzoeksverrichtingen worden gesteld. Wel werden de onderzoeksbevoegdheden al geschetst die een extraterritoriale werking kunnen hebben. Deze studie vormt het juridische referentie- en toetsingskader wanneer het Comité, desgevallend, kon vaststellen dat beide diensten daadwerkelijk operationele inlichtingenactiviteiten ontwikkelen in het buitenland.

144 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?

I.11.8. OCAD EN DE ONDERSTEUNENDE DIENSTEN (OPVOLGING)

In juni 2020 rondde het Vast Comité I, gezamenlijk met het Vast Comité P, een toezichtonderzoek af naar de ondersteunende diensten van het Coördinatieorgaan voor de dreigingsanalyse (OCAD).[145] 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).[146] 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 een opvolgingsonderzoek opgestart. De resultaten hiervan werden in april 2021 voorgelegd aan de Begeleidingscommissie.

I.11.9. OCAD EN DE 'BIJKOMENDE' ONDERSTEUNENDE DIENSTEN

Zoals hierboven werd vermeld, kan het OCAD beroep doen op diverse zgn. 'ondersteunende diensten', te weten politie- en inlichtingendiensten, maar ook de Dienst Vreemdelingenzaken (FOD Binnenlandse Zaken), de FOD Buitenlandse Zaken, de FOD Mobiliteit en Vervoer, en de Administratie Douane en Accijnzen van de FOD Financiën.

Bij KB van 17 augustus 2018 werd deze 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 onderzoek 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

145 Cf. I.1. De ondersteunende diensten van het OCAD' (*supra*).

146 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').

zich op. Ook hiervan werden de resultaten ter bespreking voorgelegd aan de parlementaire Begeleidingscommissie in april 2021.

I.11.10. 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 bekloeg zich over het feit dat zijn werkgever informatie had opgevraagd over hem bij een inlichtingendienst en op basis daarvan disciplinaire stappen wou ondernemen.

Het Comité besloot in de loop van de behandeling van de klacht om vooreerst een juridische analyse te voeren 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. Daarenboven stelde zich de vraag in welke gevallen de betrokken inlichtingendienst hierop een antwoord mag of moet formuleren en aan welke vereisten dit antwoord vervolgens moet voldoen. Deze juridische analyse werd in het eerste trimester van 2021 besproken met de Begeleidingscommissie.

I.11.11. 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[147] 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

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

intern (binnen de diensten) als extern (Rekenhof, Vast Comité I...). Diverse aanbevelingen werden geformuleerd.

Sinds 2018 (VSSE) en 2020 (ADIV) uitte het Rekenhof het voornemen om eveneens een periodieke controle te doen van deze fondsen.[148] Daarbij kon het Rekenhof beroep doen op de technische ondersteuning zoals voorgeteld door het Vast Comité I.[149] 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.

I.11.12. TOEZICHT OP DE OPVOLGING VAN POLITIEKE MANDATARISSEN

Veelvuldig werd in (parlementaire) debatten[150] de vraag gesteld of en in welke mate de Belgische inlichtingendiensten politieke mandatarissen (mogen) opvolgen en welke regels ze daarbij in acht moeten nemen. Vanaf begin 2018 wordt in deze binnen de VSSE de als 'vertrouwelijk' geclassificeerde dienstnota van 13 december 2017 toegepast.[151] De VSSE zendt twee types van rapporten naar de minister van Justitie en de Premier, met kopie naar het Vast Comité I. Het betreft enerzijds punctuele rapporten over politieke mandatarissen die bijdragen aan de totstandkoming van een dreiging alsook een trimestrieel overzicht van het geheel van documenten waarin melding wordt gemaakt van deze mandatarissen.[152] De minister

---

148 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.

149 *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*".

150 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).

151 Om de rapportage ten aanzien van de directie inzake disruptieve activiteiten te verbeteren, werd de dienstnota in juni 2020 geactualiseerd. 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

152 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).

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*'.[153]

Gezien nergens wordt vermeld wat het Comité wordt geacht aan te vangen met voormelde informatie, nam het zelf het initiatief een methodologie uit te werken omtrent de 'problematiek van de opvolging van de politieke mandatarissen door de inlichtingendiensten en de rol van het Vast Comité I'. Deze methodologie werd in 2020 door de parlementaire Begeleidingscommissie goedgekeurd. In navolging van deze methodologie werd in 2020 een (periodiek) toezichtonderzoek opgestart.

153 *'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'.

HOOFDSTUK II

DE CONTROLE OP DE BIJZONDERE EN BEPAALDE GEWONE INLICHTINGENMETHODEN

In 2020 vierde de Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (gekend als de wet op de bijzondere inlichtingenmethoden, kortweg de BIM-Wet[154]) haar tiende verjaardag en dat verdiende de onverdeelde aandacht. Onder auspiciën van de Kamer van Volksvertegenwoordigers, organiseerde het Vast Comité I daartoe op 31 januari 2020 het colloquium 'Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulières de renseignement: de l'ombre à la lumière'.[155]

Met de inwerkingtreding van deze wet, dewelke ingrijpend werd gewijzigd bij Wet van 30 maart 2017 (de zogenaamde BIM-actualisatiewet)[156], werden de mogelijkheden voor beide inlichtingendiensten om informatie te verzamelen, aanzienlijk uitgebreid.

Toen de wetgever in 2010 eindelijk besloot de inlichtingendiensten nieuwe bevoegdheden te verlenen, werd ook een belangrijke taak toevertrouwd aan het Vast Comité I, dat samen met de BIM-Commissie moest gaan toezien op de uitvoering van deze BIM's, dewelke per definitie zeer ingrijpend zijn op het vlak van individuele rechten en vrijheden. Artikel 35 W.Toezicht verplicht het Comité tot transparantie in zijn werkzaamheden hierover.

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') en van de gewone methoden waarin aan het Comité een bijzondere controleopdracht wordt toegekend. Tevens wordt verslag gedaan over de wijze waarop het Vast Comité I zijn jurisdictionele

154 *BS* 10 maart 2010.

155 Waren daarbij vertegenwoordigd: de minister van Justitie, diverse Volksvertegenwoordigers, leden van de inlichtingen- en veiligheidsdiensten, academici, journalisten, mensenrechteninstellingen, de advocatuur, de gerechtelijke wereld, toezichthouders en internationale relaties. Hierover verscheen een verslagboek: J. VANDERBORGHT (ed.), *Bijzondere inlichtingenmethoden in de schijnwerpers*, Intersentia, Antwerpen, 2020, 151 p.

156 *BS* 28 april 2017.

controletaak op deze methoden heeft waargenomen. Naast een aantal cijfers over het aantal beslissingen en de wijze waarop het Comité werd gevat, wordt de essentie weergegeven van de jurisprudentie van het Vast Comité I. De rechtspraak werd ontdaan van operationele gegevens; alleen die elementen die van belang zijn voor het juridische vraagstuk, worden opgenomen.

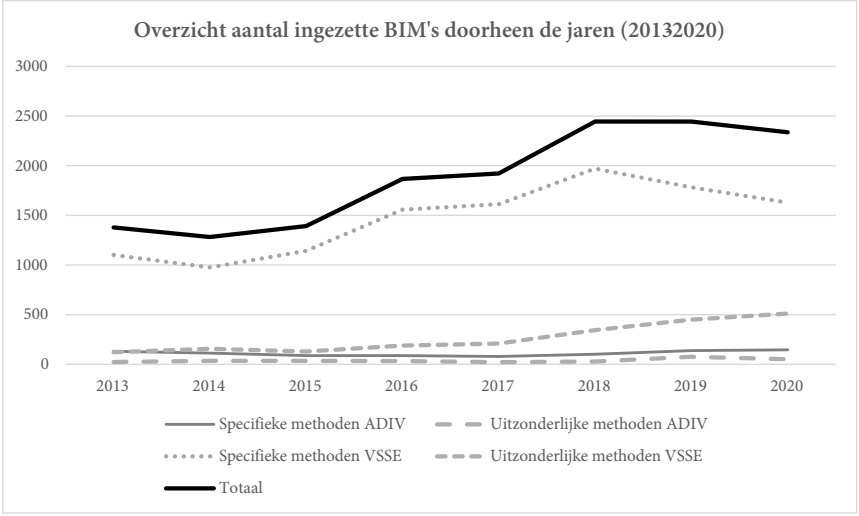
II.1. CIJFERS MET BETREKKING TOT DE BIJZONDERE EN BEPAALDE GEWONE METHODEN

Tussen 1 januari en 31 december 2020 werden door de twee inlichtingendiensten samen 2337 toelatingen verleend tot het aanwenden van bijzondere inlichtingenmethoden: 2140 door de VSSE (waarvan 1629 specifieke en 511 uitzonderlijke) en 197 door de ADIV (waarvan 146 specifieke en 51 uitzonderlijke). Naar luid van de BIM-verantwoordelijken van zowel de VSSE als de ADIV heeft de COVID-pandemie geen impact gehad op het aantal ingezette bijzondere inlichtingenmethoden.

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

Dit kan als volgt grafisch worden weergegeven:



Na een constante stijging van het aantal ingezette BIM's de afgelopen jaren en een stagnatie in 2019, kan voor het eerst een (te verwaarlozen) daling worden opgetekend: het totale aantal ingezette methoden bleef eerder stabiel in 2020. Let wel, per toegelaten methode kunnen wel meerdere targets (zoals personen, organisaties, plaatsen, voorwerpen, communicatiemiddelen…) worden geviseerd.

De VSSE blijft het leeuwendeel van de ingezette methoden voor zijn rekening nemen (91,5%).

Als deze cijfers evenwel worden uitgesplitst, wordt bij de ADIV de ingezette stijging van specifieke methoden (van 138 naar 146) voortduren. Het aantal ingezette uitzonderlijke methoden daalt evenwel sterk (een afname van circa één derde: van 76 naar 51).[157]

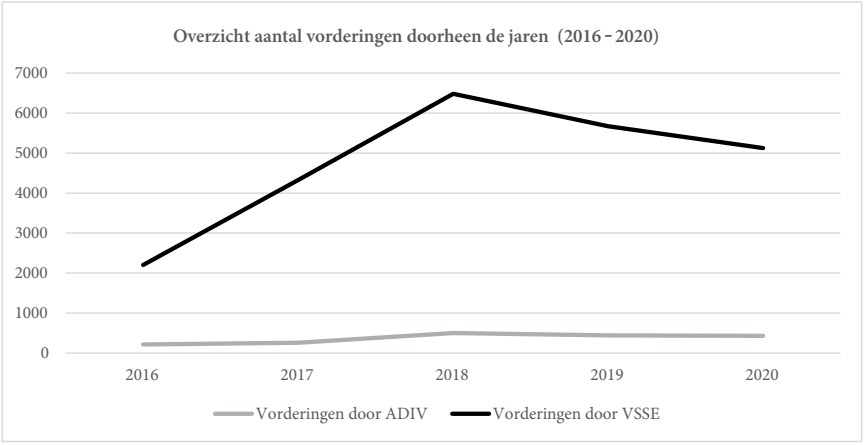
De VSSE laat het tegenovergestelde optekenen. Er wordt een opmerkelijke daling opgetekend van het aan ingezette specifieke methoden (van 1781 in 2019 naar 1629 in 2020), tegenover (opnieuw) een aanzienlijke stijging van het aantal ingezette uitzonderlijke methoden (van 449 in 2019 naar 511 in 2020 of een stijging met ca. 14%). Het Comité beperkt zich in deze tot de weergave van brute cijfergegevens.

157 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*).

Wat betreft de gewone methoden van vorderingen gericht aan de telecomoperatoren en -providers om bepaalde communicatiemiddelen te identificeren (*cf.* art. 16/2 W.I&V), wordt opnieuw een daling (ca. 10 % opgetekend (een tiental vorderingen minder bij de ADIV in vergelijking met 2019, tegenover meer dan 550 vorderingen minder door de VSSE).

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

In een grafiek weergegeven geeft dit volgend beeld:



Het Comité stelde reeds eerder[158] dat het "*niet om de vaststelling heen [kon] dat er sinds de invoering van de versoepelde procedure ex artikel 16/2 W.I&V veel meer identificaties worden verricht*". Hoewel het aantal vorderingen opnieuw afnam in 2020, blijft dit een vrij omvangrijk aantal. Vanuit zijn algemene toezichtsbevoegdheid onderzocht het Comité de redenen hiertoe; de resultaten werden opgenomen in zijn in 2019 geopende '*toezichtonderzoek naar de toepassing en de interne controle door de inlichtingendiensten naar de methoden en instrumenten die recent door de wetgever zijn ingevoerd of aangepast en waarbij het Vast Comité I een bijzondere toezichtsrol werd toebedeeld*' (cf. I.11.1).

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

II.1.1. METHODEN AANGEWEND DOOR DE ADIV

II.1.1.1. Gewone methoden 'plus'

Identificatie van de gebruiker van telecommunicatie

De identificatie van de gebruiker van telecommunicatie (bijv. gsm-nummer of IP-adres) of van een gebruikt communicatiemiddel wordt als een gewone methode beschouwd in de mate waarin dit gebeurt via een vordering aan telecomoperatoren of -providers of via een rechtstreekse toegang tot hun klantenbestanden.[159] 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.[160] Er werd ook bepaald dat het Comité maandelijks een lijst van de gevorderde identificaties en van elke toegang moet ontvangen. Voor wat betreft de ADIV, kende het aantal vorderingen in 2020 een lichte afname (van 442 in 2019 naar 433 in 2020). Deze thematiek vormde ook het voorwerp van het in 2019 geopende toezichtonderzoek (*supra*).

Identificatie van prepaid-kaarthouder

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.*' Net als in 2018 en 2019 werd hier door de beide inlichtingendiensten nog geen gebruik van gemaakt.

Toegang tot PNR-gegevens

Begin 2017[161] werd de mogelijkheid ingebouwd voor de inlichtingendiensten om toegang te krijgen tot informatie die berust bij de Passagiersinformatie-eenheid en dit bij wijze van gerichte opzoekingen (art. 16/3 W.I&V en art. 27 PNR-wet van 25 december 2016). Het Comité wordt in kennis gesteld van de aanwending van deze methode en kan ze desgevallend verbieden.[162]

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 daalde van 38 in 2019 naar 28 in 2020.

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).[163][164]

De cijfers

Gewone methoden (ADIV)	**Aantal toelatingen**
Identificatie van de gebruiker van telecommunicatie	433
Identificatie van prepaid-kaarthouder	0
Gerichte opzoekingen PNR-gegevens	28
Doorgifte PNR-gegevens o.b.v. hits	Niet aangeleverd
Gebruik van politionele camerabeelden	Niet in werking[165]

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

164 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).

165 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.1.1.2. De specifieke methoden

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

Specifieke methoden (ADIV)	**Aantal toelatingen**
Observeren in publiek toegankelijke plaatsen met een technisch middel of al dan niet met behulp van een technisch middel observeren in een niet voor het publiek toegankelijke plaats die niet aan het zicht onttrokken is (art. 18/4 W.I&V)[166]	6
Doorzoeken van publiek toegankelijke plaatsen met een technisch middel, de inhoud van vergrendelde voorwerpen doorzoeken of deze voorwerpen meenemen (art. 18/5 W.I&V)	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator (art. 18/6 W.I&V)	0
Vervoers- en reisgegevens vorderen van private vervoers- en reisdiensten (art. 18/6/1 W.I&V)	2
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
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
Opsporen van verkeersgegevens van elektronische communicatiemiddelen en het vorderen van de medewerking van een operator (art. 18/8, § 1, 1° W.I&V)	69
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
TOTAAL	146

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 (136 van de 146 ingezette specifieke methoden). De observatie in publiek toegankelijke plaatsen met een

166 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.

technisch middel, is met de helft afgenomen ten overstaan van 2019 (van 12 naar 6 in 2020).

II.1.1.3. De uitzonderlijke methoden

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

Uitzonderlijke methoden (ADIV)	Aantal toelatingen
Al dan niet met behulp van technische middelen, observeren in niet voor het publiek toegankelijke plaatsen die aan het zicht onttrokken zijn en betreden van al dan niet aan het zicht onttrokken niet voor het publiek toegankelijke plaatsen om te observeren, een technisch middel te installeren, een voorwerp te openen of mee te nemen (art. 18/11 W.I&V) [167]	2
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
Een rechtspersoon als bedoeld in art. 13/3 § 1 W.I&V inzetten om gegevens te verzamelen (art. 18/13 W.I&V)	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post (art. 18/14 W.I&V)	0
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen (art. 18/15 W.I&V)	6
Binnendringen in een informaticasysteem (art. 18/16 W.I&V)	4
Afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V)	39
TOTAAL	51

De procentueel sterke daling (meer dan 30 %) van het aantal door de ADIV ingezette uitzonderlijke methoden, situeert zich voornamelijk in het kader van het verzamelen van gegevens betreffende bankrekening en bankverrichtingen (art. 18/15 W.I&V): waar deze methode in 2019 nog 20 keer werd ingezet, is dit teruggeschroefd tot 6 keer. Ook het aantal keer dat werd binnengedrongen in een informaticasysteem (art. 18/16 W.I&V) nam met de helft af tegenover 2019 (van 8 naar 4).

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

II.1.1.4. De opdrachten en de dreigingen die de inzet van de gewone en bijzondere methoden rechtvaardigen[168]

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

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

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

4. **Het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied (art. 11, 5° W.I&V).**

Deze methoden kunnen dus niet ingezet worden in het kader van veiligheidsonderzoeken of andere door of krachtens bijzondere wetten aan de ADIV toevertrouwde opdrachten (bijv. het verrichten van veiligheidsverificaties voor kandidaat-militairen). Wel is de inzet van bijzondere methoden sinds de inwerkingtreding van de Wet van 30 maart 2017 niet meer beperkt tot het Belgische grondgebied (art. 18/1, 2° W.I&V).[169] De praktijk wijst uit dat per toelating verschillende dreigingen aan de orde kunnen zijn.

Zowat twee derden van de specifieke en uitzonderlijke methoden worden door de ADIV aangewend in het kader van de opdracht 'inwinnen, analyseren en verwerken van inlichtingen van activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied' (art. 11, 5° W.I&V). Toch mag hier niet uit worden afgeleid dat de ADIV sinds 2017 een 'nieuwe soort' dreiging opvolgt; de opvolging van buitenlandse diensten werd voorheen immers sneller aangeknoopt bij de 'inlichtingenopdracht' in het kader van de strijd tegen 'spionage'. Verder kan worden genoteerd dat het aantal ingezette BIM's voor wat betreft de dreigingen 'terrorisme' en 'extremisme' in belangrijkheid toenamen, ten nadele van 'inmenging', dat met de helft afnam.

AARD DREIGING	AANTAL 2020
Spionage	139
Inmenging	19
Extremisme	20
Terrorisme	19
Criminele organisatie	-
Andere	-
Totaal	197

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.[170] Dit gebeurde vooralsnog niet; het Comité herhaalt in dat kader dan ook zijn eerder geformuleerde aanbeveling.

169 Er werden in 2020 door de ADIV geen bijzondere inlichtingenmethoden ingezet in het buitenland.

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

II.1.2. METHODEN AANGEWEND DOOR DE VSSE

II.1.2.1. De gewone methoden 'plus'

Gewone methoden (VSSE)	Aantal toelatingen
Identificatie van de gebruiker van telecommunicatie	5123
Identificatie van prepaid-kaarthouder	0
Gerichte opzoekingen PNR-gegevens	30
Doorgifte PNR-gegevens o.b.v. hits	Niet aangeleverd
Gebruik van politionele camerabeelden	Niet in werking[171]

Zoals gezegd, zal het Comité de wijze waarop deze methode wordt ingezet, nader onderzoeken in zijn in 2019 opgestart toezichtonderzoek.

II.1.2.2. De specifieke methoden

Specifieke methoden (VSSE)	Aantal toelatingen
Observeren in publiek toegankelijke plaatsen met een technisch middel of al dan niet met behulp van een technisch middel observeren in een niet voor het publiek toegankelijke plaats die niet aan het zicht onttrokken is (art. 18/4 W.I&V)	245
Doorzoeken van publiek toegankelijke plaatsen met een technisch middel, de inhoud van vergrendelde voorwerpen doorzoeken of deze voorwerpen meenemen (art. 18/5 W.I&V)	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator (art. 18/6 W.I&V)	1
Vervoers- en reisgegevens vorderen van private vervoers- en reisdiensten (art. 18/6/1 W.I&V)	70
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
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
Opsporen van verkeersgegevens van elektronische communicatiemiddelen en het vorderen van de medewerking van een operator (art. 18/8, §1, 1° W.I&V)	650

171 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).

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
TOTAAL	1629

Zoals hierboven vermeld, nam de inzet van het aantal specifieke methoden in 2020 ten overstaan van 2019 duidelijk af (van 1781 naar 1629 methoden). Deze daling is gradueel vast te stellen bij zowat alle specifieke methoden, uitgezonderd evenwel het vorderen van vervoers- en reisgegevens van private vervoers- en reisdiensten, dat erg toenam (van 48 methoden in 2019 naar 70 in 2020).

II.1.2.3. De uitzonderlijke methoden

Uitzonderlijke methoden (VSSE)	**Aantal toelatingen**
Al dan niet met behulp van technische middelen, observeren in niet voor het publiek toegankelijke plaatsen die aan het zicht onttrokken zijn en betreden van al dan niet aan het zicht onttrokken niet voor het publiek toegankelijke plaatsen om te observeren, een technisch middel te installeren, een voorwerp te openen of mee te nemen (art. 18/11 W.I&V)	9
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
Een rechtspersoon als bedoeld in art. 13/3 § 1 W.I&V inzetten om gegevens te verzamelen (art. 18/13 W.I&V)	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post (art. 18/14 W.I&V)	11
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen (art. 18/15 W.I&V)	186
Binnendringen in een informaticasysteem (art. 18/16 W.I&V)	74
Afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V)	223
TOTAAL	511

In tegenstelling tot de inzet van specifieke methoden, nam het aantal door de VSSE ingezette uitzonderlijke methoden gestaag toe (+14% ten overstaan van 2019). Deze stijging is volledig te wijten aan een meer dan verdubbeling van de inzet van de methoden tot 'verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen' (art. 18/15 W.I&V) (van 95 in 2019 naar 186 in 2020) en het 'binnendringen in een informaticasysteem' (art. 18/16 W.I&V) (van 48 in 2019 naar 74 in 2020). Alle andere uitzonderlijke methoden werden minder ingezet ten overstaan van 2019.

II.1.2.4. De opdrachten en de dreigingen die de inzet van de gewone en bijzondere methoden rechtvaardigen

De volgende tabel toont in het kader van welke (potentiële) dreigingen de VSSE specifieke en uitzonderlijke toelatingen verleende. Uiteraard kan één methode gericht zijn tegen meerdere dreigingen. De VSSE kan de specifieke methoden aanwenden in het kader van alle dreigingen die tot haar bevoegdheid behoren (art. 8 W.I&V). De wet hanteert volgende definities:

1. Spionage: het opzoeken of het verstrekken van inlichtingen die voor het publiek niet toegankelijk zijn en het onderhouden van geheime verstandhoudingen die deze handelingen kunnen voorbereiden of vergemakkelijken;
2. Terrorisme: het gebruik van geweld tegen personen of materiële belangen om ideologische of politieke redenen met het doel zijn doelstellingen door middel van terreur, intimidatie of bedreigingen te bereiken;
   Radicaliseringproces: een proces waarbij een individu of een groep van individuen op dusdanige wijze wordt beïnvloed dat dit individu of deze groep van individuen mentaal gevormd wordt of bereid is tot het plegen van terroristische handelingen
3. Extremisme: racistische, xenofobe, anarchistische, nationalistische, autoritaire of totalitaire opvattingen of bedoelingen, ongeacht of ze van politieke, ideologische, confessionele of filosofische aard zijn, die theoretisch of in de praktijk strijdig zijn met de beginselen van de democratie of de mensenrechten, met de goede werking van de democratische instellingen of andere grondslagen van de rechtsstaat;
4. Proliferatie: de handel of de transacties betreffende materialen, producten, goederen of knowhow die kunnen bijdragen tot de productie of de ontwikkeling van non-conventionele of zeer geavanceerde wapensystemen. In dit verband worden onder meer bedoeld de ontwikkeling van nucleaire, chemische en biologische wapenprogramma's, de daaraan verbonden transmissiesystemen, alsook de personen, structuren of landen die daarbij betrokken zijn;
5. Schadelijke sektarische organisaties: elke groep met filosofische of religieuze inslag of die voorwendt dat te zijn en die qua organisatie of in haar praktijk schadelijke onwettige activiteiten uitoefent, individuen of de maatschappij nadeel berokkent of de menselijke waardigheid schendt;
6. Inmenging: de poging om met ongeoorloofde, bedrieglijke of clandestiene middelen beslissingsprocessen te beïnvloeden;
7. Criminele organisaties: iedere gestructureerde vereniging van meer dan twee personen die duurt in de tijd, met als oogmerk het in onderling overleg plegen van misdaden en wanbedrijven, om direct of indirect vermogensvoordelen te verkrijgen, waarbij gebruik gemaakt wordt van intimidatie, bedreiging, geweld, listige kunstgrepen of corruptie, of waarbij commerciële of andere structuren

worden aangewend om het plegen van misdrijven te verbergen of te vergemakkelijken. In dit kader worden bedoeld de vormen en structuren van de criminele organisaties die wezenlijk betrekking hebben op de activiteiten bedoeld in voorgaande dreigingen of die destabiliserende gevolgen kunnen hebben op het politieke of sociaaleconomische vlak.

Sinds de inwerkingtreding van de Wet van 30 maart 2017 mogen de bijzondere methoden ook worden ingezet '*vanaf het grondgebied van het Rijk*' en dus niet alleen meer '*op*' het grondgebied (art. 18/1, 1° W.I&V).

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

AARD DREIGING	AANTAL
Spionage	816
Inmenging	27
Extremisme	296
Proliferatie	3
Schadelijke sektarische organisaties	0
Terrorisme	998
Criminele organisaties	0
Activiteiten buitenlandse diensten in België opvolgen	(inbegrepen in bovenstaande cijfers)
TOTAAL	2140

Bovenstaande cijfers tonen aan dat 'terrorisme', wat betreft de inzet van BIM-methoden in 2020 weliswaar afneemt (van 1118 naar 998), maar toch de absolute prioriteit blijft voor van de VSSE en dit op de voet gevolgd door spionage (816). Net als bij de ADIV, kan ook bij de VSSE een sterke afname van het aantal 'inmengingsdossiers' worden vastgesteld (van 87 in 2019 naar 27 in 2020). Gezien schadelijke sektarische alsook criminele organisaties sinds 2015 niet meer het voorwerp uitmaken van actieve opvolging, hoeft het niet te verbazen dat deze dreigingen niet voorkomen in de cijfergegevens.

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

1. De inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde zijnde,
   a) de veiligheid van de instellingen van de Staat en het vrijwaren van de continuïteit van de regelmatige werking van de rechtsstaat, de democratische instellingen, de elementaire beginselen die eigen zijn aan iedere rechtsstaat, alsook de mensenrechten en de fundamentele vrijheden;
   b) de veiligheid en de fysieke en morele vrijwaring van personen en de veiligheid en de vrijwaring van goederen

2. De uitwendige veiligheid van de Staat en de internationale betrekkingen: het vrijwaren van de onschendbaarheid van het nationaal grondgebied, van de soevereiniteit en de onafhankelijkheid van de Staat, van de belangen van de landen waarmee België gemeenschappelijke doeleinden nastreeft, alsook van de internationale en andere betrekkingen die België met vreemde Staten en internationale of supranationale instellingen onderhoudt;
3. De vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel.

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

Zoals gezegd, beschikt het Comité niet over de cijfers met betrekking tot de geviseerde dreiging en de te verdedigen belangen wat betreft de in dit hoofdstuk bedoelde gewone methoden.

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

II.2.1. CONTROLE OP BEPAALDE GEWONE METHODEN

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.[172] 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.'*

[172] VAST COMITÉ I, *Activiteitenverslag 2017*, 25 voetnoot 40.

Wat betreft de toegang tot PNR-gegevens die berusten bij de Passagiersinformatie-eenheid, bepaalt artikel 16/3 W.I&V dat die toegang alleen kan na beslissing van het diensthoofd en '*mits afdoende motivering*'. Het Comité moet hiervan in kennis worden gesteld en '*verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen*'. In 2020 werd door het Comité één dergelijk verbod uitgesproken (*infra*).

Ten slotte werden aan het Comité bijzondere controlemodaliteiten toegekend in het kader van de mogelijkheid voor de inlichtingendiensten om toegang te krijgen tot informatie afkomstig van politionele camerabeelden (artikel 16/4 W.I&V): een *a priori*-controle[173] en een *a posteriori*-controle.[174]

II.2.1.2. De corrigerende beslissingen

Hieronder wordt de essentie weergegeven van de corrigerende beslissingen die het Vast Comité I in 2020 nam binnen zijn controle op de aanwending van de vernoemde gewone inlichtingenmethoden.

Wat betreft de VSSE gaven twee gevallen aanleiding tot een beslissing om bijkomende informatie te verzoeken en werd geen exploitatieverbod uitgesproken. Wat betreft de ADIV daarentegen werden in dat kader in 2020 vier beslissingen genomen: in drie gevallen werd om bijkomende informatie verzocht; eenmaal werd overgegaan tot een beslissing tot exploitatieverbod. Wat dat laatste betreft, doet het Vast Comité I opmerken dat artikel 16/3 inderdaad hierover spreekt, maar dat een exploitatieverbod zonder vernietigingsbevel weinig zin heeft. Een vernietigingsbevel is evenwel altijd mogelijk op grond van de Gegevensbeschermingswet. Een combinatie van artikel 16/ W.I&V en artikel 51/3 W.Toezicht lijkt bijgevolg aangewezen.

---

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

174 *'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.*'

II.2.2. CONTROLE OP BIJZONDERE METHODEN

II.2.2.1. De cijfers

In dit onderdeel wordt ingegaan op de activiteiten van het Vast Comité I met betrekking tot de specifieke en uitzonderlijke inlichtingenmethoden. Daarbij zal uitsluitend aandacht besteed worden aan de ter zake genomen jurisdictionele beslissingen en niet aan de operationele gegevens. Vooraf dient evenwel te worden onderlijnd dat het Comité *alle* toelatingen tot de inzet van bijzondere methoden aan een *prima facie*-onderzoek onderwerpt, en dit met het oog op de al dan niet vatting. Tevens woont een lid van de Dienst Enquêtes de (tweewekelijkse) vergaderingen bij waarop de betrokken inlichtingendienst de BIM-Commissie inlicht over de uitvoering van de uitzonderlijke methoden. Hierover wordt een verslag opgemaakt ten behoeve van het Vast Comité I, dat op deze wijze een beter zicht heeft op deze methoden.[175]

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

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

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

[175] Het Comité beval in 2017 de ADIV aan ook dergelijke tweewekelijkse vergaderingen te organiseren. Het betreft immers een wettelijke verplichting (art. 18/10 §1, derde lid, W.I&V en art. 9 KB 12 oktober 2010). Sinds eind januari 2018 wordt – gezien het geringe aantal ingezette BIM-methoden – maandelijks vergaderd, en (in principe) tweewekelijks gerapporteerd.

WIJZE VAN VATTING	2013	2014	2015	2016	2017	2018	2019	2020
1. Op eigen initiatief	16	12	16	3	1	1	4	2
2. Gegevensbeschermingsautoriteit	0	0	0	0	0	0	0	0
3. Klacht	0	0	0	1	0	0	0	0
4. Exploitatieverbod door BIM-Commissie176	5	5	11	19	15	10	12	9
5. Toelating minister	2	1	0	0	0	0	0	0
6. Prejudicieel adviesverlener	0	0	0	0	0	0	0	0
TOTAAL	23	18	27	23	16	11	16	11

Het aantal door het Comité genomen beslissingen blijft dalen. Bovendien zijn – op twee na – alle vattingen het gevolg van een schorsing door de BIM-Commissie.

Eens gevat, kan het Comité verschillende soorten (tussen)beslissingen nemen.

1. Nietigheid van de klacht wegens vormgebrek of afwezigheid van een persoonlijk en rechtmatig belang (art. 43/4, eerste lid, W.I&V);
2. Beslissing om geen gevolg te geven aan een klacht die kennelijk niet gegrond is (art. 43/4, eerste lid, W.I&V);
3. Schorsing van de betwiste methode in afwachting van een definitieve beslissing (art. 43/4, laatste lid, W.I&V);
4. Vordering tot bijkomende informatie ten aanzien van de BIM-Commissie (43/5 § 1, eerste tot derde lid, W.I&V);
5. Vordering tot bijkomende informatie ten aanzien van de betrokken inlichtingendienst (43/5 § 1, derde lid, W.I&V);
6. Onderzoeksopdracht voor de Dienst Enquêtes I (art. 43/5 § 2 W.I&V). In deze rubriek wordt zowel verwezen naar de veelvuldige bijkomende informatie die door de Dienst Enquêtes I op eerder informele wijze wordt ingewonnen vóór de eigenlijke vatting als naar informatie die op verzoek van het Comité wordt ingewonnen na de vatting;
7. Horen van de BIM-Commissieleden (art. 43/5 § 4, eerste lid, W.I&V);
8. Horen van het diensthoofd of de leden van de betrokken inlichtingendienst (art. 43/5 § 4, eerste lid, W.I&V);
9. Beslissing over geheimen die betrekking hebben op een lopend opsporings- of gerechtelijk onderzoek waarvan de leden van de inlichtingendiensten drager zijn, na overleg met de bevoegde magistraat (art. 43/5 § 4, tweede lid, W.I&V);
10. Uitspraak door de voorzitter van het Vast Comité I, na het diensthoofd te hebben gehoord, indien het lid van de inlichtingendienst meent het geheim waarvan hij drager is te moeten bewaren omdat de onthulling ervan nadelig

176 Ze vloeien voort uit opnameproblemen of bij de verwijdering van apparatuur.

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
Beslissingen voorafgaand aan de vatting							
1. Nietige klacht	0	0	0	0	0	0	0
2. Kennelijk ongegronde klacht	0	0	0	0	0	0	0
Tussenbeslissingen							
3. Schorsing methode	3	2	1	0	0	0	1
4. Bijkomende informatie van BIM-Commissie	0	0	0	0	0	0	0
5. Bijkomende informatie van inlichtingendienst	1	1	4	0	0	0	1
6. Onderzoeksopdracht Dienst Enquêtes[177]	54	48	60	35	52	52	24
7. Horen BIM-Commissieleden	0	2	0	0	0	0	0
8. Horen leden inlichtingendiensten	0	2	0	0	0	1	1
9. Beslissing m.b.t. geheim van onderzoek	0	0	0	0	0	0	0
10. Gevoelige informatie tijdens verhoor	0	0	0	0	0	0	0
Eindbeslissingen							
11. Stopzetting methode	3	3	6	9	4	11	10

[177] 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
12. Gedeeltelijke stopzetting methode	10	13	4	6	6	4	0
13. (Gedeeltelijke) opheffing verbod van BIM-Commissie	0	4	11	0	0	0	0
14. Onbevoegd	0	0	0	0	0	0	0
15. Wettige toelating / Geen stopzetting methode / Ongegrond	4	6	2	1	1	0	0
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 2020 nam binnen zijn jurisdictionele controle op de aanwending van de bijzondere inlichtingenmethoden.[178] 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 drie 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.

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

Prejudiciële vraag aan het grondwettelijk hof

Het Vast Comité I heeft in 2020 voor het eerst sinds de inwerkingtreding van de BIM-Wet van 4 februari 2010 een prejudiciële vraag gesteld aan het Grondwettelijk Hof aangaande de BIM-wetgeving (dossier2020/9606).[179] De aanleiding hiervoor bestond in de beslissing van een inlichtingendienst om de in artikel 18/8, §1, 1° en 2° W.I&V bedoelde specifieke methoden aan te wenden tegenover een arts. Meer in het bijzonder bestond de toelating van het betrokken diensthoofd enerzijds in het opsporen van de verkeersgegevens van een elektronisch communicatiemiddel

178 In sommige dossiers werd het Comité gevat in 2019, maar werd een eindbeslissing genomen in 2020.

179 Eerder sprak het Grondwettelijk Hof zich over deze wetgeving in twee vernietigingsarresten uit (nr. 145/2011 en nr. 41/2019).

van waaruit of waarnaar elektronische communicaties worden of werden gedaan en anderzijds in het lokaliseren van de oorsprong of de bestemming van elektronische communicaties. Deze methode diende te worden uitgevoerd tegenover een door de betrokken arts gebruikt telefoonnummer, en dit gedurende een periode van vier maanden voorafgaand aan de beslissing van het diensthoofd alsook gedurende twee maanden te rekening vanaf de kennisgeving van de beslissing aan de BIM-Commissie. Via een gewone methode bleek het geviseerde telefoonnummer enkel op naam van de betrokken arts in België te zijn geregistreerd. Hoewel de inlichtingendienst de hoedanigheid van arts in hoofde van betrokkene niet betwiste, volgde de inlichtingendienst de gewone toelatingsprocedure voor specifieke methoden. Het diensthoofd nam zodoende een 'beslissing' en bracht die vervolgens (*i.c.* dezelfde dag) ter kennis van de BIM-Commissie. Reeds de daaropvolgende dag beval de Commissie om de betrokken methode, wegens haar onwettig karakter, te schorsen.

Volgens de Commissie was verkeerdelijk gebruik gemaakt van de gewone procedure voor specifieke methoden. Gelet op de hoedanigheid van de geviseerde persoon, zijnde arts, moest volgens de Commissie namelijk gebruik gemaakt worden van de in artikel 18/3, §5 W.I&V bepaalde procedure, zijnde dat *'(d)e specifieke methoden (…) slechts (kunnen) 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 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 erop neer dat wanneer een inlichtingendienst een specifieke methode wenst aan te wenden jegens bepaalde beschermde beroepscategorieën de procedure bij uitzonderlijke methoden dient gevolgd te worden, en dat zodoende elke methode voor zijn aanwending onderworpen wordt aan een voorafgaande controle van de BIM-Commissie. Volgens de Commissie is dit ook vereist om tegemoet te kunnen komen aan de procedure in artikel 18/2, §3 W.I&V dat voorschrijft dat als een in specifieke of uitzonderlijke methode *'aangewend wordt ten opzichte van een advocaat, een arts of een journalist, of van hun lokalen of communicatiemiddelen die zij voor beroepsdoeleinden gebruiken, of van hun woonplaats of verblijfplaats, (…) deze methode niet (mag) uitgevoerd worden zonder dat, naargelang het geval, de voorzitter van de Orde van de Vlaamse balies, van de Ordre des barreaux francophones et germanophone, van de Nationale Raad van de Orde van Geneesheren of van de Vereniging van Beroepsjournalisten of in geval van ziekte of verhindering van de voorzitter diens plaatsvervanger hiervan vooraf op de hoogte is gebracht door de voorzitter van de commissie bedoeld in artikel 3, 6°. De voorzitter van de commissie is verplicht om de nodige inlichtingen te verstrekken aan de voorzitter van de Orde of van de Vereniging van Beroepsjournalisten, waarvan de advocaat,*

de arts of de journalist deel uitmaakt of aan de plaatsvervanger van de voorzitter. De betrokken voorzitter en zijn plaatsvervanger zijn tot geheimhouding verplicht. (…).' Als een specifieke of uitzonderlijke methode *'aangewend wordt ten opzichte van een advocaat, een arts of een journalist, van hun lokalen of communicatiemiddelen die zij voor beroepsdoeleinden gebruiken, of van hun woonplaats of verblijfplaats, gaat de voorzitter van de commissie na of de via deze methode verkregen gegevens een rechtstreeks verband hebben met de potentiële dreiging, wanneer zij beschermd worden door het beroepsgeheim van een advocaat of arts of door het bronnengeheim van een journalist. Zo geen rechtstreeks verband is aangetoond, verbiedt de Commissie de inlichtingen- en veiligheidsdiensten deze gegevens te exploiteren.'* Naast de schorsing van de betrokken methode, legde de BIM-Commissie een exploitatieverbod op voor de, desgevallend, reeds verkregen gegevens. Daarnaast beval de Commissie eveneens in een tijdelijke specifieke bewaring ervan.

Krachtens artikel 43/4 W.I&V is het Vast Comité I van rechtswege gevat telkens als de commissie een specifieke of een uitzonderlijke methode wegens onwettigheid heeft geschorst en de exploitatie van de gegevens heeft verboden wegens wederrechtelijkheid van een specifieke of uitzonderlijke methode. Gelet op het belang van het bijzondere beschermingsregime van vernoemde beroepscategorieën en vanuit zijn hoedanigheid van rechtsprekend orgaan[180] binnen het toezicht op de specifieke en uitzonderlijke methoden aangewend door de inlichtingendiensten besloot het Comité om een prejudiciële vraag te stellen aan het Grondwettelijk Hof. Deze vraag was als volgt gemotiveerd: *'Le Comité permanent R relève que le prescrit de l'article 18/2, § 3, alinéas 1 & 2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) restreint la protection accordée aux avocats, médecins et journalistes par rapport aux moyens de communication qu'ils utilisent à des fins professionnelles. Il en découlerait du texte actuel que les moyens de communication à des fins non professionnelles ne seraient pas couverts par la protection légale. Le Comité permanent R se pose la question de savoir comment les services de renseignement peuvent-ils, préalablement, s'assurer de la finalité, professionnelle ou non professionnelle, du moyen de communication concerné (téléphone, GSM…). Est-il possible, a priori, de déterminer dans l'historique des appels téléphoniques d'un avocat, médecin ou journaliste, qu'un numéro présente un caractère exclusivement professionnel. Le législateur n'a pas procédé à cette distinction dans la procédure pénale et plus particulièrement dans les articles 90ter à 90decies du Code d'instruction criminelle. Le législateur a déterminé les conditions strictes auxquelles les services de renseignement, sous le contrôle préalable de la commission BIM, peuvent légalement prendre connaissance des communications conformément à l'article 8, § 2 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH). (…) Le Comité permanent R constate que l'article 90octies du Code d'instruction criminelle en matière d'interception de communications ou télécommunications, pour les mêmes méthodes et pour les mêmes professions protégées,*

180 GwH 22 september 2011, nr. 145/2011, overw. B.38.1

prévoit une protection indépendamment de la finalité (professionnelle ou non professionnelle) de l'usage de moyen de communication. Cette protection est, donc, différente de celle prévue dans la loi du 30 novembre 1998 sans qu'une justification objective n'apparaisse et semble, dès lors contraire aux principes d'égalité de traitement et de non-discrimination et/ou à l'article 8 de la CEDH'..[181]

Het Vast Comité I besloot volgende vraag te stellen aan het Grondwettelijk Hof: *"L'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité viole-t-il les articles 10 et 11 de la Constitution, lus seuls ou conjointement avec l'article 22 de la Constitution et/ou combinés ou non avec l'article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 et approuvée par la loi du 13 mai 1955, en tant qu'il ne prévoit pas en faveur de l'avocat, du médecin ou du journaliste de protection particulière pour les moyens de communication qu'ils utilisent à des fins autre que professionnelles?'*.[182] [183]

---

181 *'Het Vast Comité I merkt op dat artikel 18/2, §3, eerste en tweede lid van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (W.I&V) de aan advocaten, artsen en journalisten verleende bescherming beperkt tot de communicatiemiddelen die zij die zij voor beroepsdoeleinden gebruiken. Uit de huidige tekst volgt dat communicatiemiddelen zij voor andere dan beroepsdoeleinden gebruiken niet onder de wettelijke bescherming vallen. Het Vast Comité I vraagt zich af hoe de inlichtingendiensten kunnen nagaan of de betrokken communicatiemiddelen (telefoon, GSM, …) al dan niet voor beroepsdoeleinden worden gebruikt. Is het mogelijk om a priori uit de historiek van telefoongesprekken van een advocaat, arts of journalist af te leiden of een nummer uitsluitend een professioneel karakter heeft? De wetgever heeft dit onderscheid niet gemaakt in de strafprocedure, meer bepaald in de artikelen 90ter tot 90decies van het Wetboek van strafvordering. De wetgever heeft de strikte voorwaarden vastgelegd waaronder de inlichtingendiensten, onder de voorafgaande controle van de BIM-Commissie, wettig kennis mogen nemen van de communicaties overeenkomstig het artikel 8, §2 van het Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM). Het Vast Comité I stelt vast dat artikel 90octies van het Wetboek van strafvordering m.b.t. de onderschepping van (tele)communicaties, voor dezelfde methoden en dezelfde beschermde beroepen, een bescherming voorziet los van de vraag of de communicatiedoeleinden al dan niet voor beroepsdoeleinden worden gebruikt. De in de wet van 30 november 1998 voorziene bescherming wijkt hiervan af, zonder dat daarvoor een objectieve rechtvaardiging lijkt te bestaan, en lijkt dus in strijd te zijn met het gelijkheids- en non-discriminatiebeginsel en/of met het artikel 8 van het EVRM.'* (vrije vertaling)

182 *'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?'* (vrije vertaling)

183 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"*. In: Grondwettelijk Hof, Arrest nr. 64/2021 van 22 april 2021 (rolnummer 7416).

Niet-tijdige notificatie aan de BIM-commissie

Krachtens artikel 18/3, §1, tweede lid W.I&V kan een specifieke methode slechts worden aangewend na een schriftelijke en met redenen omklede beslissing van het diensthoofd én na kennisgeving van deze beslissing aan de BIM-Commissie. Deze kennisgeving wordt in de praktijk de 'notificatie' genoemd. In dossier 2020/10.218 had het betrokken diensthoofd de toelating gegeven tot het vorderen van een telecomoperator om de verkeersgegevens te bekomen van een bepaald elektronisch communicatiemiddel van waaruit of waarnaar elektronische communicaties worden of werden gedaan. De notificatie van deze beslissing aan de BIM-Commissie vond echter pas een grote maand later plaats. De gegevens die de inlichtingendienst van de telecomoperator verkreeg voor deze notificatie waren zodoende onwettig verkregen. Ze moesten door het Comité bijgevolg worden vernietigd.

In dossier 2019/8968 wenste een inlichtingendienst een lopende observatie (specifieke methode) te verlengen. Krachtens artikel 18/3, §4 W.I&V kan een verlenging (of hernieuwing) van een specifieke methode slechts plaatsvinden na een nieuwe beslissing van het diensthoofd én na een kennisgeving hiervan aan de BIM-Commissie. De eerste specifieke methode liep van de 25e van maand X en met de 24e van maand Y. De beslissing van het diensthoofd tot verlenging van de observatie werd echter pas op de 27e van maand Y 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.

Ook in dossier 2020/9595 wenste een inlichtingendienst een lopende observatie (specifieke methode) te verlengen. De eerste methode liep hierbij tot en met de 19e van maand X. De lopende observatie moest dientengevolge eindigen op deze datum, maar om technisch redenen werd het verzamelen van informatie niet stopgezet en liep door tot en met de 26e van maand X. Het diensthoofd gaf zijn toelating tot verlenging op de 26e van maand X, die aan de BIM-Commissie werd genotificeerd op de 27e. Tussen de 19e en de 27e werden zodoende de gegevens niet op rechtmatige wijze verzameld. Gezien daarenboven de eerste observatie eindigde op de 19e en de beslissing tot verlenging van het diensthoofd pas op de 26e werd genomen, ging het *de iure* daarenboven niet om een verlenging van de methode maar om een hernieuwing. Hoewel artikel 18/3, §4 W.I&V geen onderscheid maakt tussen een verlenging en een hernieuwing wat betreft de toepassingsvoorwaarden (*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.

Onvoldoende motivering

In het kader van een specifieke methode was het gebrek aan een gedegen motivering van de beslissing van het diensthoofd aan de orde (dossier 2019/8768). De inlichtingendienst wenste de gegevens te bekomen over telefonische communicaties van een bepaald persoon voor een periode van twaalf maanden voorafgaand aan de datum van de beslissing van het diensthoofd. Het Comité oordeelde echter dat de in de BIM-beslissing opgegeven motivering het niet mogelijk maakte *'te beslissen of de in toepassing gebrachte BIM voldoet aan de door de wet gestelde vereisten, inzake bevoegdheid van de dienst en proportionaliteit van de methode'*. Zoals vermeld in het activiteitenverslag 2019 vatte het Comité zich ambtshalve en stelde een aantal bijkomende vragen aan de betrokken inlichtingendienst.[184] Volgend op een mondeling onderhoud tussen de inlichtingendienst en het Comité en een aanvullende nota van de inlichtingendienst met bijkomende informatie besloot het Comité in het werkingsjaar 2020 om haar ambtshalve vatting in te trekken, en zodoende dat de inlichtingendienst ter zake bevoegd was en de methode proportioneel.

Ook in dossier 2020/9805 was het gebrek aan een gedegen motivering van de toelating aan de orde. In betrokken zaak wou een inlichtingendienst overgaan tot het vastleggen van beeld- en geluidsopnames van een gesprek dat plaatsvond op een niet voor het publiek toegankelijke plaats die aan het zicht onttrokken was (*cf.* artikel 18/11, §§1 en 2 en artikel 18/17, §§1 en 2 W.I&V). Uit het administratief dossier, voornamelijk samengesteld uit de machtiging van het diensthoofd en het eensluidend advies van de BIM-Commissie, kon het Comité evenwel niet afleiden waarom de inlichtingendienst een dergelijke werkwijze wou toepassen noch wat exact de finaliteit van de betrokken operatie was. Ook in dit dossier ging het Comité over tot een ambtshalve vatting en vroeg bijkomende informatie aan de inlichtingendienst. Na een nota van de inlichtingendienst die *'op omstandige wijze de werkwijze en de finaliteit van de kwestieuze BIM uiteenzette'*, besloot het Comité dat de uitzonderlijke methode wettig was.

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 de dossiers 2020/10.023 en 2020/10.180 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 verkeersgegevens inzake elektronische communicatie bedoeld in artikel 18/8, §1, 1° W.I&V). Ook in de daaropvolgende vordering aan de telecomoperator werd dit verkeerd

184 Zie hieromtrent: Vast Comité I, *Activiteitenverslag 2019*, 56-57.

oproepnummer vermeld. De dienst merkte dit in beide dossiers zelf op, evenwel nadat de gevorderde gegevens reeds van de telecomoperator werden verkregen. De inlichtingendienst plaatste telkenmale eigenmachtig de verkregen gegevens in elektrische quarantaine en bracht de BIM-Commissie van de vergissing op de hoogte. De Commissie verbood de exploitatie van de onrechtmatig verkregen gegeven, verwittigde het Vast Comité I, waarop laatstgenoemde het bevel gaf om de onwettelijk bekomen gegevens te vernietigen.

De wettigheid van de uitvoering van een wettige methode

Technische hulpmiddelen

De Inlichtingenwet omschrijft een technische middel als *'een configuratie van componenten die signalen detecteert, deze overbrengt, hun registratie activeert en de signalen registreert'* (art. 3, 14° W.I&V). Een fototoestel en, in slechts zeer beperkte gevallen, een mobiele camera[185] worden niet als een technisch middel beschouwd. Diverse BIM-methoden kunnen uitgevoerd worden met behulp van technische middelen. In dossier 2019/8987 werd gebruik gemaakt van een camera met microfoon, en werd hiervoor na eensluidend advies van de BIM-Commissie machtiging verleend door het diensthoofd (*i.c.* voor de methode voorzien in artikel 18/11 W.I&V – observatie als uitzonderlijke methode – in combinatie met de methode voorzien in artikel 18/17 W.I&V – communicatietap). Hoewel de machtiging slechts liep tot de 3e van de maand, bleef de apparatuur evenwel beeld- en geluidopnames maken na deze datum en dit *'om technische redenen, omdat de camera met microfoon niet van op afstand kon bediend worden.'* Zodoende *'(bleef) de geplaatste camera (…) beelden maken en de microfoon verder geluid (opnemen)'* hoewel er hiervoor geen toelating meer bestond. Het Comité volgde het exploitatieverbod van de BIM-Commissie voor de na deze datum ingewonnen gegevens en gaf een bevel tot vernietiging ervan.

Ook in het eerder vernoemd dossier 2020/9595 werd een observatie (specifieke methode) om technische redenen niet stopgezet en werd na tussenkomst van de BIM-Commissie door het Comité het bevel gegeven om de onrechtmatig verkregen gegevens te vernietigen.

185 Meer in het bijzonder wordt uitgesloten, *'een mobiel apparaat dat gebruikt wordt voor de opname van bewegende beelden indien het nemen van foto's de discretie en de veiligheid van de agenten niet kan verzekeren en op voorwaarde dat dit gebruik voorafgaand is toegestaan door het diensthoofd of zijn gedelegeerde'*. In dergelijk geval *'(worden) (e)nkel relevant geachte vaste beelden (…) bewaard. De overige beelden worden vernietigd binnen een maand na de dag van de opname'* (art. 3, 14°, b W.I&V).

Verschil tussen de toelating van het diensthoofd en de vordering

In drie beslissingen bleek de toelating van het diensthoofd om een specifieke of uitzonderlijke methode in te zetten volkomen wettig, maar stelde er zich een probleem op het vlak van de uitvoering in die zin dat de vordering van de gegevens niet overeenstemde met het initiële mandaat. Ofwel kwam de afluisteringstermijn in de vordering niet overeen met deze in de machtiging (dossier 2020/9204) ofwel werd een verkeerd telefoonnummer meegedeeld aan de telecomprovider (dossier 2019/8964) ofwel *'(werd) per vergissing aan de uitvoerende telecommunicatiedienst niet alleen een eenmalige intrusie (…) gevraagd'*, meer bepaald een *'eenmalige toegang (…) tot het mailverkeer'* van het target (cf. art. 18/16 W.I&V), *'maar (…) werd (ook) gevraagd om een live acces te voorzien'* (dossier 2020/9829). Vermeldenswaardig in dit laatste geval is dat de inlichtingendienst deze vergissing zelf vaststelde, en vervolgens overeenkomstig artikel 18/10, §1, vierde lid W.I&V de *live acces* eigenmatig stopzette. De inlichtingendienst besloot om de onrechtmatig verkregen gegevens apart te bewaren. De BIM-Commissie sprak daaropvolgend een exploitatieverbod uit en voorzag eveneens in een tijdelijke specifieke bewaring. Het Comité bevestigde tot slot het exploitatieverbod van de Commissie en beval de vernietiging van de via de live acces bekomen gegevens.

Verkeerde gegevens verstrekt door de telecomoperator of -provider

In drie afzonderlijke dossiers had een inlichtingendienst de betrokken netwerkoperator op wettige wijze gevorderd, maar stelde zich een probleem bij de overmaking van de gevorderde gegevens in de zin dat de door de operator overgemaakte gegevens geen betrekking hadden op de gevorderde gegevens. In de dossiers 2020/9167 en 2020/9225 betrof het telkenmale *'een telefonie-onderzoek en een afluistermaatregel'* en dit op drie respectievelijk twee telefoonnummers. In het dossier 2019/8934 betrof het louter een vordering binnen het opsporen van de verkeers- en lokalisatiegegevens van elektronische communicatiemiddelen. In alle drie de gevallen *'(werden) de betreffende data op wederrechtelijke wijze (…) meegedeeld aan'* de betrokken inlichtingendienst. Dit gebeurde zodoende *'buiten de wil van'* de inlichtingendienst *'om'*. De BIM-Commissie sprak telkenmale een exploitatieverbod uit, gevolgd door een vernietigingsbevel van het Comité.

II.3. CONCLUSIES

Het Vast Comité I formuleert volgende algemene conclusies:

– Tussen 1 januari en 31 december 2020 werden door de twee inlichtingendiensten samen 2337 toelatingen verleend tot het aanwenden van bijzondere inlichtingenmethoden: 2140 door de VSSE (waarvan 1629 specifieke en 511

uitzonderlijke) en 197 door de ADIV (waarvan 146 specifieke en 51 uitzonderlijke). Na een constante stijging van het aantal ingezette BIM's de afgelopen jaren en een stagnatie vorig jaar, kan voor het eerst een lichte daling worden opgetekend. Naar luid van de BIM-verantwoordelijken van zowel de VSSE als de ADIV heeft de COVID-pandemie geen impact gehad op het aantal ingezette bijzondere inlichtingenmethoden.

- De VSSE blijft het leeuwendeel van de ingezette methoden voor zijn rekening nemen (91,5 %), met andere woorden, minder dan 1 op 10 methoden worden uitgevoerd door de ADIV.
- Als de globale cijfers worden uitgesplitst, kan een stijging bij de ADIV worden opgetekend van de inzet van specifieke methoden (van 138 naar 146) maar een opmerkelijke daling van het aantal ingezette uitzonderlijke methoden (van 76 in 2019 naar 51 in 2020). De VSSE laat een daling optekenen van het aantal ingezette specifieke methoden (van 1781 naar 1629); het aantal ingezette uitzonderlijke methoden nam dan weer met 14% toe ten overstaan van 2019.
- Wat 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 van ca. 9% opgetekend.
- Verder kan worden genoteerd dat het aantal ingezette BIM's voor wat betreft de dreigingen 'terrorisme' en 'extremisme' in belangrijkheid toenamen, ten nadele van 'inmenging', dat met de helft afnam.
- De ADIV richtte zich bij de inzet van BIM-methoden vooral op de dreigingen 'terrorisme' en 'extremisme', ten nadele van 'inmenging' dat met de helft afnam, voor de VSSE was de aard van de dreiging hoofdzakelijk 'terrorisme', gevolgd door 'spionage'.
- Het Comité werd gevat in elf dossiers, waarvan twee vattingen op eigen initiatief en negen van rechtswege nadat de BIM-Commissie een specifieke of een uitzonderlijke methode wegens onwettigheid had geschorst (art. 43/4 W.I&V). Onwettigheden betroffen onder meer een onvoldoende motivering, de niet-tijdige verwittiging van de BIM-Commissie, of nog, een onduidelijk voorwerp.
- Het Vast Comité I heeft in 2020 voor het eerst sinds de inwerkingtreding van de BIM-Wet van 4 februari 2010 een prejudiciële vraag gesteld aan het Grondwettelijk Hof aangaande de BIM-wetgeving.

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[186]

Al in 2017 werd de bevoegdheid van de Algemene Dienst Inlichting en Veiligheid (ADIV) in het kader van de veiligheidsintercepties uitgebreid.[187] De intercepties konden sindsdien voor communicaties '*uitgezonden of ontvangen in het buitenland*'. Deze mogelijkheid geldt voor *quasi* alle opdrachten van de ADIV. Daarbij is het niet onbelangrijk te vermelden dat de opdrachtomschrijvingen zelf, ook werden verruimd. Tegelijkertijd voerde de wetgever twee andere methoden in, te weten de 'intrusie in een informaticasysteem' (art. 44/1 W.I&V) en de 'opname van bewegende beelden' (art. 44/2 W.I&V). En ook de wijze waarop het Comité deze methoden kan controleren, werd gewijzigd.

De controle *voorafgaand* aan de intercepties, intrusies of beeldopnames gebeurt op basis van jaarlijks opgestelde lijsten.[188] Dit betekent dat er naast een jaarlijks interceptieplan, ook een intrusie- en beeldplan dient te worden opgesteld door de ADIV.[189] 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

---

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

187 Over de opeenvolgende wetswijzigingen inzake de interceptiebevoegdheid van de ADIV, zie Vast Comité I, *Activiteitenverslag 2018*, 61 e.v.

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

189 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[190] die op zijn beurt de lijsten, voorzien van de toelating van de minister, overzendt aan het Vast Comité I.[191]

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[192], werd evenwel nog steeds geen dergelijk interceptie-KB getroffen.[193] Het Comité beveelt dan ook opnieuw aan om dit zo spoedig mogelijk te doen.

---

190 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.

191 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.

192 Vast Comité I, *Activiteitenverslag 2018*, 129.

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

III.2. HET IN 2020 VERRICHTE TOEZICHT

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

Het Vast Comité I ontving, weliswaar op fractionele wijze, alle plannen aangaande intercepties, intrusies en beeldopnamen. Het interceptie- en beeldopnameplan, dat begin januari 2020 door de minister van Defensie was goedgekeurd, werd evenwel pas in juni 2020 toegezonden aan het Vast Comité I, en dit na verschillende herinneringen. Het intrusieplan bleek, omwille van een vergetelheid, niet ter goedkeuring aan de minister zijn toegezonden. Na een interpellatie van het Vast Comité I, werd dit euvel geregulariseerd.

Niettegenstaande bij het interceptieplan slechts enkele kleine opmerkingen dienden te worden geformuleerd, drong het Vast Comité I erop aan dat toekomstige plannen voor beeldopnames en intrusies zouden voldoen aan alle wettelijke vereisten. Het Comité stelde voor dat de betrokken afdelingen zich daarbij zouden laten inspireren door het interceptieplan.

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

In 2020 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 vast te stellen dat de ADIV een nieuw logboek had geopend dat evenwel niet meer in overeenstemming was met de aanbevelingen van het Comité. Daarnaast kon het Vast Comité I ook vaststellen dat de ADIV doorgaat met de uitvoering van projecten in verband met de toepassing van artikel 44 W.I&V.

Ondanks de beperkingen opgelegd door de sanitaire crisis, heeft het Vast Comité I zijn toezichtopdracht van de door de ADIV ontwikkelde activiteiten in het kader van de toepassing van artikel 44 W.I&V, in 2020 verdergezet. Zo werd, op het einde van het jaar, een werkvergadering georganiseerd in de schoot van de ADIV met alle actoren die bij de uitvoering van dit artikel betrokken zijn. Deze bijeenkomst heeft het mogelijk gemaakt bepaalde aandachtspunten te verduidelijken en te werken aan de standaardisering van de verschillende plannen.

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 vormen het voorwerp van een toezichtonderzoek dat werd geopend in 2019.

HOOFDSTUK IV
BIJZONDERE OPDRACHTEN

In de loop der jaren kreeg het Vast Comité I een aantal specifieke opdrachten toegekend dewelke hun oorsprong niet vinden in een wettelijke bepaling, maar een antwoord bieden op een concrete nood. Deze bijkomende opdrachten werden in nauw overleg met het Comité aan hem toegewezen.

IV.1. TOEZICHT OP DE ACTIVITEITEN VAN HET ISTAR-BATALJON

De oprichting van het ISTAR-bataljon (*Intelligence Surveillance Target Acquisition and Reconnaissance*) kwam tegemoet aan een toenemende behoefte aan *battlefield intelligence* bij buitenlandse operaties van Defensie. De organieke Wet van 30 november 1998 erkent evenwel slechts twee inlichtingendiensten (art. 2 W.I&V). Het Vast Comité I wees dan ook het Parlement, de minister van Defensie als de CHOD op het feit dat dit bataljon – zij het gedeeltelijk – inlichtingenactiviteiten ontwikkelt. Ook de Parlementaire Onderzoekscommissie Aanslagen had hierop geattendeerd: '*De onderzoekscommissie acht de opdrachten van ISTAR belangrijk voor de veiligheid van onze militairen, doch meent dat de verhouding tussen dit bataljon en de ADIV formeel geregeld moet worden middels een samenwerkingsprotocol, waarin duidelijk wordt omschreven op welke wijze en onder welke voorwaarden ISTAR kan bijdragen aan de versterking van de informatiepositie van de ADIV. In dat kader lijkt het tevens aangewezen om het Vast Comité I te belasten met het toezicht op deze ondersteunende taak van ISTAR*'.[193]

Aangezien er op korte termijn geen wettelijke of structurele oplossingen voorhanden bleken, werd eind mei 2018 een voorlopige oplossing uitgewerkt door middel van een protocolakkoord tussen de ADIV en de Chief of Defence (CHOD).[194] Hierin worden onder meer de taken en opdrachten van het ISTAR-bataljon inzake HUMINT- en analysecapaciteiten vastgelegd. Daarnaast wordt ook de organisatie

193 *Parl. St.* Kamer, 2016-17, nrs. 54K1752/008, 306.

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

van een technische en juridische controle uitgewerkt.[195] Deze taken berusten bij de ADIV.

Het ISTAR-bataljon bezorgt de ADIV daartoe uit eigen beweging de interne reglementen en richtlijnen. De controle vindt plaats door middel van bezoeken aan de installaties van het ISTAR-bataljon en aan de zones waar het zijn operaties en activiteiten uitvoert. De controle wordt ook uitgevoerd op basis van een analyse van documenten en van verhoren.

Het initiële protocolakkoord werd gesloten voor een termijn van twee jaar. Half april 2020 werd een interne *staffing* in Defensie georganiseerd om in een verlenging voor twee jaar te voorzien. Op 19 mei 2020 ondertekenden de CHOD en de Chef ADIV deze verlenging.

Het Vast Comité I werd in het protocol aangewezen om een – zij het onrechtstreeks – toezicht uit te oefenen over de activiteiten van het bataljon. Daartoe overhandigt de ADIV aan de minister van Defensie, de CHOD en het Vast Comité I een trimesterieel verslag betreffende iedere onderzoeksopdracht. Het Comité ontving in 2020 meerdere controlerapporten. Uit de rapporten bleek dat het ISTAR-bataljon weinig activiteiten ontvouwde die onder toepassing van het bovenvermelde protocolakkoord vielen. De door het ISTAR-bataljon ontwikkelde inlichtingenactiviteiten, beantwoordden volgens de ADIV aan de opgelegde voorschriften en richtlijnen.[196]

IV.2. CONTROLE OP DE SPECIALE FONDSEN

Het Rekenhof controleert de wettigheid, de rechtmatigheid en de doelmatigheid van alle uitgaven. Dat geldt in principe ook voor alle uitgaven van de inlichtingendiensten. Echter, omwille van de gevoeligheid van de materie werd een deel van het budget van de VSSE en de ADIV (met name de 'speciale fondsen' met uitgaven voor bijvoorbeeld operaties en informanten) niet onderzocht door het Rekenhof. Voor de VSSE werd de controle van deze specifieke uitgaven alleen verricht door de directeur algemeen beleid van de minister van Justitie. Halfweg 2018 uitte het Rekenhof het voornemen om vanaf het afsluiten van de rekening van 2018 eveneens een periodieke controle te doen van deze fondsen.[197]

---

195 Technische controle is de controle op de correcte toepassing van de richtlijnen inzake analyse en van de HUMINT-richtlijnen en van de bijzondere akkoorden tussen de CHOD en de ADIV. Onder juridische controle wordt de controle op de correcte toepassing van het protocol verstaan.

196 De analyse van deze verslagen zal het voorwerp uitmaken van verder onderzoek. Gelet op het feit dat ISTAR weinig HUMINT-activiteiten ontwikkelt, heeft het Comité hiervan geen prioriteit gemaakt.

197 Het Comité kreeg in 2020 kopie van de in 2019 door het Rekenhof uitgevoerde controle 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.

Ook de formele controle op de rekeningen van de ADIV wordt sinds 2020 uitgevoerd door het Rekenhof, dat daarvoor beroep kan doen op de technische ondersteuning door het Vast Comité I.[198] Daardoor kon het Comité "*exercer sa mission avec plus d'attention sur l'utilisation de ces dits fonds*". Er werd dan ook beslist om een opvolgonderzoek op te starten naar het beheer, het gebruik en de controle van de speciale fondsen (cf. Hoofdstuk I.11.11).[199]

IV.3. TOEZICHT OP DE OPVOLGING VAN POLITIEKE MANDATARISSEN

Of en in welke mate de Belgische inlichtingendiensten politieke mandatarissen (mogen) opvolgen en welke regels ze daarbij in acht moeten nemen, blijft een actueel vraagstuk.[200]

Vanaf begin 2018 wordt in deze binnen de VSSE de als 'vertrouwelijk' geclassificeerde dienstnota van 13 december 2017 toegepast.[201] De VSSE zendt twee types van rapporten naar de minister van Justitie en de Premier, met kopie naar het Vast Comité I. Het betreft enerzijds punctuele rapporten over politieke mandatarissen die bijdragen aan de totstandkoming van een dreiging alsook een trimestrieel overzicht van het geheel van documenten waarin melding wordt gemaakt van deze mandatarissen.[202] 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*'.[203]

198 *« 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 ».*

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

200 Vraag van S. Creyelman aan de minister van Buitenlandse Zaken over 'politieke dossiers bij het ADIV' (Vr. en Ant. Kamer 2019-20, 24 februari 2020, QRVA 12, 352, Vr. nr. 143); Vraag van S. Creyelman aan de minister van Buitenlandse Zaken over 'politieke dossiers bij de VSSE' (Vr. en Ant. Kamer 2019-20, 24 februari 2020, QRVA 12, 353, Vr. nr. 145).

201 Om de rapportage ten aanzien van de directie inzake disruptieve activiteiten te verbeteren, werd de dienstnota in juni 2020 geactualiseerd.

202 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).

203 '*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 personne exerçant un mandat politique'.

In uitvoering van de principes vermeld in bovenstaande dienstnota, werd het Comité in 2020 effectief door de VSSE van beide types van rapporten op de hoogte gesteld.

Net zoals de VSSE werd de ADIV 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. Maar ook in 2020 mocht het Comité geen informatie in die zin ontvangen. De ADIV beschikte, ondanks herhaaldelijk verzoek, niet over een specifieke procedure (SOP) om met deze informatie om te gaan noch werd bepaald hoe het Vast Comité I hiervan op de hoogte te brengen.

Gezien nergens wordt vermeld wat het Comité wordt geacht aan te vangen met van de VSSE verkregen informatie, nam het zelf het initiatief een methodologie uit te werken omtrent de 'problematiek van de opvolging van de politieke mandatarissen door de inlichtingendiensten en de rol van het Vast Comité I'. Deze methodologie werd in 2020 door de parlementaire Begeleidingscommissie goedgekeurd. De opvolging van politieke mandatarissen vormde in 2020 het voorwerp van een (periodiek) toezichtonderzoek (cf. Hoofdstuk I. 11.12).

HOOFDSTUK V

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

V.1. INLEIDING

De Algemene Verordening Gegevensbescherming 2016/679 (AVG)[204] en de Richtlijn 2016/680 (Richtlijn)[205] 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)[206] – de opvolger van de Privacycommissie – opgericht en in juli 2018 werd een nieuwe Gegevensbeschermingswet (GBW) gestemd.[207] Deze wet wijzigde op zijn beurt de Toezichtwet van 18 juli 1991. Het Vast Comité I werd immers als gegevensbeschermingsautoriteit aangeduid voor verwerkingen van persoonsgegevens die kaderen binnen het domein van de 'nationale veiligheid'.

De rol van het Comité in deze staat omschreven in de Wet tot oprichting van de Gegevensbeschermingsautoriteit (GBA-Wet), in de Gegevensbeschermingswet (GBW) en in de Toezichtwet (W.Toezicht).[208]

---

204 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.

205 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.

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

207 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.

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

In 2019-2020 heeft het Comité diverse activiteiten ontwikkeld om deze bijkomende taak en verplichtingen waar te kunnen nemen. Reeds in 2018 werd een *Data Protection Officer* (DPO) voor alle verwerkingen van het Comité die buiten de 'nationale veiligheid' vallen (bijv. verwerkingen in het kader van het personeelsbeheer en logistiek) aangesteld (*infra* XI.2). Verder werden diverse vergaderingen gehouden met de drie andere bevoegde toezichthoudende overheden (*infra, V.2*). Met het Vast Comité P werden afspraken gemaakt om een voorstel tot wijziging van de Toezichtwet uit te werken. Diverse bepalingen zijn immers niet aangepast aan de nieuwe bevoegdheid van beide Comités. Voor het overige heeft het Comité zijn besprekingen ook intern voortgezet. Deze denkoefening gaf aanleiding tot een eerste algemene commentaar die kan bijdragen tot de volgende evaluatie van de GBW[209] (*infra* V.7). Ten slotte heeft het Comité een aantal interne werkprocessen uitgewerkt in het kader van zijn adviesfunctie en voor wat betreft de onderzoeken van verzoeken van burgers.

In wat volgt wordt gerapporteerd over deze bijzondere rol van het Comité: achtereenvolgens wordt de samenwerking tussen de diverse bevoegde toezichthoudende autoriteiten besproken, is er aandacht voor de controle op persoonsgegevensverwerkingen door BELPIU, voor de juridische adviesverlening van het Comité alsook voor de behandeling van individuele verzoeken. Dit alles past in het kader van artikel 35 §3 W.Toezicht, dat stelt dat het Vast Comité I '*jaarlijks verslag uit[brengt] bij de Kamer van volksvertegenwoordigers omtrent de gegeven adviezen in zijn hoedanigheid van gegevensbeschermingsautoriteit, omtrent de onderzoeken die werden uitgevoerd en de maatregelen die werden genomen in dezelfde hoedanigheid alsook omtrent haar samenwerking met de andere gegevensbeschermingsautoriteiten*'.

V.2. SAMENWERKING TUSSSEN DE BEVOEGDE TOEZICHTHOUDENDE AUTORITEITEN

België telt op federaal niveau niet minder dan vier bevoegde toezichthoudende autoriteiten. Naast het Vast Comité I, zijn er de Gegevensbeschermingsautoriteit (GBA) die een algemene en residuaire bevoegdheid heeft, het Controleorgaan op de politionele informatie (COC), dat vnl. verwerkingen controleert die kaderen binnen Titel 2 van de Gegevensbeschermingswet, en het Vast Comité P dat samen met het Vast Comité I controle uitvoert op verwerkingen van het OCAD (art. 161 GBW). Bovendien zijn het COC en het Vast Comité I gezamenlijk bevoegd ten aanzien van de gemeenschappelijke gegevensbanken zoals bedoeld in artikel 44/11/3*bis* van de Wet op het politieambt (WPA) (artikel 44/11/3*quinquies* WPA).

209 Zie artikel 286 GBW.

Behoudens in de twee laatste genoemde gevallen, handelt het Vast Comité I autonoom. Dit betekent niet dat er geen overleg of samenwerking is tussen de vier instanties, integendeel. De wet stelt immers dat er in bepaalde gevallen moet of kan worden samengewerkt of dat er informatie moet worden uitgewisseld (artt. 98 en 131 GBW).

De bevoegde toezichthoudende autoriteiten (BTA) zijn verplicht om nauw samen te werken, onder meer voor wat betreft de verwerking van klachten, adviezen en aanbevelingen die raken aan de bevoegdheden van twee of meerdere BTA's en dit met het oog op de consequente toepassing van de nationale, Europese en internationale regelgeving inzake gegevensbescherming (art. 54/1 §1 GBA-Wet). Deze bepaling stelt ook dat de gezamenlijke behandeling van klachten, adviezen en aanbevelingen aan de hand van het 'één-loketmechanisme' moet gebeuren. Bovendien moeten de BTA's een protocol sluiten ter uitvoering van die vereiste samenwerking. In 2019 hebben de verschillende diensten een protocol uitgewerkt en daarover onderhandelingen gevoerd; het protocol werd in 2020 aangenomen en gepubliceerd.[210]

V.3. DE CONTROLE OP PERSOONSGEGEVENSVERWERKINGEN DOOR BELPIU

V.3.1. CONTROLE OP BELPIU GEKADERD

Met de Wet van 25 december 2016 betreffende de verwerking van passagiersgegevens (PNR-Wet), werd uitvoering gegeven aan de Europese doelstellingen om tegelijk terrorisme en samenhangende ernstige misdrijven te voorkomen en te bestrijden. Daartoe werd binnen de FOD Binnenlandse Zaken een '*Belgian Passenger Information Unit*' opgericht, i.e. de Belgische passagiersinformatie-eenheid (BELPIU), die de passagiersgegevens in een gegevensbank bijhoudt met het oog op het voorkomen en bestrijden van de in de PNR-Wet vastgelegde misdrijven of dreigingen.

Op grond van ondertitel 5 van Titel 3 van de GBW is het Vast Comité I de bevoegde toezichthoudende autoriteit ten aanzien van "*elke verwerking van persoonsgegevens door de PIE in het kader van de finaliteiten bedoeld in artikel 8, §1, 4°, van de wet van 25 december 2016*" (art. 169 GBW) of met andere woorden verwerkingen die kaderen "*in de artikelen 7, 1° en 3°/1 en 11, §1, 1° tot 3° en 5° van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst*"

[210] Zie https://www.comiteri.be/images/pdf/publicaties/samenwerkingsprotocol_DPAS_NL_2020_11_24.pdf.

(art. 8, § 1, 4° PNR-Wet). Bedoeld wordt met andere woorden verwerkingen die door de VSSE en de ADIV gebeuren in het kader van hun reguliere inlichtingenopdracht. Het Comité is alleen bevoegd om de werking van de PIE te controleren in de mate waarin deze eenheid medewerking verleent aan de vragen om informatie en inlichtingen komende van een van de twee inlichtingendiensten, ongeacht of dit gebeurt onder de vorm van gerichte zoekingen, *watchlists* of profielen.

V.3.2. RESULTAAT VAN DE GELIJKTIJDIGE VISITATIE

Gelet op hun respectieve bevoegdheden als bevoegde toezichthoudende autoriteiten ten aanzien van de gegevensverwerkingen door de passagiersinformatie-eenheid, beslisten het Controleorgaan op de politionele informatie (COC) en het Vast Comité I op eigen initiatief gelijktijdig een visitatie te verrichten bij deze dienst. Immers, de bevoegdheden van beide diensten ten aanzien van de PIE zijn dan wel niet volledig identiek, maar minstens overlappend.[211] De visitatie was niet het gevolg van een (individuele) klacht of het bestaan van (concrete) aanwijzingen over het niet naleven van de wet- en regelgeving.

De invalshoek van de visitatie was opgezet met de nadruk op *compliance based*: gebeurt de verwerking van passagiersgegevens in overeenstemming met de wet en wordt daarbij een hoge veiligheidsstandaard gehanteerd? De visitatie was meer gericht op informatieveiligheid dan op juridische aspecten.[212]

De visitatie was beperkt tot twee domeinen, te weten enerzijds de ICT-beveiliging en informatieveiligheid en anderzijds de proportionaliteit van de gegevensverwerking. De reden voor een beperkte visitatie was eenvoudig. Om te beginnen was de PIE pas operationeel sinds begin 2018. Daarnaast waren nog niet alle geviseerde passagiersvervoerders en reisoperatoren technisch geconnecteerd met de PIE.

Het onderzoeksrapport werd in juni 2020 gefinaliseerd en voorgesteld aan de parlementaire Begeleidingscommissie. In 2021 zal het Comité, samen met het COC, controleren welke opvolging BELPIU heeft gegeven aan de aanbevelingen waartoe het onderzoek aanleiding gaf.

De belangrijkste conclusies, wat betreft de bevoegdheid van het Vast Comité I, resulteerden uit de gelijktijdige uitoefening van de bevoegdheden van het Comité en het COC inzake de informatieveiligheid. Specifieke leerpunten met betrekking tot gegevensverwerking voor inlichtingendoeleinden, zullen worden behandeld in het in 2018 opgestarte toezichtonderzoek naar '*de toepassing en de interne controle*

211 Deze visitatie had geen betrekking op de wijze waarop de twee Belgische inlichtingendiensten hun bevoegdheden in dit kader hanteren. Dit aspect werd door het Comité behandeld in een apart toezichtonderzoek dat in 2018 werd opgestart (cf. I.7.2).

212 Deze invalshoek stond er niet aan in de weg dat het COC of het Vast Comité I gepaste maatregelen neemt wanneer evidente wettelijke tekortkomingen worden vastgesteld.

bij de inlichtingendiensten van de methoden en instrumenten die de wetgever onlangs heeft ingevoegd of aangepast en in verband waarmee een specifieke toezichtrol werd toegewezen aan het Vast Comité I.

Wat betreft de informatieveiligheid, komt het er samengevat op neer dat het Comité en het COC algemeen gezien de gestructureerde benadering van de gegevensbescherming en de informatieveiligheid waarderen, inzonderheid wat betreft de initiatieven en de adviezen van de *Data Protection Officer*. Toch hebben het Comité en het COC ook een reeks aandachtspunten geïdentificeerd met betrekking tot de organisatie van die informatieveiligheid (voltooiing en validatie van een impactanalyse betreffende de gegevensbescherming en van een actieplan in verband daarmee, uitwerking van een geschikt proces voor incidentbeheer…). Er is ook bijzondere aandacht besteed aan een incident in verband met de creatie en het gebruik door bevoorrechte gebruikers; verder onderzoek dringt zich in deze op. Het Comité en het COC hebben ook gewezen op een probleem in verband met de inachtneming van het principe van '*closed-box*'[213], hoewel dit concept juridisch gezien niet in het gedrang wordt gebracht door BELPIU. Naar aanleiding van die vaststellingen zijn er aanbevelingen geformuleerd die zullen worden opgenomen in hoofdstuk XII van dit activiteitenverslag.

V.4. ADVIESVERLENING

Het Comité kan in twee gevallen een advies uitbrengen '*over een ontwerp van wet, van koninklijk besluit, van circulaire of over enig ander document waarin beleidslijnen van de bevoegde ministers worden geformuleerd*': wanneer de wet zijn advies vereist of op verzoek van de Kamer van volksvertegenwoordigers of van de bevoegde minister (artikel 33, lid 8 W. Toezicht). Dergelijk advies heeft specifiek betrekking op de problematiek van de gegevensverwerking en moet dus onderscheiden worden van de algemene adviesbevoegdheid die bijvoorbeeld ook betrekking kan hebben op de efficiëntie en de coördinatie (cf. Hoofdstuk VII. 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.

213 Dit principe verwijst naar de *Operational Travel Intelligence Room* (OTIR), i.e. een afgesloten ruimte van de FOD Binnenlandse Zaken waar de gedetacheerde leden toegang hebben tot de gegevensbank van de passagiers. Het gaat om een ruimte die hermetisch is afgesloten voor derden en onbevoegden en die enkel toegankelijk is voor een beperkt aantal specifiek aangewezen personen. De toegang tot de passagiersgegevensbank is gelieerd aan de uitvoering van een specifieke opdracht van het gedetacheerde lid van de PIE. De betrokkene heeft enkel toegang tot de passagiersgegevens in verband met de aanwijzing(en) van zijn dienst, op basis van individuele toegangsprofielen.

Het Comité heeft in 2020 in totaal vier adviezen verleend in deze hoedanigheid, waarvan twee wat betreft de uitwisseling van geclassificeerde informatie[214] en twee andere over de bestuurlijke handhaving en de oprichting van een Directie Integriteitsbeoordelingen; het ene als exclusief bevoegde toezichthoudende autoriteit en het andere als gezamenlijk bevoegde toezichthoudende autoriteit (met het Vast Comité P)[215]:

— Advies 001/VCI-BTA/2020 van 26 augustus 2020 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 de Italiaanse Republiek inzake de wederzijdse bescherming van geclassificeerde informatie, gedaan te Rome op 31 januari 2017*';
— Advies 002/VCI-BTA/2020 van 26 augustus 2020 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 de Franse Republiek inzake de wederzijdse bescherming van geclassificeerde informatie, gedaan te Parijs op 11 juli 2017*'.
— Advies 001/VCI-BTA/2020 van 30 oktober 2020 aangaande een '*wetsvoorstel tot wijziging van diverse bepalingen betreffende bestuurlijke handhaving en houdende de oprichting van een Directie Integriteitsbeoordelingen voor openbare besturen*', VSSE en ADIV;
— Gezamenlijk advies 003/VCI-VCP-BTA/2020 van 17 september 2020 aangaande een '*wetsvoorstel tot wijziging van diverse bepalingen betreffende bestuurlijke handhaving en houdende de oprichting van een Directie Integriteitsbeoordelingen voor openbare besturen*', OCAD.

V.5. INFORMATIE VAN DE GECONTROLEERDE DIENSTEN

De door het Vast Comité I gecontroleerde diensten moeten een hele reeks gegevens ter beschikking houden of stellen van het Comité.[216] Zo moet de verwerkingsverantwoordelijke binnen de kortste termijn en indien mogelijk 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

214 In 2019 werden in die zin al adviezen verleend over de uitwisseling van geclassificeerde informatie met de Republiek Cyprus, Hongarije, de Republiek Finland en het Koninkrijk Spanje.
215 Zie *in extenso* op de website van het Vast Comité I.
216 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.

natuurlijke personen (artikelen 89, 122, 155 en 180 GBW). Er werden in 2020 geen inbreuken op de beveiliging (*data breach*)[217] gemeld aan het Comité.

Het Comité stelde op zijn website een formulier ter beschikking dat toelaat om inbreuken op de beveiliging met de vereiste nauwkeurigheid te melden.[218] In dit formulier wordt meer bepaald benadrukt dat meldingen die niet met behulp van het formulier worden verricht, niet worden geregistreerd als een melding van een inbreuk op de beveiliging, maar hooguit als een vraag of een klacht.[219]

V.6. 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).[220] 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.[221]

De onderstaande tabel bevat een overzicht van de in 2020 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).[222]

---

217 Artikel 26, 11° GBW: "'inbreuk op de beveiliging': een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde bekendmaking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens". In de praktijk en in rechte, buiten de context van de GBW, wordt veeleer verwezen naar 'gegevensschendingen' of 'data breaches'.

218 https://www.comiteri.be/images/pdf/FormDB_nl.pdf.

219 Er bestaat bijgevolg geen zekerheid dat de mededeling van informatie via andere kanalen wordt geregistreerd en onderzocht als zijnde een melding van een inbreuk op de beveiliging (data breach).

220 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).

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

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

Behandeling van individuele verzoeken[223]

2020	Vast Comité I	Vaste Comités I en P	Vaste Comités I en P, en COC	Totaal
1. Dossier geopend in 2018	1	0	0	1
2. Dossiers geopend in 2019	4	0	0	4
3. Dossiers geopend in 2020	17	1	3	21
4. Beweerde concrete inmenging in rechten en vrijheden	15	1	2	17
5. Geen beweerde concrete inmenging in rechten en vrijheden	7	0	1	8
6. Lopende dossiers	7	1	3	11
7. Afgesloten dossiers	15	0	0	15
8. Verzoek onontvankelijk	1	0	0	1
9. Verwerking overeenkomstig de GBW	14	-	-	14
10. Verwerking niet overeenkomstig de GBW	-	-	-	0
11. Totale aantal verzoeken	22	1	3	26

De tabel heeft betrekking op een totaal van 26 dossiers. Daarvan werden 11 dossiers nog niet afgesloten. 15 dossiers werden wel afgesloten: één dossier werd als onontvankelijk beschouwd, de andere 14 gaven aanleiding tot de vaststelling dat de gegevens werden verwerkt overeenkomstig de bepalingen van de GBW. In de ontvankelijke en afgesloten dossiers werden de klagers stelselmatig in kennis gesteld van het feit dat de vereiste verificaties werden uitgevoerd.

223 Regels 1 tot 3 tonen het aantal dossiers volgens het jaar waarin ze werden geopend. Regels 4 en 5 verdelen de dossiers naargelang de betrokkene al dan niet melding maakt van concrete inmenging in zijn rechten en vrijheden in het kader van de verwerking van gegevens door de verwerkingsverantwoordelijke. Dit zou bijvoorbeeld het geval zijn in het kader van een procedure van nationaliteitsverklaring waarbij een inlichtingendienst informatie verstrekt aan het openbaar ministerie, wanneer de betrokkene beweert het voorwerp te zijn van regelmatige politiecontroles, wanneer de betrokkene vaststelt dat hem de toegang tot een bepaald gebied wordt geweigerd, wanneer gegevens van een inlichtingendienst werden gebruikt in een strafrechtelijke procedure enzovoort. Regels 6 en 7 tonen de status van de dossiers in 2020 (afgesloten of nog in behandeling). Tot slot verdelen regels 8 tot 10 de afgesloten dossiers volgens hun resultaat (vaststelling van naleving of gebrek aan naleving van de GWB – NB: het gebrek aan verwerking van persoonsgegevens wordt beschouwd als een verwerking van gegevens conform de GBW).

In 70% van de verzoeken beweren de betrokkenen[224] 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 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.

De resterende 30% 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 vaststelling 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.

V.7. 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 en rekening houdend met de ervaring die het recentelijk heeft verworven als toezichthoudende autoriteit, formuleerde het Comité enkele aanbevelingen ter attentie van de wetgever.

Het Vast Comité I is zich bewust van de sleutelrol die het als toezichthoudende autoriteit vervult op het vlak van de van gegevensbescherming in het kader van de nationale veiligheid. Aangezien voor laatstgenoemde een minder restrictief wetgevingskader geldt waarin de rechten van de betrokkenen bijzonder beperkt zijn,

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

wordt het Comité een hoofdrolspeler bij het waarborgen van de doeltreffendheid van de regels inzake gegevensbescherming.

Het is in de eerste plaats met het oog op die doeltreffendheid dat onderstaande aanbevelingen werden gedaan.

V.7.1. NUTTIG COMMUNICEREN MET DE BETROKKEN PERSONEN

Ongeacht de omvang en het resultaat van de controle door het Comité, kan het niet anders dan vaststellen dat diegene die een klacht indient of zijn of haar rechten op indirecte wijze uitoefent bij het Comité, stelselmatig moet volstaan met een cryptisch antwoord: "*De nodige verificaties werden verricht*".[225]

Het kan evenwel niet worden uitgesloten dat het legitiem en aangewezen zou kunnen zijn om toch bepaalde informatie aan de betrokkene mee te delen.

De wetgever heeft zich bijvoorbeeld al in die zin uitgesproken in het aanvankelijke bevoegdheidsdomein van het Comité. In het kader van de verwerking van klachten en aangiften kan het Comité (of *moet* het zelfs), wanneer een onderzoek is afgesloten, het resultaat ervan meedelen 'in algemene bewoordingen'.[226] Het COC van zijn kant, dat zijn bevoegdheid als toezichthoudende autoriteit uitoefent in het domein van de politionele informatie waar ook een zekere vertrouwelijkheid vereist is, *mag*, in het kader van de indirecte uitoefening van hun rechten door de betrokkenen, "*bepaalde contextuele informatie verstrekken aan de betrokkene*".[227]

Het Vast Comité I beveelt de wetgever dan ook aan om in bepaalde gevallen te voorzien in de mogelijkheid van mededeling van bepaalde informatie aan de betrokkene op grond van Titel 3 van de GBW.

V.7.2. DE TOEPASSING VAN DE GEGEVENSBESCHERMINGSREGELS OP HET JUISTE MOMENT CONTROLEREN

Het Vast Comité I doet opmerken dat het kan worden gevat door personen die betrokken zijn of worden bij gerechtelijke of bestuurlijke, burgerlijke procedures (bijv. naturalisatie-procedure, ordemaatregelen…) waarbij analyses of gegevens van een inlichtingendienst of het OCAD centraal staan.

Het Comité is van mening dat de wetgever in dergelijke gevallen, wanneer geschillen in een contentieuze fase komen, zou kunnen overwegen dat de bevoegde

225 Artikel 80, lid 2 GBW; artikel 34, lid 6 W.Toezicht.

226 Artikel 34, lid 6 W.Toezicht.

227 Artikelen 42, lid 3, en 43, lid 3 GBW. Het blijft echter wachten op een koninklijk besluit dat moet bepalen welke categorieën van contextuele informatie mogen worden meegedeeld aan de betrokkene.

rechter, wanneer hij geconfronteerd wordt met een ernstige betwisting van de voor hem gebruikte gegevens, en indien hij dat nodig acht (en in voorkomend geval alleen op verzoek van de betrokkene), zijn zaak kan schorsen. De bevoegde rechter kan dit vervolgens via het wettelijk mechanisme van het type 'prejudiciële beslissing' voorleggen aan het Vast Comité I, opdat het Comité de nodige verificaties kan verrichten en advies kan uitbrengen.

V.7.3. DE GEZAMENLIJKE OF GELIJKTIJDIGE BEVOEGDHEDEN TUSSEN BTA'S BETER AFSTEMMEN

De wetgever heeft ervoor gekozen voornamelijk een organiek criterium te gebruiken in de wijze waarop hij het toepassingsgebied van de Belgische regels inzake gegevensbescherming evenals de bevoegdheden van de Belgische BTA heeft gedefinieerd. Vereenvoudigd kan worden gesteld dat het Controleorgaan op de politonele informatie bevoegd is ten aanzien van de geïntegreerde politie, de GBA ten aanzien van de private sector en het Vast Comité I ten aanzien van de VSSE en de ADIV.

Naast deze vrij duidelijke bevoegdheidsverdeling, heeft de wetgever ook voorzien in gezamenlijke bevoegdheden voor het Vast Comité I: deze hebben enerzijds betrekking op het OCAD (gezamenlijke bevoegdheid met het Vast Comité P),[228] en anderzijds op de gemeenschappelijke gegevensbanken (gezamenlijke bevoegdheid met het COC).[229] Dit leidt er soms toe dat eenzelfde vraag van een burger met betrekking tot de werking van het OCAD aanleiding geeft tot twee afzonderlijke verificaties: een eerste samen met het COC betreffende de rol van het OCAD in het kader van de gemeenschappelijke gegevensbanken, een tweede samen met het Vast Comité P betreffende de overige aspecten van de werking van het OCAD.

Er kan ook sprake zijn van gelijktijdige bevoegdheden, daar de bevoegdheid van elke toezichthoudende autoriteit afzonderlijk juridisch gezien exclusief is, maar in de praktijk ten minste gedeeltelijk op gelijktijdige wijze wordt uitgeoefend, zodat de ene autoriteit moeilijk zou kunnen handelen zonder de andere autoriteit (inzonderheid gelet op het risico dat een verwerkingsverantwoordelijke wordt onderworpen aan tegenstrijdige bevelen). De gelijktijdige visitatie van het COC en het Vast Comité I bij BELPIU is daarvan een voorbeeld (*supra* V.3.2.).

Deze gezamenlijke of gelijktijdige bevoegdheden vloeien voort uit het hybride karakter van de betrokken instellingen (OCAD, BELPIU) of informatiesystemen (gemeenschappelijke gegevensbanken en passagiersgegevensbanken), waarbij beide, zo nodig met een verschillende mate van verantwoordelijkheid, samenstellende entiteiten zijn die in beginsel onder de (organieke) bevoegdheid van de ene of de andere toezichthoudende autoriteit vallen.

---

228 Zie artikel 161 GBW evenals ondertitel 4 van titel 3 GBW.

229 Zie de artikelen 44/11/3bis tot 44/11/3quinquies/2 WPA.

Deze situatie illustreert dat een 'organische logica' van de toepassing van de gegevensbeschermingsregels ook een zekere complexiteit met zich meebrengt, en bijgevolg ook mogelijke administratieve lasten die een echte bron van inefficiëntie kunnen zijn. Met andere woorden, een organisch criterium is niet meer een wondermiddel dan een doelcriterium, dat de wetgever ook had kunnen gebruiken en dat hierna verder zal worden besproken.

Met het oog op de efficiëntie, beveelt het Vast Comité I het Parlement aan alleen duidelijke en exclusieve bevoegdheden aan de BTA's toe te kennen.

V.7.4. DE REGELS INZAKE GEGEVENSBESCHERMING DIE TOEPASSELIJK ZIJN OP DE BTA'S IN DE SECTOR VAN DE NATIONALE VEILIGHEID VERDUIDELIJKEN

Het was duidelijk de intentie van de wetgever dat Titel 3 van de GBW de sector van de nationale veiligheid (VSSE, OCAD, ADIV…) regelt alsook de regels inzake gegevensbescherming die toepasselijk zijn op deze sector op autonome en exclusieve wijze binnen deze titel bekrachtigt. Die regels worden vastgelegd op basis van de internationale norm die wordt gevormd door het Verdrag nr. 108 van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens en zijn Aanvullend Protocol, recentelijk gemoderniseerd in 'Verdrag 108+' (door België ondertekend op 10 oktober 2018 maar nog niet bekrachtigd).[230]

Ondertitel 6 van Titel 3 van de GBW met betrekking tot de regels inzake gegevensbescherming die inzonderheid van toepassing zijn op het Vast Comité I en de BIM-Commissie als verwerkingsverantwoordelijken, is bijzonder lacunair.

In dit verband beveelt het Vast Comité I aan dat de wetgever duidelijk bepaalt welke gegevensbeschermingsregeling van toepassing is op het Comité en de BIM-Commissie bij de uitoefening van hun taken op het gebied van de nationale veiligheid. Deze wettelijke regeling moet worden verankerd in Titel 3 van de GBW en moet worden aangepast aan de specifieke kenmerken van voornoemde instellingen. In dit opzicht kan de wetgever zich laten inspireren door de gegevensbeschermingsregels die van toepassing zijn op inlichtingen- en veiligheidsdiensten. Dit is de geest waarin de huidige Ondertitel 6 van Titel 3 van de GBW is opgesteld.

230 Zie in dit verband: https://www.coe.int/fr/web/data-protection/convention108-and-protocol. Gemoderniseerd verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, 128e Sessie van het Comité van de Ministers, Helsingør, Denemarken, 17-18 mei 2018.

V.7.5. HET VAST COMITÉ I DE MOGELIJKHEID BIEDEN OP EIGEN INITIATIEF ADVIEZEN UIT TE BRENGEN

De wetgever heeft voor het Comité niet in de mogelijkheid voorzien om adviezen op eigen initiatief uit te brengen, en dit in tegenstelling tot de mogelijkheden die worden geboden aan de GBA en het COC.[231] Tenzij de wetgever dat oplegt, kan het Vast Comité I enkel een advies uitbrengen wanneer het daartoe een verzoek ontvangt van de Kamer van volksvertegenwoordigers of van de bevoegde minister. Nochtans valt niet uit te sluiten dat het Vast Comité I in het kader van de uitoefening van zijn bevoegdheid op achterhaalde teksten of praktijken botst waarop het graag de aandacht zou vestigen door middel van een advies, en dit ongeacht of er al dan niet een wetgevingsproces mee gemoeid is.

V.7.6. EEN BETERE RECHTSZEKERHEID IN DE REGELING VAN GEGEVENSBESCHERMING DIE VAN TOEPASSING IS OP HET DOMEIN VAN DE NATIONALE VEILIGHEID

Het Belgisch recht inzake de bescherming van persoonsgegevens is op complexe wijze opgesteld en dit schaadt de leesbaarheid ervan. Het is nochtans een domein waar de helderheid van de teksten een Grondwettelijke en verdragsrechtelijke vereiste is.

Het Vast Comité I wenst in de eerste plaats te wijzen op het doorslaggevende karakter dat zijns inziens kan worden gegeven aan het doel van de gegevensverwerking bij het bepalen van de toepasselijke regels van gegevensbescherming. In het positief recht regelt de wetgever immers, althans gedeeltelijk, de bevoegdheid van de toezichthoudende autoriteit op basis van een organiek criterium. Het is de *finaliteit* van een gegevensverwerking die zou moeten bepalen of die verwerking al dan niet tot het toepassingsgebied behoort van een volledige Titel 3, wat betreft de nationale veiligheid, inzonderheid rekening gehouden met het feit dat naast de inlichtingendiensten nog andere actoren een rol spelen in het kader van de inlichtingencyclus.

In eenzelfde oogmerk van helderheid en rechtszekerheid merkt het Vast Comité I vervolgens op dat de criteria waarin is voorzien om de verwerkingsverantwoordelijke te identificeren, een bron van rechtsonzekerheid zijn. Voor het domein van de nationale veiligheid zou de wetgever in de GBW de (gezamenlijke) verwerkingsverantwoordelijke(n) kunnen identificeren[232] op basis van hun

231 Zie artikel 23, § 1 Wet GBA en artikel 236, § 2 GBW.

232 In het domein van de gemeenschappelijke gegevensbanken heeft de wetgever de verantwoordelijkheden bijvoorbeeld verdeeld tussen betrokken entiteiten, zie meer bepaald artikel 44/11/3bis WPA.

concrete verantwoordelijkheden ten opzichte van die opdrachten en hun relatieve autonomie, of zelfs onafhankelijkheid.

V.7.7. INTERNATIONALE DIMENSIE VAN DE GEGEVENSVERWERKINGEN

In de gezamenlijke verklaring van Bern[233] hebben het Vast Comité I en sommige van zijn homologe diensten gewezen op de beperkingen van hun respectieve *nationale* toezichtsmandaten. Vervolgens werd een *Charter of the Intelligence Oversight Working Group* aangenomen en werd een *Oversight Working Group* opgericht.[234]

Mutatis mutandis kan een soortgelijke vaststelling worden gemaakt in het kader van de bescherming van natuurlijke personen ten opzichte van de verwerking van persoonsgegevens.

In deze context vestigt het Vast Comité I de aandacht van de wetgever op de nakende bekrachtiging van het Verdrag 108+ dat een mechanisme voor samenwerking en wederzijdse bijstand tussen partijen invoert. In tegenstelling met de samenwerkingsmechanismen van het Europees recht (i.e. van de Europese Unie), zal dit internationale instrument betrekking hebben op de verwerkingen met de finaliteit van nationale veiligheid. Om dit mechanisme ten uitvoer te leggen, bepaalt artikel 16, 2., a) dat elke partij een of meerdere toezichthoudende autoriteiten in de betekenis van artikel 15 van het Verdrag 108+ dient aan te wijzen.

Vooralsnog bepaald de wetgever in artikel 55, § 1 van de GBA-wet wat volgt: "*De Gegevensbeschermingsautoriteit kan samenwerken met enige instantie of andere gegevensbeschermingsautoriteit van een andere staat door gebruik te maken van de bevoegdheden die haar zijn toegekend krachtens de Verordening 2016/679 of door de nationale wetgeving.*"

Gelet op de onafhankelijkheid van beide instellingen, i.e. de GBA en het Vast Comité I, als bevoegde toezichthoudende autoriteiten, vraagt het Comité aan de wetgever om na te denken over de mogelijkheid voor het Comité om, rekening gehouden met de regels die zijn activiteiten regelen (incl. de W.C&VM), te kunnen

233 'Versterking van het toezicht op de internationale gegevensuitwisselingen tussen de inlichtingen- en veiligheidsdiensten', 22 oktober 2018.

234 Zie https://www.comiteri.be/images/pdf/Charter_Intelligence_Oversight_Working_Group_signed_12_December_2019.pdf.

beschikken over een eigen bevoegdheid inzake internationale samenwerking in het domein van de gegevensbescherming in de inlichtingensector.[235]

Naast deze kwestie van internationale samenwerking als dusdanig, leidt de internationale dimensie van gegevensstromen *op het niveau van de Belgische diensten* ook tot een verlies van controle over de gegevens die het Belgisch rechtsgebied verlaten ten gevolge de grensoverschrijdende gegevensstroom.

Hoewel de wetgever er wat betreft dit punt niet voor heeft gekozen om het principe van '*accountability*' ('aansprakelijkheid') bindend te maken voor de inlichtingendiensten[236], is het Vast Comité I de mening toegedaan dat bepaalde wijzigingen van de regels betreffende de grensoverschrijdende gegevensstromen in de richting van een grotere '*accountability*' van de diensten, zouden kunnen leiden tot een versterking van de effectiviteit van de gegevensbescherming.

Het Comité onderstreept het belang voor dit onderdeel van de regels inzake gegevensbescherming. Er moet worden voorkomen dat persoonsgegevens, eenmaal doorgegeven door de Belgische inlichtingendiensten, volledig aan hun controle ontsnappen en ongerechtvaardigde (of niet langer gerechtvaardigde) gevolgen hebben voor de rechten en vrijheden van de betrokken personen in het buitenland. In een verbonden wereld waar individuen zich steeds vlotter en vrijer bewegen, moet de noodzaak om de gegevens bijvoorbeeld bij te werken, effectief kunnen worden toegepast in een internationale context. Kortom, de noodzaak om gegevens inzake nationale veiligheid op het internationale toneel uit te wisselen, gaat gepaard met de noodzaak om ook in deze context doeltreffende regels inzake gegevensbescherming voor de betrokkenen uit te werken.

---

235 In het 'Samenwerkingsprotocol voor samenwerking tussen de Belgische federale toezichthoudende autoriteiten op het vlak van dataprotectie' hebben de Vaste Comités I en P, het COC en de GBA opgemerkt dat "het elke A vrij staat – binnen het kader van haar specifieke bevoegdheden (bv. politie, inlichtingen- en veiligheidsdiensten, …) en onverminderd artikel 116 WOG – aan te sluiten bij of lid te worden van een bepaald(e) fora/instelling of documenten via de GBA op te vragen die aansluiten bij hun bevoegdheid", overweging nr. 36. Wanneer de W.Toezicht echter, in haar afdeling 4 van hoofdstuk III ('Toezicht op de inlichtingendiensten'), de bevoegdheden van het Vast Comité I regelt als gegevensbeschermingsautoriteit, voorziet ze niet in enige bevoegdheid van het Comité op internationaal vlak.

236 Over dit principe, zie meer bepaald de artikelen 5, 2. en 24, 1. AVG, evenals artikel 10, 1. van het Verdrag 108+.

HOOFDSTUK VI

DE CONTROLE VAN DE GEMEENSCHAPPELIJKE GEGEVENSBANKEN

In 2016 werd door de ministers van Binnenlandse Zaken en Justitie de gemeenschappelijke gegevensbank '*foreign terrorist fighters*' (GGB FTF) opgericht. De doelstelling ervan was bij te dragen tot de analyse, de evaluatie en de opvolging van personen met banden met deze problematiek. Deze gemeenschappelijke gegevensbank (GGB) werd in 2018 omgevormd: ze heet voortaan gemeenschappelijke gegevensbank '*terrorist fighters*' (GGB TF) en omvat naast de (bestaande) algemene categorie van de *'foreign terrorist fighters'* tevens een nieuwe categorie van '*homegrown terrorist fighters*'. Daarnaast werd in 2018 ook een aparte gemeenschappelijke gegevensbank opgericht voor '*haatpropagandisten*' (GGB HP).[237]

Bij Koninklijk besluit van eind 2019[238] werden nog twee bijkomende categoriën van personen in de GGB TF opgenomen, zijnde de 'potentieel gewelddadige extremisten' (PGE) en 'terrorisme-veroordeelden' (TV).

VI.1. DE BELANGRIJKSTE WIJZIGINGEN AAN DE REGELGEVING

Het Koninklijk besluit van 20 december 2019, gepubliceerd in januari 2020, beoogt een drieledig doel. Vooreerst worden nieuwe categorieën toegevoegd aan de gemeenschappeljke gegevensbank TF, te weten de 'potentieel gewelddadige extremisten' en de 'terrorisme-veroordeelden'. Daarnaast worden een aantal zogenaamde 'technische wijzigingen' aangebracht aan de KB's TF en HP tengevolge de wijziging van de Wet van 5 augustus 1992 door de Wet van 22 mei 2019. Ten slotte was het

237 Artikel 44/6 WPA wijst de controle op de verwerking van de in de GGB vervatte informatie en persoonsgegevens toe aan het Controleorgaan op de politionele informatie (COC) en aan het Vast Comité I (verder 'de toezichthoudende autoriteiten').

238 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.

opzet te voorzien in een directe toegang voor de Algemene administratie van de Thesaurie van de FOD Financiën tot de gegevensbanken TF en HP.

VI.1.1. DE TOEVOEGING VAN POTENTIEEL GEWELDDADIGE EXTREMISTEN (PGE) IN DE GGB TF

De 'potentieel gewelddadige extremist' wordt gedefinieerd als elke natuurlijke persoon die een aanknopingspunt heeft met België en voldoet aan onderstaande, cumulative criteria:

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

VI.1.2. DE TOEVOEGING VAN TERRORISME-VERVOORDEELDEN (TV) IN DE GGB TF

Naast 'potentieel gewelddadige extremisten', werd een tweede categorie toegevoegd in de GGB TF, te weten terrorisme-veroordeelden. Het betreft personen die voldoen aan onderstaande cumulatieve voorwaarden:

– ze hebben een aanknopingspunt met België ;
– ze werden veroordeeld of kregen een gerechtelijke beslissing tot internering, of in het geval van minderjarigen, die een beschermingsmaatregel kregen voor terroristische misdrijven zoals bepaald in Boek 2, Titel I Ter van het Strafwetboek (in België), of voor gelijkaardige inbreuken in het buitenland;

– en waarvan het niveau van dreiging dat van hen uitgaat door het OCAD wordt ingeschaald als gemiddeld (niveau 2), ernstig (niveau 3) of zeer ernstig (niveau 4).

Door de invoering van deze nieuwe categorie in de gegevensbank TF, worden alle actoren die een opvolging moeten verzekeren van terrorisme-veroordeelden (zoals DG EPI, Justitiehuizen, Politie, gesloten asielcentra, de VSSE, de Lokale *Task Forces*...) proactief, op tijd en volledig geïnformeerd over de betrokkenen.

VI.1.3. RECHTSTREEKSE TOEGANG TOT DE GGB TF EN HP VOOR EEN NIEUWE DIENST

Middels het KB van 20 december 2019 zag ook de Algemene administratie van de Thesaurie zich een rechtstreekse toegang toegekend tot de GGB TF en HP.[239] Het betreft *in casu* de bevoegde overheid op het vlak van financiële sancties door het bevriezen van tegoeden en economische middelen van personen of entiteiten die terroristische misdrijven plegen of pogen te plegen, ze vergemakkelijken of eraan meewerken.

VI.2. DE CONTROLEOPDRACHT EN HET VOORWERP VAN CONTROLE

Voor wat betreft 2020, 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.

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 het jaar 2020 te laten plaatsvinden. Verschillende diensten werden bevraagd, waaronder de NVO, het OCAD

239 Er dient te worden opgemerkt dat de toegang voor de Algemene adminstratie van de Thesaurie niet figureerde in het ontwerp KB noch in de bijkomende voorafgaandelijke aangifte dewelke werd voorgelegd aan het Vast Comité I en het COC.

(operationeel beheerder van de gemeenschappelijke gegevensbanken), de Federale Politie (technisch beheerder) en de *data protection officer* (DPO). Het onderzoek werd afgesloten met een vergadering met de waarnemend directeur van OCAD en de DPO van de gemeenschappelijke gegevensbanken. Het verslag werd ingepland voor de eerste helft van 2021.

VI.3. DE ADVIESOPDRACHT

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

Zo moeten de ministers van Binnenlandse Zaken en Justitie, voorafgaand aan de oprichting van een gemeenschappelijke gegevensbank alsook van de verwerkingsmodaliteiten, waaronder deze met betrekking tot de registratie van de gegevens en van de verschillende categorieën en types van persoonsgegevens en informatie die verwerkt worden, hiervan aangifte doen bij het Vast Comité I en het COC. Deze dienen op hun beurt een gezamenlijk een advies uit te brengen binnen de 30 dagen vanaf de ontvangst van de aangifte (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 2020 niet om een dergelijk advies verzocht.[240]

240 Een gemeenschappelijk advies werd verstrekt in 2019 aangaande het KB van 20 december 2019 en verscheen in het Belgisch Staatsblad op 27 januari 2020 (www.comiteri.be).

HOOFDSTUK VII
ADVIEZEN

Artikel 33, zevende lid, W.Toezicht bepaalt dat het Comité '*enkel op verzoek van de Kamer van volksvertegenwoordigers of van de bevoegde minister advies [mag] uitbrengen over een ontwerp van wet, van koninklijk besluit, van circulaire of over enig ander document waarin de beleidslijnen van de bevoegde ministers worden geformuleerd.*' In 2020 werd het Comité herhaaldelijk om advies verzocht.

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

VII.1. ADVIES BIJ HET WETSVOORSTEL TOT AUTOMATISCHE DECLASSIFICATIE EN DOORZENDING VAN STUKKEN NAAR HET RIJKSARCHIEF

In november 2019 werd een wetsvoorstel ingediend tot invoering van een algemene declassificatieregeling voor geclassificeerde stukken.[241] Het voorstel bepaalde op welke manier en onder welke omstandigheden geclassificeerde stukken moeten worden gedeclassificeerd. Daarmee wordt, aldus de auteurs, een belangrijke lacune opgevuld in de wetgeving op de classificatie, die grote gevolgen heeft voor het historisch onderzoek en voor de transparantie van de overheid. België blijkt immers een van de weinige West-Europese landen zonder declassificatieprocedure, waardoor geclassificeerde stukken altijd geclassificeerd blijven.

Bij het opstellen van een geclassificeerd stuk wordt in principe meteen ook het moment van declassificatie bepaald. Gedeclassificeerde stukken van de inlichtingendiensten zouden dan sneller naar het Rijksarchief worden overgebracht. Net als de inlichtingen- en veiligheidsdiensten, kon het Vast Comité I begin januari 2020 zijn advies over het wetsvoorstel in de Commissie Binnenlandse Zaken van de Kamer toelichten.[242]

---

241 *Parl. St.* Kamer 2019-2020, 55K0732/001.

242 Het volledige advies is beschikbaar op : www.comiteri.be

Het voorstel bevatte twee regelingen die weliswaar verband houden met elkaar, maar die ook duidelijk moeten worden onderscheiden: de automatische declassificatie en de doorzending van stukken naar het Rijksarchief. Beide regelingen staan in die zin los van elkaar dat de al dan niet archivering van informatie betrekking kan hebben op zowel geclassificeerde als op niet-geclassificeerde inlichtingen of omgekeerd, en dat de declassificatie van een stuk niet noodzakelijk betekent dat het mag worden gearchiveerd. Het is niet omdat het mogelijks niet meer gevoelig is, dat het niet meer nuttig is voor het inlichtingenwerk. Dit laatste aspect is ook zeer belangrijk om in herinnering te brengen: zolang een stuk nog nuttig is voor het inlichtingenwerk, kan er geen sprake zijn van een archivering in de zin van de Archiefwet, ook al is dat stuk ouder dan dertig jaar.

VII.1.1. AUTOMATISCHE DECLASSIFICATIE

In het verleden toonde het Comité zich reeds voorstander van een automatische declassificatie.[243] Wel hanteerde het Comité ruimere tijdsmarges dan het ingediende wetsvoorstel: voor een 'GEHEIM' stuk stelde het Comité een declassificatie voor na dertig jaar; voor een 'ZEER GEHEIM' stuk, na vijftig jaar. Die langere termijnen maken het voor de inlichtingendiensten iets meer werkbaar. Dit belet volgens het Comité niet dat de zogenaamde 'overheid van oorsprong' op verzoek of op eigen initiatief een stuk eerder zou kunnen declassificeren. Ook werd gesuggereerd te voorzien in een systeem waarbij het Vast Comité I wordt aangeduid als orgaan dat, op eigen initiatief of op verzoek, een classificatie zou kunnen *overrulen* indien ze manifest niet of niet langer beantwoordt aan de finaliteiten van een classificatie.[244] Alleszins mag aan het Comité alleen een marginale toetsingsbevoegdheid worden gegeven, te weten een beperkte controle over de vraag of de classificatie zelf of zijn duurtijd niet manifest onwettelijk of onredelijk is. Het Comité mag immers niet in de plaats treden van de uitvoerende macht en zelf een beleid ter zake voeren.

VII.1.2. ARCHIVERING

Het Comité benadrukte geen bijzondere opmerkingen te hebben bij het voorstel waarin wordt voorzien om documenten onder drie cumulatieve voorwaarden naar het Rijksarchief over te brengen: het betreft documenten gecreëerd ouder dan dertig jaar (in plaats van vijftig jaar), het gaat om niet-geclassificeerde stukken en ze hebben hun administratieve nut verloren.

---

243 VAST COMITE I, *Activiteitenverslag 2011*, 81 e.v.
244 VAST COMITE I, *Activiteitenverslag 2006*, 137.

Maar er zijn meer belangrijke kwesties. Zo hield het voorstel geen rekening met het bestaande juridische arsenaal in het kader van de bescherming van persoonsgegevens. Zowel wanneer het gaat om gegevens van targets, van gewone burgers of nog, van bronnen, vereisen deze voorgaande vragen een fundamenteel debat. Het Comité was dan ook van oordeel dat het wetsvoorstel rekening moest houden met achtereenvolgens artikel 21 van de Inlichtingenwet dat voorziet in een verplichte vernietiging van bepaalde persoonsgegevens, met een gelijkaardige bepaling uit de Classificatiewet met betrekking tot persoonsgegevens uit veiligheidsonderzoeken, met de verplichting om te allen tijde de bronnen van inlichtingendiensten te beschermen, maar zeker ook met de (nieuwe) regels inzake de verwerking van persoonsgegevens voor historische, wetenschappelijke of statistische doeleinden zoals opgenomen in de Gegevensbeschermingswet (artt. 99 GBW e.v.).

Ten slotte diende ook gekeken te worden in welke mate de voorgestelde regeling van declassificatie en archivering van gevoelige gegevens één logisch geheel vormt met de mogelijkheden geboden door de Wet op de openbaarheid van het bestuur (WOB). Het Comité legde in dat kader de nadruk op de invoering van een voldoende lange declassificatie-termijn, op de mogelijkheid tot '*overruling*' van een initiële of verlengde classificatie en op coherentie met voornoemde regelgeving.

VII.2. ADVIES BETREFFENDE HET 'VERSLAG VAN HET OVERLEGCOMITÉ BETREFFENDE HET INRICHTING VAN EEN KRUISPUNTBANK VEILIGHEID'

Begin februari 2020 bracht het Comité advies uit aan de minister van Justitie en aan de minister van Veiligheid en Binnenlandse Zaken aangaande het 'verslag van het overlegcomité betreffende het inrichten van een Kruispuntbank Veiligheid'.[245] Dat rapport bevatte enkele door de beleidsmakers te nemen grote oriëntaties inzake de door de Parlementaire Onderzoekscommissie 'Terroristische aanslagen' geïnitieerde 'Kruispuntbank Veiligheid'. De onderzoekscommissie was immers de mening toegedaan dat er dringend nood was aan een globale visie en strategie voor het geïntegreerd inrichten en organiseren van de informatiehuishouding, alsook aan loyale samenwerking tussen alle betrokken politie-, justitie-, inlichtingen- en veiligheidsdiensten.[246]

Voorgesteld werd om binnen de veiligheidsarchitectuur gebruik te maken van het systeem van een kruispuntbank als instrument voor een geïntegreerd gegevensbeheer en coördinatie tussen de verschillende diensten en instanties. Deze kruispuntbank – naar het voorbeeld van de kruispuntbank Sociale Zekerheid en

---

245 De adviesaanvraag dateerde van 24 oktober 2019. Het onderwerp van aanvraag betrof een rapport/verslag van het 'overlegcomité' en was als dusdanig geen regelgevende tekst of tekst met normatieve draagwijdte.

246 *Parl. St.* Kamer 2016-2017, 54K1752/008, 251.

van het *e-health platform* - moet een efficiënt systeem van veilige elektronische gegevensdeling tussen (bestaande) elektronische gegevensbanken, die onder de verantwoordelijkheid van verschillende instantie vallen, vormen.[247]

Het Comité was in zijn advies van oordeel dat dit project alleen zal kunnen uitgevoerd worden indien daartoe de noodzakelijke financiële, technologische en menselijke investeringen op duurzame wijze worden gegarandeerd en zonder dat de beperkte budgetten van de inlichtingendiensten daarbij in het gedrang komen. De creatie van een dergelijke kruispuntbank moet daarbij beantwoorden aan een dubbele garantie: enerzijds dient een systeem te worden ingevoerd dat een doeltreffend antwoord biedt op de vóór de aanslagen in Zaventem en Maalbeek vastgestelde problemen inzake informatiebeheer (opslag, verwerking en gebruik) en uitwisseling van deze informatie; anderzijds dient te worden voldaan aan de noden tot bescherming van de fundamentele rechten en vrijheden, de bescherming van persoonsgegevens alsook het waarborgen van andere essentiële belangen, zoals de regel van de derde dienst en de classificatienormen.

VII.3. ADVIES BIJ HET WETSVOORSTEL MET HET OOG OP HET INVOEREN VAN WEGINGSNOTITIES VOOR DE SAMENWERKING MET BUITENLANDSE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

Het wettelijk kader voor (inter)nationale samenwerking en uitwisseling van informatie wordt in hoofdorde gevormd door de artikelen 19, eerste lid en 20 § 3 W.I&V. Artikel 19, eerste lid W.I&V regelt de algemene bevoegdheid tot mededeling en doorgifte van inlichtingen aan derde instanties.[248] De wetgever zelf was in 1998 echter de mening toebedeeld dat betrokken regeling onvoldoende was. Daarom schrijft artikel 20 §3 W.I&V voor dat de Nationale Veiligheidsraad (NVR), onder meer, de internationale samenwerking en informatie-uitwisseling

247 De bedoeling bestaat er niet in om bestaande gegevensbanken te dupliceren of te centraliseren, maar wel om de relevante informatie beschikbaar in de onderscheiden gegevensbanken op een geïntegreerde, efficiënte en veilige wijze te delen.

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

verder moet uitwerken. Via de Richtlijn van 30 september 2016 heeft de Nationale Veiligheidsraad aan deze wettelijke plicht (deels) voldaan.[249]

Halfweg juni 2020 werd het Vast Comité I door de Voorzitter van de Commissie voor Binnenlandse Zaken, Veiligheid, Migratie en Bestuurszaken van de Kamer van volksvertegenwoordigers gevraagd zijn advies te verlenen bij het wetsvoorstel tot wijziging van de Wet van 30 november 1998 houdende regeling van inlichtingen- en veiligheidsdiensten met het oog op het invoeren van wegingsnotities voor de samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten.[250]

Het wetsvoorstel strekt ertoe de samenwerking van de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichting en Veiligheid (ADIV) met inlichtingen- en veiligheidsdiensten van andere landen te voorzien van een formeel juridische grondslag. Centraal staat de weging van het belang van de samenwerkingsrelatie versus de risico's ervan. De weging van de risico's wordt vastgelegd in een zogenaamde 'wegingsnotitie', die de grondslag vormt waarop de samenwerking van de diensten berust. Niet alleen nieuwe, maar ook bestaande samenwerkingsrelaties die worden voortgezet, hebben een dergelijk juridisch fundament nodig.

Het Vast Comité I kon het wetsvoorstel alleen maar toejuichen; reeds meerdere jaren houdt het Comité immers een pleidooi voor een wettelijke regeling van de internationale samenwerking van de Belgische inlichtingen- en veiligheidsdiensten.[251] Het Comité formuleerde dan ook een bijzonder omstandig advies.[252] In de gevallen dat een tekstuele verduidelijking van het wetsvoorstel een meerwaarde kon bieden voor de rechtsbescherming van de burger of voor de praktische toepassing van de regeling door de inlichtingen- en veiligheidsdiensten werden voorstellen van tekstaanpassing toegevoegd.

---

249 De Richtlijn van 30 september 2016 van de Nationale Veiligheidsraad 'aangaande de relaties van de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichtingen en Veiligheid (ADIV) met buitenlandse inlichtingendiensten'. Er werd geopteerd om deze (kwaliteitsvolle) NVR-richtlijn te classificeren (niveau Vertrouwelijk). Het Comité begrijpt niet waarom dit document dient geclassificeerd te worden. Het betrokken document bevat geen operationele gegevens, noch operationele methodologieën, noch andersoortige gevoelige gegevens. Te meer omdat de NVR-richtlijn een onderdeel vormt van het juridisch toetsingskader voor het internationaal handelen van de inlichtingen- en veiligheidsdiensten, zijn er volgens het Comité geen redenen om een dergelijk document blijvend te classificeren. De vraag rees eveneens of deze richtlijn aangepast en geactualiseerd moet worden ten gevolge van de inwerkingtreding van de Gegevensbeschermingswet van 30 juli 2018. Aangezien de betrokken NVR-richtlijn niet het voorwerp van het advies uitmaakte, werd hier niet dieper op ingegaan.

250 *Parl. St.* Kamer 2019-20, DOC 55K0956/001. Het advies van het Comité werd eind augustus verstuurd aan de Voorzitter van de Commissie voor Binnenlandse Zaken van de Kamer van volksvertegenwoordigers Het voorstel was bij het afsluiten van het activiteitenrapport nog hangende in de Kamer.

251 Vast Comité I, *Activiteitenverslag 1997,* 168; Vast Comité I, Activiteitenverslag 2007, 53; Vast Comité I, *Activiteitenverslag 2008*, 109-110; Vast Comité I, Activiteitenverslag 2009, 4, 106-107; Vast Comité I, *Activiteitenverslag 2012*, 2 en 95; en Vast Comité I, Activiteitenverslag 2016, 119.

252 Voor het integrale advies en de gecoördineerde tekstvoorstellen wordt verwezen naar www.comiteri.be

Indien het wetsvoorstel door het parlement wordt goedgekeurd, behoeft betrokken NVR-richtlijn een aanpassing en actualisering. Het Comité was niettemin van oordeel dat het wetsvoorstel en de NVR-richtlijn naast elkaar kunnen bestaan, mits de richtlijn als juridisch ondergeschikte rechtsnorm op een aantal punten wordt gewijzigd.

VII.4. BRUSSEL PREVENTIE & VEILIGHEID, DE TOEGANG TOT DE GEMEENSCHAPPELIJKE GEGEVENSBANK TERRORIST FIGHTERS EN DE MEDEDELING VAN LIJSTEN AAN DERDEN

In een juridische analyse beantwoordde het Vast Comité I de vraag om advies van de Begeleidingscommissie[253] rond de mededeling van informatie uit de gemeenschappelijke gegevensbank *Terrorist Fighters* (GGB TF) aan de dienst Brussel Preventie & Veiligheid (BPV), een instelling van openbaar nut (ION).[254] Het Comité deed daarbij opmerken dat er een onderscheid diende gemaakt te worden tussen de (rechtstreekse of onrechtstreekse) toegang tot de GGB TF enerzijds en de mededeling van lijsten aan derden (d.w.z. degenen die geen toegang hebben tot de GGB TF) anderzijds.

VII.4.1. (ON)RECHTSTREEKSE TOEGANG TOT DE GGB TF

Artikel 7 van het koninklijk besluit van 21 juli 2016 betreffende de gegevensbank *terrorist fighters* (KB TF)[255] voorziet in een gradatie van de toegangen tot de gegevensbanken: rechtstreekse toegang voor de zogenaamde basisdiensten (waaronder de inlichtingen- en veiligheidsdiensten) alsook sommige partnerdiensten (waaronder het Openbaar Ministerie) en een rechtstreekse toegang voor een aantal andere diensten, evenwel beperkt tot gegevens over de TF in het kader van de hen toegekende opdrachten (bijv. gerechtelijke begeleiding en toezicht).

253 Vraag van de Parlementaire Begeleidingscommissie d.d. 3 juni 2020.

254 Brussel Preventie & Veiligheid (BPV), opgericht bij Ordonantie van 28 mei 2015 (*BS* 10 juni 2015) coördineert enerzijds de preventie en veiligheid in het Brussels Hoofdstedelijk Gewest en ondersteunt anderzijds alle betrokken veiligheidsactoren om de veiligheid van de inwoners en bezoekers van het Gewest te verzekeren (www.bps-bpv.brussels/nl/home-nl).

255 Koninklijk besluit van 21 juli 2016 betreffende de gegevensbank terrorist fighters, *BS* 22 september 2016.

Artikel 44/11/3*ter*, § 3 WPA laat een uitbreiding toe tot andere diensten[256], en dit door middel van een koninklijk besluit, beraadslaagd in de ministerraad, na advies van het Vast Comité I en het COC.

Begin augustus 2019 brachten het COC en het Vast Comité I een advies[257] uit over een ontwerp van KB tot wijziging van het KB TF. Een van de elementen van het ontwerp betrof de toekenning van het recht tot rechtstreekse bevraging[258] van de GGB TF door Brussel Preventie & Veiligheid. Het was voor beide toezichtinstanties evenwel volstrekt onduidelijk in welk verband deze instelling als een partnerdienst werd aangeduid. In de aan de BPV wettelijk toegekende opdracht kon allerminst een (duidelijke) opdracht in de strafrechtketen of bescherming van de openbare veiligheid worden gelezen. Het was, aldus het Comité en het COC, dan ook niet aanvaardbaar *"dat een nieuwe instelling aan de reeds bestaande uitgebreide lijst van ontvangers van zeer privacygevoelige gegevens wordt toegevoegd zonder dat de pertinentie en de maatschappelijke meerwaarde ervan wordt aangetoond."*

Brussel Preventie & Veiligheid werd dan ook niet opgenomen als begunstigde dienst in het KB.

VII.4.2. DE MEDEDELING VAN LIJSTEN AAN DERDE INSTANTIES

De extractie en mededeling van lijsten worden dan weer geregeld in artikel 11, §2 KB TF. De extractie is alleen toegestaan voor diensten die rechtstreeks toegang hebben, de mededeling van lijsten is niet toegestaan, behalve onder een aantal cumulatieve modaliteiten.[259] [260]

Sinds 2017 konden het COC en het Vast Comité I vaststellen dat er toch lijsten aan BPV worden meegedeeld. Dat werd bevestigd in 2019 :

---

256 Andere Belgische openbare overheden, andere openbare organen of organismen of andere organen of organismen van openbaar nut aanwijzen die door de wet belast zijn met de toepassing van de strafwet of die wettelijke opdrachten van openbare veiligheid hebben, die, wanneer zij belast zijn met bevoegdheden in de domeinen die voorzien zijn in artikel 44/2, § 2, op basis van de behoefte om te kennen, onder meer op strategisch, tactisch of operationeel vlak een toegang kunnen hebben tot de gemeenschappelijke gegevensbanken.

257 Advies 001/CPR-C.O.C/2019 van 1 augustus 2019 (www.comiteri.be)

258 Onder de vorm van een « hit/no hit ».

259 Als daar zijn : de doorgifte wordt uitgevoerd door een basisdienst; dit gebeurt na een evaluatie door de beheerder (federale politie), de operationeel verantwoordelijke (OCAD) en de (andere) basisdiensten (lokale politie en inlichtingendiensten; de bestemmeling is een overheidsinstantie of een openbare dienst ; het doel van de lijst valt binnen de wettelijke opdracht van de bestemmeling…

260 Artikel 44/11/3*quater* WPA laat de mededeling van lijsten aan een derde instantie of entiteit toe onder een dubbele voorwaarde: enerzijds de naleving van de modaliteiten vastgelegd bij koninklijk besluit en anderzijds een gezamenlijke evaluatie door de geïntegreerde politie, het OCAD en de inlichtingendiensten.

« (…) Blijkens de informatie die het OCAD d.d. 6 februari 2020 heeft bezorgd, bestaat de praktijk er thans in dat een lijst van de persoonsgegevens en informatie in de GGB TF en HP per e-mail maandelijks wordt doorgegeven aan onder meer de FOD Werkgelegenheid, het FANC en Brussel Preventie & Veiligheid.[…] [H]et is dan des te bedenkelijker dat diezelfde instelling zonder een duidelijke evaluatie of mededeling van voorwaarden van mededeling, is opgenomen in een extensieve mailinglijst die indruist tegen de afbakening van doorgifte van politiegegevens, zoals geëxpliciteerd in de WPA. »

VII.3.3. CONCLUSIES

Het Vast Comité stelde dan ook dat :

— indien de Regering wenste dat Brussel Preventie & Veiligheid toegang kreeg tot de gemeenschappelijke gegevensbanken, daartoe een koninklijk besluit moest worden opgesteld dat vergezeld gaat van een gedetailleerd Verslag aan de Koning.[261]

— Indien de regering wou dat BPV voordeel bleef hebben van de door het OCAD verstrekte lijsten, herhaalde het Vast Comité I de (samen met het COC) gedane aanbevelingen en verzocht het de bevoegde autoriteiten onverwijld alle aanbevolen maatregelen te nemen.

Het Comité stelde tot slot dat in de tussentijd het OCAD belast was met de naleving en handhaving van de wettelijke voorschriften.

---

261 Overeenkomstig artikel 44/11/3*ter* § 3 WPA, moet dit ontwerp van KB voor advies voorgelegd worden aan het C.O.C. en het Vast Comité I. Vervolgens moet de verklaring van behandeling als bedoeld in artikel 44/11/3*bis*, § 3 WPA, indien nodig, worden ingevuld.

HOOFDSTUK VIII

DE OPSPORINGS- EN GERECHTELIJKE ONDERZOEKEN

Naast zijn medewerking aan de toezichtonderzoeken, voert de Dienst Enquêtes I van het Comité ook onderzoeken naar leden van de inlichtingendiensten die verdacht worden van een misdaad en/of wanbedrijf.[262] Dit doet de enquêtedienst in opdracht van de gerechtelijke overheden. Deze bevoegdheid staat omschreven in artikel 40, derde lid van de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse. Met de Wet van 10 juli 2006 betreffende de analyse van de dreiging werd deze bevoegdheid uitgebreid tot misdaden of wanbedrijven gepleegd door de leden van het Coördinatieorgaan voor de dreigingsanalyse (OCAD).[263]

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).

---

262 Met een schrijven van 13 januari 2020 gericht aan het College van Procureurs-generaal bracht de Voorzitter van het Vast Comité I de toepassing van art. 38 W.Toezicht alsook de COL 8/2014 (versie van 11 januari 2018) in herinnering. Daarin wordt onder meer gesteld dat ambtshalve een kopie dient te worden verstuurd naar het Comité van de vonnissen en arresten betreffende misdaden en wanbedrijven begaan door leden van inlichtingendiensten of het OCAD.

263 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).

Ook in 2020 voerde de Dienst Enquêtes I onderzoeksdaden uit in het kader van zijn gerechtelijke opdracht, meer bepaald in drie opsporingsonderzoeken. In totaal werden 25 processen-verbaal opgesteld.

Op vraag van de onderzoeksrechter te Charleroi en onder leiding van het Federaal Parket verrichtte de Dienst Enquêtes I een aantal onderzoeksdaden in het kader van een onderzoek naar misdrijven die door een criminele bende gepleegd werden en naar de vraag of de inlichtingendiensten eventueel over informatie desbetreffende beschikten.

Op vraag van een onderzoeksrechter werd een onderzoek gevoerd naar een medewerker van een inlichtingendienst. Deze zou onder valse voorwendselen contact hebben opgenomen met de Federale Politie, om vervolgens de bekomen informatie door te sluizen aan personen nauw betrokken in het criminele milieu.

Naar aanleiding van een klacht neergelegd bij het Vast Comité I door een medewerker van een inlichtingendienst inzake 'enkele professionele aangelegenheden', besloot de Dienst Enquêtes I een proces-verbaal op te stellen (art. 29 Sv.) en aldus de gerechtelijke overheden in te lichten van mogelijke strafrechtelijke inbreuken vanwege één of meerdere leden van een inlichtingdienst. In dat kader volgde in 2020 enkele opdrachten voor de Dienst Enquêtes I.

Ten slotte verzocht een Brusselse onderzoeksrechter in het kader van een onderzoek naar spionage de Dienst Enquêtes I om advies. Hierop volgend besloot de onderzoeksrechter dat het onderzoek zou worden uitgevoerd door de Federale Politie, hierin gesteund door de Dienst Enquêtes I. Er werden in dat kader evenwel nog geen onderzoeksdaden verricht.

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 2020 geen meldingen in die zin.

HOOFDSTUK IX
EXPERTISE EN EXTERNE CONTACTEN

IX.1. COLLOQUIUM NAAR AANLEIDING VAN TIEN JAAR BIM-WET

De zogenaamde 'BIM-Wet' vierde in 2020 haar tiende verjaardag en dit verdiende de onverdeelde aandacht. Sinds de Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten kunnen de VSSE en de ADIV gebruik maken van de zogenaamde 'bijzondere inlichtingenmethoden'. Toen de wetgever in 2010 besloot de inlichtingendiensten nieuwe bevoegdheden te geven, werd ook een belangrijke taak toevertrouwd aan het Vast Comité I: het moest, samen met de BIM-Commissie toezien op de uitvoering van de specifieke en uitzonderlijke inlichtingenmethoden, die per definitie zeer ingrijpend zijn op het vlak van de individuele rechten en vrijheden.

Het Vast Comité I achtte het aangewezen om een decennium na de invoegetreding van de BIM-Wet een kritische evaluatie op te maken en, samen met specialisten ter zake, een blik in de toekomst te werpen.

Daartoe werd, onder auspiciën van de Kamer van volksvertegenwoordigers, op 31 januari 2020 het colloquium *'Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulière de renseignement: de l'ombre à la lumière'* voor de brede inlichtingenwereld georganiseerd. Onder meer de Kamervoorzitter, de minister van Justitie, vertegenwoordigers van de ADIV en de VSSE, mensenrechteninstellingen, de media en de advocatuur, maar ook academici en toezichthouders namen er, ieder vanuit hun ervaring, expertise en interesse, het woord. Ook de *United Nations Special Rapporteur for the Protection and Promotion of Human Rights while Countering Terrorism* mocht niet op het appèl ontbreken.

Het verslagboek[264] met een weergave van de uiteenzettingen, werd voor de gelegenheid aangevuld met enkele internationale bijdragen vanuit Nederland, Zwitserland en Frankrijk.

---

[264] J. VANDERBORGHT (ed.), *Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulières de renseignement: de l'ombre à la lumière*, Lefebvre Sarrut Belgium, Brussel, 2020, 151 p.

IX.2. SAMENWERKINGSPROTOCOL MENSENRECHTENINSTELLINGEN

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.[265] De creatie van een nationaal mensenrechteninstituut, een engagement dat werd aangegaan bij de ondertekening van het Protocol bij het VN-verdrag tegen foltering, liet lang op zich wachten.

In tussentijd werden op recurrente tijdstippen vergaderingen – en omwille van de strikte coronamaatregelen eveneens videoconferences – georganiseerd met diverse instellingen met een mandaat op het gebied van mensenrechten.[266] Middels een samenwerkingsprotocol[267] kwamen alle deelnemende instanties overeen om praktijken en methoden uit te wisselen, om gemeenschappelijke kwesties te onderzoeken en om de onderlinge samenwerking te bevorderen. Zo was er onder meer aandacht voor de circulaire 'geweld tegen politie', de *facial recognition* voor politiediensten en het gebruik van de *bodycam*, maar ook COVD-19 gerelateerde bekommernissen en aandachtspunten zoals de camera's aan de kust en in steden voor druktemeting, de *contact tracing app*, het gebruik van geanonimiseerde telecomdata voor de inschatting van de mobiliteit… vormden voorwerp van overleg. De inhoudelijke inbreng van het Vast Comité I in deze is bijzonder beperkt.

Ondertussen werd het nieuw opgerichte instituut diverse opdrachten toegekend: zo verstrekt het op verzoek of op eigen initiatief adviezen en aanbevelingen betreffende aangelegenheden die verband houden met de bevordering en de bescherming van de fundamentele rechten, volgt het de tenuitvoerlegging op van de internationale verplichtingen die door de Belgische overheden werden aangegaan en stimuleert het de bekrachtiging van nieuwe internationale mensenrechten instrumenten. In 2020 werd door de Kamer een raad van bestuur samengesteld door de benoeming van twaalf onafhankelijke personen uit de academische en gerechtelijke wereld, uit het maatschappelijk middenveld en van de sociale partners.

Het Vast Comité I participeerde aan het onderzoek van de studenten van de Legal Clinic Mensenrechten en Migratierecht van de UGent over de bevoegdheden van dat nieuwe Federale Instituut voor de bescherming en de bevordering van de rechten van de mens.[268]

---

265 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.

266 Zoals het Unia, het Federaal Migratiecentrum, het Instituut voor de gelijkheid van vrouwen en mannen, de Gegevensbeschermingsautoriteit, de federale Ombudsman, de Hoge Raad voor Justitie, de Vaste Comités I en P. De fakkel van het voorzitterschap werd in 2021 door Unia doorgegeven aan het Steunpunt Armoedebestrijding.

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

268 J. BREMS et al., *De bevoegdheden van het Federaal Instituut voor de Rechten van de Mens*, Legal Clinic Mensenrechten en Migratierecht, UGent, 2020-2021.

IX.3. EEN MULTINATIONAAL INITIATIEF INZAKE INTERNATIONALE INFORMATIE-UITWISSELING

Uiteraard brengt de niet af te wenden toegenomen internationale gegevensuitwisseling tussen inlichtingen- en veiligheidsdiensten uitdagingen mee voor de nationale toezichtorganen. De toezichtorganen van (oorspronkelijk) vijf Europese landen (België, Denemarken, Nederland, Noorwegen[269] en Zwitserland)[270] werken daarom sinds enkele jaren samen 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 försvarunderättelse-verksamhet (SIUN))*, de *Swedish Board of Inventions (Statens uppfinnarnämnd, (SUN))* en de Duitse *G10 Commission*.

Tengevolge de invoege getreden beperkingen omwille van COVID-19, bleven de internationale activiteiten in 2020 bijzonder beperkt. Halfweg januari 2020 – en dus net voor de COVID-19 pandemie toesloeg — vond in Oslo (Noorwegen) nog een *expert meeting* plaats met vertegenwoordigers van de diverse toezichthouders, waarbij methoden, *best practices*, juridische en praktische problemen werden besproken en ervaringen uitgewisseld. Onder meer thema's als '*tools for log analysis*', de organisatie van het toezicht op *bulk collection* en de mogelijkheid tot het delen van informatie tussen de verschillende deelnemende toezichthouders… waren aan de orde. Het Vast Comité I gaf ook toelichting bij 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 voor het vierde kwartaal van 2021.

Ook de eerstvolgende meeting die zou plaatsvinden in Bern (Zwitserland), werd om bovenvernoemde reden tot nader order uitgesteld.

De Nederlandse Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten nam op zijn beurt het initiatief om de regels die worden vastgelegd op basis van de internationale norm die wordt gevormd door het Verdrag nr. 108 van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens en zijn Aanvullend Protocol, recentelijk gemoderniseerd in 'Verdrag 108+' (door België ondertekend op 10 oktober 2018

---

269 De Noorse toezichthouder bracht de vergadering op de hoogte van de nieuwe *Intelligence Service Act* voor de Noorse inlichtingendienst. Deze vervangt de wet uit 1998 en trad in voege op 1 januari 2021. In de wet is er bijzondere aandacht voor de '*bulk collection of metadata that crosses Norwegian borders*'.

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

maar nog niet bekrachtigd)[271] aan een studie te onderwerpen en verzocht daarbij om *input* van de overige toezichthouders.

IX.4. CONTACTEN MET BUITENLANDSE TOEZICHTHOUDERS

Sinds 2018 worden er opnieuw jaarlijkse conferenties voor nationale toezichthouders georganiseerd. Na de eerste conferentie in Parijs in 2018 – in een organisatie van de Franse CNCTR en het Vast Comité I – vond de tweede conferentie in december 2019 plaats in Den Haag. In 2020 zou de *European Intelligence Oversight Conference* in Rome te gast zijn bij de Italiaanse toezichthouder, de *Procura Generale della Corte di Cassazione*. De conferentie, die moest worden afgelast, zal uiteindelijk plaatsvinden in oktober 2021. Delegaties van de CTIVD, de CNCTR en IPCO brachten vooralsnog in juli 2020 een bezoek aan de Italiaanse toezichthouder om de planning en het programma van de komende conferentie te bespreken.

In het verlengde van de *European Intelligence Oversight Conference 2019* in Den Haag, bereidde de Franse *Commission nationale de contrôle des techniques de renseignement* (CNCTR) een vragenlijst over '*ex ante oversight*' voor. De toezichthouders uit alle deelnemende landen werden verzocht deze vragenlijst te beantwoorden. Met dit initiatief wordt beoogd de kennis van de in Europa toegepaste beste praktijken op het gebied van *ex ante* toezicht te verbeteren. Het opzet bestond erin de vragenlijst als basis te laten dienen voor de bespreking en uitwisseling van ervaringen tijdens de volgende bijeenkomst. Het Vast Comité I leverde, in nauwe samenwerking met de BIM-Commissie, zijn antwoorden op deze vragenlijst in. In juli 2020 lanceerde de Nederlandse toezichthouder CTIVD een gelijkaardig initiatief. Het betrof een vragenlijst over *complaint handling* (klachtenbehandeling). Het doel van dit initiatief is gelijklopend (*supra*): de beste praktijken in Europa op het gebied van klachtenbehandeling verzamelen en analyseren met de betrachting deze vervolgens te kunnen verbeteren. Beide initiatieven dienden evenwel *on hold* te worden gezet.

Vanuit het Bulgaarse *National Special Intelligence Devices Control Bureau* ten slotte werd in maart 2020 een project opgezet '*for strenghtening the capacities of the oversight bodies to protect the rights and freedoms of citizens against unlawful use of special intelligence devices*'. Vooralsnog werd hier geen verder gevolg aan gegeven.

---

271 Zie in dit verband: https://www.coe.int/fr/web/data-protection/convention108-and-protocol. Gemoderniseerd verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, 128e Sessie van het Comité van de Ministers, Helsingør, Denemarken, 17-18 mei 2018.

HOOFDSTUK X

HET BEROEPSORGAAN INZAKE VEILIGHEIDSMACHTIGINGEN, -ATTESTEN EN -ADVIEZEN[272]

X.1. INLEIDING

Het Beroepsorgaan is het administratief rechtscollege bevoegd voor geschillen die betrekking hebben op administratieve beslissingen in vier domeinen: de veiligheidsmachtigingen, de veiligheidsattesten die toegang moeten verlenen tot plaatsen waar zich geclassificeerde documenten bevinden, de veiligheidsattesten die toegang moeten verlenen tot welbepaalde plaatsen waar zich een dreiging voordoet en, tot slot, de veiligheidsadviezen. Daarnaast kan het Beroepsorgaan ook optreden als 'annulatierechter' tegen beslissingen van publieke of administratieve overheden om in een bepaalde sector, voor een bepaalde plaats of voor een bepaald evenement veiligheidsattesten of -adviezen aan te vragen.[273]

Het Beroepsorgaan is samengesteld uit de voorzitters van het Vast Comité I, het Vast Comité P en van de Geschillenkamer van de Gegevensbeschermingsautoriteit. Als ze verhinderd zijn, kunnen de drie voorzitters worden vervangen door een effectief lid-raadsheer van de instelling waartoe de betrokken voorzitter behoort.

De voorzitter van het Vast Comité I neemt het voorzitterschap van het Beroepsorgaan waar. De griffiefunctie 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 collegiale samenstelling van het Beroepsorgaan levert bovendien een multidisciplinaire bijdrage aan de beraadslaging betreffende elk dossier.

De werking van het Beroepsorgaan is integraal ten laste van het Vast Comité I. Het gaat daarbij enerzijds om de terbeschikkingstelling van de voorzitter en zijn plaatsvervangende leden en de griffier, maar ook de juristen als '*toegevoegde griffiers*'

---

272 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.

273 Voor meer informatie, zie VAST COMITÉ I, *Activiteitenverslag 2006*, 87-120 en VAST COMITÉ I, *Activiteitenverslag 2018*, 111-124.

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. In tegenstelling met het Vast Comité I en het Vast Comité P geniet het Beroepsorgaan geen portvrijdom, ook al verstuurt het al zijn zendingen per aangetekend schrijven met ontvangstbewijs.

Over de beslissingen wordt op collegiale wijze beraadslaagd.

Kenmerkend voor dit orgaan is het feit dat het geen kosten aanrekent. In tegenstelling tot de meeste andere administratieve rechtscolleges of rechtscolleges van de gerechtelijke orde hoeft er niet te worden betaald voor de indiening van een verzoekschrift. Bovendien wordt de partij die haar geschil verliest krachtens de wet niet veroordeeld tot de betaling van welke kosten ook.

Tot slot werd in 2020 de website van het administratief rechtscollege gecreëerd, namelijk www.beroepsorgaan.be. De website wil voor burgers, rechtsonderhorigen en advocaten noodzakelijke en nuttige informatie ter beschikking stellen met het oog op het instellen van een vordering en het voeren van een proces voor het collegiaal rechtscollege.

X.2. EEN JURISDICTIE GECONFRONTEERD MET DE PANDEMIE

De COVID-19-pandemie heeft een impact op de werking van het Beroepsorgaan. Naast de problemen van *lockdown* vanaf de maand maart 2020 hebben problemen bij de post tot gevolg dat aangetekende zendingen van de verzoekers of bepaalde dossiers niet meer aankwamen bij de griffie. Tussen 13 maart en 27 mei 2020 zag het Beroepsorgaan zich gedwongen een aantal zittingen te annuleren als gevolg van de *lockdown*, daar de zittingzaal niet toegankelijk was door de sluiting van de gebouwen van de Kamer van Volksvertegenwoordigers.

Teneinde de goede werking van de openbare rechtsbedeling te garanderen en geen achterstand te creëren, heeft het Beroepsorgaan het aantal zittingen na de *lockdown* echter sterk verhoogd. Gemiddeld hield het orgaan meer dan drie zittingen per maand in juni, juli, september en oktober 2020, in plaats van de twee zittingen per maand in normale tijden.

X.3. EEN BIJ WIJLEN ZWARE EN COMPLEXE PROCEDURE

Niettegenstaande de daling van het aantal beroepen dat in 2020 werd ingediend (van 196 in 2019 tot 144 in 2020), blijkt dat het aantal in 2020 verleende beslissingen is gestegen (van 166 in 2019 tot 176 in 2020) (*infra*). Het Beroepsorgaan komt

opnieuw tot de vaststelling dat zijn werklast is toegenomen. Het administratief beheer van de dossiers, de zittingen en de beslissingen wordt immers complexer. De voorbereiding van de dossiers van deze beroepsinstantie vergt capaciteiten die thans ontoereikend zijn. In de toekomst zou het wenselijk zijn over meer personeel te beschikken om bepaalde taken uit te voeren, ten einde een betere werking van het rechtscollege te garanderen.

Het Beroepsorgaan vestigt de aandacht op volgende problemen:

- De niet-naleving van de wettelijke termijn voor doorgifte van het administratief dossier door de veiligheidsoverheid aan het Beroepsorgaan. Zo wordt het voor het Beroepsorgaan onmogelijk om de termijn waarin het een beslissing moet nemen, te respecteren.
- De administratieve dossiers die door de diverse veiligheidsoverheden worden toegezonden, blijken niet steeds volledig. De griffie dient dan bijkomende handelingen te stellen of het rechtscollege neemt beslissingen alvorens recht te doen wat betreft de grond teneinde die grond te zien aanvullen.
- De toepassing van artikel 5 § 3 W.Beroepsorgaan is vaak problematisch. Deze bepaling laat het Beroepsorgaan toe op verzoek van een inlichtingen- of politiedienst te beslissen om sommige stukken uit het dossier ter inzage van de verzoeker of zijn advocaat te halen. Dit is het geval indien de verspreiding ervan een gevaar kan inhouden voor de bescherming van de bronnen, de persoonlijke levenssfeer van derden, de vervulling van de wettelijke opdrachten van de inlichtingendiensten of het geheim van een lopend opsporings- of gerechtelijk onderzoek. Het verzoek is echter zelden (correct) gemotiveerd of gaat uit van een overheid die hiertoe niet wettelijk bevoegd is, zodat de griffie ook hier soms bijkomende informatie moet inwinnen. Vaak blijven deze overheden ook verkeerdelijk vasthouden aan de idee dat de verzoeker en diens advocaat geen inzage kunnen krijgen van geclassificeerde gegevens, zonder dat dit een nadere motivering behoeft, en dit ondanks de vaste rechtspraak van het Beroepsorgaan volgens dewelke de W.Beroepsorgaan een *lex specialis* is t.o.v. de Classificatiewet. Tot slot zijn er ook gevallen waarin de voorzitter van het Beroepsorgaan ambtshalve elementen uit het dossier moet verwijderen omdat de betrokken dienst manifest heeft nagelaten zich te beroepen op art. 5 § 3 W.Beroepsorgaan ter bescherming van de persoonlijke levenssfeer van derden.
- De beslissingen van de veiligheidsoverheden zijn onvoldoende gemotiveerd en er wordt – in strijd met de wettelijke vereisten – geen volledig gemotiveerde beslissing opgesteld in de gevallen waarbij artikel 22, vijfde lid W.CV&VM toelaat om bepaalde elementen weg te laten in de aan de betrokkene ter kennis gegeven beslissing. Bovendien moet de veiligheidsoverheid in de motivering duidelijk maken welke concrete feiten een tegenindicatie uitmaken, rekening houdend met het reglementair vastgestelde doel van een bepaalde

veiligheidsverificatie. Alleen zo kan het Beroepsorgaan nagaan of een beslissing proportioneel is.
- Verder wijst het Beroepsorgaan er nog op dat diverse veiligheidsoverheden niet getuigen van zorgvuldigheid en respect voor de formele beginselen van het administratief recht (beslissingen zonder data en identiteit van de functionaris die de beslissing neemt; betrokkene wordt nooit gehoord; het gebruik van de taal in bestuurszaken).
- Tot slot, volgen de veiligheidsoverheden – zonder dit op omstandige wijze te motiveren – de vaste rechtspraak van het Beroepsorgaan niet (bijv. inzake de problematiek van onderzoeken of verificaties naar personen die niet beschikken over de Belgische nationaliteit).

Hoewel de kwaliteit van het samengestelde dossier een steeds weerkerend probleem vormt, heeft ook de steeds frequentere tussenkomst van advocaten een grote impact op de werking van het rechtscollege. Het Beroepsorgaan is immers – terecht – verplicht zijn beslissingen te motiveren door te antwoorden op de relevante argumenten die een raadsman ter verdediging van de belangen van zijn cliënt aanvoert.

Volgens het Beroepsorgaan zijn de wet en zijn koninklijke besluiten niet aangepast aan de moderne eisen van toegang tot het gerecht. 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 die te maken krijgen met toegang tot het gerecht, leven deze regels niet na. Meestal is dit het gevolg van een begrijpelijke, onvoldoende beheersing van de procedureregels. Het ten behoeve van de Kamer van Volksvertegenwoordigers opgestelde wetsvoorstel wil hieraan tegemoetkomen. Er moet immers beter rekening worden gehouden met de hoedanigheid en zelfs de kwetsbaarheid van tal van verzoekers en er moet worden voorzien in wettelijke bepalingen die geen nietigheid van rechtswege met zich meebrengen. Ook het beslissingsproces zelf vergt meer tijd dan een aantal jaren geleden. Hiervoor zijn twee belangrijke redenen aan te halen. Enerzijds is er het grote aantal procedurele kwesties (bijv. ontvankelijkheid, taalgebruik, rechten van verdediging of delegering van de bevoegdheid van de instantie die de beslissing neemt). Anderzijds wordt het Beroepsorgaan vaker geconfronteerd met extreem gevoelige dossiers. Bovendien moeten soms specifieke veiligheidsmaatregelen worden genomen.

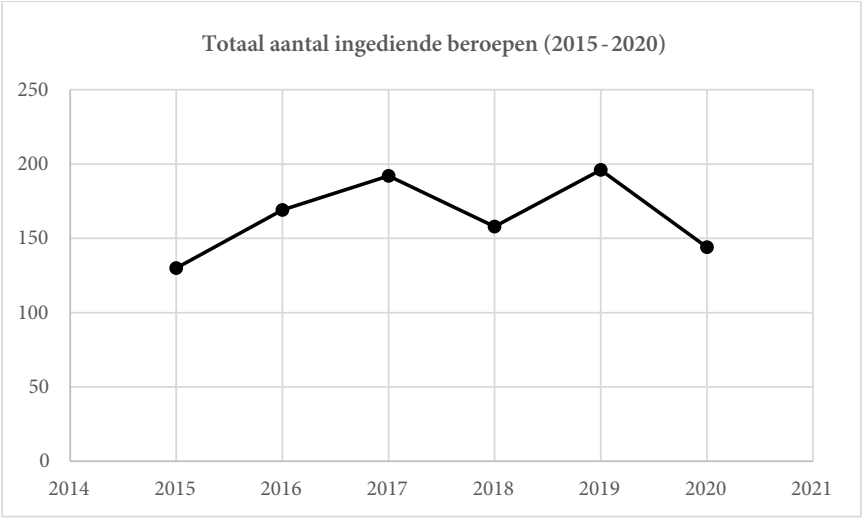
X.4. GEEN EVOLUTIE VAN HET WETGEVEND KADER

Terwijl het wetgevend kader in 2018 en 2019 sterk veranderd is, zowel wat de W.C&VM. als de W.Beroepsorgaan betreft, is er in 2020 geen enkel wet- of regelgevend initiatief genomen.

X.5. 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.

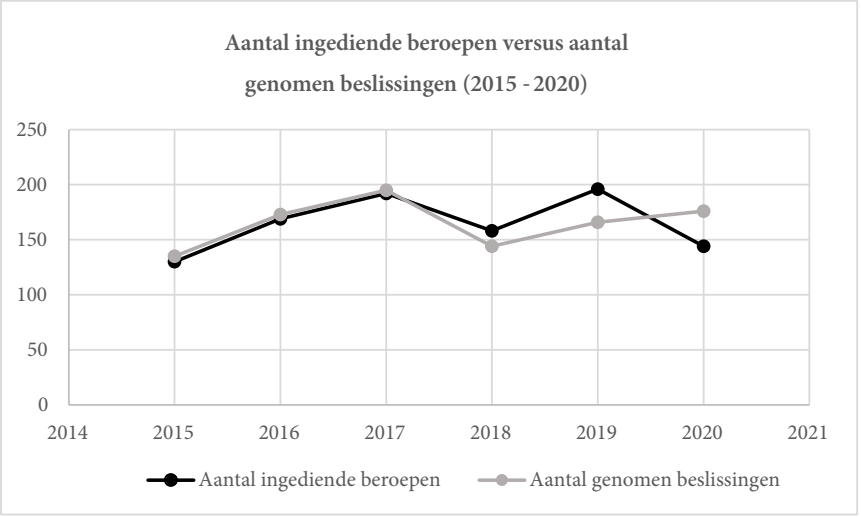
Tabel 1. Aantal ingediende beroepen (2015-2020)



De algemene trend in de cijfers van de afgelopen jaren laat een afname zien van het aantal beroepen dat bij het Beroepsorgaan wordt ingediend. Die daling speelt zich af rond drie grote spillen: ten eerste een afname van het aantal beroepen met betrekking tot veiligheidsmachtigingen (van 36 in 2018 naar 51 in 2019 en 32 in 2020). Ten tweede zijn de geschillen over veiligheidsadviezen na een jaar van achteruitgang ook sterk afgenomen (van 115 in 2019 naar 99 in 2020). En ten derde waren er ook veel minder beroepen met betrekking tot de weigering van veiligheidsattesten voor de nucleaire sector (van 17 in 2019 naar 7 in 2020).

Er valt echter een belangrijke vaststelling te maken. Niettegenstaande de daling van het aantal beroepen dat in 2020 werd ingediend, blijkt dat het aantal in 2020 genomen beslissingen is gestegen. Onderstaande tabel vergelijkt het aantal ingediende beroepen met het aantal genomen beslissingen.

Tabel 2. Aantal ingediende beroepen versus aantal genomen beslissingen (2015-2020)



We stellen vast dat het Beroepsorgaan voor het eerst de kwestie van de toekenning van een veiligheidsattest aan een imam om in Belgische gevangenissen te werken heeft behandeld op basis van wat werd bepaald in het koninklijk besluit van 17 mei 2019[274].

Bij het rechtscollege werd ook een zaak aanhangig gemaakt over de kwestie van de toekenning van het veiligheidsadvies voor douanebeambten die een wapen moeten dragen in het kader van de uitoefening van hun functie, in overeenstemming met wat werd bepaald in het koninklijk besluit van 15 december 2013[275].

Tevens werd bij het Beroepsorgaan voor het eerst de kwestie aanhangig gemaakt van de toekenning van het veiligheidsadvies voor leveranciers, onderaannemers en hun personeel van de Europese instellingen als gevolg van een protocol dat werd gesloten tussen Buitenlandse Zaken en de Europese instellingen[276].

Voor zover het Beroepsorgaan weet, is er nog geen gebruikgemaakt van de nieuwe veiligheidsadviesprocedure die in het activiteitenverslag van 2018 werd beschreven. Volgens bepaalde geruchten wil men in de toekomst de controles van de

274 Koninklijk besluit van 17 mei 2019 betreffende de aalmoezeniers, de consulenten van de erediensten en de moreel consulenten bij de gevangenissen (artikel 3§3,1°).

275 Koninklijk besluit van 15 december 2013 tot vaststelling van de diensten bij de Algemene Administratie van de Douane en Accijnzen waar de uitoefening van een functie afhankelijk wordt gesteld van een veiligheidsverificatie.

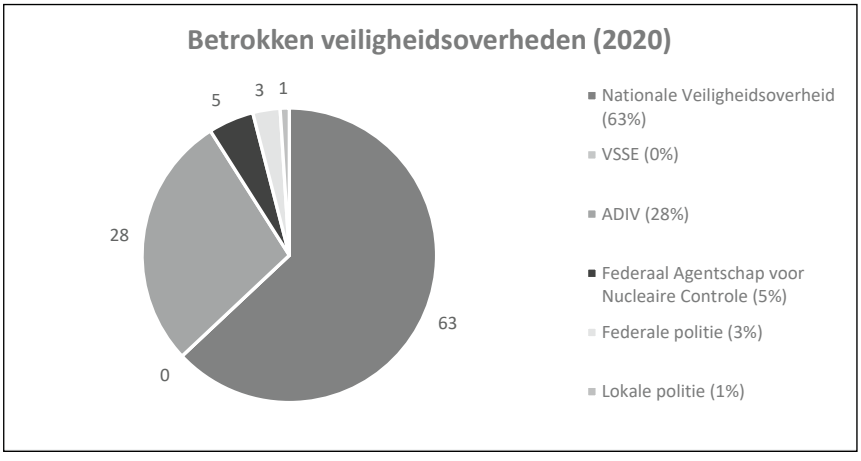
276 Zie in verband hiermee het koninklijk besluit van 8 mei 2018 tot vaststelling van de activiteitensectoren en de bevoegde administratieve overheden bedoeld in artikel 22*quinquies*, § 7, van de W.C.&VM dat aan de leidend ambtenaar van de FOD Buitenlandse Zaken de bevoegdheid toekent voor de 'activiteitensector' van de internationale instellingen. Op 21 mei 2019 werd een 'memorandum of understanding' gesloten tussen deze laatste en de Europese instellingen.

integriteit en moraliteit van het personeel van de havens opvoeren. Het is mogelijk dat de nieuwe veiligheidsadviesprocedure daarvoor wordt toegepast.
Tot slot vonden er 26 zittingen van het Beroepsorgaan plaats in 2020.

Tabel 3. Betrokken veiligheidsoverheden (2015-2020)

	2015	2016	2017	2018	2019	2020
Nationale Veiligheidsoverheid	68	92	129	113	114	91
Staatsveiligheid	1	0	0	0	0	0
Algemene Dienst Inlichting en Veiligheid	47	68	53	32	61	41
Federaal Agentschap voor Nucleaire Controle	10	8	7	10	17	7
Federale politie	3	1	3	3	3	4
Lokale politie	1	0	0	0	1	1
TOTAAL	130	169	192	158	196	144

Onderstaande grafiek toont de verdeling van de betrokken veiligheidsoverheden in 2020.



Tabel 4. Aard van de bestreden beslissingen

	2015	2016	2017	2018	2019	2020
Veiligheidsmachtigingen (Art. 12 e.v. W.C&VM)						
Vertrouwelijk	9	5	1	2	5	0
Geheim	35	38	33	31	39	27
Zeer geheim	4	7	6	3	7	5
Weigering	36	28	30	26	39	23
Intrekking	7	9	7	4	16	8
Weigering en intrekking	0	0	0	0	0	0
Machtiging voor beperkte duur	3	4	1	1	3	0
Machtiging voor een lager niveau	0	1	0	0	0	0
Geen beslissing binnen de termijn	2	7	2	5	0	0
Geen beslissing binnen de verlengde termijn	0	1	0	0	0	0
Andere						1[277]
SUBTOTAAL VEILIGHEIDSMACHTIGINGEN	48	50	40	36	51	32
Veiligheidsattesten voor geclassificeerde zone (art. 22*bis*, al. 1 W.C&VM)						
Weigering	6	1	3	3	1	0
Intrekking	0	0	0	0	0	0
Geen beslissing binnen de termijn	0	0	0	0	0	0
Veiligheidsattesten voor plaats of evenement (art. 22*bis*, al. 2 W.C&VM)						
Weigering	12	9	20	15	12	6
Intrekking	1	0	0	0	0	0
Geen beslissing binnen de termijn	0	0	0	0	0	0
Veiligheidsattesten voor nucleaire sector (art. 8*bis* W.C&VM)						
Weigering	-	7	7	11	17	7
Intrekking	-	1	0	0	0	0
Geen beslissing binnen de termijn	-	0	0	1	0	0
Veiligheidsadviezen (art. 22*quinquies* W.C&VM)						
Negatief advies	63	101	122	92	115	99

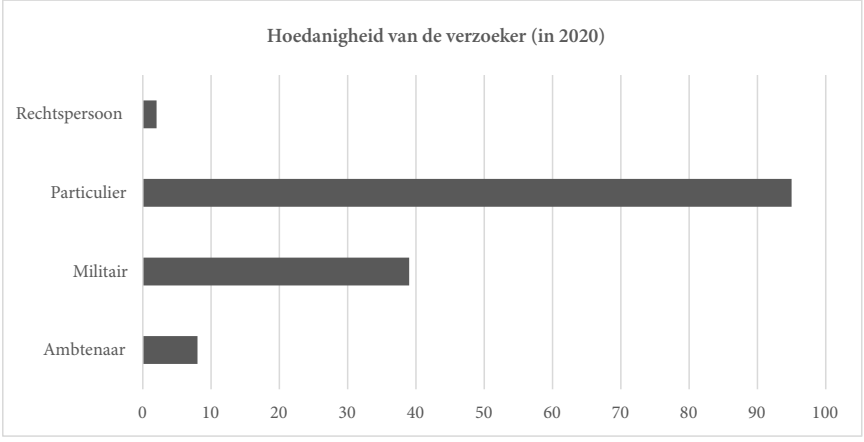
277 'Waarschuwing van de verzoeker'. Aan een persoon werd de veiligheidsmachtiging voor een periode van vijf jaar met een waarschuwing toegekend. De betrokkene heeft beroep ingesteld tegen deze waarschuwing.

	2015	2016	2017	2018	2019	2020
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
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	82	119	152	122	145	112
TOTAAL BESTREDEN BESLISSINGEN	130	169	192	158	196	144

Tabel 5. Hoedanigheid van de verzoeker

	2015	2016	2017	2018	2019	2020
Ambtenaar	4	2	4	5	4	8
Militair	29	23	20	8	27	39
Particulier	93	139	164	140	163	95
Rechtspersoon	4	5	4	5	2	2

Onderstaande grafiek toont de verdeling volgens de 'hoedanigheid van de verzoeker' in 2020.



Tabel 6. Taal van de verzoeker

	2015	2016	2017	2018	2019	2020
Franstalig	75	99	115	83	101	83
Nederlandstalig	54	70	77	75	95	61
Duitstalig	0	0	0	0	0	0
Anderstalig	1	0	0	0	0	0

Tabel 7. Handelingen van de griffie

	2015	2016	2017	2018	2019	2020
Volledig dossier opvragen (1)	130	167	191	154	191	141
Vraag om bijkomende informatie (2) en herinneringen verstuurd naar de veiligheidsoverheden (3)	7	23	36	12	39	41

(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 [278]

	2015	2016	2017	2018	2019	2020
Horen van een lid van een overheidsinstantie (1)	7	10	0	1	6	1
Beslissing van de voorzitter (2)	0	0	0	0	0	0
Verwijderen van informatie uit het dossier door het Beroepsorgaan (3)	50	54	80	72	77	50
Beslissingen alvorens recht te doen (4)	/	/	/	/	9	9

(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

	2015	2016	2017	2018	2019	2020
Inzage van het dossier door de verzoeker en/of zijn advocaat	84	87	105	69	96	96
Horen van de verzoeker (al dan niet bijgestaan door zijn advocaat)[279]	107	127	158	111	143	135

278 De cijfers voor 'voorbereidende gerechtelijke handelingen' (tabel 6), 'wijze waarop de verzoeker zijn rechten van verdediging uitoefent' (tabel 7) of 'aard van de beslissingen van het Beroepsorgaan' (tabel 8) komen niet noodzakelijkerwijs overeen met het aantal ingediende verzoeken (zie tabellen 1 tot 4). Sommige dossiers werden bijvoorbeeld al opgestart in 2019, terwijl de beslissing pas viel in 2020.

279 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.

Tabel 10. Aard van de beslissingen van het Beroepsorgaan

	2015	2016	2017	2018	2019	2020
Veiligheidsmachtigingen (art. 12 e.v. W.C&VM)						
Beroep onontvankelijk	4	0	3	0	1	1
Beroep zonder voorwerp	3	7	0	4	3	3
Beroep ongegrond	19	18	13	12	12	16
Beroep gegrond (volledige of gedeeltelijke toekenning)	24	24	24	12	25	14
Bijkomende onderzoeksdaden door de overheidsinstantie	0	2	0	1	1	2
Bijkomende termijn voor de overheidsinstantie	1	2	1	1	0	3
Verleent akte van afstand van beroep	1	0	0	3	2	2
Veiligheidsattesten voor geclassificeerde zone (art. 22*bis*, al. 1 W.C&VM)						
Beroep onontvankelijk	0	0	1	0	0	0
Beroep zonder voorwerp	0	0	1	0	0	0
Beroep ongegrond	4	1	0	1	1	0
Beroep gegrond (toekenning)	2	1	1	0	3	0
Verleent akte van afstand van beroep	-	-	-	-	1	0
Veiligheidsattesten voor plaats of evenement (art. 22*bis*, al. 2 W.C&VM)						
Beroep onontvankelijk	0	0	1	2	4	2
Beroep zonder voorwerp	0	0	1	0	0	0
Beroep ongegrond	8	2	12	2	4	4
Beroep gegrond (toekenning)	10	4	7	3	4	1
Verleent akte van afstand van beroep	2	0	1	2	0	0
Veiligheidsattesten voor nucleaire sector (art. 8*bis*, §2 W.C&VM)						
Beroep onontvankelijk	-	1	1	0	1	0
Beroep zonder voorwerp	-	1	0	1	0	0
Beroep ongegrond	-	0	1	1	5	2
Beroep gegrond (toekenning)	-	7	5	6	7	4
Verleent akte van afstand van beroep	-	-	-	2	0	0

	2015	2016	2017	2018	2019	2020
Veiligheidsadviezen (art. 22*quinquies* W.C&VM)						
Beroepsorgaan onbevoegd	0	0	20[280]	12	0	0
Beroep onontvankelijk	6	15	10	3	7	8
Beroep zonder voorwerp	0	0	1	3	1	6
Bevestiging van negatief advies	28	42	49	46	40	51
Omzetting in positief advies	23	46	41	27	43	52
Verleent akte van afstand van beroep	0	0	1	0	1	5
Beroep tegen normatieve rechtshandelingen van een administratieve overheid (art. 12 W.Beroepsorgaan)	0	0	0	0	0	0
TOTAAL	135[281]	173	195	144	166	176

X.6. VOORSTEL TOT HERVORMING

Op aansturen van de voorzitter zijn er uitgebreide reflecties en stappen ondernomen om de werking van het Beroepsorgaan te moderniseren. Er zijn enkele belangrijke doelstellingen bepaald: de vereenvoudiging en standaardisering van de procedure, de verbetering van de toegang tot het rechtscollege voor burgers en de gedigitaliseerde verwerking van dossiers door de griffie. Net als andere rechtscolleges, heeft het Beroepsorgaan zich geëngageerd om zijn juridisch taalgebruik te vereenvoudigen.

In deze context heeft het Vast Comité I op 24 november 2020 een tekst bezorgd aan de Kamer van Volksvertegenwoordigers, na de tekst eerst te hebben overgelegd aan de voorzitters van het Vast Comité P en de Geschillenkamer van de Gegevensbeschermingsautoriteit.

De tekst is het resultaat van een reflectie die de voorzitter van het Beroepsorgaan al jaren geleden had opgestart. Deze reflectie steunde op de expertise van de heer Ivan Verougstraete, voormalig voorzitter van het Hof van Cassatie. Er wordt voorgesteld om een Raad voor geschillen inzake veiligheid op te richten en de Wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen op te heffen. Met de

280 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.

281 Er waren nog twee specifieke beslissingen van verlenen van akte van afstand van beroep, waardoor het totaal in 2015 op 137 kwam.

oprichting van dit rechtscollege zou er gevolg worden gegeven aan de intentie van het Beroepsorgaan, daar de opstellers van de tekst pleiten voor een functie van 'natuurlijke rechter' op het vlak van veiligheid, wat betreft zowel de veiligheidsmachtigingen, -attesten en -adviezen als op het vlak van bewaking en privédetectives. De onafhankelijkheid van dit rechtscollege wordt versterkt door de aanwezigheid van drie leden als 'experten': het Vast Comité I voor de aspecten 'Wet inzake machtigingen' en 'Inlichtingenwet'; het Vast Comité P voor de Wet op het politieambt en de Geschillenkamer van de Gegevensbeschermingsautoriteit voor de bescherming van de persoonlijke levenssfeer. De tekst[282] stelt een vereenvoudiging van de procedures en een grotere transparantie voor, in het bijzonder door de invoering van de digitalisering van de dossiers. Als het wordt aangenomen, zou het voorstel tot hervorming moeten voorzien in de mogelijkheid om een beroep op elektronische wijze in te dienen. Bovendien zullen de partijen via dit platform met de griffie in contact kunnen treden over hun dossier. Er is contact opgenomen met de balie met als doel nuttige contacten te ontwikkelen om de toegang voor rechtsonderhorigen te bevorderen. De nieuwe procedureregels zullen de procedure flexibeler en transparanter maken door de verschillende termijnen voor beroep te herleiden tot een enkele termijn van dertig dagen. De huidige termijn van acht dagen (voor veiligheidsattesten en -adviezen) is immers te kort om de burger toe te laten zijn rechten van verdediging naar behoren uit te oefenen. Zo wordt rekening gehouden met de belangen van zowel de Staat als de burgers. Tot slot handhaaft het voorstel het principe van de gratis toegang voor rechtsonderhorigen.

De voorzitter van het Beroepsorgaan onderzoekt de mogelijkheid om aan studenten of advocaten de kans te bieden stage te lopen bij het orgaan.

We merken ook nog op dat er wordt overwogen om de beslissingen te publiceren op die website. Het is belangrijk dat de rechtspraak van het Beroepsorgaan voor iedereen toegankelijk is. Dat is een garantie voor de transparantie van een instelling voor burgers. Die publicatie zal gebeuren in geanonimiseerde vorm, in aanmerking genomen dat de informatie niet van die aard mag zijn dat ze gevaren inhoudt voor een fundamenteel staatsbelang, de geheimhouding van informatie of van een lopend gerechtelijk onderzoek, de bescherming van de bronnen of de bescherming van de persoonlijke levenssfeer van derden. Bovendien onderzoekt het Beroepsorgaan het idee om op zijn website een rubriek 'kroniek van rechtspraak' te creëren.

282 De tekst van het voorstel zal worden gepubliceerd op de website van het Beroepsorgaan nadat het huidige verslag zal zijn voorgesteld aan de begeleidingscommissie van het Vast Comité I van de Kamer van Volksvertegenwoordigers.

HOOFDSTUK XI

DE INTERNE WERKING VAN HET VAST COMITÉ I

XI.1. SAMENSTELLING VAN HET VAST COMITÉ I

2020 was een jaar met heel wat personeelswissels. Serge Lipszyc (F), eerste substituut arbeidsauditeur bij het arbeidsauditoraat van Luik, die in al september 2018 de eed aflegde[283], bleef zijn opdracht als voorzitter vervullen. Pieter-Alexander De Brock (N), wiens eerste mandaat verliep in mei 2019, werd herbenoemd halfweg januari 2020.[284] Eind november 2020 deelde Laurent Van Doren (F) de Kamer mee dat hij met ingang van 31 december 2020 ontslag nam als Franstalig lid van het Vast Comité I.[285] Thibaut Vandamme (F), substituut Procureur des konings van het arrondissement Luxemburg, benoemd tijdens de plenaire vergadering van 22 november 2018 tot eerste plaatsvervanger, aanvaardde per 1 december 2020 om het mandaat van lid uit te oefenen.[286]

Begin januari 2020 deelde de griffier Wouter De Ridder zijn opruststelling mee. Per brief van eind april 2020 verzocht de voorzitter van het Comité dat de Kamer de procedure voor de benoeming van een nieuwe griffier zou opstarten.[287] Een oproep tot benoeming van griffier van het Vast Comité I verscheen halfweg mei 2020 in het Belgisch Staatsblad.[288]

---

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

284 *Hand.* Kamer 2019-20 CRIV55PLEN020, 52. Op 24 september 2020 werd Linda Schweiger benoemd als eerste plaatsvervangend lid (*Hand.* Kamer 2019-20 CRIV55PLEN055, 85) en op 29 oktober 2020 werd Wauter Van Laethem benoemd als tweede plaatsvervangend lid (*Hand.* Kamer 2019-20, CRIV55PLEN067, 16).

285 *Hand.* Kamer 2020-21 CRIV55PLEN074, 47.

286 Overeenkomstig artikel 30, derde lid W.Toezicht dient de Kamer bij het openvallen van een plaats van plaatsvervangend lid onverwijld over te gaan tot de benoeming van een nieuw plaatsvervangend lid. De oproep tot kandidaten daartoe verscheen in het Belgisch Staatsblad van 18 december 2020. De eerste plaatsvervanger, Thierry Werts, werd benoemd tijdens de plenaire vergadering van 21 mei 2021 (*Hand.* Kamer 2020-21 CRIV55PLEN105, 47). Michel Croquet blijft tweede plaatsvervanger van het Franstalig lid.

287 *Hand.* Kamer 2019-20, CRIV55PLEN038, 70.

288 Bij het afsluiten van voorliggend activiteitenverslag werd nog geen griffier aangeduid. 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, in: *Parl. St.* Kamer 2020-21, 55K2064/001.

En ook bij de Dienst Enquêtes I werden wijzigingen opgetekend. Frank Franceus (N) zocht nieuwe oorden op en werd als directeur vervangen door Fabian Poncelet (F), die bijkomend ook de rol van veiligheidsofficier voor zijn rekening nam. In september 2020 trad tevens een nieuwe Nederlandstalige commissaris-auditor aan.

Ten slotte bleef ook de administratieve staf van het Vast Comité I, onder leiding van plaatsvervangend griffier Wauter Van Laethem (N), niet ongewijzigd. In maart 2020 vervoegde een Nederlandstalige statutaire jurist de rangen van de Afdeling documentatie en juridische analyse, gevolgd door een Franstalige statutaire jurist in december 2020. Ook de selectie-examens voor een Nederlandstalige en een Franstalige statutaire secretaris/secretaresse vonden plaats in 2020. Eind 2020 telde de administratieve staf 18 personeelsleden.

XI.2. DE *DATA PROTECTION OFFICER* OP HET COMITÉ

Het Comité kon blijven beroep doen op de *Data Protection Officer* (DPO)[289] aangesteld voor alle gegevensverwerkingen die buiten de 'nationale veiligheid' vallen. Deze functionaris voor gegevensbescherming houdt het register van verwerkingsactiviteiten bij dat werd opgesteld in overleg met de verschillende diensten binnen het Vast Comité I en werd gevalideerd door de voorzitter en raadsheren van het Vast Comité I. Er werd ook advies verleend bij de nieuwe website (bijv. overheidsopdracht) en aanwervingsprocedures (bijv. informatieplicht naar de betrokkenen). Ondertussen wordt de DPO ook actief betrokken bij onder andere het gebruik en toegang van het Rijksregister(nummer), het gebruik van camerabewaking en de informatieplicht naar de betrokkenen (o.a. interne medewerkers).

XI.3. VERGADERINGEN MET DE BEGELEIDINGSCOMMISSIE

Al in 2019 paste de Kamer van volksvertegenwoordigers het Kamerreglement aan. Hierdoor werd de samenstelling van de Bijzondere commissie belast met de parlementaire begeleiding van het Vast Comité van Toezicht op de politiediensten en het Vast Comité van Toezicht op de veiligheids- en inlichtingendiensten gewijzigd. Voortaan worden zoveel leden als nodig is benoemd opdat elke in de vaste commissie vertegenwoordigde politieke fractie in de commissie vertegenwoordigd zou zijn door ten minste één lid. Elke politieke fractie die niet vertegenwoordigd is in de commissie, wijst onder haar leden een lid aan dat zal deelnemen aan de

[289] De DPO vervult deze functie voor verschillende instellingen.

werkzaamheden van de commissie, zonder evenwel stemgerechtigd te zijn.[290] In het zog van de federale verkiezingen van mei 2019, kende de Begeleidingscommissie een andere samenstelling. Maken voortaan als stemgerechtigde leden deel uit van de commissie: Peter Buysrogge (N-VA), Joy Donné (N-VA), Cécile Thibaut (Ecolo-Groen), Stefaan Van Hecke (Ecolo-Groen), André Flahaut (PS), Ahmed Laaouej (PS), Ortwin Depoortere (VB), Marijke Dillen (VB), Dennis Ducarme (MR), Servais Verherstraeten (CD&V), Nabil Boukli (PVDA-PTB), Patrick Dewael (Open Vld) en Bert Moyaers (Vooruit). Halfweg oktober 2020 nam Kamervoorzitter Eliane Tillieux (PS) de fakkel over van Patrick Dewael (Open Vld). Georges Dallemagne (cdH) neemt deel als niet-stemgerechtigd lid.

In de loop van 2020 vonden, ondanks de sanitaire crisis, toch een aantal vergaderingen plaats. Net voor de uitbraak van de coronacrisis (2 maart 2021) werden de leden van de Begeleidingscommissie voor een werkvergadering uitgenodigd in de kantoren van Comité. Opzet was om de nieuwe commissieleden kennis te laten maken met de werkzaamheden van het Comité en met de vertrouwde gezichten diepgaander van gedachten te kunnen wisselen. Tijdens de andere commissievergaderingen werden – achter gesloten deuren – diverse door het Vast Comité I afgesloten toezichtonderzoeken besproken. Ook werd tijd uitgetrokken voor de bespreking van het jaarlijkse verslag over de toepassing van de specifieke en uitzonderlijke methoden door de inlichtingendiensten en de controle door het Vast Comité I (art. 35 W.Toezicht) alsook het verslag opgesteld in het kader van zijn controlebevoegdheid – samen met het Controleorgaan op de politionele informatie (COC) – aangaande de gemeenschappelijke gegevensbanken (art. 44/6 WPA). Tijdens haar vergadering van 16 december 2020 werd het algemeen *Activiteitenverslag 2019* besproken.[291] De Commissie benadrukte '*de hoge kwaliteit van het jaarverslag, waarin een volledig beeld van de activiteiten van het Comité I wordt geschetst*'.[292] Een aantal thema's weerhielden de bijzondere aandacht van de Kamerleden, zoals de *follow-up* van sekten, het personeelstekort bij de inlichtingendiensten, de veiligheidsmachtigingen en het Beroepsorgaan, of nog, de

---

290 *BS* 25 oktober 2019. '*De reglementswijziging zorgt in de huidige samenstelling van het Parlement voor een kleinere samenstelling van de begeleidingscommissie, wat hopelijk de efficiëntie ten goede zal komen*', in *Hand.* Kamer 2019-20, 17 oktober 2019, CRIV55PLEN009, 33.

291 De Commissie verwijst daartoe naar artikel 66*bis*, §2, W.Toezicht, zoals gewijzigd bij de wet van 6 januari 2014 tot wijziging van diverse wetten tot hervorming der instellingen (*BS* 31 januari 2014).

292 Niettegenstaande de commissieleden gezien de politieke situatie en de lastige omstandigheden begrip toonden voor de late indiening van het verslag, werd het Comité verzocht het eerstvolgende activiteitenverslag sneller te bezorgen. Een opmerking waar het Comité terdege rekening mee heeft gehouden.

follow-up van de aanbevelingen.[293] De Commissie nam als eindconclusie '*akte van het activiteitenverslag 2019 van het Comité I en onderschrijft diens aanbevelingen*'.[294]

XI.4. GEMEENSCHAPPELIJKE VERGADERINGEN MET HET VAST COMITE P

In 2020 vonden, naast informele contacten op de werkvloer, enkele gemeenschappelijke vergaderingen plaats. De artikelen 52 tot 55 W.Toezicht bepalen de gevallen waarin en de wijze waarop het Vast Comité I en het Vast Comité P gemeenschappelijke vergaderingen dienen te organiseren. Het voorzitterschap van deze gezamenlijke vergaderingen wordt afwisselend waargenomen door de voorzitters van beide Vaste Comités (art. 54 W.Toezicht). Het doel van de vergaderingen is tweeërlei: enerzijds het uitwisselen van informatie en anderzijds het opstarten en bespreken van lopende gemeenschappelijke toezichtonderzoeken.

In 2020 waren twee 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.11.8) en het toezichtonderzoek naar de vier 'bijkomende' ondersteunende diensten van het OCAD (cf. I.11.9). Er werd beslist geen bijkomende gemeenschappelijke onderzoeken op te starten.

Verder werden uiteenlopende punten geagendeerd. Zo werd onder meer het door het Vast Comité P voorgestelde ontwerp van wetswijziging van de Toezichtswet besproken; een voorstel dat ertoe strekt om de noodzaak om houder te zijn van een veiligheidsmachtiging van het niveau 'zeer geheim' tevens in te schrijven voor alle leden van het administratief personeel van de Vaste Comités I en P en voor alle leden van de Dienst Enquêtes P. Ook werd de stand van zaken in de ontwikkeling van een internetcollectetool ten voordele van de ADIV, de VSSE

---

293 Om de opvolging van de aanbevelingen van de Vaste Comités I en P te verbeteren, werd in december 2019 een voorstel tot herziening van het Reglement van de Kamer van Volksvertegenwoordigers ingediend door twee commissieleden. Er werd voorgesteld artikel 149 van het Kamerreglement als volgt aan te passen: '*Wanneer de Commissie vaststellen dat de bevoegde ministers niet het minste gevolg hebben gegeven aan de aanbevelingen van de Vaste Comités I en P, dan wel dat de genomen maatregelen niet passend of ontoereikend zouden zijn, kan ze de bevoegde ministers verzoeken verslag bij haar uit te brengen. De bevoegde ministers bezorgen de commissie jaarlijks minstens eenmaal een verslag over de staat van implementering van de aanbevelingen. Daartoe houden de bevoegde ministers een vaste boordtabel bij inzake de opvolging van de aanbevelingen […] die aan de commissie wordt bezorgd*'. *Parl. St*. Kamer 2019-20, 55K0868/001, 11 december 2019. Het voorstel werd evenwel niet weerhouden.

294 *Parl. St.* Kamer 2020-21, nr. 55K1689/001, 29 december 2020 (Activiteitenverslag 2019 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).

en de Federale politie geagendeerd[295], werd nagedacht over het verzoek tot toegang tot het Rijksregister voor de commissaris-auditoren, of nog, werden ideeën uitgewisseld in de zoektocht naar mogelijke synergiën tussen beide instellingen. Wat dat laatste betreft, werd bestudeerd of kon worden overgegaan tot de aankoop van gemeenschappelijke *software* voor videoconference (of videobellen) om vergaderingen op afstand, interne vergaderingen, *events*, *webinars* of lezingen te *hosten*.

XI.5. FINANCIËLE MIDDELEN EN BEHEERSACTIVITEITEN

Het 'budget 2020' van het Vast Comité I werd vastgelegd op 4,615 miljoen euro, wat een vermeerdering inhield van 9,5% ten aanzien van het budget 2019.[296]

Naast de natuurlijke verhogingen (indexering…) is deze verhoging ingegeven door twee projecten die ter goedkeuring aan het Parlement werden voorgelegd: ten eerste een project voor de digitalisering van de werkprocessen en de communicatiemiddelen (website) en ten tweede een herziening van het administratieve kader om het profiel van het toekomstige personeel aan te passen aan de ontwikkeling van het takenpakket van het Comité, hetwelk operationeel in plaats van ondersteunend personeel vereist.

De financieringsbronnen van het budget werden door de Kamer van volksvertegenwoordigers[297] als volgt toegewezen: 85,84 % dotatiebudget en 14,16 % boni van 2018.

De uitvoering van het budget 2020 leverde een budgettaire bonus op van 463,045 euro, te weten het vastgestelde verschil tussen de inkomsten en de samengestelde uitgaven.

Het budget is traditiegetrouw gebaseerd op verschillende financieringsbronnen en de enige nieuwe bijdrage in termen van eigen beheer, staat ingeschreven in de dotatie van de algemene uitgavenbegroting van de Staat. Tot 2017 was deze dotatie onvoldoende om de reële uitgaven van het Comité te dekken, wat een structureel verlies als gevolg met zich meebracht. De tendens om zoveel mogelijk artikel 57, lid 1, W.Toezicht toe te passen hetwelke vermeldt dat de kredieten die noodzakelijk zijn voor de werking dienen te worden uitgetrokken op de begroting van de dotaties, laat heden ten dage het Comité toe zijn activiteiten te financieren.

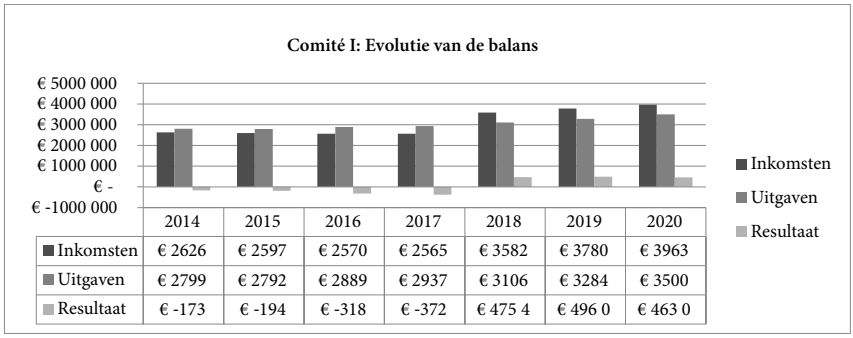
---

295 De tool bestaat uit een combinatie van softwaremodules en hardware en moet de politie- en inlichtingendiensten in staat stellen om sneller en gerichter naar informatie op sociale media e websites te zoeken. De aankoop werd al in augustus 2016 op de Ministerraad goedgekeurd. Midden februari 2021 werd het contract met de Nederlandse softwareontwikkelaar BAVAK evenwel stopgezet omdat de zoekrobot niet voldeed aan de verwachtingen. Hierover: K. CLERIX, *Knack*, 23 februari 2021 ('Nieuwe topman Philippe Boucké zet ADIV op scherp').

296 *Hand.* Kamer 2019-20, CRIV55PLEN018, 72.

297 *Parl. St.* Kamer 2019-2020 , 55K0867/001, 24-27.

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 zal naar alle verwachting nog enkele jaren aanhouden en dit ten gevolge de aanwervingsprocedures die voortvloeien uit de nieuwe taken van het Comité, maar ook als gevolg van de vervanging van de huidige personeelsleden die hun pensioenrechten (zullen) opeisen. Dit alles zal voor het Comité een uitdaging vormen, niet in het minst om de opgebouwde ervaring te beheren en door te geven aan de nieuwe medewerkers. Het valt echter te verwachten dat, van zodra deze nieuwe personeelsleden zijn aangeworven, er een natuurlijk *ceteris paribus* evenwicht zal zijn tussen de inkomsten en uitgaven.



	2014	2015	2016	2017	2018	2019	2020
Inkomsten	€ 2626	€ 2597	€ 2570	€ 2565	€ 3582	€ 3780	€ 3963
Uitgaven	€ 2799	€ 2792	€ 2889	€ 2937	€ 3106	€ 3284	€ 3500
Resultaat	€ -173	€ -194	€ -318	€ -372	€ 475 4	€ 496 0	€ 463 0

Parallel met de verwerving van de nieuwe taken die werden toegewezen, waakte het Comité erover dat het synergiën blijft zoeken en uitvoeren tussen de verschillende dotatiegerechtigde instellingen. Het Comité staat volledig achter deze aanpak wanneer daardoor de efficiëntie en de doeltreffendheid worden verhoogd alsook mogelijke besparingen worden gerealiseerd, zonder dat daarbij evenwel de veiligheidsvereisten in het gedrang komen. Concreet werd tussen het Comité enerzijds en de bibliotheek van het Parlement anderzijds een contract van bewaargeving afgesloten waarbij het Comité zijn beperkte doch gespecialiseerde collectie van monografieën, tijdschriften en andere publicaties aangaande de werking, de bevoegdheden en bevoegdheidsdomeinen alsook de controle op de inlichtingen- en veiligheidsdiensten in een brede (internationale) context, in bewaring heeft gegeven. In de loop van 2020 werden alle fysieke boeken en tijdschriften overgeheveld naar de bibliotheek van het Parlement : zo worden toekomstige dubbele aankopen vermeden, werd een ruimere ontsluiting van de aanwezige literatuur gerealiseerd en konden op het Comité bijkomende bureaus worden gecreëerd.

XI.6. IMPLEMENTATIE VAN DE AANBEVELINGEN VAN DE AUDIT VAN HET REKENHOF

Op verzoek van de Commissie van de Comptabiliteit van de Kamer van Volksvertegenwoordigers startte het Rekenhof al in december 2017 samen met Ernst and Young een onderzoek naar de dotatiegerechtigde instellingen, waaronder het Vast Comité I. Het Rekenhof richtte zich vooral op de budgettaire aspecten (een analyse van de inkomsten en uitgaven) en op de afbakening van de taken van de diverse instellingen. Ernst and Young op zijn beurt analyseerde de processen, de systemen en de organisatie die in elk van deze instellingen aanwezig zijn. Het auditverslag[298] werd eind maart 2018 opgeleverd. Het formuleerde aanbevelingen voor de 'opdrachten' van de negen bij de audit betrokken dotatiegerechtigde instellingen. Het gemeenschappelijk kenmerk in de opdrachten van deze instellingen *'ligt in het doel om tot een betere rechtsbescherming voor burgers te komen door het uitoefenen van verschillende vormen van toezicht in specifieke beleidsdomeinen'*.

Naar aanleiding van de bespreking van de opvolgingsaudit van de instellingen door het Rekenhof besliste de Commissie voor de Comptabiliteit half november 2020 om aan de diensten van de Quaestuur te vragen een stand van zaken op te stellen van de uitvoering van de aanbevelingen in de audit. Er werd ook gevraagd om na te gaan op welke wijze bijkomende synergiën kunnen worden geïmplementeerd teneinde verdere besparingen en efficiëntiewinsten te realiseren.

XI.7. VORMING

Omwille van het belang voor de organisatie, moedigt het Vast Comité I zijn leden en medewerkers aan tot het volgen van algemene (informatica, management…) of sectoreigen opleidingen en conferenties.[299] Gezien de naleving van de strikte coronamaatregelen konden geen externe opleidingen worden bijgewoond in de loop van 2020. Wel konden een beperkt aantal interne briefings worden georganiseerd waarbij experten het Comité voorlichtten over actuele en belangrijke thema's binnen de (brede) *intelligence community* (bijv. Prof. Christian Behrendt, verbonden aan de ULiège en de KULeuven, deskundige voor staatsrechtelijke vragen op (inter)nationaal niveau, Prof. Damien Van Puyvelde, *lecturer in intelligence and international security*, Glasgow).

---

298 *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.

299 Er vonden wel de door de medewerkers verplicht bij te wonen veiligheidsbriefings plaats.

HOOFDSTUK XII
AANBEVELINGEN

Op basis van de in 2020 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 OCAD en de ondersteunende diensten als op de optimalisatie van de toezichtmogelijkheden van het Vast Comité I.

XII.1. AANBEVELINGEN IN VERBAND MET DE COÖRDINATIE EN DE EFFICIËNTIE VAN DE INLICHTINGENDIENSTEN, HET OCAD EN DE ONDERSTEUNENDE DIENSTEN

XII.1.1. DIVERSE AANBEVELINGEN NAAR AANLEIDING VAN HET GEMEENSCHAPPELIJK TOEZICHTONDERZOEK NAAR HET OCAD EN DE ONDERSTEUNENDE DIENSTEN[300]

XII.1.1.1. Aandacht voor de interne communicatie en informatiesessies voor gedetacheerde deskundigen

Een betere interne communicatie, meer bepaald tussen de departementen van het OCAD, zou het mogelijk moeten maken om beter te weten *wie wat doet*, ook de gedetacheerde deskundigen. Zo zou een regelmatige actualisering van de lijst met personeelsleden en hun respectieve bevoegdheden ook een meerwaarde zijn (waarbij de lijst dan ook verspreid wordt onder het personeel).

Er werd vastgesteld dat de gedetacheerde deskundigen (departement Punctuele Analyse) hun oorspronkelijke dienst nog amper of helemaal niet meer bezoeken en dat sommigen er zelfs zeer weinig contact mee hebben. Een opleiding of informatiesessie om hun kennis bij te spijkeren van hun oorspronkelijke dienst en

[300] Zie 'Hoofdstuk I.1. De ondersteunende diensten van het OCAD'.

eventuele wijzigingen, bijvoorbeeld van de wetgeving of de interne voorschriften, zou een meerwaarde vormen.

XII.1.1.2. Optimalisatie van de contacten tussen het OCAD en de ondersteunende diensten

Wanneer er rechtstreekse contacten zijn tussen de ondersteunende dienst en het OCAD, is het belangrijk om het voornaamste contactpunt van de ondersteunende dienst op de hoogte te houden via zijn functionele mailbox door het bij elke uitwisseling van informatie in kopie te zetten. Zo kan verlies van informatie zoveel mogelijk voorkomen worden.

Bij bilaterale contacten ontwikkeld door een personeelslid van het OCAD (of van de ondersteunende dienst) met leden van de ondersteunende dienst (of van het OCAD) moet worden verzekerd dat bij vertrek (of afwezigheid) een ander personeelslid het contact kan overnemen. Het risico bestaat namelijk dat de kwaliteit van de informatiestroom daalt door het vertrek (of de afwezigheid) van een personeelslid dat goede contacten heeft ontwikkeld met bepaalde leden van de ondersteunende dienst (of het OCAD).

Voor de ondersteunende diensten waarmee de informatiestroom zeer beperkt is, zou het goed zijn om een synergie te ontwikkelen tussen het OCAD en het contactpunt om het personeel bewust te maken van de opdrachten van het OCAD en dat, voor zover mogelijk, bij alle verschillende delen van de ondersteunende dienst (bijvoorbeeld door middel van infosessies). Het is aan de ondersteunende diensten om initiatieven te nemen om hun personeel zo goed mogelijk te informeren.

XII.1.1.3. Het naleven van de wettelijke verplichtingen door de Administratie Douane en Accijnzen

Niettegenstaande de Administratie Opsporing van de Algemene Administratie Douane en Accijnzen (FOD Financiën) het belang van de samenwerking met het OCAD niet inziet en niet weet welke informatie het zou kunnen doorgeven, blijft deze administratie wel een door de wet aangestelde ondersteunende dienst van het OCAD. Het is dus aan de dienst om een interne analyse uit te voeren om te bepalen welke soort informatie die worden verzameld, nuttig zouden kunnen zijn voor het OCAD. Op basis daarvan kan eventueel een ander contactpunt binnen de Douane en Accijnzen worden aangeduid.

De Algemene Administratie Douane en Accijnzen moet daarenboven werk maken van gepaste maatregelen om te voldoen aan de wettelijk verplicht na te leven minimumnormen met betrekking tot de bewaring en raadpleging van geclassificeerde documenten.

XII.1.2. DIVERSE AANBEVELINGEN NAAR AANLEIDING VAN HET TOEZICHTONDERZOEK NAAR DE OPVOLGING VAN EXTREEMRECHTS[301]

XII.1.2.1. Aanbevelingen wat betreft de beleidsmatige afbakening van het inlichtingendoel

De verschillende diensten die zich bezighouden met de opvolging van extreemrechts / rechts-extremisme zouden moeten komen tot het gebruik van een gemeenschappelijke, uniforme terminologie, en de ontwikkeling van zo objectief mogelijke criteria om te bepalen welke individuen en/of groepen het voorwerp moeten uitmaken van hun opvolging. Een goede uitwisseling van gegevens en samenwerking is ermee gebaat dat alle betrokken diensten dezelfde terminologie hanteren.
Er zijn meerdere opties, waaruit de wetgevende en de uitvoerende macht kunnen kiezen:

- Ofwel kan de wetgever overwegen om het begrip 'extremisme' in de W.I&V van 30 november 1998 beter te omschrijven en daarbij ook de termen 'rechts-extremisme' (en logischerwijze ook 'linksextremisme') te verduidelijken.[302] Eventueel kunnen daarbij ook andere begrippen, zoals 'nationalisme' worden meegenomen;
- Ofwel neemt de NVR het voortouw, zoals het KB betreffende de oprichting van dit orgaan trouwens wil;
- Ofwel nemen de bevoegde ministers het initiatief om de diensten duidelijke instructies te geven over hoe de bedreiging moet worden beschouwd.

In al deze gevallen kan aan de diensten die deel uitmaken van de Werkgroep Extreemrechts van het Plan R gevraagd worden om een insteek te doen. In dit verband is het theoretische denkkader trouwens voorhanden en heeft het OCAD een goede positie om hierbij samen met de diensten tot een conclusie te komen die daarna op een hoger niveau kan worden geformaliseerd.

Tevens moet de hoegrootheid van de bedreiging worden bepaald. Het zijn niet enkel de inlichtingendiensten die hierover informatie (kunnen) verzamelen. De ontwikkeling van dergelijk cijfermateriaal is niet de verantwoordelijkheid van de inlichtingendiensten alleen. Samenwerking en coördinatie met de politiediensten en de Parketten is bijvoorbeeld vereist om cijfermateriaal te verzamelen over politiek en ideologisch gemotiveerde misdrijven. In deze kan de Werkgroep Extreemrechts van het Actieplan Radicalisme een centrale rol opnemen, onder

---

301 Zie 'Hoofdstuk I.7. De opvolging van extreemrechts door de Belgische inlichtingendiensten'.

302 De VSSE merkt hierbij terecht op dat een duidelijke definitie zowel voor- als nadelen heeft: het creëert een goed actueel kader, maar de definitie moet flexibel genoeg zijn om (toekomstige) fenomenen mee te nemen.

aansturing van de Nationale Veiligheidsraad (NVR) om te bepalen wie daarin wat kan bijdragen.

XII.1.2.2. Aanbevelingen wat betreft de organisatie en planning

Het Vast Comité I beveelt aan dat de inlichtingendiensten zouden evalueren of hun interne planning (operationeel, tactisch) adequaat is om het te bereiken strategische doel te realiseren, en of de inzet van middelen proportioneel is aan de op te volgen bedreiging. Er is echter een voorafgaande voorwaarde: de duidelijke omschrijving van het fenomeen en van de hoegrootheid ervan (zie aanbeveling hierboven).

XII.1.2.3. Aanbevelingen wat betreft collecte en verwerking

Het Vast Comité I beveelt aan dat de VSSE bij de opbouw van zijn databank het mogelijk maakt om via de MPG-assen (of op een soortgelijke manier aangezien de VSSE van plan is de databank te vervangen door een nieuwe oplossing) informatie op te zoeken en bijeen te brengen.

Wat de ADIV betreft, beveelt het Vast Comité I aan dat de dienst een meer onafhankelijke HUMINT-positie opbouwt (los van de S2-officieren) en daarvoor meer *handlers* inzet. Tevens moet de dienst onderzoeken hoe het komt dat de informatie traag doorstroomt en dat er een achterstand is inzake de input in de databank. Remedies moeten worden gevonden en toegepast.

XII.1.2.4. Aanbevelingen wat betreft analyse, verspreiding en samenwerking

De diensten moeten – samen en met het OCAD – onderzoeken hoe meer algemene fenomeenanalyses kunnen worden opgemaakt. Er is afstemming nodig tussen de VSSE en het OCAD – wellicht in de schoot van het Actieplan R om te bepalen wie daarbij wat zou moeten doen.

Bij de VSSE bestaat een instrument dat tot doel heeft de mate van radicalisering en gewelddadigheid van een persoon te beoordelen. De VSSE heeft niet de mankracht om het volledig uit te rollen en het vergt trouwens zeer veel informatie (50-tal indicatoren). Volgens de VSSE is het wellicht niet het meest geschikt om *lone actors* te detecteren. Er moet dus onderzocht worden of dit instrument eventueel kan worden verlicht en of er andere methoden zijn om de *lone actors* beter te detecteren. Er zijn bij andere diensten (onder ander het OCAD) nog andere instrumenten in gebruik of bestudeerd.

Het Vast Comité I is van mening dat er meer samenwerking en coördinatie noodzakelijk is tussen de diensten met betrekking tot de ontwikkeling, het gebruik van, en opleidingen over, dergelijke tools. Het Vast Comité I is ook van mening dat wanneer dergelijke tools voorhanden zijn die kunnen helpen bij het detecteren en

evalueren van dreigingen, deze ook systematisch dienen te worden toegepast bij de opvolging van alle vormen van extremisme, en dat hiervoor de nodige personele middelen dienen te worden ingezet. Dit temeer omdat de inlichtingendiensten verklaren dat mogelijke terreurdaden, gepleegd door *lone actor* momenteel de grootste dreiging vormt die uitgaat van het rechts-extremisme.

Wat ten slotte de sensibilisering van de verschillende maatschappelijke actoren betreft met betrekking tot (de ernst van) de bedreiging, heeft de VSSE – en *a fortiori* de ADIV – weinig initiatieven ontplooid. Gelet op de politieke aard van de bedreiging ligt het voor de hand dat het eventueel naar buiten treden van deze diensten op publieke fora door de NVR of door de bevoegde ministers moet worden gedekt.

XII.1.2.5. Aanbevelingen wat betreft feedback

Het Vast Comité I beveelt aan beide diensten aan om expliciet en periodiek aan de bestemmelingen van de inlichtingen de vraag te stellen welke *feedback* deze kunnen geven. Het is aan deze bestemmelingen om daarop te antwoorden zodat de diensten op basis daarvan hun inlichtingendoelen kunnen verfijnen en/of bijsturen.

XII.1.3. AANPASSING VAN DE RICHTLIJN AANGAANDE DE RELATIES VAN BELGISCHE INLICHTINGENDIENSTEN MET BUITENLANDSE INLICHTINGENDIENSTEN[303]

Op 26 september 2016 werd de 'Richtlijn aangaande de relaties van Belgische inlichtingendiensten met buitenlandse inlichtingendiensten' uitgevaardigd. Evenwel wordt daarin het doorgeven van informatie/persoonsgegevens aan buitenlandse diensten slechts zeer summier behandeld. Het Comité houdt wat dit betreft dan ook vast aan zijn eerdere aanbevelingen en acht een initiatief prioritair. Hierbij moet alleszins aandacht zijn voor het beginsel dat de inlichtingendiensten bij de informatie-uitwisseling zorgvuldig tewerk moeten gaan.

Bovenvermelde richtlijn streeft ernaar een inschatting te maken van buitenlandse inlichtingendiensten met als doel de aard van de relatie met elke dienst te bepalen. Het vormt een beleidsondersteunend instrument voor de bilaterale

[303] Deze aanbevelingen vloeien voort uit 'Hoofdstuk I.3. Brexit en de relatie tussen Belgische en Britse inlichtingendiensten' en 'Hoofdstuk I.5. Het Memorandum of Understanding tussen de ADIV en de Rwandese inlichtingendiensten'.

samenwerking. De bepalingen uit de richtlijn dienen blijvend te worden nageleefd.[304] Er dienst in een gezamenlijke evaluatie te worden voorzien, met name met betrekking tot het criterium 'belemmeringen', wanneer de buitenlandse partner samenwerkt met de VSSE én de ADIV.

Indien er op een bepaald moment repercussies zouden kunnen ontstaan inzake de bescherming van persoonsgegevens (omdat het Verenigd Koninkrijk eventueel zou afwijken van de GDPR-regels) dan komt het de inlichtingendiensten die daarmee geconfronteerd worden toe om de verschillende nationale bevoegde instanties (de bevoegde ministers en de verschillende databeschermingsautoriteiten) daarover te vatten.[305]

Verder wordt de ADIV aanbevolen om de minister van Defensie te verzoeken om samen met de minister van Justitie de richtlijn van 26 september 2016 aan te passen om voortaan voorafgaand aan elke (formele of informele) samenwerking met een buitenlandse partner (al dan niet uitgaand van een staat) een ministeriële toestemming te voorzien.

Ten slotte dient de ADIV binnen een termijn van twee jaar al zijn internationale relaties te evalueren in het licht van richtlijn van 26 september 2016. Deze evaluatie dient de concrete elementen te specifiëren die tot de indeling in categorieën hebben geleid. De tweejaarlijkse evaluatie van de buitenlandse inlichtingendiensten en de opvolging van de samenwerking moet systematisch worden uitgevoerd overeenkomstig de richtlijn van 26 september 2016.

XII.1.4. AANPASSING VAN ARTIKEL 20 W.I&V

Er wordt aanbevolen dat de ADIV binnen de minister van Defensie verzoekt, om samen met de minister van Justitie, een wetsontwerp in te dienen om artikel 20 W.I&V te laten aanpassen om te zorgen dat de Franse en Nederlandse versie overeenstemmen.

---

304 Op 23 januari 2020 werd door de kamerleden Meryame Kitir en Kris Verduyckt een wetsvoorstel ingediend om een dergelijke evaluatie van de samenwerking met buitenlandse diensten in te schrijven in de W.I&V. Deze evaluatie zou gebaseerd zijn op tenminste zes criteria. Wetsvoorstel tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, *Parl. St.*, Kamer 2019-20, 23 januari 2020, 0956/001. Het Comité formuleerde daarover een omstandig advies (www.comiteri.be).

305 Omgekeerd is het ook belangrijk dat wanneer nationale instanties weet zouden hebben van gevolgen van de Brexit die ook voor de inlichtingendiensten van belang zijn, zij deze tijdig zouden vatten en bij eventuele discussies zouden betrekken.

XII.1.5. VOORAFGAANDELIJKE MINISTERIËLE TOESTEMMING BIJ HET AFSLUITEN VAN SAMENWERKINGSAKKOORDEN EN DE SYSTEMATISCHE CLASSIFICATIE

Het Vast Comité I beveelt aan dat de ADIV systematisch een voorafgaande ministeriële toestemming verkrijgt bij het afsluiten van samenwerkingsakkoorden zonder daarvoor te wachten op de wijziging van de richtlijn. De ADIV heeft zich daartoe al verbonden voor de MoU's.[306]

Tevens dienen nieuwe samenwerkingsovereenkomsten met buitenlandse partners systematisch te worden geclassificeerd overeenkomstig de Wet van 11 december 1998.

XII.1.6. HET AFSLUITEN VAN EEN SAMENWERKINGSAKKOORD TUSSEN DE VSSE EN DE ADIV

Het Vast Comité I beveelt de Nationale Veiligheidsraad en de twee inlichtingendiensten aan om uitvoering te geven aan de verplichting vervat in artikel 20 § 4 W.I&V[307] om respectievelijk een richtlijn en een samenwerkingsakkoord op te stellen. Het Vast Comité I is van oordeel dat het model van een *Joint Intelligence Task Force* een geslaagd initiatief is. Dit initiatief zou met evenveel succes kunnen worden toegepast op andere thematieken in de toekomst. De directies van beide diensten dienen daarbij wel rekening te houden met minpunten van het project, zoals deze door de VSSE en de ADIV in hun interne evaluaties werden vastgesteld.

XII.1.7. GEAUTOMATISEERDE TOOLS VOOR DE MONITORING VAN SOCIALE MEDIA

Het Vast Comité I stelde vast dat de monitoring van sociale media door de inlichtingendiensten nog op een grotendeels arbeidsintensieve manier gebeurt.[308] De diensten beschikken momenteel over te weinig geautomatiseerde tools om een

---

306 Het Comité werd op de hoogte gebracht dat de ADIV projecten ontwikkelt in het kader van het afsluiten van MoU's, aangaande het beheer van zijn strategische betrekkingen alsook wat betreft de te volgen procedure bij zijn internationale contacten. Het Comité zal de uitvoering van deze projecten evalueren in het jaar dat volgt op deze aanbevelingen.

307 "*Voor de opdrachten omschreven in artikel 7, 3°/1 en artikel 11, §1, 5°, sluiten de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid een samenwerkingsakkoord op grond van richtlijnen verkregen van de Nationale Veiligheidsraad*". Deze opdrachten betreffen "*het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied*".

308 Zie 'Hoofdstuk I.6. Informatie- en communicatietechnologieën in het inlichtingenproces bij de ADIV'.

meer efficiënte aanpak mogelijk te maken. Het Vast Comité I acht het aangewezen om hier in de toekomst in te investeren, gezien het toenemende belang van sociale en alternatieve media bij de verspreiding van propaganda en desinformatie ter beinvloeding van de publieke opinie.

XII.1.8. NALEVEN VAN DE TUCHTRECHTELIJKE EN GERECHTELIJKE PROCEDURES DOOR DE ADIV (TIJDENS BUITENLANDSE MISSIES)

Naar aanleiding van incidenten in een niet nader vernoemde buitenlandse operatiezone,[309] werden door het Comité diverse punctuele maatregelen (onder meer in verband met de bronwerking) aanbevolen om de veiligheid van de ingezette manschappen te vrijwaren.

De ADIV wordt aanbevolen om de geldende tuchtrechtelijke en gerechtelijke procedures rigoureus na te leven.

Het Comité komt ook terug op een eerdere aanbeveling[310] waarbij werd gesteld dat de ADIV van ieder veiligheidsincident een uitvoerig verslag moet opmaken dat alle dimensies (niet alleen technisch, maar ook op vlak van het gedrag) onderzoekt en analyseert, vooral wanneer een van de betrokkenen houder is van een veiligheidsmachtiging. Dit verslag moet worden bezorgd aan de bevoegde veiligheidsoverheid, eventueel samen met een voorstel van besluit.

XII.2. AANBEVELING IN VERBAND MET DE DOELTREFFENDHEID VAN HET TOEZICHT

XII.2.1. EEN STRIKTE NALEVING VAN ARTIKEL 33 W.TOEZICHT DOOR DE ADIV

Het Vast Comité I blijft herhalen dat artikel 33 W.Toezicht moet worden nageleefd door de ADIV. In bijzonderheid wordt de ADIV aanbevolen om alle MoU's en de bijbehorende ministeriële toestemming systematisch aan het Comité door te gegeven, evenals de ministeriële goedkeuringen in het geval van informele samenwerking.

309 Zie 'Hoofdstuk I.10. Incidenten in een buitenlandse operatiezone'.
310 Zie VAST COMITE I, *Activiteitenverslag 2015*, 109.

XII.2.2. DE REALISATIE VAN EEN SYSTEEM VAN INTERNE CONTROLE DOOR DE ADIV

Het Vast Comité beveelt de ADIV aan om een systeem van interne controle in te voeren om de naleving van alle procedures met betrekking tot internationale relaties te waarborgen.

XII.2.3. HERINNERING AAN DE TOEPASSING VAN ARTIKEL 38 W.TOEZICHT

Artikel 38 W.Toezicht voorziet in twee vormen van communicatie van de gerechtelijke autoriteiten naar de voorzitter van het Vast Comité I.

Vooreerst wordt voorzien dat de procureur-generaal en de auditeur-generaal ambtshalve een kopie sturen van de vonnissen en arresten betreffende misdaden of wanbedrijven begaan door leden van de inlichtingendiensten en het OCAD. Een tweede paragraaf stelt dat de procureur des Konings, de arbeidsauditeur, de Federale Procureur of de Procureur-generaal, al naar het geval, de voorzitter op de hoogte brengen telkens als tegen een lid van een inlichtingendienst of het OCAD een opsporingsonderzoek of gerechtelijk onderzoek wegens misdaad of wanbedrijf wordt ingesteld.

De COL 8/2014 preciseert dit door te stellen dat er sprake is van een 'systematische communicatie'.

Aangezien (in hoofdzaak de tweede paragraaf van) artikel 38 W.Toezicht niet steeds wordt nageleefd, wordt deze verplichting in herinnering gebracht.[311]

[311] De Omzendbrief van het College van Procureurs-generaal (COL 08/2014) houdende mededeling van opsporingsonderzoeken, vervolgingen en veroordelingen van ambtenaren, en personen die taken van openbaar belang waarnemen of die functies uitoefenen die doorgaans een gezagsrealtie met minderjarigen of kwetsbare personen impliceren, werd herzien op 9 januari 2020.

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 2020 TOT 31 DECEMBER 2020)

Wet van 8 juli 2020 tot wijziging van de wet van 21 maart 2018 tot wijziging van de wet op het politieambt om het gebruik van camera's door de politiediensten te regelen, en tot wijziging van de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en van de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid, *BS* 15 juli 2020

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

K.B. 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* 1 oktober 2020

K.B. 8 mei 2018 tot vaststelling van de activiteitensectoren en de bevoegde administratieve overheden bedoeld in artikel 22*quinquies*, § 7, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen — Duitse vertaling, *BS* 15 december 2020

M.B. 18 april 2020 tot delegatie van de bevoegdheid om een verzoek tot inzage, uitleg of mededeling in afschrift van een bestuursdocument dat de Veiligheid van de Staat onder zich heeft, af te wijzen, *BS* 18 mei 2020

M.B. 27 april 2020 houdende overdracht van bevoegdheid en handtekening inzake personeelsaangelegenheden voor de Veiligheid van de Staat aan de administrateur-generaal van de Veiligheid van de Staat, *BS* 18 mei 2020

Vergelijkende selectie van Nederlandstalige Documentalisten Inlichtingen en Veiligheid (m/v/x) (niveau B) voor het Ministerie van Defensie — selectienummer: ANG19407, *BS* 6 januari 2020

Resultaat van de vergelijkende selectie van Franstalige ICT Specialisten (m/v/x) (niveau A) voor het Ministerie van Defensie — selectienummer: AFG19342, *BS* 13 januari 2020

Vergelijkende selectie van Franstalige Media-Analist (m/v/x) (niveau A1) voor het Ministerie van Defensie — selectienummer: AFG19394, *BS* 13 januari 2020

Resultaat van de vergelijkende selectie van Nederlandstalige Psychologen (m/v/x) (niveau A1) voor Veiligheid van de Staat — selectienummer: ANG19287, *BS* 14 januari 2020

Vergelijkende selectie van Franstalige Juristen data governance (m/v/x) (niveau A2) voor de Veiligheid van de Staat — selectienummer: MFG20008, *BS* 13 februari 2020

Vergelijkende selectie van Nederlandstalige Juristen data governance (m/v/x) (niveau A2) voor de Veiligheid van de Staat — selectienummer: MNG20014, *BS* 13 februari 2020

Vergelijkende selectie van Franstalige servicedesk medewerkers (m/v/x) (niveau C) voor de Veiligheid van de Staat — selectienummer: AFG20031, *BS* 13 februari 2020

Benoeming van de griffier van het Vast Comité van Toezicht op de inlichtingendiensten (Comité I), *BS* 13 mei 2020

Aanwerving voor onmiddellijke indiensttreding en samenstelling van een wervingsreserve van een Nederlandstalige statutaire secretaris/secretaresse, (niv. B), *BS* 2 juni 2020

Vergelijkende selectie van Franstalige Cyber Security Experts (m/v/x) (niveau A2) voor de Algemene Dienst Inlichting en Veiligheid van het Ministerie van Defensie — selectienummer: AFG20056, *BS* 3 juni 2020

Vergelijkende selectie van Nederlandstalige Cyber Security Experts (m/v/x) (niveau A2) voor de Algemene Dienst Inlichting en Veiligheid van het Ministerie van Defensie —selectienummer: ANG20078, *BS* 3 juni 2020

Resultaat van de vergelijkende selectie van Nederlandstalige Juristen data governance (m/v/x) (niveau A2) voor de Veiligheid van de Staat — selectienummer: MNG20014, *BS* 9 juni 2020

Vergelijkende selectie van Franstalige technisch expert in elektronica (m/v/x) (niveau B), voor het Ministerie van Defensie — selectienummer: AFG20122, *BS* 15 juni 2020

Vergelijkende seledie van Franstalige Cyber Threat Intelligence Analyst (A2) (m/v/x) (niveau A2) voor het Ministerie van Defensie — selectienummer: AFG20128, *BS* 15 juni 2020

Resultaat van de vergelijkende selectie van Franstalige Juristen data governance (m/v/x) (niveau A2) voor Veiligheid van de Staat — selectienummer: MFG20008, *BS* 18 juni 2020

Bericht voorgeschreven bij artikel 74 van de bijzondere wet van 6 januari 1989 Bij beslissing van 1 juli 2020, waarvan de expeditie ter griffie van het Hof is ingekomen op 6 juli 2020, heeft het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten de volgende prejudiciële vraag gesteld : «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, al dan niet in samenhang gelezen met artikel 22 van de Grondwet en/of al dan niet in samenhang gelezen met artikel 8 van het Europees Verdrag voor de rechten van de mens en de fundamentele vrijheden, ondertekend te Rome op 4 november 1950 en goedgekeurd bij de wet van 13 mei 1955, in zoverre het niet in een bijzondere bescherming voorziet, ten gunste van een advocaat, een arts of een journalist, voor de communicatiemiddelen die zij gebruiken voor andere dan beroepsdoeleinden ?». Die zaak is ingeschreven onder nummer 7416 van de rol van het Hof, *BS* 31 augustus 2020

Vergelijkende selectie van Nederlandstalige Management Assistants (m/v/x) (niveau B) voor de Veiligheid van de Staat — selectienummer: ANG20321, *BS* 13 november 2020

Resultaat van de vergelijkende selectie van Franstalige data officers (m/v/x) (niveau B) voor de Veiligheid van de Staat — selectienummer: AFG19290, *BS* 1 december 2020

Resultaat van de vergelijkende selectie van Franstalige case officers (m/v/x) (niveau B) voor de Veiligheid van de Staat — selectienummer: AFG19291, *BS* 1 december 2020

Resultaat van de vergelijkende selectie van Nederlandstalige data officers (m/v/x) (niveau B voor de Veiligheid van de Staat — selectienummer: ANG19326, *BS* 1 december 2020

Resultaat van de vergelijkende selectie van Nederlandstalige Management Assistants (m/v/x) (niveau B) voor de Veiligheid van de Staat — selectienummer: ANG20321, *BS* 31 december 2020

BIJLAGE B.
OVERZICHT VAN DE BELANGRIJKSTE WETSVOORSTELLEN, WETSONTWERPEN, RESOLUTIES EN PARLEMENTAIRE BESPREKINGEN MET BETREKKING TOT DE WERKING, DE BEVOEGDHEDEN EN HET TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN EN HET OCAD (1 JANUARI 2020 TOT 31 DECEMBER 2020)

Kamer van volksvertegenwoordigers

Wetsvoorstel tot wijziging van het Wetboek van de Belgische nationaliteit teneinde de vervallenverklaring van nationaliteit ingevolge terrorisme mogelijk te maken, Parl. St. Kamer 2019-20, nr. 55K0068/004

Voorstel van resolutie over het HR-beleid bij Defensie, Parl. St. Kamer 2019-20, nr. 55K0567/006

Activiteitenverslag 2018 van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Parl. St. Kamer 2019-20, nr. 55K0888/001

Wetsvoorstel tot wijziging van de wet van 30 november 1998 houdende regeling van inlichtingen- en veiligheidsdiensten met het oog op het invoeren van wegingsnotities voor de samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten, Parl. St. Kamer 2019-20, nr. 55K0956/001

Wetsvoorstel tot wijziging van het Strafwetboek, teneinde de terbeschikkingstelling van de strafuitvoeringsrechtbank uit te breiden tot alle terroristische misdrijven, Parl. St. Kamer 2019-20, nr. 55K0969/001

De uitrol van het 5G-netwerk, hoorzitting, verslag, Parl. St. Kamer 2019-20, nr. 55K981/001

Jaarverslag 2018 van Unia, hoorzitting, verslag, Parl. St. Kamer 2019-20, nr. 55K996/001

Voorstel van resolutie tot afschaffing van Operation Vigilant Guardian, Parl. St. Kamer 2019-20, nr. 55K1004/001

Wetsontwerp tot opening van voorlopige kredieten voor de maanden april, mei en juni 2020, Parl. St. Kamer 2019-20, nr. 55K1052/001

Wetsontwerp tot wijziging van de wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten, Parl. St. Kamer 2019-20, nr. 55K1072/001

Voorstel van resolutie over de toekomst van de opdrachten van Defensie inzake hulp aan de natie, Parl. St. Kamer 2019-20, nr. 55K1196/001

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten — vervanging van de griffier — oproep tot kandidaten (*Hand*. Kamer 2019-20, 30 april 2020, CRIV55PLEN038, 70)

Wetsvoorstel houdende diverse bepalingen inzake justitie, onder meer in het kader van de strijd tegen de verspreiding van het coronavirus, Parl. St. Kamer 2019-20, nr. 55K1295/001

Wetsvoorstel tot wijziging van de wet van 21 maart 2018 tot wijziging van de wet op het politieambt om het gebruik van camera's door de politiediensten te regelen, en tot wijziging van de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en van de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid, Parl. St. Kamer 2019-20, nrs. 55K1322/001 en 55K1322/004

Wetsvoorstel tot wijziging van diverse bepalingen betreffende bestuurlijke handhaving en houdende de oprichting van een Directie Integriteitsbeoordelingen voor Openbare Besturen, Parl. St. Kamer 2019-20, nr. 55K1381/001

Wetsvoorstel tot wijziging van de wet van 13 juni 2005 betreffende de elektronische communicatie wat de veiligheid en integriteit van openbare elektronische communicatienetwerken en -diensten betreft, Parl. St. Kamer 2019-20, nr. 55K1488/001

Comité I — benoeming van de eerste plaatsvervanger en van de tweede plaatsvervanger van een Nederlandstalig werkend lid (*Hand*. Kamer 2019-20, 17 september 2020, CRIV55PLEN055, 84)

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten — benoeming van de eerste plaatsvervanger van een Nederlandstalig werkend lid (*Hand*. Kamer 2019-20, 24 september 2020, CRIV55PLEN055, 53)

Wetsontwerp houdende aanpassing van de wet van 30 juni 2020 tot opening van voorlopige kredieten voor de maanden november en december 2020, Parl. St. Kamer 2019-20, nr. 55K1532/001

Gedachtewisseling met Admiraal Michel Hofman, nieuwe Chef Defensie, Parl. St. Kamer 2019-20, nr. 55K1544/001

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten — benoeming van de tweede plaatsvervanger van de heer Pieter-Alexander De Brock, Nederlandstalig werkend lid (*Hand*. Kamer 2019-20, 29 oktober 2020, CRIV55PLEN066, 47)

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten — benoeming van de tweede plaatsvervanger van de heer Pieter-Alexander De Brock, Nederlandstalig werkend lid — uitslag van de stemming (*Hand*. Kamer 2019-20, 29 oktober 2020, CRIV55PLEN067, 10)

Wetsontwerp houdende de Middelenbegroting voor het begrotingsjaar 2021, Parl. St. Kamer 2020-21, nrs. 55K1577/001 en 55K1577/004

Wetsontwerp houdende de Algemene uitgavenbegroting voor het begrotingsjaar 2021, Parl. St. Kamer 2020-21, nrs. 55K1578/001, 55K1578/003, 55K1578/007, 55K1578/012, 55K1578/016, 55K1578/018, 55K1578/023, 55K1578/033, 55K1578/041, 55K1578/042

Verantwoording van de Algemene Uitgavenbegroting voor het begrotingsjaar 2021, Parl. St. Kamer 2020-21, nrs. 55K1579/002, 55K1579/006, 55K1579/007, 55K1579/009 en 55K1579/010

Algemene beleidsnota van de eerste minister, Parl. St. Kamer 2020-21, nrs. 55K1580/005 en 55K1580/016

Beleidsverklaring van de minister van Justitie, Parl. St. Kamer 2020-21, nr. 55K1610/015

Wetsvoorstel teneinde de democratie beter te wapenen tegen elke daad die verband houdt met het nazisme en aanverwant ideologisch gedachtegoed, Parl. St. Kamer 2020-21, nr. 55K1637/001

Operatieplan 2021, hoorzitting, Parl. St. Kamer 2020-21, nr. 55K1706 /001

Voorstel tot wijziging van het Reglement van de Kamer van Volksvertegenwoordigers betreffende de specifieke regels geldend voor de bijzondere commissies teneinde de commissie belast met de controle op de legeraankopen en -verkopen openbaar te kunnen laten vergaderen wanneer de commissie daartoe beslist (1319/1-2) (*Hand*. Kamer 2020-21, 3 december 2020, CRIV55PLEN073, 48)

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten — vervanging van een Franstalig lid — oproep tot kandidaten (*Hand*. Kamer 2020-21, 10 december 2020, CRIV55PLEN074, 31)

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten — rekeningen van het begrotingsjaar 2019 (1676/1-4) *Hand*. Kamer 2020-21, 17 december 2020, CRIV55PLEN081, 68)

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 2020 TOT 31 DECEMBER 2020)

Senaat

Schriftelijke vraag van C. Van Cauter aan de minister van Justitie over de 'extreemrechts en extreemlinks — geweldsdreiging — toename — internationale contacten van de extreemrechts groeperingen — nood aan onderzoek' (Senaat 2019-20, 8 januari 2020, Vr. nr. 7-271)

Schriftelijke vraag van C. Van Cauter aan de minister van Binnenlandse Zaken over de 'extreemrechts en extreemlinks — geweldsdreiging — toename — internationale contacten van de extreemrechts groeperingen — nood aan onderzoek' (Senaat 2019-20, 8 januari 2020, Vr. nr. 7-272)

Schriftelijke vraag van C. Van Cauter aan de minister van Justitie over de 'cybercrime — cyberveiligheid — bedrijfsleven — Veiligheid van de Staat — samenwerking' (Senaat 2019-20, 31 januari 2020, Vr. nr. 7-331)

Schriftelijke vraag van C. Van Cauter aan de minister van Binnenlandse Zaken over de 'cybercrime — cyberveiligheid — bedrijfsleven — Veiligheid van de Staat — samenwerking' (Senaat 2019-20, 31 januari 2020, Vr. nr. 7-332)

Schriftelijke vraag van C. Van Cauter aan de minister van Justitie over 'cybercrime — cyberveiligheid — bedrijfsleven — veilige emailstandaarden' (Senaat 2019-20, 31 januari 2020, Vr. nr. 7-334)

Schriftelijke vraag van C. Van Cauter aan de minister van Justitie over 'cybercrime — cyberveiligheid — bedrijfsleven — Veiligheid van de Staat — offensieve cyberaanvallen — informatiebeveiligingsadviezen' (Senaat 2019-20, 31 januari 2020, Vr. nr. 7-337)

Schriftelijke vraag van C. Van Cauter aan de minister van Binnenlandse Zaken over 'cybercrime — cyberveiligheid — bedrijfsleven — Veiligheid van de Staat — offensieve cyberaanvallen — informatiebeveiligingsadviezen' (Senaat 2019-20, 31 januari 2020, Vr. nr. 7-338)

Schriftelijke vraag van C. Van Cauter aan de minister van Binnenlandse Zaken over 'extreemrechts en extreemlinks — geweldsdreiging — Duitsland — chatsites' (Senaat 2019-20, 9 maart 2020, Vr. nr. 7-385)

Schriftelijke vraag van C. Van Cauter aan de eerste minister over 'cybercrime — cyberveiligheid — bedrijfsleven — Veiligheid van de Staat — samenwerking' (Senaat 2019-20, 25 maart 2020, Vr. nr. 7-419)

Schriftelijke vraag van C. Van Cauter aan de eerste minister over 'cybercrime — cyberveiligheid — bedrijfsleven — Veiligheid van de Staat — offensieve cyberaanvallen — informatiebeveiligingsadviezen' (Senaat 2019-20, 25 maart 2020, Vr. nr. 7-420)

Schriftelijke vraag van S. D'Hose aan de minister van Binnenlandse Zaken over de 'Coronacrisis — destabilitatiecampagne — fake news – ondermijning van de democratie' (Senaat 2019-20, 31 maart 2020, Vr. nr. 7-422)

Schriftelijke vraag van S. D'Hose aan de minister van Buitenlandse Zaken over de 'Coronacrisis — destabilitatiecampagne — fake news – ondermijning van de democratie' (Senaat 2019-20, 31 maart 2020, Vr. nr. 7-423)

Schriftelijke vraag van B. De Brabandere aan de minister van Binnenlandse Zaken over 'extreemlinkse gewelddadige groeperingen — groeperingen actief in België' (Senaat 2019-20, 5 juni 2020, Vr. nr. 7-589)

Schriftelijke vraag van R. Daems aan de minister van Justitie over 'inlichtingendiensten — gevolgen van de Brexit — veiligheid — terrorisme — Europees aanhoudingsmandaat' (Senaat 2020-21, 9 november 2020, Vr. nr. 7-757)

Schriftelijke vraag de G. D'haeseleer aan de minister van Justitie over 'personen veroordeeld voor terrorisme — personen gevolgd voor radicalisme — cijfers' (Senaat 2020-21, 9 november 2020, Vr. nr. 7-763)

Schriftelijke vraag de G. D'haeseleer aan de minister van Justitie over 'personen veroordeeld voor terrorisme — personen gevolgd voor radicalisme — cijfers' (Senaat 2020-21, 9 november 2020, Vr. nr. 7-764)

Schriftelijke vraag van S. D'Hose aan de minister van Justitie over 'extreemrechts en extreemlinks — geweldsdreiging — Duitsland – chatsites' (Senaat 2020-21, 9 november 2020, Vr. nr. 7-769)

Schriftelijke vraag van S. D'Hose aan de aan de staatssecretaris voor Digitalisering over ' cybercrime – cyberveiligheid – bedrijfsleven – Veiligheid van de Staat – offensieve cyberaanvallen – informatiebeveiligingsadviezen' (Senaat 2020-21, 9 november 2020, Vr. nr. 7-803)

Kamer van volksvertegenwoordigers

Vraag van M. Freilich aan de eerste minister over '5G – veiligheidsrisico's' (*Vr. en Ant*. Kamer 2019-20, 7 januari 2020, QRVA 8, 80, Vr. nr. 11)

Vraag van J. Chanson aan de minister van Binnenlandse Zaken over de 'strijd tegen sektarische uitwassen' (*Vr. en Ant*. Kamer 2019-20, 7 januari 2020, QRVA 8, 150, Vr. nr. 269)

Vraag van J. Arens aan de minister van Binnenlandse Zaken over de 'situatie van de vijf FGP's van de federale politie' (*Vr. en Ant*. Kamer 2019-20, 7 januari 2020, QRVA 8, 164, Vr. nr. 279)

Vraag van M. Freilich aan de minister van Telecommunicatie over '5G – veiligheidsrisico's' (*Vr. en Ant*. Kamer 2019-20, 7 januari 2020, QRVA 8, 227, Vr. nr. 44)

Actualiteitsdebat over de problematiek van de FTF'ers en toegevoegde vragen van K. Jadin, M. Ben Achour, G. Dallemagne, E. Samyn en S. Cogolati aan de minister van Buitenlandse Zaken over 'het terugsturen van Belgische jihadisten door Turkije' (*Hand.* Kamer 2019-20, 8 januari 2020, CRIV55COM083, 38, Vr. nrs. 1550, 1563, 1566, 1646, 1565, 1681 en 2239)

Samengevoegde vragen van S. Cogolati, W. De Vriendt en E. Van Hoof aan de minister van Buitenlandse Zaken over 'de inmengingen van de Rwandese inlichtingendiensten in België' (*Hand.* Kamer 2019-20, 21 januari 2020, CRIV55COM091, 19, Vr. nrs. 1884, 1895 en 2305)

Samengevoegde vragen van S. Cogolati en W. De Vriendt aan de minister van Buitenlandse Zaken over 'de cyberaanvallen op de Belgische delegatie in China' (*Hand.* Kamer 2019-20, 21 januari 2020, CRIV55COM091, 28, Vr. nrs. 1890 en 1897)

Vraag van M. Freilich aan de minister van Binnenlandse Zaken over het 'toenemend antisemitisme' (*Vr. en Ant*. Kamer 2019-20, 22 januari 2020, QRVA 9, 153, Vr. nr. 284)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over de 'Federale politie — personeelsbestand' (*Vr. en Ant*. Kamer 2019-20, 22 januari 2020, QRVA 9, 169, Vr. nr. 293)

Vraag van S. Rohonyi aan de minister van Justitie over de 'follow-up van wegens terrorisme veroordeelde gedetineerden tijdens en na de detentie' (*Hand.* Kamer 2019-20, 29 januari 2020, CRIV55COM099, 13, Vr. nr. 2666)

Samengevoegde vragen van B. Pas, J.-M. Dedecker en P. De Roover aan de eerste minister over 'de repatriëring van IS-kinderen' (*Hand*. Kamer 2019-20, 30 januari 2020, CRIV55PLEN022, 1, Vr. nrs. 394, 401 en 411)

Vraag van T. Vandenput aan de minister van Binnenlandse Zaken over 'de Vias-studie over de inzameling van biometrische gegevens' (*Hand*. Kamer 2019-20, 30 januari 2020, CRIV55PLEN022, 11, Vr. nr. 405)

Vraag van O. Depoortere aan de minister van Justitie over 'het onderzoek naar de activiteiten van de zogenaamde Grijze Wolven in België' (*Hand.* Kamer 2019-20, 5 februari 2020, CRIV55COM103, 8, Vr. nr. 2778)

Actualiteitsdebat over 5G en toegevoegde vragen van M. Freilich, L. Dierick, V. Matz en K. Verhelst aan de minister van Telecommunicatie over 'de vermeende samenwerking tussen Huawei en de Chinese veiligheidsdiensten' (*Hand.* Kamer 2019-20, 5 februari 2020, CRIV55COM104, 1, Vr. nrs. 2594, 2822, 2978, 3075, 3076 en 3085)

Vraag van D. Van Langenhove aan de minister van Justitie over 'salafisme in België' (*Hand.* Kamer 2019-20, 6 februari 2020, CRIV55PLEN023, 13, Vr. nr. 421)

Samengevoegde vragen van P. De Roover, B. Pas en S. Cogolati aan de eerste minister over 'de acties van de regering naar aanleiding van het vonnis over de IS-kinderen' (*Hand.* Kamer 2019-20, 6 februari 2020, CRIV55PLEN023, 20, Vr. nrs. 423, 433 en 442)

Vraag van J. Soors aan de minister van Justitie over 'delen van informatie over terreur en radicalisering met de Verenigde Saten' (*Vr. en Ant*. Kamer 2019-20, 13 februari 2020, QRVA 11, 48, Vr. nr. 234)

Gedachtewisseling met de minister van Buitenlandse Zaken naar aanleiding van zijn recent bezoek aan Jordanië, Irak en Libanon en toegevoegde vragen van K. Jadin, M. Ben Achour, S. Cogolati, J. Soors, E. Samyn, P. De Roover, G. Dallemagne en W. De Vriendt aan de minister van Buitenlandse Zaken over 'de situatie in Irak' (*Hand.* Kamer 2019-20, 18 februari 2020, CRIV55COM113, 1, Vr. nrs. 2129, 2173, 2564, 2686, 2711, 2840, 2887, 3103, 3132, 3183, 3184, 3197, 3404 en 3442)

Vraag van E. Samyn aan de minister van Buitenlandse Zaken over de 'Belgische gevangenen in Syrië en Irak' (*Vr. en Ant*. Kamer 2019-20, 24 februari 2020, QRVA 12, 326, Vr. nr. 99)

Vraag van S. Cogolati aan de minister van Buitenlandse Zaken over 'Rwandese doodseskader in België' (*Vr. en Ant*. Kamer 2019-20, 24 februari 2020, QRVA 12, 331, Vr. nr. 107)

Vraag van S. Creyelman aan de minister van Buitenlandse Zaken over 'politieke dossiers bij de ADIV' (*Vr. en Ant*. Kamer 2019-20, 24 februari 2020, QRVA 12, 352, Vr. nr. 143)

Vraag van S. Creyelman aan de minister van Buitenlandse Zaken over 'politieke dossiers bij de VSSE' (*Vr. en Ant*. Kamer 2019-20, 24 februari 2020, QRVA 12, 353, Vr. nr. 145)

Vraag van A. Ponthier aan de minister van Buitenlandse Zaken over de 'gebruik sociale media bij militairen' (*Vr. en Ant*. Kamer 2019-20, 24 februari 2020, QRVA 12, 368, Vr. nr. 165)

Vraag van M. Freilich aan de minister van Buitenlandse Zaken over '5G-netwerken – impact op Defensie en de nationale veiligheid' (*Vr. en Ant*. Kamer 2019-20, 24 februari 2020, QRVA 12, 373, Vr. nr. 182)

Vraag van Y. Van Camp aan de minister van Sociale Zaken over 'het meldpunt voor radicalisering' (*Hand.* Kamer 2019-20, 3 maart 2020, CRIV55COM123, 43, Vr. nr. 2633)

Vraag van V. Scourneau aan de minister van Justitie over het 'illegaal gsm-gebruik in gevangenissen' (*Vr. en Ant*. Kamer 2019-20, 10 maart 2020, QRVA 13, 148, Vr. nr. 186)

Vraag van V. Matz aan de minister van Binnenlandse Zaken over het 'Actieplan Radicalisme — bijwerking' (*Vr. en Ant*. Kamer 2019-20, 10 maart 2020, QRVA 13, 225, Vr. nr. 337)

Vraag van M. Depraetere aan de minister van Telecommunicatie over 'beveiligingsmaatregelen 5G' (*Vr. en Ant*. Kamer 2019-20, 24 maart 2020, QRVA 14, 367, Vr. nr. 110)

Vraag van T. Van Grieken aan de minister van Buitenlandse Zaken over 'islamitische militairen' (*Vr. en Ant*. Kamer 2019-20, 24 maart 2020, QRVA 14, 417, Vr. nr. 204)

Vraag van V. Scourneau aan de minister van Justitie over het 'aantal imams in ons land' (*Vr. en Ant*. Kamer 2019-20, 9 avril 2020, QRVA 15, 115, Vr. nr. 181)

Vraag van C. Thibaut aan de minister van Binnenlandse Zaken over de 'antifascistische betoging te Gilly' (*Vr. en Ant*. Kamer 2019-20, 9 avril 2020, QRVA 15, 211, Vr. nr. 389)

Vraag van S. Cogolati aan de minister van Justitie over 'de bescherming van de Koerdische gemeenschap in België' (*Hand.* Kamer 2019-20, 22 april 2020, CRIV55COM156, 43, Vr. nr. 5102)

Vraag van Ch. Lacroix aan de minister van Buitenlandse Zaken over 'de hervorming van de ADIV' (*Hand.* Kamer 2019-20, 29 april 2020, CRIV55COM162, 19, Vr. nr. 3923)

Samengevoegde vragen van Ch. Lacroix en B. Delvaux aan de minister van Buitenlandse Zaken over 'de strijd tegen fake news en extreemrechts' (*Hand.* Kamer 2019-20, 29 april 2020, CRIV55COM162, 45, Vr. nrs. 5339 en 5524)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over 'IS op sociale media' (*Vr. en Ant*. Kamer 2019-20, 4 mai 2020, QRVA 17, 153, Vr. nr. 444)

Actualiteitsdebat over de repatriëringen vanuit Marokko en toegevoegde vragen van A. Van Bossuyt, S. Cogolati, G. Daems, N. Boukili, M. Ben Achour, F. De Smet, M. De Maegd, J. Crombez, en N. Lanjri over 'de repatriëringen uit Marokko' (*Hand.* Kamer 2019-20, 19 mei 2020, CRIV55COM179, 1, Vr. nrs. 5511, 5645, 5695, 6238, 5761, 5842, 6066, 6073, 6224, 6236 en 6249)

Samengevoegde interpellatie en vragen van A. Van Bossuyt, G. Dallemagne, T. Francken, M. Bihet en A. Ponthier aan de minister van Buitenlandse Zaken over 'de Chinese desinformatie' (*Hand.* Kamer 2019-20, 19 mei 2020, CRIV55COM179, 44, Vr. nrs. 5788, 5876, 5997, 6045, 6051 en 12I)

De impact van COVID-19 op justitie: actualiteitsdebat en toegevoegde vragen van S. Cogolati, S. Van Hecke, L. Hennuy, Ph. Pivin, O. Ozan, S. Thémont, V. Matz, B. Segers, K. Gabriëls, N. Boukili, K. Aouasti en N. Gilson over de 'Chinese spionage in België tijdens de COVID-19-crisis' (*Hand.* Kamer 2019-20, 19 mei 2020, CRIV55COM182, 1, Vr. nrs. 5867, 5885, 5935, 6041, 6062, 6078, 6079, 6148, 6159, 6191, 6228, 6247 en 6242)

Samengevoegde vragen van K. Metsu, B. Segers en Ph. Pivin aan de minister van Justitie over 'de opvolging van vrijgelaten terroristen' (Hand. Kamer 2019-20, 19 mei 2020, CRIV55COM182, 16, Vr. nrs. 5863, 6005 en 6063)

Vraag van M. Freilich aan de minister van Buitenlandse Zaken over de 'staatsteun voor Huawei' (*Vr. en Ant*. Kamer 2019-20, 27 mai 2020, QRVA 19, 370, Vr. nr. 283)

Samengevoegde vragen van S. De Wit, K. Bury en B. Slegers aan de minister van Justitie over 'de ontvoering van een kind door geradicaliseerde moslims' (*Hand.* Kamer 2019-20, 3 juni 2020, CRIV55COM193, 46, Vr. nrs. 6674, 6716 en 6729)

Mondmaskers: actualiteitsdebat en toegevoegde vragen van P. Prévot, J. Bertels, P. Buysrogge, K. Verduyckt, S. Creyelman, J. Crombez, Y. Van Camp, N. Moscufo, H. Bayet, J. Chanson, G. Dallemagne, W. De Vriendt, K. Depoorter en M. Freilich aan de minister van Sociale Zaken over 'de bestelling van 15 miljoen mondmaskers bij het Luxemburgse bedrijf Avrox' (*Hand.* Kamer 2019-20, 3 juni 2020, CRIV55COM195, 1, Vr. nrs. 6195, 6290, 6340, 6354, 6359, 6389, 6393, 6403, 6435, 6461, 6486, 6610, 6618, 6627, 6684, 6690 en 6724)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over de 'waarschuwing tegen extreemrechts'. (*Vr. en Ant*. Kamer 2019-20, 9 juin 2020, QRVA 20, 204, Vr. nr. 516)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over 'extreemlinks'. (*Vr. en Ant*. Kamer 2019-20, 9 juin 2020, QRVA 20, 207, Vr. nr. 517)

Vraag van S. Mahdi aan de minister van Buitenlandse Zaken over 'de aanpak van de dronedreigingen' (*Hand.* Kamer 2019-20, 17 juni 2020, CRIV55COM210, 33, Vr. nr.6187)

Vraag van Ph. Pivin aan de minister van Justitie over 'recidivisme bij Belgische terreurveroordeelden' (*Hand.* Kamer 2019-20, 17 juni 2020, CRIV55COM216, 1, Vr. nr. 6818)

Vraag van L. Dierick aan de minister van Justitie over de 'FOD Justitie — betalingstermijnen' (*Vr. en Ant*. Kamer 2019-20, 18 juin 2020, QRVA 21, 96, Vr. nr. 306)

Vraag van J. Soors aan de minister van Justitie over 'eindevaluatie Kadernota Integrale Veiligheid' (*Vr. en Ant*. Kamer 2019-20, 18 juin 2020, QRVA 21, 101, Vr. nr. 364)

Vraag van S. Van Hecke aan de minister van Justitie over de 'betalingsachterstanden overheid — invoeren FEDCOM bij FOD Justitie' (Vr. en Ant. Kamer 2019-20, 18 juin 2020, QRVA 21, 103, Vr. nr. 373)

Vraag van M. Freilich aan de minister van Buitenlandse Zaken over '5G en de F-35' (*Vr. en Ant*. Kamer 2019-20, 18 juin 2020, QRVA 21, 378, Vr. nr. 374)

Samengevoegde vragen van S. De Wit en K. Bury aan de minister van Justitie over 'de opvolging van de ontvoering van een minderjarige jongen door moslimextremisten' (*Hand.* Kamer 2019-20, 24 juni 2020, CRIV55COM219, 4, Vr. nrs. 7238 en 7256)

Vraag van G. Colebunders aan de minister van Justitie over 'de bezorgdheid van de inlichtingendiensten over de groei van extreemrechts' (*Hand.* Kamer 2019-20, 24 juni 2020, CRIV55COM219, 14, Vr. nr. 7388)

Vraag van J. Soors aan de minister van Justitie over 'de dreiging van extreemrechts' (*Hand.* Kamer 2019-20, 25 juni 2020, CRIV55PLEN047, 19, Vr. nr. 863)

Samengevoegde vragen van K. Verhelst en M. Freilich aan de minister van Telecommunicatie over 'de beslissingen van de NVR met een impact op de selectie van de 5G-providers' (*Hand.* Kamer 2019-20, 25 juni 2020, CRIV55PLEN047, 28, Vr. nrs. 852 en 870)

Actualiteitsdebat over COVID-19 en toegevoegde vragen van P. De Spiegeleer, M. Kitir, M. Bihet, C. Thibaut, O. Depoortere, T. Vandenput, F. Demon, J. Donné, C. Thibaut, B. Segers, K. Metsu, D. Senesael, L. Zanchetta en J. Chanson aan de minister van Binnenlandse Zaken over de 'interventies in treinen en stations n.a.v. de BLM-protesten' (*Hand.* Kamer 2019-20, 30 juni 2020, CRIV55COM223, 1, Vr. nrs. 6955, 6957, 7027, 7032, 7223, 7248, 7363, 7373, 7399, 7463, 7514, 7431, 7503, 7525 en 7527)

Samengevoegde vragen van Ph. Pivin en S. Rohonyi aan de minister van Justitie over 'de info van de SURB met betrekking tot de wegens terrorisme veroordeelde gedetineerden' (*Hand.* Kamer 2019-20, 1 juli 2020, CRIV55COM226, 10, Vr. nrs. 7446 tot 7449 en 7496)

Samengevoegde vragen van C. Taquin, Z. Khattabi en S. Van Hecke aan de minister van Justitie over 'de maatregelen voor de controle op en de bestrijding van sektarische organisaties' (*Hand.* Kamer 2019-20, 1 juli 2020, CRIV55COM226, 22, Vr. nrs.7475, 7515 en 7574)

Samengevoegde vragen van K. Metsu en B. Pas aan de minister van Justitie over 'de repatriering van Syriëstrijders' (*Hand.* Kamer 2019-20, 1 juli 2020, CRIV55COM226, 36, Vr. nrs. 7544 en 7577)

Vraag van S. Cogolati aan de minister van Binnenlandse Zaken over 'de seismische activiteit in Duitsland en de normen inzake nucleaire veiligheid' (*Hand.* Kamer 2019-20, 1 juli 2020, CRIV55COM228, 14, Vr. nr. 7262)

Vraag van V. Matz aan de minister van Binnenlandse Zaken over 'het verslag van de AIG van 2019 over de integriteitscontroles bij de politie' (*Hand.* Kamer 2019-20, 1 juli 2020, CRIV55COM228, 21, Vr. nr. 6940)

Vraag van O. Depoortere aan de minister van Binnenlandse Zaken over 'links-extremisme in België' (*Hand.* Kamer 2019-20, 1 juli 2020, CRIV55COM228, 31, Vr. nr. 7372)

Vraag van C. Taquin aan de minister van Binnenlandse Zaken over 'de maatregelen voor de controle op en de bestrijding van sektarische organisaties' (*Hand.* Kamer 2019-20, 1 juli 2020, CRIV55COM228, 33, Vr. nr. 7476)

Vraag van J. Soors aan de minister van Buitenlandse Zaken over de 'extreemrechtse trainingskampen in Rusland' (*Vr. en Ant*. Kamer 2019-20, 2 juli 2020, QRVA 22, 145, Vr. nr. 526)

Vraag van M. Freilich aan de minister van Buitenlandse Zaken over 'de operationaliteit van DAB' (*Vr. en Ant*. Kamer 2019-20, 2 juli 2020, QRVA 22, 224, Vr. nr. 299)

Vraag van M. Kitir aan de minister van Buitenlandse Zaken over 'de veiligheidsmachtigingen voor het personeel van Brussels Airport' (*Vr. en Ant.* Kamer 2019-20, 2 juli 2020, QRVA 22, 390, Vr. nr. 301)

Vraag van T. Vandenput aan de minister van Binnenlandse Zaken over 'het behoud van de veiligheidsmachtiging van de werknemers van Swissport bij Alyzia' (*Hand.* Kamer 2019-20, 14 juli 2020, CRIV55COM235, 35, Vr. nr. 7757)

Vraag van G. Dallemagne aan de minister van Buitenlandse Zaken over 'de brief van de Chinese ambassade aan La Libre' (*Hand.* Kamer 2019-20, 14 juli 2020, CRIV55COM235, 39, Vr. nr. 7797)

Samengevoegde vragen van S. Cogolati en K. Metsu aan de minister van Justitie over 'het gevaar voor standrechtelijke executies van Belgen in Irak' (*Hand.* Kamer 2019-20, 14 juli 2020, CRIV55COM236, 2, Vr. nrs. 7770 en 7851)

Vraag van S. Schlitz aan de minister van Binnenlandse Zaken over 'de bezorgdheid van Europol m.b.t. de incels, extreemrechts terrorisme en de antifeministen' (*Hand.* Kamer 2019-20, 14 juli 2020, CRIV55COM239, 1, Vr. nr. 7553)

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)

Vraag van J. Soors aan de minister van Justitie over 'fake news over COVID-19 en 5G' (*Vr. en Ant.* Kamer 2019-20, 16 juli 2020, QRVA 23, 78, Vr. nr. 424)

Vraag van E. Burton aan de minister van Binnenlandse Zaken over de 'kidnapping in Genk' (*Vr. en Ant.* Kamer 2019-20, 16 juli 2020, QRVA 23, 141, Vr. nr. 618)

Vraag van Ph. Pivin aan de minister van Justitie over de 'Veiligheid van de Staat — economische spionage in België' (*Vr. en Ant.* Kamer 2019-20, 5 augustus 2020, QRVA 24, 195, Vr. nr. 323)

Vraag van J. Soors aan de minister van Binnenlandse Zaken over 'rechts-extremisme in België' (*Vr. en Ant.* Kamer 2019-20, 5 augustus 2020, QRVA 24, 299, Vr. nr. 640)

Vraag van V. Scourneau aan de minister van Buitenlandse Zaken over 'OSINT' (*Vr. en Ant.* Kamer 2019-20, 5 augustus 2020, QRVA 24, 465, Vr. nr. 407)

Vraag van J. Soors aan de minister van Justitie over 'het jaarrapport van de Veiligheid van de Staat' (*Vr. en Ant.* Kamer 2019-20, 27 augustus 2020, QRVA 25, 161, Vr. nr. 588)

Vraag van B. Friart aan de minister van Justitie over de 'Veiligheid van de Staat' (*Vr. en Ant.* Kamer 2019-20, 27 augustus 2020, QRVA 25, 164, Vr. nr. 590)

Vraag van G. Colebunders aan de minister van Binnenlandse Zaken over 'de bezorgdheid van de veiligheidsdiensten over de extreemrechtse dreiging' (*Vr. en Ant.* Kamer 2019-20, 27 augustus 2020, QRVA 25, 193, Vr. nr. 663)

Vraag van L. Dierick aan de minister van Telecommunicatie over '5G Proximus' (*Vr. en Ant.* Kamer 2019-20, 8 september 2020, QRVA 26, 303, Vr. nr. 252)

Vraag van S. Cogolati aan de minister van Buitenlandse Zaken over de 'rol van de ADIV bij het surveilleren van Belgische jihadisten' (*Vr. en Ant.* Kamer 2019-20, 8 september 2020, QRVA 26, 373, Vr. nr. 460)

Samengevoegde vragen van K. Verduyckt, A. Ponthier, A. Vicaire en S. Mahdi aan de minister van Buitenlandse Zaken over 'de verlenging van de steun van Defensie aan bewakingsopdrachten in het kader van OVG' (*Hand.* Kamer 2020-22, 16 september 2020, CRIV55COM259, 19, Vr. nrs. 8364, 8386, 8493 en 8784)

Vraag van Z. Khattabi aan de minister van Justitie over de 'betalingsachterstand' (*Vr. en Ant.* Kamer 2019-20, 22 september 2020, QRVA 27, 93, Vr. nr. 593)

Vraag van E. Thiébaut aan de minister van Justitie over de 'regeling voor het bezoek van journalisten aan de Belgische gevangenissen' (*Vr. en Ant.* Kamer 2019-20, 22 september 2020, QRVA 27, 107, Vr. nr. 639)

Samengevoegde vragen van S. Van Hecke, S. De Wit, K. Gabriëls en N. Lanjri aan de Minister van Justitie over 'justitie en het drugsgeweld in Antwerpen' (*Hand.* Kamer 2020-22, 23 september 2020, CRIV55COM268, 13, Vr. nrs. 8511, 8512, 8649, 8757 en 8872)

Samengevoegde vragen van S. Van Hecke en Z. Khattabi aan de minister van Justitie over 'het gebrek aan toezicht op de sekten' (*Hand.* Kamer 2020-22, 23 september 2020, CRIV55COM268, 21, Vr. nrs. 8540 en 8725)

Samengevoegde vragen van S. Van Hecke aan de minister van Justitie over 'de vertrouwenspersoon en het meldpunt voor integriteitsschendingen bij de Staatsveiligheid' (*Hand.* Kamer 2020-22, 23 september 2020, CRIV55COM268, 46, Vr. nrs. 8894 en 8895)

Vraag van J. Soors aan de minister van Justitie over 'buitenlandse trainingskampen' (*Vr. en Ant*. Kamer 2019-20, 30 september 2020, QRVA 28, 54, Vr. nr. 586)

Vraag van J. Chanson aan de minister van Binnenlandse Zaken over het 'isolement bij slachtoffers van sektarische organisaties' (*Vr. en Ant*. Kamer 2019-20, 30 september 2020, QRVA 28, 107, Vr. nr. 707)

Vraag van J. Soors aan de minister van Buitenlandse Zaken over de 'negatieve veiligheidsadviezen van de Nationale Veiligheidsoverheid' (*Vr. en Ant*. Kamer 2019-20, 30 september 2020, QRVA 28, 406, Vr. nr. 424)

Vraag van A. Ponthier aan de minister van Buitenlandse Zaken over 'het veiligheidscertificaat voor militairen' (*Vr. en Ant*. Kamer 2019-20, 30 september 2020, QRVA 28, 433, Vr. nr. 466)

Vraag van S. Cogolati aan de minister van Buitenlandse Zaken over de 'samenwerkingsakkoord tussen ADIV en de Rwandese NISS' (*Vr. en Ant*. Kamer 2019-20, 30 september 2020, QRVA 28, 451, Vr. nr. 495)

Outsourcing: actualiteitsdebat en toegevoegde vragen van A. Ponthier, K. Jadin, J. Pillen, R. D'Amico en J. aan de minister van Defensie over 'de samenwerking tussen Defensie en Katoen Natie i.k.v. outsourcing' (*Hand.* Kamer 2020-22, 14 oktober 2020, CRIV55COM278, 1, Vr. nrs. 9181, 9382, 9637, 9660 en 9672)

Vraag van A. Van Bossuyt aan de minister van Justitie over 'de aanpak van de Chinese spionage en de opvolging door de Staatsveiligheid' (*Hand.* Kamer 2020-22, 14 oktober 2020, CRIV55COM281, 19, Vr. nr. 9255)

Samengevoegde vragen van G. Dallemagne en J. Soors aan de minister van Justitie over 'de bezorgdheid inzake de middelen en de personeelssterkte van de inlichtingendiensten' (*Hand.* Kamer 2020-22, 14 oktober 2020, CRIV55COM281, 26, Vr. nrs. 9357, 9361 en 9457)

Vraag van G. Dallemagne aan de minister van Justitie over 'het conflict bij de VSSE' (*Hand.* Kamer 2020-22, 14 oktober 2020, CRIV55COM281, 30, Vr. nr. 9358)

Vraag van K. Metsu aan de eerste minister over 'terrorismebestrijding n.a.v. de initiatieven van de Franse president' (*Hand.* Kamer 2020-22, 22 oktober 2020, CRIV55PLEN065, 36, Vr. nr. 1051)

Samengevoegde vragen van O. Depoortere en Ph. Pivin aan de minister van Binnenlandse Zaken over 'de aanpak van islamitische verenigingen na nieuwe terreur in Duitsland en Frankrijk' (*Hand.* Kamer 2020-22, 22 oktober 2020, CRIV55PLEN065, 39, Vr. nrs. 1046 en 1052)

Vraag van A. Van Bossuyt aan de eerste minister over de 'Chinese cyberaanvallen op België' (*Hand.* Kamer 2020-2021, 28 oktober 2020, CRIV55COM291, 12, Vr. nr. 9252)

Vraag van K. Metsu aan de minister van Justitie over 'de imamopleiding' (*Hand.* Kamer 2020-2021, 28 oktober 2020, CRIV55COM295, 28, Vr. nr. 10116)

Samengevoegde vragen van S. Cogolati, B. Segers, Koen Metsu en K. Bury aan de minister van Justitie over 'de aanwezigheid van Syrische oorlogsmisdadigers in België' (*Hand.* Kamer 2020-2021, 28 oktober 2020, CRIV55COM295, 46, Vr. nrs. 10264, 10298, 10350 en 10405)

Vraag van K. Metsu aan de minister van Justitie over de 'Belgische islamitische organisaties die aanzetten tot haat, geweld en discriminatie' (*Hand.* Kamer 2020-2021, 28 oktober 2020, CRIV55COM295, 63, Vr. nr. 10349)

Samengevoegde vragen van K. Metsu en M. Dillen aan de eerste minister over 'de aanslag in Nice' (*Hand.* Kamer 2020-21, 29 oktober 2020, CRIV55PLEN066, 19, Vr. nrs. 1072 en 1076)

Vraag van Y. Van Camp aan de minister van Migratie over 'geradicaliseerde moslims' (*Hand.* Kamer 2020-2021, 30 oktober 2020, CRIV55COM296, 20, Vr. nr. 10086)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over 'de samenwerking tussen de politie en Defensie in de strijd tegen het terrorisme' (*Hand.* Kamer 2020-21, 12 november 2020, CRIV55PLEN070, 30, Vr. nr. 1104)

Actualiteitsdebat over de terrorismedreigin en toegevoegde vragen van M. De Maegd, K. Metsu, O. Depoortere, Ph. Pivin, T. Vandenput, F. Demon, E. Thiébaut, D. Ducarme, G. Dallemagne en F. De Smet, aan de minister van Binnenlandse Zaken over 'het antwoord op de terreurdreiging in België' (*Hand.* Kamer 2020-2021, 16 november 2020, CRIV55COM303, 1, Vr. nrs. 10001, 10412, 10424, 10516, 10522, 10525, 10524, 10526, 10565, 10679, 10690, 10692, 10724, 10812, 10813, 10814, 10816 en 10817)

Vraag van K. Metsu aan de minister van Justitie over 'recidive bij terreurveroordeelden' (*Vr. en Ant.* Kamer 2019-20, 2 december 2020, QRVA 29, 184, Vr. nr. 6)

Vraag van J. Soors aan de minister van Justitie over 'de nationale terroristenlijst' (*Vr. en Ant.* Kamer 2019-20, 2 december 2020, QRVA 29, 188, Vr. nr. 11)

Vraag van M. Dillen aan de minister van Justitie over de 'vrijlating veroordeelde terroristen NISS' (*Vr. en Ant.* Kamer 2019-20, 2 december 2020, QRVA 29, 222, Vr. nr. 95)

Vraag van K. Metsu aan de minister van Justitie over de 'positieve verderzetting Zweedse projecten veiligheid' (*Vr. en Ant.* Kamer 2019-20, 2 december 2020, QRVA 29, 260, Vr. nr. 82)

Vraag van M. Vindevoghel aan de minister van Ambtenarenzaken over 'de rol van bpost en Proximus bij de coronavaccins' (*Hand.* Kamer 2020-2021, 8 december 2020, CRIV55COM313, 53, Vr. nr. 11472)

Vraag van K. Verduyckt aan de minister van Binnenlandse Zaken over 'de toegang tot versleutelde informatie en chats in de strijd tegen terrorisme' (*Hand.* Kamer 2020-2021, 9 december 2020, CRIV55COM315, 43, Vr. nr. 11428)

Vraag van S. Verherstraeten aan de minister van Justitie over 'het strafproces n.a.v. de verijdelde bomaanslag door een Iraans-Belgisch koppel' (*Hand.* Kamer 2020-2021, 9 december 2020, CRIV55COM316, 18, Vr. nr. 11196)

Vraag van C. Thibaut aan de minister van Justitie over de 'QAnon-aanhangers op het Belgische grondgebied' (*Hand.* Kamer 2020-2021, 9 december 2020, CRIV55COM316, 27, Vr. nr. 11299)

Vraag van C. Thibaut aan de minister van Justitie over 'de mogelijke activiteiten in België van figuren die het ideeëngoed van de Grijze Wolven delen' (*Hand.* Kamer 2020-2021, 9 december 2020, CRIV55COM316, 29, Vr. nr. 11300)

Samengevoegde vragen van C. Thibaut aan de minister van Justitie over 'de rol en de traagheid van de federale overheid in de erkenning van de Grote Moskee in Brussel' (*Hand.* Kamer 2020-2021, 9 december 2020, CRIV55COM316, 30, Vr. nrs. 11301 en 11386)

Vraag van M. Freilich aan de minister van Justitie over 'TikTok' (*Vr. en Ant.* Kamer 2020-21, 9 december 2020, QRVA 30, 257, Vr. nr. 49)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over de 'negatieve veiligheidsadviezen voor douaniers' (*Vr. en Ant.* Kamer 2020-21, 9 december 2020, QRVA 30, 352, Vr. nr. 12)

Vraag van K. Bury aan de minister van Justitie over de 'radicaalislamitische imams, moskeeën en verenigingen' (*Vr. en Ant.* Kamer 2020-21, 16 december 2020, QRVA 31, 315, Vr. nr. 58)

Vraag van T. Van Grieken aan de minister van Justitie over 'de erkenning van moskeeën' (*Vr. en Ant.* Kamer 2020-21, 16 december 2020, QRVA 31, 318, Vr. nr. 63)

Vraag van T. Van Grieken aan de minister van Justitie over de 'screening van kandidaat-asielzoekers' (*Vr. en Ant.* Kamer 2020-21, 16 december 2020, QRVA 31, 339, Vr. nr. 115)

Vraag van S. Van Hecke aan de minister van Justitie over de 'VSSE – welzijn – vertrouwenspersoon en integriteit' (*Vr. en Ant.* Kamer 2020-21, 16 december 2020, QRVA 32, 383, Vr. nr. 57)

Vraag van K. Gabriëls aan de minister van Justitie over 'VSSE – recente hervormingen' (*Vr. en Ant.* Kamer 2020-21, 16 december 2020, QRVA 32, 385, Vr. nr. 67)

Vraag van Ph. Pivin aan de minister van Justitie over de 'screening van gevangenisbezoekers' (*Vr. en Ant.* Kamer 2020-21, 16 december 2020, QRVA 33, 238, Vr. nr. 181)

RAPPORT D'ACTIVITÉS 2020
ACTIVITEITENVERSLAG 2020

Quis custodiet ipsos custodes ?

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

Rédaction

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

Déjà parus dans cette série

1) D. Van Daele, en B. Vangeebergen, *Inlichtingendiensten en strafprocedure in Nederland, Duitsland en Frankrijk,* 2006, 166 p.
2) Comité permanent R, *Rapport d'activités 2006,* 2007, 147 p.
3) Comité permanent R, *Rapport d'activités 2007,* 2008, 87 p.
4) Belgian Standing Committee I (ed.), *All Source Threat Assessments in the Fight against Terrorism - Fusion Centres throughout Europe*, 2010, 220 p.
5) Comité permanent R, *Rapport d'activités 2008,* 2009, 131 p.
6) W. Van Laethem, D. Van Daele en B. Vangeebergen (eds.), *De Wet op de bijzondere inlichtingenmethoden,* 2010, 298 p.
7) Comité permanent R, *Rapport d'activités 2009,* 2010, 127 p.
8) Comité permanent R, *Rapport d'activités 2010,* 2011, 119 p.
9) Comité permanent R, *Rapport d'activités 2011,* 2012, 134 p.
10) W. Van Laethem et J. Vanderborght, *Regards sur le contrôle. Vingt ans de contrôle démocratique sur les services de renseignement*, 2013, 565 p.
11) Comité permanent R, *Rapport d'activités 2012*, 2013, 127 p.
12) Comité permanent R, *Rapport d'activités 2013*, 2014, 212 p.
13) Comité permanent R, *Rapport d'activités 2014*, 2015, 141 p.
14) Comité permanent R, *Rapport d'activités 2015*, 2016, 131 p.
15) Comité permanent R, *Rapport d'activités 2016*, 2017, 227 p.
16) Comité permanent R, *Rapport d'activités 2017*, 2018, 152 p.
17) Comité permanent R, *Rapport d'activités 2018*, 2019, 167 p.
18) J. Vanderborght (ed.), *Les méthodes particulières de renseignement : de l'ombre à la lumière*, 2019, 151 p.
19) Comité permanent R, *Rapport d'activités 2019*, 2020, 148 p.
20) Comité permanent R, *Rapport d'activités 2020*, 2021, 189 p.

RAPPORT D'ACTIVITÉS 2020

Comité permanent de Contrôle des services de renseignement et de sécurité

Comité permanent de Contrôle des services
de renseignement et de sécurité

Le présent Rapport d'activités 2020 a été approuvé par le Comité permanent de Contrôle des services de renseignement et de sécurité lors de la réunion du 12 juillet 2021.

(soussignés)
Serge Lipszyc, président
Pieter-Alexander De Brock, conseiller
Thibaut Vandamme, conseiller
Wauter Van Laethem, greffier faisant fonction

Rapport d'activités 2020
Comité permanent de Contrôle des services de renseignement et de sécurité

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

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

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS

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

BELPIU	*Belgian Passenger Information Unit* (Unité belge d'information des passagers)
BINII	*Belgian Intelligence Network Information Infrastructure*
BNG	Banque de données nationale générale
BPR	*Business Process Re-engineering*
BPS	Bruxelles Prévention & Sécurité
BSS	*British Security Service* (MI5)
CCB	Centre pour la Cybersécurité Belgique
CCIRM	*Collection Coordination Information Requirement Management* (SGRS)
CCRS	Comité de coordination du renseignement et de la sécurité
CEDH	Convention européenne des droits de l'homme
CGRA	Commissariat général aux réfugiés et aux apatrides
CHOD	*Chief of Defence*
CI	*Counterintelligence*
CIA (model)	*Confidentiality, Integrity & Availability (model)*
CNCIS	Commission nationale de contrôle des interceptions de sécurité
CNCTR	Commission nationale de contrôle des techniques de renseignement
CNS	Conseil national de sécurité
C.O.C.	Organe de contrôle de l'information policière
Comité permanent P	Comité permanent de Contrôle des services de police
Comité permanent R	Comité permanent de Contrôle des services de renseignement et de sécurité
Commission BIM	Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité
CRABV	Compte Rendu Analytique – *Beknopt Verslag*
CRIV	Compte Rendu Intégral – *Integraal Verslag*
CSIL	Cellule de Sécurité Intégrale Locale
CTG	*Counter Terrorism Group*
CTIVD	*Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten*
DA	Directeur Analyse
DGCC	Direction générale du Centre de crise
DIA	*Defence Intelligence Agency*
DISCC	*Defense Intelligence and Security Coordination Centre* (SGRS)
Doc. parl.	Documents parlementaires de la Chambre et du Sénat
DoD	*US Department of Defense*

DPA	*Data Protection Authority*
DPO	*Data Protection Officer*
DRP	*Disaster recovery plan*
EEAS	*European External Action Service*
ELSJ	Espace de liberté, de sécurité et de justice
EPV	Extrémistes potentiellement violents
ERM	École Royale Militaire
ERS	École de Renseignement et de Sécurité
EU INTCEN	*EU Intelligence and Analyses Centre*
EUMS	*European Union Military Staff*
FTF	*Foreign terrorist fighters*
GCHQ	*General Communications Headquarters*
GRU	Service de renseignement militaire russe
HTF	*Homegrown terrorist fighters*
HUMINT	*Human intelligence*
ICP	*Intelligence collection plan*
ICT	*Information and communications technology*
IFDH	Institut fédéral pour la protection et la promotion des droits humains
IMINT	*Image intelligence*
IPCO	*Investigatory Powers Commissioner's Office*
ISTAR (Bataillon)	*Intelligence, surveillance, target acquisition and Reconnaissance* (Bataillon)
ITIL	*Information Technology Infrastructure Library*
JDR	*Joint Detection Reports*
JTIF	*Joint Intelligence Task Force*
L.Contrôle	Loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace
L.C&HS	Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité
LFP	Loi du 5 août 1992 sur la fonction de police
L.OCAM	Loi du 10 juillet 2006 relative à l'analyse de la menace
Loi APD	Loi du 3 décembre 2017 portant création de l'Autorité de protection des données
Loi MRD	Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité
Loi PNR	Loi du 25 décembre 2016 relative au traitement des données des passagers
L.Org.recours	Loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité

LPA	Loi du 11 avril 1994 relative à la publicité de l'administration
LPD	Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (Loi protection des données)
L.R&S	Loi du 30 novembre 1998 organique des services de renseignement et de sécurité
LTF	*Local task force*
M.B.	Moniteur belge
MEDINT/MEDINTEL	*Medical intelligence*
MoU	*Memorandum of Understanding*
MPG	Matière, problématique, géographie
MRD	Méthodes de recueil des données
NA	Note aux autorités
NISS	Service de renseignement rwandais
NOS	*Nato Office of Security*
NSO	*NATO Standardization Office*
OCAM	Organe de coordination pour l'analyse de la menace
OE	Office des étrangers
OSINT	*Open sources intelligence*
OTAN	Organisation du Traité de l'Atlantique Nord
PCT	Personnes condamnées pour terrorisme
PES	Potentiel économique et scientifique
PH	Propagandistes de haine
Plan R	Plan d'action Radicalisme
PROTEUS	Banque de données de l'OCAM
PSNR	Plan Stratégique National de Renseignement
Q. et R.	Questions et réponses écrites (Chambre ou Sénat)
RFI	*Request for information*
RGPD	Règlement Général sur la Protection des Données
SGRS	Service Général du Renseignement et de la Sécurité
SIDIS Suite	Banque de données pénitentiaire
SIGINT	*Signal intelligence*
SIS	*Secret Intelligence Service* (MI6)
SITRAN	Signalétique transversale (banque de données SPF Finances)
SOP	*Standard Operating Procedures*
SPF	Service public fédéral
SQL	*Structured query language*
TCEI	*Transatlantic Commission on Election Integrity*
TF	*Terrorist fighters*
UE	Union européenne
VSSE	Sûreté de l'État

PRÉFACE

Deux mille vingt, pour le Comité permanent R, a débuté par l'organisation d'un colloque international avec pour thème 'Les dix ans de la Loi BIM' (Loi MRD). À cette occasion sont intervenus le Président de la Chambre, le Vice-premier ministre et ministre de la Justice, la '*Special Rapporteur*' de l'ONU, les Chefs des services de renseignement, le Procureur fédéral, mais également le Barreau, la Presse et des représentants de la Société civile. Leur participation essentielle porta sur le bien-fondé des méthodes particulières de renseignement en Belgique. Les intervenants ont développé leurs réflexions tant sur l'importance de la défense de la protection de l'État que des libertés individuelles. Nos collègues français et suisses des autorités indépendantes de contrôle ont également participé à cette réflexion sur cet équilibre si fragile.

Quelques semaines plus tard, nous apprenions à connaître le Sars-CoV2. Son développement planétaire a non seulement soulevé – et soulève encore – les questions de protection du citoyen et de respect des droits et libertés individuels, mais a également redonné vigueur au fléau de 'l'intox', des '*fake news*' et aux tentatives de déstabilisation de nos démocraties.

Notre société a été blessée par l'impact que cette pandémie a eu sur nos personnes et nos institutions. Notre quotidien en a été bouleversé.

Pour ne parler que du télétravail, celui-ci a, pendant une longue période, été rendu obligatoire tant pour les entreprises publiques que pour le secteur privé. Cependant, les acteurs de 'la sécurité' ont dû constater que, tant pour les deux services de renseignement que pour le Comité permanent R, ce télétravail était impossible à mettre en œuvre. Cette impossibilité résulte sans doute de la nature de la fonction et, suivant l'expression consacrée, de la nécessité de la continuité du 'service'. Mais la cause principale de cette obligation de rester dans nos bureaux sécurisés est la conséquence de l'absence de système de communication et de travail externe sécurisé en Belgique.

Il est, en effet, toujours impossible au 21ème siècle de travailler depuis son domicile ou ailleurs que dans l'enceinte de nos institutions sur un document 'classifié' ou de pouvoir communiquer, de manière sécurisée, sur un élément SECRET ou TRÈS SECRET. L'absence persistante d'investissement de la part de l'État dans ce domaine régalien finirait par faire penser que les pouvoirs publics sont indifférents au monde du renseignement.

Malgré ce constat, le Comité permanent R entend souligner et se féliciter que l'activité des deux services de renseignement comme celui de l'organe de contrôle s'est poursuivi sans défaillance durant toute la pandémie, souvent en tension par rapport au respect scrupuleux des règles sanitaires individuelles. Pour preuve,

l'absence du moindre plan de vaccination pour ces femmes et ces hommes de 'l'ombre' qui ont œuvré durant toute cette période.

Le contrôle démocratique de ces services s'est renforcé. Le Comité a présenté à la Chambre des représentants sa méthodologie de vérification continue garantissant que l'intervention des services de renseignement en ce qui concerne le travail des 'mandataires politiques' ne faisait pas l'objet d'une surveillance ou d'un contrôle en dehors du cadre légal.

L'évolution de l'extrême droite, en Europe et dans bon nombre de démocraties, nous a amenés à procéder, pour la première fois de l'histoire de ces services, à l'analyse de la manière dont ils appréhendaient cette menace.

Notre engagement s'est également porté sur la manière dont les relations entre les deux services de renseignement avec les partenaires étrangers se concrétisaient. Le Comité permanent R souligna à cette occasion que le contrôle gouvernemental devait rester la clé de voûte de la 'politique internationale' des services de renseignement.

Soucieux d'améliorer le bon fonctionnement de la juridiction administrative en matière d'habilitation, attestations et avis de sécurité, nous avons communiqué au Parlement un texte de révision de son fonctionnement. L'objectif poursuivi consiste non seulement à en faire le 'juge naturel' en matière de sécurité, mais également à faciliter l'accès du justiciable. C'est la raison pour laquelle un site spécifique a été créé pour l'Organe de recours (http://www.organederecours.be).

Notre travail au quotidien, c'est aussi le traitement des plaintes introduites par le citoyen. Elles reçoivent une réponse, soit du Comité permanent R seul, soit en concertation avec les autres organes compétents que sont le Comité permanent P, l'Organe de contrôle de l'information policière (C.O.C.), l'Autorité de protection des données, ou encore le Médiateur fédéral. Le citoyen est confronté à une avalanche d'institutions en matière de protection des données. Le Comité permanent R est demandeur, dans ce domaine, d'une simplification à l'occasion de la révision annoncée de la loi.

Ce qui précède, au demeurant, n'est qu'un reflet des activités multiformes que nous menons sous nos diverses et nombreuses casquettes : nous sommes des contrôleurs/auditeurs dans le cadre de nos enquêtes, nous sommes des conseillers juridiques dans le cadre de plusieurs avis importants au niveau parlementaire, nous sommes à l'écoute dans le débat sur le statut social des agents des services de renseignement, nous sommes des réformateurs en ce qui concerne le changement de management au sein du SGRS, nous sommes initiateurs de projets législatifs, (co-)auteurs de tous les rapports d'activités que nous impose le législateur (par ex. dans le cadre de BELPIU, les bases de données communes, l'Autorité de protection de données, l'utilisation des méthodes particulières de renseignement), comptables quand il s'agit des fonds spéciaux, ou encore, juges avec plus de 200 décisions prises par l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité. Et comme Aristote l'a écrit : « *le tout est plus que la somme des parties* ».

Alors que ces missions ne cessent de croître, nous pensons qu'au moment où la Chambre a lancé une réflexion, notamment sur les synergies entre certaines institutions ou sur le statut du personnel de celles-ci, les questions des moyens budgétaires alloués au Comité permanent R, sur ses réseaux informatiques sécurisés, ne peuvent-être esquivées plus longtemps. Il faut solidifier le Comité permanent R. Et il faut faire vite : nos collaborateurs sont inquiets et pareille inquiétude est la porte ouverte à une démotivation dont on se passerait volontiers en ces temps agités. L'inertie administrative *sensu lato,* l'incertitude du devenir de notre institution et la fragilité de la position juridique offerte par la loi ont d'ailleurs motivé la démission de l'un des trois membres du Comité. Mais bien plus que le sort de notre institution et de nos personnes, c'est l'avenir de la démocratie qui est en jeu.

Ne pas assurer au Comité permanent R les moyens indispensables à l'accomplissement de ses missions légales engage lourdement la responsabilité du monde politique : le Comité est la balise Argos de notre État. On peut bien entendu prendre la mer sans elle, mais lorsque le navire entre dans la tourmente, elle seule permettra d'acheminer les secours là où ils seront nécessaires.

Les attentats de Zaventem et de Bruxelles sont les exemples les plus évidents de cette nécessité d'investissement dans la lutte contre les différentes formes de menace qui font plus que nous guetter. Nous savons aujourd'hui que personne n'est à l'abri. Avec les services de renseignement, le Comité permanent R participe à cette lutte quotidienne contre ces dangers létaux qui ont pour nom, entre autres, 'terrorisme' 'extrémisme', 'espionnage', 'ingérence', 'prolifération', 'organisation criminelle', 'organisations sectaires' et 'cyberattaque'.

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

28 juin 2021

CHAPITRE I
LES ENQUÊTES DE CONTRÔLE

En 2020, le Comité permanent R a finalisé huit enquêtes de contrôle, dont une conjointement avec le Comité permanent de contrôle des services de police (I.1 à I.8). Diverses instances et personnes peuvent 'saisir' le Comité permanent R d'une enquête de contrôle : la Commission parlementaire de suivi, les ministres compétents, toute personne (morale) qui souhaite introduire une plainte ou faire une dénonciation, etc. Le Comité peut lui aussi prendre l'initiative d'ouvrir une enquête de contrôle. Ce fut le cas pour sept des huit enquêtes finalisées en 2020. Seule une enquête a été effectuée à la demande de la Commission parlementaire de suivi. Le Comité a par ailleurs initié sept nouvelles enquêtes en 2020. Une description succincte des enquêtes en cours et/ou des enquêtes figure au chapitre I.11. Les recommandations émises à l'issue des enquêtes de contrôle ont été regroupées au Chapitre XII.

Le Comité permanent R a reçu, au total, 62 plaintes ou dénonciations en 2020.[1] Après une brève pré-enquête et la vérification de plusieurs données objectives, le Comité a rejeté 55 plaintes ou dénonciations parce qu'elles étaient manifestement non fondées[2] (art. 34 L.Contrôle), et dans un cas, parce que le Comité n'était pas compétent pour en traiter les griefs. Dans ce dernier cas, le plaignant a été renvoyé vers l'instance compétente (en l'occurrence, le procureur du Roi de Bruxelles). Trois des six plaintes traitées ont pu être clôturées en 2020, deux plaintes sont toujours en cours de traitement et une plainte a été requalifiée dans une autre catégorie, à savoir dans la catégorie des plaintes APD (cf. Chapitre V).

Outre les enquêtes de contrôle, le Comité permanent R ouvre ce que l'on appelle des 'dossiers d'information'. Ceux-ci doivent permettre de répondre à des questions relatives au fonctionnement des services de renseignement et de

1 Dans un premier temps, la recevabilité de la plainte est examinée. Elle est ensuite classée dans une catégorie ('ordinaire', plainte APD, plainte MRD, etc.). Dans le cas d'une problématique générale, le Comité peut décider d'ouvrir une enquête de contrôle, sinon l'enquête reste limitée à la plainte (une enquête relative à une plainte).

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

l'OCAM.[3] Si ces dossiers font apparaître des indices de dysfonctionnement ou des aspects fonctionnels des services de renseignement qui requièrent un examen approfondi, le Comité peut procéder à l'ouverture d'une enquête de contrôle formelle. Si toutefois il apparaît qu'une telle enquête n'apporterait pas de plus-value au regard des finalités du Comité, aucune suite n'est donnée. En 2020, des dossiers d'information ont été ouverts, entre autres, sur le dysfonctionnement (plus précisément sur le flux d'informations défaillant) des administrations et des services publics, en l'occurrence le 'cloisonnement' qui ne permet pas de garantir[4] la sécurité du citoyen. Le développement d'une Banque carrefour de la sécurité a par ailleurs fait l'objet d'une réflexion. Trois de ces dossiers d'information (la question du coronavirus et la compétence des services de renseignement, la concertation sociale au sein de la Sûreté de l'État et les incidents survenus dans une zone d'opération à l'étranger) ont été discutés avec la Commission parlementaire de suivi et sont repris dans le présent chapitre.

I.1. LES SERVICES D'APPUI DE L'OCAM

Le Comité permanent R a, conjointement avec le Comité permanent P, effectué une enquête de contrôle sur les services d'appui de l'Organe de coordination pour l'analyse de la menace (OCAM).[5] Cette enquête portait en particulier sur quatre services d'appui : le SPF Intérieur (Office des étrangers), le SPF Affaires étrangères, le SPF Mobilité et Transports et le SPF Finances (Administration des Douanes et Accises). Sa finalité était l'examen des relations entre ces services d'appui et l'OCAM en matière de collaboration et d'échange d'informations, en prêtant attention à la légalité, à l'efficacité et à la coordination. Les services de renseignement (VSSE et SGRS) et les services de police (la Police fédérale et les zones de police locale) n'étaient pas concernés par cette enquête[6], pas plus que les services qui se sont ajoutés à la liste des services d'appui en 2018 (le Centre de Crise du SPF Intérieur,

---

3 Le Comité permanent R peut ouvrir un dossier d'information pour des raisons très diverses : une plainte a été déposée et le Comité permanent R souhaite exclure le plus rapidement possible l'absence manifeste de fondement ; la direction d'un service de renseignement fait état d'un incident et le Comité souhaite vérifier comment cet incident a été traité ; les médias signalent un événement et le Comité souhaite déterminer si ces faits sont conformes à la réalité et s'ils relèvent d'une problématique plus générale.

4 Le Comité a également souligné le caractère récurrent de ce problème, qui avait déjà été mis en évidence lors des travaux de la Commission d'enquête parlementaire sur les attentats terroristes du 22 mars 2016.

5 L'enquête a été ouverte mi-janvier 2018 et clôturée mi-juin 2020.

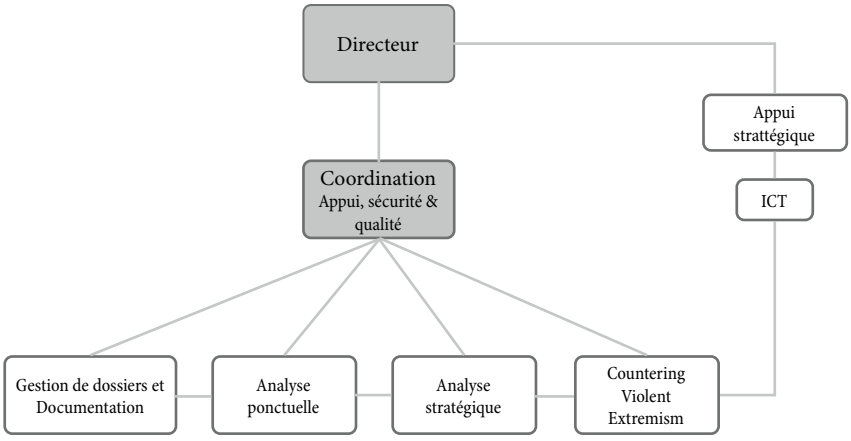
6 Les services de renseignement et de police avaient déjà fait l'objet d'une enquête de contrôle commune sur les services d'appui de l'OCAM, COMITÉ PERMANENT R, *Rapport d'activités 2010*, 45-46 ('II.12.6. Communication de renseignements à l'OCAM par les services d'appui') et plus en détail : COMITÉ PERMANENT R, *Rapport d'activités 2011*, 25-33 ('II.4. Les flux d'informations entre l'OCAM et ses services d'appui').

la Trésorerie du SPF Finances, les Établissements pénitentiaires et le Service Laïcité et Cultes de la Direction générale de la Législation et des Libertés et Droits fondamentaux du SPF Justice).[7]

I.1.1. CADRE GÉNÉRAL

I.1.1.1. L'OCAM : compétences, structure et gestion de l'information

La mission principale de l'OCAM consiste à effectuer des évaluations ponctuelles ou stratégiques, d'office ou à la demande de certaines autorités, sur les menaces en matière de terrorisme et d'extrémisme.[8] En outre, l'Organe de coordination accomplit encore d'autres missions, à savoir collaborer avec des services étrangers et internationaux homologues, coordonner le Plan d'action Radicalisme (Plan R) du Gouvernement fédéral, assurer la fonction de responsable opérationnel de la banque de données commune *Terrorist Fighters* et Propagandistes de haine (BDC TF&PH), effectuer des évaluations stratégiques de la menace visant les infrastructures critiques, effectuer les évaluations pouvant déboucher sur le gel des avoirs et émettre un avis lors de l'engagement de la procédure de retrait de la carte d'identité.
Sur le plan organisationnel, l'OCAM se compose, en principe, d'un directeur et d'un directeur adjoint, de quatre départements opérationnels (gestion des dossiers et documentation, analyse ponctuelle, analyse stratégique et *countering violent extremism*), d'un service de coordination et de deux départements d'appui (appui stratégique et technologies de l'information).



7 Par l'A.R. du 17 août 2018, ces quatre services sont venus s'ajouter à la liste des services d'appui de l'OCAM. Ces services ne faisaient pas l'objet de la présente enquête, étant donné que l'analyse des flux d'informations et des processus mis en œuvre dans ce cadre était prématurée (cf. I.11.9.).

8 Ces missions sont décrites dans la Loi du 10 juillet 2006 relative à la menace (L.OCAM) et l'Arrêté royal du 28 novembre 2006 portant exécution de la loi de juillet 2006 relative à l'analyse de la menace (AR OCAM).

Le département gestion de dossiers/documentation, composé de membres du personnel administratif[9], est chargé d'actualiser la banque de données de l'OCAM et la banque de données commune. Ce département, qui est à la fois '*front office*' (gestion de la permanence et des informations entrantes[10]) et '*back office*' (dans la gestion des dossiers), est le centre névralgique de la gestion des informations de l'OCAM. Le recueil et le traitement des informations via les médias sociaux et l'*'open source intelligence*' fait également partie de ses missions.

Le département Analyse ponctuelle est composé de membres du personnel détachés des services d'appui (les 'experts').[11] Ce département est chargé de rédiger des évaluations ponctuelles de la menace et d'assurer la liaison avec les services d'appui de l'OCAM. Il traite également les documents transmis par les services d'appui et effectue les demandes d'informations (*Request for Information*, RFI) aux services. Les experts participent aussi aux groupes de travail du Plan R, aux task forces locales (LTF)[12] et prévoient le suivi d'un certain nombre de *terrorist fighters* et/ou de propagandistes de haine. En dehors des heures de bureau, ils assurent la fonction d'officier de permanence.

Le département Analyse stratégique est composé de membres du personnel qui sont dotés d'un statut spécifique exclusivement lié à l'OCAM (les 'analystes'). Ce département s'attache surtout à identifier périodiquement les principales menaces pesant sur notre pays et sur les intérêts belges à l'étranger, ainsi qu'à en esquisser l'évolution possible dans des notes et analyses stratégiques. Le département *countering violent extremism* est composé de membres du personnel qui ont été mis à disposition de l'OCAM par le SPF Intérieur ou qui ont détachés par certains services d'appui. Ce département est surtout chargé de la gestion et de la coordination du Plan R. En outre, ces collaborateurs participent aux task forces locales (LTF) et sont impliqués dans le suivi d'un certain nombre de *terrorist fighters* et/ou de propagandistes de haine.

---

9 Les membres du personnel de l'OCAM ont des statuts différents. Chaque expert détaché ou membre détaché conserve le statut de son service d'origine. Il y a également des analystes et des administratifs engagés sur fonds propres. Ces différents statuts posent problème au sein de l'OCAM, tel que souligné lors des différents entretiens : ils peuvent être à la base de frustrations, en particulier la différence de traitement au niveau des permanences, payées pour certains et récupérées pour d'autres, et la différence de statut entre les experts détachés et les analystes (statut A3).

10 L'OCAM assure en effet une permanence 24h/24 7j/7.

11 Les experts détachés des services d'appui le sont pour une période renouvelable de cinq ans. Ils ne font pas l'objet d'une évaluation spécifique dans le cadre de leur fonction à l'OCAM. Leur statut se fonde sur celui qui est le leur dans leur service d'origine. Une certaine stabilité au sein des experts est préférable, selon la direction de l'OCAM, car ceux-ci sont formés par l'OCAM dans les matières du terrorisme/radicalisme (ils ne le sont pas dans leur service d'origine).

12 Task Force Locale (TFL) : la TFL est une '*plateforme de concertation décentralisée où s'échangent des informations relatives à la radicalisation violente et où se concluent des accords de coordination portant sur l'obtention de telles informations*' (Troisième rapport intermédiaire sur le volet 'Architecture de la sécurité', Commission d'enquête parlementaire, *doc. parl.* Chambre, 2017-18, 54-1752/008 p. 162).

Enfin, le service de coordination se charge de traduire les décisions de la direction de l'OCAM en lignes opérationnelles pour les différents départements et il est responsable de la répartition du travail et de la coopération interdépartementale.

L'OCAM gère et traite une grande quantité d'informations et de documents. Afin d'en organiser la gestion, l'Organe de coordination dispose d'une banque de données, appelée PROTEUS, uniquement accessible à son personnel. Tout membre du personnel, qu'il soit statutaire ou détaché, a la possibilité d'encoder des données dans cette banque de données.

I.1.1.2. Les services d'appui : obligation de notification, moyens et procédures

L'échange d'informations entre l'OCAM et les services d'appui est réglementé par la loi et divers arrêtés royaux. Tout d'abord, la L.OCAM prévoit une obligation de notification. En vertu de l'article 6 L. OCAM, les instances publiques qui sont désignées comme services d'appui sont en effet tenues de communiquer à l'OCAM, d'office ou à la demande de son directeur, tous les renseignements dont elles disposent dans le cadre des missions d'évaluation de l'OCAM. Le non-respect de cette obligation de notification par les fonctionnaires des services d'appui est sanctionné pénalement.[13]

Ensuite, l'article 11 § 1er AR OCAM stipule que chaque service d'appui désigne en son sein un 'point de contact central' qui sera chargé de : (1) l'échange de renseignements avec l'OCAM , (2) la diffusion efficace de ces renseignements au sein du service d'appui dont il dépend, et (3) la communication d'office et dans les meilleurs délais vers l'OCAM de tout renseignement dont le service d'appui dont il dépend dispose dans le cadre de ses missions légales et qui se révèle pertinent pour la bonne exécution des missions de l'OCAM. L'AR OCAM ne précise cependant pas ce qu'il y a lieu d'entendre par 'point de contact central'. Il peut tout aussi bien s'agir d'un membre du personnel qui a été désigné pour occuper cette fonction ou d'un service qui est composé de plusieurs personnes. Il n'est pas non plus précisé que la désignation d'un 'point de contact central' exclut toute possibilité d'autres points de contacts au sein du service d'appui.[14] L'application de l'A.R. suppose, par contre, qu'un membre du personnel (ou qu'un service) soit clairement identifié comme étant le point de contact central avec l'OCAM, spécifiquement chargé des missions confiées à ce point de contact.

Comme l'impose l'article 7 § 1er L.OCAM, l'OCAM doit se composer, entre autres, d'experts qui sont détachés des services d'appui. L'Arrêté royal du 23 janvier 2007 relatif au personnel de l'Organe de coordination pour l'analyse de la menace prévoit, en outre, que les experts détachés servent d'officiers de liaison

13 Article 14 L.OCAM.

14 En ce sens, il est préférable de parler du point de contact principal.

pour leur service d'origine.[15] Dans le cadre des attributions de cette catégorie de personnel, un des éléments consiste dès lors à s'assurer d'un lien avec leur service d'origine et ainsi qu'à favoriser le flux d'informations avec le service d'appui. Mais les experts ne sont pas les seuls points de contacts avec leur service d'origine. Des contacts directs peuvent, en effet, être établis entre d'autres membres du personnel de l'OCAM et les services d'appui. Pour la direction de l'OCAM, cela ne nuit en rien à l'échange d'informations vu que toutes les informations pertinentes sont enregistrées dans la banque de données PROTEUS.

Le flux d'informations concret entre l'OCAM et ses services d'appui est organisé en fonction de la classification ou non des documents. Le flux d'informations est donc organisé conformément à la Loi relative la classification du 11 décembre 1998[16] et à l'Arrêté d'exécution du 24 mars 2000.[17] Ces deux normes juridiques contiennent des règles strictes en matière de conservation, consultation, reproduction, transmission et destruction d'informations classifiées. L'OCAM et les services d'appui peuvent échanger des documents classifiés via le système BINII.[18] Si le service d'appui ne dispose pas de ce système, les documents classifiés sont envoyés par courrier. L'installation de ce système BINII, géré par le SGRS, permet de satisfaire à l'article 11 § 7 AR OCAM, qui précise qu'un système de communication et d'information sécurisé et crypté doit être instauré afin de faciliter la vitesse de communication entre l'OCAM et les services d'appui. Les services d'appui doivent répondre à certaines exigences de sécurité, parmi lesquelles des règles de sécurité au niveau de l'infrastructure et l'existence d'un officier de sécurité.

La boîte fonctionnelle de l'OCAM est au cœur de l'échange et de la gestion de tous les documents non classifiés entrants et sortants. Pendant les heures de bureau, c'est le département Gestion de dossiers et documentation qui assure le suivi de cette boîte. En dehors des heures de bureau, c'est l'officier de permanence désigné, c'est-à-dire un expert détaché (département Analyse ponctuelle), qui est chargé de prendre connaissance de l'information ou de la demande et de la traiter.[19]

---

15 Annexe 3.B. Description du profil de l'expert détaché auprès de OCAM de niveau A de l'A.R. du 23 janvier 2007.

16 Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

17 A.R. du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

18 BINII est l'acronyme de *Belgian Intelligence Network Information Infrastructure*.

19 L'officier de permanence est désigné à tour de rôle parmi les experts détachés.

I.1.2. LE FLUX D'INFORMATIONS ENTRE L'OCAM ET LES QUATRE SERVICES D'APPUI EXAMINÉS

I.1.2.1. SPF Intérieur – Office des étrangers[20]

Au sein de l'Office des étrangers (OE), il y a essentiellement deux services qui sont en contact avec l'OCAM : la cellule Radicalisme et la cellule Recherches. La cellule Radicalisme a été mise en place en mai 2016 et était composée, au moment de la clôture de l'enquête de contrôle, de huit collaborateurs.[21] La cellule Radicalisme dépend du service Appui stratégique, dépendant lui-même directement de la direction générale de l'Office des étrangers. La cellule Recherches relève de la Direction contrôle intérieur et frontières. Une vingtaine de personnes y travaillent. Cette cellule est considérée comme le point de contact de l'Office des étrangers pour tous les services partenaires.[22] Cependant, c'est la cellule Radicalisme qui est le point de contact principal de l'OCAM.

Deux experts sont détachés de l'Office des étrangers auprès de l'OCAM, dont un est responsable du département Analyse ponctuelle. C'est surtout le deuxième expert détaché qui est l'officier de liaison pour l'Office des étrangers. Les deux experts n'ont pas d'accès direct aux banques de données de l'OE, Evibel et VisaNet.[23]

L'échange d'informations avec ce service d'appui est actuellement le plus important de tous les services d'appui, après les services de police et les services de renseignement. De plus, les procédures mises en place donnent des garanties limitant fortement les éventuelles pertes d'information.[24] Par ailleurs, l'Office des étrangers participe aux task forces locales, ce qui permet d'assurer une collaboration régulière avec l'OCAM.

Le flux d'informations considérable entre l'OCAM et l'OE s'explique en grande partie par l'augmentation sensible du nombre de screenings de sécurité[25] des demandeurs d'asile qui ont été demandés à l'OCAM après les attentats de Paris et Bruxelles (via la cellule Radicalisme). L'arrivée d'un deuxième expert détaché en 2016 et le rôle actif de l'OE dans le cadre de la banque de données communes (dont l'OCAM est le responsable opérationnel) contribuent également à l'ampleur du flux d'informations.[26] Les demandes de screenings de sécurité soulèvent une question d'opportunité. En effet, l'Office des étrangers envoie déjà des demandes à d'autres services (comme la VSSE et les services de police). De même, se pose la

---

20 L'Office des étrangers est une direction générale du SPF Intérieur qui est placée sous la direction d'un directeur général.

21 En juin 2019, la cellule Radicalisme n'était plus composée que de six personnes.

22 Le responsable de la cellule Recherches est également l'officier de sécurité de l'Office des étrangers.

23 Ils n'ont pas non plus accès à la banque de données pénitentiaire Sidis Suite.

24 Les boîtes fonctionnelles sont mises en copie.

25 Pour vérifier si des personnes sont connues ou pour recevoir des informations actualisées sur des personnes déjà connues.

26 Tous les membres de la cellule Radicalisme ont accès à la banque de données commune.

question de la compétence de l'OCAM pour répondre, étant donné qu'il n'est pas le détenteur initial de l'information (règle du tiers service [27]).

Les mesures de sécurité relatives aux documents classifiés sont respectées et appliquées par l'officier de sécurité (système de double enveloppes, mallette pour le transport de documents classifiés, pièce sécurisée avec coffre-fort, habilitations de sécurité, contenu adapté des dossiers relatifs aux étrangers, etc. [28]). L'officier de sécurité a pris toutes les mesures de sécurité dans le bâtiment dans lequel l'Office des étrangers a emménagé.

I.1.2.2. SPF Affaires étrangères

Le point de contact principal de l'OCAM au sein du SPF Affaires étrangères est le service M1.3. Ce service est chargé de la lutte contre le terrorisme et de coordination du Plan R au sein du SPF.[29] À ce titre, le service participe aux différents groupes de travail et transmet, dans ce cadre, les informations pertinentes au sein du SPF. Il transmet également les informations des postes diplomatiques aux autres services.[30] Le service M1.3 ne traite cependant pas de cas individuels. En outre, l'OCAM a des contacts directs avec d'autres services du SPF Affaires étrangères, principalement avec le service C1.2 (Coopération judiciaire internationale [31]), le service C2.3 (Gestion des documents de voyage et d'identité[32]), la direction

---

27 La règle du tiers service veut que seul le détenteur de l'information, c'est-à-dire celui qui en est à l'origine, peut décider qui peut en être le destinataire.

28 Les informations classifiées ou les informations à diffusion restreinte ne sont pas visibles dans le dossier individuel du demandeur d'asile ou, plus généralement, du migrant. Tout membre de l'OE traitant ce type de dossier peut voir que des informations sont disponibles à la cellule Radicalisme ou à l'officier de sécurité.

29 Le service Lutte contre le terrorisme (M1.3) relève de la direction Politique de sécurité de la direction générale des Affaires multilatérales et de la Mondialisation (DGM).

30 Outre l'OCAM, il s'agit par exemple de la VSSE, du SGRS, de la police, de l'OE, etc.

31 Le service Coopération judiciaire internationale (C1.2) est placé sous la direction Assistance d'urgence et affaires judiciaires (C1) de la direction générale des Affaires consulaires (DGC). Le service est l'unique point de contact 'terrorisme' pour les postes diplomatiques à l'étranger. Il reçoit des informations venant de ces postes et les transmet (notamment) à l'OCAM (avec le service M1.3 en copie). Il s'agit ici des dossiers de coopération judiciaire internationale en matière de terrorisme, des cas individuels connus pour terrorisme/radicalisme et des prisonniers belges à l'étranger.

32 Le service Monitoring (C2.3) relève de la direction Document de voyage et d'identité (C2) de la direction générale des Affaires consulaires (DGC). Le service est chargé de la gestion de procédure PASSBAN, la procédure pour le retrait des documents de voyage (passeports).

S1 (Security33) et la direction P (Protocole et Sécurité[34]). La direction générale des Affaires bilatérales a également des contacts avec l'OCAM en ce qui concerne l'élaboration d'analyses générales de situations (géo)politiques, ceci dans le but d'élaborer la position politique de la Belgique.[35] Un expert a été détaché du SPF Affaires étrangères à l'OCAM.

Selon l'OCAM et le SPF, la multiplicité de contacts n'empêche pas une bonne circulation des informations. Au cours de leur enquêtes, les Comités ont cependant remarqué que des informations risquaient de se perdre au SPF Affaires étrangères compte tenu de la multitude de contacts directs avec l'OCAM. Pour éviter que cela se produise, il convient, au sein du SPF Affaires étrangères, de penser à informer le service M1.3 des échanges d'informations (par ex. via la boîte fonctionnelle).

En matière de sécurité, le SPF Affaires étrangères est le seul des quatre services d'appui à bénéficier du BINII.[36] Les procédures liées aux documents classifiés sont également respectées. Le SPF Affaires étrangères dispose de plusieurs officiers de sécurité.

I.1.2.3. SPF Mobilité et Transports

Au sein du SPF Mobilité et Transports, la Cellule de crise[37], créée en 2015, est le principal contact avec l'OCAM.[38] Cette cellule est également le point de contact pour le Centre de crise national (DGCC), l'Autorité nationale de sécurité (ANS), le Centre pour la Cybersécurité Belgique (CCB) et l'OTAN. La Cellule de crise est

---

33 La direction Security (S1) dépend directement du président du Comité de direction du SPF. Elle est notamment composée du service Centre de crise (S1.1) qui gère les dossiers de crise des postes diplomatiques et du centre de crise, et du service Sécurité (S1.2), qui est principalement chargé de la sécurité des membres du personnel et des bâtiments, tant à l'Administration centrale que dans les postes diplomatiques et consulaires à l'étranger. Cette direction est ainsi chargée de la sécurité interne du SPF Affaires étrangères.

34 La direction Protocole et Sécurité (P) dépend directement du président du Comité de direction du SPF. La direction est notamment responsable de la protection des personnes et des biens qui font partie des missions diplomatiques en Belgique. Au cours de l'enquête, le Protocole a dit ne pas toujours comprendre la logique derrière l'analyse de l'OCAM. Parfois, en raison d'une personne ou de liens avec notre pays, des visites de personnalités méritent de se voir attribuer le niveau 2, mais ne reçoivent que le niveau 1, alors que d'autres visites, pour lesquelles on pourrait attendre le niveau 1, se voient attribuer le niveau 2. Le service souhaiterait également être informé des modifications du niveau de la menace lorsque certains VIP passent au niveau 3.

35 Des réunions interdépartementales sont organisées avec la participation du département Analyse stratégique de l'OCAM.

36 Au moment de l'enquête de contrôle (mi-2018), l'Office des étrangers et le SPF Mobilité et Transports avaient indiqué qu'ils allaient disposer de ce système.

37 Au moment de l'enquête de contrôle, cette cellule était composée de trois personnes, qui, ensemble, représentaient deux équivalents temps plein.

38 Avant 2015, le Bureau des Plans Civils de Défense (BPCD) assurait au sein du SPF le contact avec l'OCAM. Il y avait également, au sein de chaque direction générale, une personne qui était chargée de tout ce qui se rapporte au terrorisme. Ces personnes étaient clairement identifiées, mais il n'y avait pas de système structuré.

également chargée de gérer le service de garde du SPF.[39] La cellule, ou la personne de garde, est responsable de la diffusion des évaluations de l'OCAM aux directions générales, cellules stratégiques et autres parties prenantes concernées (par ex. Infrabel, Belgocontrol). Le SPF Mobilité et Transports a détaché un expert auprès de l'OCAM.

Depuis sa création, la Cellule de crise a mis en place une série de mesures efficaces qui fournissent de très bonnes conditions pour l'échange d'informations avec l'OCAM (entre autres un programme et une procédure pour la gestion de l'échange d'informations, une pièce sécurisée pour la conservation et la consultation de documents classifiés[40]). Sur le terrain, le flux d'informations est cependant très limité, ce qui peut s'expliquer par l'utilisation d'autres canaux de communication (par ex. via la police aéroportuaire), mais aussi par le manque de connaissances des membres du personnel du SPF sur les missions de l'OCAM et la fonction de la Cellule de crise comme point de contact pour l'OCAM. De plus, il n'est pas exclu que des contacts directs soient établis entre le SPF Mobilité et Transports et l'OCAM, sans passer par la Cellule de crise. Afin d'éviter toute perte d'informations, il convient de rappeler au personnel du SPF Mobilité et Transports de tenir la Cellule de crise informée de ses échanges avec l'OCAM.

I.1.2.4. SPF Finances – Douanes et Accises[41]

Le point de contact de l'OCAM au sein de l'Administration des Douanes et Accises du SPF Finances est la section enquêtes et recherche.[42] Cette administration se compose d'une cellule et de onze services externes qui sont responsables de la recherche judiciaire, d'un point de vue fiscal, mais aussi non fiscal (par ex. le trafic de drogues).[43] Il y a trois domaines d'enquête : fraude douanière, fraude aux accises et fraude de droit commun. Pour chaque domaine, il existe un service distinct au sein de la cellule centrale de la section enquêtes et recherche.

Des quatre services d'appui qui faisaient l'objet de cette enquête de contrôle, c'est le flux d'informations entre l'OCAM et l'Administration des Douanes et Accises qui est le plus faible. La section enquêtes et recherche ne montre aucun intérêt pour une collaboration avec l'OCAM : son responsable y voit plus une perte de capacité qu'une plus-value dans le cadre de la gestion des dossiers des

---

39 Le service de garde du SFP est composé de huit personnes issues des quatre directions générales (Transport routier et Sécurité routière, Politique de Mobilité durable et ferroviaire, Navigation et Transport aérien).

40 L'officier de sécurité et son suppléant font en outre partie intégrante de la Cellule de crise.

41 L'Administration des Douanes et Accises est une administration générale du SPF Finances qui est dirigée par un administrateur général.

42 L'Administration des Douanes et Accises compte un total de 3.800 membres du personnel, dont 250 sont affectés à la section enquêtes et recherche.

43 En plus des enquêtes judiciaires, la section enquêtes et recherche mène des activités qui sont appelées 'rapportage'. Cela consiste en la rédaction d'un rapport contenant des informations ne faisant pas (encore) l'objet d'une procédure judiciaire.

douanes. Ceci est compréhensible compte tenu du flux d'informations très faible avec l'OCAM et le fait que, paradoxalement, c'est ce service qui a le plus grand nombre de personnes détachées (trois).[44] En outre, le responsable ne voit pas quelles informations dont dispose la section enquêtes et recherche pourraient être utiles à l'OCAM, et inversement.[45] Se pose dès lors la question de savoir s'il n'existe pas d'autres départements au sein de l'Administration des Douanes et Accises qui, eux, disposeraient d'informations pertinentes pour l'OCAM.

Par ailleurs, il y a des contacts directs entre l'OCAM – plus précisément via un expert détaché des Douanes – et d'autres services du SPF Finances, sans que la section enquêtes et recherche en soit informée. Cette situation est susceptible de constituer une perte d'informations, dans la mesure où peu de garanties sont données quant au bon enregistrement de ces informations.

Le SPF Finances dispose d'un officier de sécurité. Les règles de sécurité en matière de conservation de documents ne sont pourtant pas respectées au sein de la section enquêtes et recherche : les documents se trouvent conservés dans une simple armoire fermée à clé dans un local ouvert et accessible au personnel de nettoyage. Le responsable du service en a conscience et a déjà soulevé le problème, mais il explique qu'il est très difficile d'obtenir du matériel du service logistique.

I.1.3. CONCLUSION

Dans chacun des quatre services d'appui, un point de contact principal de l'OCAM est clairement identifiable. Par souci de facilité et d'efficacité, d'autres points de contact de l'OCAM existent parallèlement à ce(s) point(s) de contact officiel(s). Cela ne constitue pas un problème en soi si des routines de transmission et d'échange d'informations sont mises en place, dont celles de mettre en copie les boîtes fonctionnelles de l'OCAM (gérées par le département Gestion des dossiers et documentation) et les points de contact principaux des services d'appui. Cela permet de centraliser les informations et d'en prévenir toute perte.

Si les flux d'informations peuvent être considérés comme très importants pour l'Office des étrangers et le SPF Affaires étrangères, les flux d'informations sont beaucoup plus faibles avec les deux autres services d'appui, le SPF Mobilité et Transports et l'Administration des Douanes et Accises. Les raisons évoquées par ces deux dernières autorités étaient le fait qu'un certain nombre d'informations passaient déjà via d'autres canaux (entre autres via la police) et qu'elles avaient moins d'informations pertinentes pour l'OCAM. Un bon échange d'informations ne trouve pas seulement son origine dans les structures et les procédures mises

[44] Deux experts (Analyse ponctuelle) et un membre du personnel administratif (Gestion des dossiers et de la documentation).

[45] Les experts et le membre du personnel administratif détachés ont cependant un accès direct à la banque de données du SPF Finances, SITRAN (SIgnalétique TRANsversal).

en place, mais également dans la culture de l'échange d'informations au sein des services d'appui et dans le fait que le personnel de ces services sait qu'il existe au sein de leur organisation, un point de contact avec l'OCAM et connaît ses missions. Au niveau de l'Office des étrangers et du SPF Affaires étrangères, les derniers aspects cités étaient bien intégrés. En revanche, la situation est plus discutable du côté du SPF Mobilité et Transports et de l'Administration générale des Douanes et Accises.

En ce qui concerne les normes minimales de sécurité en matière de conservation de documents classifiés, le seul problème constaté l'a été à l'Administration des Douanes et Accises, où ces normes n'étaient pas respectées.

Au sein de l'OCAM, le département Gestion des dossiers et documentation est le centre névralgique de la gestion des informations. En outre, les experts détachés du département Analyse ponctuelle jouent un rôle essentiel dans l'échange d'informations entre l'OCAM et les services d'appui. Au cours de leur enquête, les Comités ont toutefois constaté que la communication entre les différents départements pouvait être améliorée, et en particulier la communication interne autour des compétences des experts pouvait être organisée de manière plus étendue.

I.2. LE FONCTIONNEMENT DE LA DIRECTION COUNTERINTELLIGENCE (CI) DU SGRS : SUIVI DES RECOMMANDATIONS (BIS)

I.2.1. CONTEXTUALISATION ET OBJET DE L'ENQUÊTE

Fin décembre 2016, le ministre de la Défense de l'époque a demandé au Comité permanent R d'effectuer une enquête sur le fonctionnement de la Direction Counterintelligence (CI). Cette enquête[46] a donné une vue sur la gravité, la complexité et la diversité des dysfonctionnements au sein de la Direction CI. Le Comité était convaincu de l'intérêt, pour la Direction CI, d'être organisée et gérée de manière à répondre aux standards d'un service public efficace et efficient. Ces standards n'étaient pas rencontrés. L'enquête a donné lieu à des recommandations détaillées.[47] En ce qui concerne le calendrier de mise en œuvre, un degré de priorité a été attribué : 'très haut' (à réaliser pour la fin 2018), 'haut' (à réaliser pour fin juin 2019) et 'moyen' (à réaliser pour fin décembre 2019).[48] Une enquête de suivi a été réalisée afin de vérifier dans quelle mesure l'ensemble des recommandations

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

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

48 COMITÉ PERMANENT R, *Rapport d'activités 2019*, 28-31 ('I.6. Le fonctionnement de la Direction Counterintelligence (CI) du SGRS : suivi des recommandations').

ont été mises en œuvre. Une deuxième enquête de suivi a démarré en mars 2020 et a été clôturée en juin 2020.[49]

I.2.2. UNE NOUVELLE STRUCTURE AU SGRS

En réaction à l'audit de la Direction CI et en vue de concrétiser les recommandations de la Commission parlementaire 'Attentats', le SGRS a décidé de lancer, en juin 2018, un *Business Process Re-engineering* (BPR). Depuis janvier 2020, la Direction Counterintelligence, tout comme d'ailleurs la Direction Intelligence, a été reprise dans une nouvelle structure. Cette opération organisationnelle n'a évidemment pas signé la disparition des missions CI du SGRS. Des membres du personnel de l'ancienne Direction CI, qui se concentraient sur le terrorisme, ont toutefois été transférés vers la 'Plateforme commune CounterTerro VSSE-SGRS'. Ces changements ont rendu certaines recommandations moins – voire plus du tout – pertinentes, ou elles devaient du moins être considérées sous un angle différent.

I.2.3. ÉTAT DES LIEUX DE LA MISE EN OEUVRE DES RECOMMANDATIONS DE L'AUDIT DE 2018

Le Comité a examiné – à nouveau par des recherches documentaires et des entretiens – la mesure dans laquelle des progrès significatifs ont été réalisés dans la mise en œuvre des recommandations.

Au premier semestre 2019, le SGRS avait déjà progressé sur le contre-espionnage, malgré les problèmes qui s'étaient posés par le passé. Le rôle et la mission de la Direction Counterintelligence au sein du SGRS et en relation avec la VSSE avaient déjà été précisés (grâce à la mise en place d'une 'Plateforme commune 'CounterTerro' avec la VSSE), une nouvelle approche stratégique avait été établie, des directives internes (SOP) avaient été élaborées, et les problèmes d'infrastructure avaient été pris à bras-le-corps.

La nouvelle structure a ouvert des perspectives : une planification plus rationalisée des différentes matières a été réalisée, une meilleure coordination entre la collecte et l'analyse a été rendue possible et on s'est attaqué aux anciennes contradictions 'culturelles' en matière de 'tradecraft'.

Le Comité permanent R a estimé que le SGRS avait consenti des efforts importants pour corriger les nombreux dysfonctionnements identifiés par

---

[49] Après discussion de son rapport (3 juin 2020), le Comité a informé la Commission de suivi, à sa demande, de l'état d'avancement des dossiers judiciaires et/ou administratifs des collaborateurs concernés. L'objectif était de permettre aux membres de la Commission de suivi d'évaluer l'opportunité d'entendre les personnes concernées (COMITÉ PERMANENT R, *État des différents dossiers impliquant des membres du SGRS*, 10 juillet 2020 (Ref. 2019/268/2)).

le Comité en 2018 dans l'ancienne Direction CI et pour mieux développer la fonction 'Counterintelligence'. Il est vrai qu'un certain nombre de points continuaient d'exiger de l'attention. Il s'agissait notamment de l'arriéré en matière de saisie de données dans la banque de données, du contrôle interne qui devait encore être renforcé et des informations de gestion nécessaires afin de pouvoir envoyer le service sur le terrain, qui devaient encore être développées. Il s'agissait également de la gestion des services provinciaux qui n'avait pas encore été finalisée, même si ceux-ci sont à présent bien mieux dotés en personnel. Un certain nombre de chantiers restent donc ouverts. Le Comité permanent R a décidé de continuer à suivre avec attention la mise en œuvre des recommandations.

I.3. LE BREXIT ET LA RELATION ENTRE LES SERVICES DE RENSEIGNEMENT BELGES ET BRITANNIQUES

En juin 2016, un référendum a été organisé au Royaume-Uni et a abouti à une sortie de l'Union européenne (UE).[50] Des négociations, qui ont traîné en longueur, ont démarré peu de temps après. Le Royaume-Uni a finalement quitté l'Union européenne le 31 janvier 2020.

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

En mai 2019, le Comité permanent R a ouvert une enquête de contrôle concernant l'impact du Brexit sur la coopération entre les services de renseignement belges (VSSE et SGRS) et les services de renseignement britanniques. Le Comité souhaitait en particulier vérifier si le Brexit risquait de mettre cette coopération en péril. Il était également question de la manière dont les services de renseignement belges s'y étaient préparés.[51]

---

50 En mars 2017, le Gouvernement britannique – avec l'assentiment du Parlement – a activé l'article 50 du Traité sur le fonctionnement de l'Union européenne, qui prévoit un mécanisme de retrait d'un État membre de l'UE (Traité de Lisbonne modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne, signé à Lisbonne le 13 décembre 2007, *Journal officiel de l'Union européenne*, 17 décembre 2007, C306, ISSN 1725-2474).

51 Au moment où l'enquête de contrôle a été effectuée (octobre – novembre 2019), il n'y avait encore aucune certitude sur le timing ni sur les circonstances précises du retrait, et ce en raison de la situation politique conflictuelle et incertaine au Royaume-Uni. Le rapport a été finalisé au premier trimestre 2020.

I.3.1. LE RENSEIGNEMENT N'EST PAS UNE COMPÉTENCE DE L'UNION EUROPÉENNE

I.3.1.1. Traité sur le fonctionnement de l'Union européenne de 2007

L'intervention de l'Union européenne se limite aux matières pour lesquelles les pays de l'UE, via les Traités, lui en ont expressément donné la compétence. Ces Traités précisent qui peut légiférer dans quel domaine : l'UE, les autorités nationales ou les deux (ce que l'on appelle les compétences partagées). En l'occurrence, le fonctionnement des services de renseignement ne relève pas de la compétence de l'UE ni des compétences partagées. Il relève de la compétence exclusive des États membres, comme cela ressort du Traité sur le fonctionnement de l'Union européenne de 2007.

Il convient néanmoins de mentionner que l'UE dispose d'une certaine capacité en matière de renseignement. Afin d'exercer leurs fonctions et de recueillir les informations dont ils ont besoin pour pouvoir exécuter leurs tâches, plusieurs départements de l'UE se chargent du recueil de renseignements, de la sécurisation de l'information et du contre-espionnage visant les institutions européennes (par ex. l'EU INTCEN).

I.3.1.2. La Déclaration politique dans le cadre du Brexit entre l'UE et le Royaume-Uni

La compétence exclusivement nationale en matière de sécurité nationale ressort également de la Déclaration politique, qui a été établie pour tracer le cadre des futures relations entre l'Union européenne et le Royaume-Uni. Cette Déclaration politique date du 17 octobre 2019. Il s'agit d'une déclaration non contraignante qui accompagne l'accord sur le Brexit.[52]

Dans cette même Déclaration politique, une partie spécifique est consacrée au 'partenariat de sécurité'. Avec cette notion, on entendait démontrer que la sécurité est et reste un domaine important de la coopération, et ce tant pour l'UE et ses États membres que pour le Royaume-Uni.

---

[52] Dans la partie IV. Dispositions institutionnelles et autres dispositions horizontales, article 133 de la Déclaration politique, il est établi que : *'Les relations futures (ndr : entre le Royaume-Uni et l'UE) devraient prévoir des exceptions appropriées concernant la sécurité ; la sécurité nationale relève de la seule responsabilité des États membres de l'Union et du Royaume-Uni, respectivement.'*

I.3.2. LA COOPÉRATION ACTUELLE ENTRE LES SERVICES BELGES ET LES SERVICES DE RENSEIGNEMENT BRITANNIQUES

I.3.2.1. Base légale de la coopération internationale

Le Traité sur le fonctionnement de l'Union européenne laisse toute la place à la coopération internationale entre les États membres de l'UE, tant entre eux qu'avec des tiers. Dans cette optique, l'article 73 stipule ce qui suit : '*Il est loisible aux États membres d'organiser entre eux et sous leur responsabilité des formes de coopération et de coordination qu'ils jugent appropriées entre les services compétents de leurs administrations chargées d'assurer la sécurité nationale.*'

La base légale pour la coopération des services de renseignement belges avec leurs partenaires étrangers figure à l'article 20 L.R&S.

En ce qui concerne la coopération avec des services étrangers, il est fait référence à la directive émise par le Conseil national de sécurité (CNS). Le 26 septembre 2016, les ministres de la Justice et de la Défense ont soumis au CNS, dans une note, une directive classifiée 'Confidentiel Loi 11.12.1998' et intitulée '*Richtlijn aangaande de relaties van Belgische inlichtingendiensten met buitenlandse inlichtingendiensten*'.[53] Cette directive vise à évaluer les services de renseignement étrangers en vue de déterminer la nature de la relation avec chacun de ces services. Elle constitue un instrument de soutien de la politique en matière de coopération bilatérale.

I.3.2.2. La Sûreté de l'État

Le Royaume-Uni compte trois services de renseignement civils. Au niveau bilatéral, la VSSE coopère avec deux de ces services, plus particulièrement avec le *Security Service (*BSS ou MI5) et le *Secret Intelligence Service* (SIS ou MI6). Les deux services sont des partenaires importants pour la VSSE. Le *Security Service* recueille et analyse les renseignements relatifs aux menaces intérieures, tandis que le *Secret Intelligence Service* collecte ses renseignements à l'étranger. La coopération entre ces deux services de renseignement britanniques avec la VSSE se situe dans les domaines de compétence que les trois services ont en commun, à savoir le terrorisme, l'espionnage et la prolifération d'armes de destruction massive. Il n'y a pas de coopération directe avec le troisième service de renseignement, le *Government Communications Headquarters* (GCHQ), qui est responsable du *signal intelligence* (SIGINT). La VSSE ne coopère pas non plus avec le service de renseignement militaire britannique.

---

[53] Directive concernant les relations des services de renseignement belges avec les services de renseignement étrangers (traduction libre).

Outre les contacts bilatéraux, il y a aussi des contacts et un échange de renseignements entre la VSSE et les services de renseignement britanniques via des forums multilatéraux, tels que le Club de Berne et le *Counter Terrorism Group* (CTG). Il est important de souligner que tant le Club de Berne que le CTG sont des structures de coopération intergouvernementales qui sont indépendantes des structures de l'Union européenne. Le service britannique, qui fait partie du Club de Berne et du CTG avait déjà exprimé le souhait de pouvoir continuer à faire partie des deux forums multilatéraux après le retrait du Royaume-Uni de l'Union européenne (comme par ex. la Norvège et la Suisse).

I.3.2.3. Le Service Général du Renseignement et de la Sécurité

En ce qui concerne le service de renseignement militaire SGRS, la coopération bilatérale et multilatérale avec ses partenaires britanniques se situe également en dehors des structures européennes. Les contacts bilatéraux sont ici aussi interétatiques et interservices. Les contacts multilatéraux ont lieu principalement au sein de l'OTAN.

Au niveau bilatéral, le SGRS coopère avec le SIS (MI6), le BSS (MI5) et le GCHQ, qui est considéré par le service comme le partenaire britannique le plus important. Les services coopèrent notamment sur le partage de l'expertise en matière de SIGINT, sur la lutte contre les cybermenaces, ainsi que sur l'échange de renseignements sur la menace (d'espionnage). Le Royaume-Uni compte également un service de renseignement militaire, le *Defence Intelligence*, qui fait partie du ministère de la Défense britannique. La mission du *Defence Intelligence* est de fournir des renseignements stratégiques militaires au ministère et aux forces armées. Ce qui est frappant, c'est que dans le cadre de cette enquête, le SGRS a déclaré ne pas avoir noué de coopération bilatérale directe avec le *Defence Intelligence*.

Par ailleurs, citons la coopération entre le SGRS et, entre autres, les services britanniques dans un cadre multilatéral. Au sein des structures de l'UE, il y a le *European Union Military Staff* (EUMS) qui fait partie du Service européen pour l'action extérieure (SEAE). Le EUMS abrite un *Intelligence Directorate* qui est chargé de réaliser des analyses stratégiques pouvant contribuer à une réaction en cas de crise et à la planification des opérations militaires de l'UE. L'*Intelligence Directorate* est composé d'analystes militaires qui sont détachés des services de renseignement nationaux des États membres de l'UE. Le SGRS a lui aussi détaché un analyste à l'EUMS.

I.3.3. CONSÉQUENCES POSSIBLES DU 'BREXIT' POUR LES SERVICES DE RENSEIGNEMENT

I.3.3.1. Hypothèses concernant l'impact du Brexit sur les services de renseignement britanniques

Le Brexit effectif étant à ce jour trop récent, il reste difficile d'évaluer quelles sont les conséquences réelles pour les services de renseignement. La littérature (essentiellement anglo-saxonne) met généralement en avant trois hypothèses ('*schools of thought*').[54]

La première école dite 'optimiste' ('*optomitic school*') considère que le Brexit est une évolution positive et qu'il ne va en aucun cas compromettre la sécurité intérieure et extérieure du Royaume-Uni. Cette vision met davantage l'accent sur la relation entre les services britanniques et ses partenaires américains que sur la relation avec les partenaires européens. En effet, Brexit oblige, le Royaume-Uni ne fera pas partie d'un futur État européen fédéral, lequel sera également compétent en matière de sécurité. Une telle appartenance aurait pu modifier et perturber le bon fonctionnement actuel des services de renseignement britanniques. Les tenants de ce courant considèrent que le Royaume-Uni peut se passer des autres États membres de l'UE (qui investissent trop peu dans leurs services de renseignement) en matière de renseignement, puisque le pays dit avoir le dispositif de renseignement le plus compétent, le plus efficace et le mieux financé. La relation qu'entretiennent actuellement les services de renseignement britanniques et ceux des autres États membres de l'UE est considérée comme déséquilibrée, les services britanniques 'donnant plus que ce qu'ils reçoivent en retour'. Par ailleurs, l'échange de renseignements se fait la plupart du temps au niveau bilatéral et pas au niveau multilatéral. Cette collaboration bilatérale avec d'autres pays, essentiellement en matière de contre-terrorisme, se poursuivra tout simplement après le Brexit.

L'école dite 'pessimiste' ('*pessimistic school*') défend par contre l'idée selon laquelle le Brexit portera gravement atteinte à la sécurité nationale britannique. Elle invoque que le Royaume-Uni perdra sa place et son rôle dans le développement de ce qui n'est encore qu'un dispositif de renseignement embryonnaire au niveau européen et dans les bases de données. Le Brexit, pourrait mener à un affaiblissement de la position des services de renseignement britanniques vis-à-vis des autres pays, en premier lieu des États-Unis. Selon cette vision, les services britanniques, justement de par leur rôle de passerelle vers d'autres pays de l'UE, représentaient une valeur ajoutée pour les Américains. Après le Brexit, les États-Unis pourraient en arriver à considérer le Royaume-Uni comme un pays de second rang et rechercher un autre partenaire privilégié au sein de l'UE (par ex. l'Allemagne).

---

[54] I.L. KONSTANTOPOULOS et J.M. NOMIKOS, *Journal of Intelligence History*, 'Brexit and intelligence: connecting the dots', 2017, Vol. 16, NO. 2, 100-107.

Le troisième courant dit 'pragmatique' se situe entre les deux précédents : le Brexit n'aurait pas d'effets significatifs sur la sécurité européenne et britannique en général, ni sur le renseignement, en particulier. Les défenseurs de ce courant estiment que la coopération en matière de renseignement se poursuivra entre les partenaires britanniques et européens, que soit au niveau bilatéral ou dans le cadre d'une relation multilatérale particulière, en vue de relever les défis et contrer les menaces internationales et d'atteindre l'objectif commun de la sécurité. Les raisons de ce choix conscient sont la rationalité et l'intérêt mutuel. Ce courant de pensée semblait être le plus présent au sein de la communauté du renseignement, du moins si l'on se base sur une série de déclarations publiques de dirigeants ou d'anciens dirigeants.

I.3.3.2. Évaluation par les services belges des conséquences du Brexit

Il est important de souligner qu'il n'a pas été demandé à la VSSE ni au SGRS de participer à une quelconque concertation (et ils n'en ont pas fait eux-mêmes la demande) avec les autorités belges, par exemple avec le ministre compétent ou au niveau du Conseil national de sécurité (CNS), sur l'impact éventuel du Brexit. Les services n'ont reçu aucune question, instruction ou directive à ce propos.

Il y a lieu de mentionner qu'en mars 2019, un Conseil des ministres thématique a été organisé au niveau du Gouvernement fédéral sur le Brexit. Une multitude de sujets ont été discutés lors de ce Conseil des ministres, mais aucun ne portait sur les services de renseignement (mais bien sur les services de police, par exemple).

Il est en outre apparu que ni la VSSE ni le SGRS n'ont établi d'analyse (de risque) formelle et structurée à propos des éventuelles répercussions du Brexit sur leur coopération avec les Britanniques. Après le lancement de l'enquête de contrôle, les deux services ont cependant mené une réflexion sur les conséquences possibles du Brexit pour leur relation avec les services de renseignement britanniques.

Sur la base de cette réflexion, la VSSE estimait que l'impact du Brexit sur sa coopération avec les services britanniques pourrait être limité, puisque cette coopération se déroule à un niveau interétatique, en dehors des structures de l'UE. Le service partait du principe que la coopération avec ses partenaires britanniques subirait à peine (voire pas du tout) les effets du retrait. Selon la VSSE, le Brexit n'aurait pas non plus de conséquences juridiques directes sur la collaboration. Toutefois, certains effets supplémentaires pourraient apparaître, par exemple en matière de vie privée ou d'accès des services britanniques aux (bases de) données qui relèvent des réglementations européennes. La VSSE a néanmoins décidé d'interroger les services partenaires britanniques sur les éventuelles conséquences du Brexit pour la future coopération belgo-britannique en matière de renseignement.[55]

---

[55] Avec l'aval des services britanniques, la VSSE a communiqué la réponse au Comité permanent R. Le document étant classifié 'SECRET Loi 11.12.1998', aucune information autre que l'appel à poursuivre la coopération ne peut être divulguée.

À l'instar de la VSSE, le SGRS estime que le retrait du Royaume-Uni n'aura pas de conséquences pour la coopération du service avec ses partenaires britanniques. Le service a affirmé de pas avoir discuté spécifiquement des conséquences éventuelles du Brexit avec ses partenaires britanniques et a rappelé ne pas avoir reçu d'instructions ou de directives de la part des autorités belges à ce propos.

I.3.4. ASPECTS COMPLÉMENTAIRES

I.3.4.1. La protection des données (à caractère personnel)

À l'estime des services de renseignement belges, le fait que la réglementation européenne ne s'applique plus au Royaume-Uni après le Brexit, plus précisément la réglementation en matière de protection des données (à caractère personnel), est un point qui pourrait se révéler délicat dans le cadre des échanges d'informations avec leurs partenaires britanniques.[56]

Étant donné que le Royaume-Uni ne sera plus membre de l'UE, des règles spécifiques – lisez : plus strictes – seront d'application dans le cadre de la transmission de données à caractère personnel. Ces règles sont reprises aux articles 93 et 94 de la Loi relative à la protection des données (LPD).

L'Accord de retrait du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord de l'Union européenne et de la Communauté européenne de l'énergie atomique, ainsi que la Déclaration politique qui y est annexée, contiennent eux aussi plusieurs dispositions relatives aux réglementations en matière de protection et de traitement des informations et des données à caractère personnel.[57]

Toujours est-il qu'il s'agit ici d'une matière qui ne concerne pas spécifiquement le renseignement, mais qui est plus générale. Cet aspect devrait, le cas échéant, être suivi par les différentes instances nationales compétentes (en Belgique, les ministres compétents et les différentes autorités de protection des données). Le Comité a dès lors jugé opportun que ces instances soient attentives aux répercussions

---

[56] Dans le *'Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2018'* également, la commission parlementaire s'est notamment penchée sur ce que pourraient être les conséquences du Brexit pour la structure du renseignement européen. Le thème de la protection des données à caractère personnel est identifié comme un problème susceptible de se poser pour la future coopération entre les services de renseignement européens (français) et britanniques. Selon les auteurs de ce rapport, *'le Royaume-Uni devra prouver qu'il garantit un niveau suffisant de protection des données personnelles et il devra aussi reconnaître la compétence de la Cour de justice de l'Union européenne appelée à connaître des recours formés en matière de traitement des données personnelles.'* (Yaël BRAUN-PIVET, '*Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2018*', Délégation parlementaire au renseignement, Assemblée nationale/Sénat, 11 avril 2019, 88).

[57] À noter que la Déclaration politique n'est pas contraignante, si bien qu'il est impossible de prévoir quand et comment les engagements qui ont été pris seront concrétisés.

possibles en matière de renseignement et, si nécessaire, impliquent les services de renseignement dans d'éventuelles discussions.

I.3.4.2. Accès du Royaume-Uni aux bases de données (policières) européennes

Une conséquence majeure du retrait du Royaume-Uni de l'UE est que le Royaume-Uni n'a plus accès aux bases de données européennes. Ce qui vient d'emblée à l'esprit, ce sont les données gérées par Europol et l'accès au Système d'information Schengen (SIS-II).[58] Toutefois, le Comité permanent R ne s'étendra pas sur le sujet étant donné qu'il s'agit ici de bases de données policières. Comme déjà mentionné, l'UE n'est pas compétente pour le renseignement *stricto sensu*, et il n'y a pas de 'bases de données de renseignements' au niveau européen. Aucun problème ne risque donc de se poser.

I.3.4.3. Une intégration européenne plus poussée en matière de renseignement après le Brexit ?

Comme cela a déjà été mentionné, les États membres se sont toujours montrés très réservés sur l'abandon de leurs compétences en matière de sécurité nationale au profit du niveau intergouvernemental, en l'occurrence de l'Union européenne. Depuis son adhésion à l'UE, le Royaume-Uni a été l'un des pays membres qui n'a eu de cesse de prôner une approche limitée et limitante de l'intégration européenne, en particulier dans le domaine de la sécurité nationale et des services de renseignement.

Un des acquis du Traité de Lisbonne était la réalisation d'un espace de liberté, de sécurité et de justice (ELSJ). Dans ce Traité, c'est surtout la Troisième Partie, Titre V (articles 67 à 89 inclus) qui est consacrée à l'ELSJ. Dans le cadre de cet ELSJ, 133 mesures ont été proposées, parmi lesquelles seulement 35 ont été adoptées par le Royaume-Uni après un *'opt in'* explicite.

D'autre part, la nécessité d'une coopération européenne plus poussée dans le domaine de la sécurité a été démontrée, surtout ces quinze à vingt dernières années. Au cours de cette période, cette coopération s'est principalement développée dans les domaines de la lutte contre la criminalité, du contre-terrorisme et de la cybersécurité.

Une des conséquences possibles du retrait du Royaume-Uni, qui était un des États membres les plus eurosceptiques, pourrait être une coopération structurelle

---

[58] L'accord sur le Brexit (Partie 1, article 8) mentionne ce qui suit : *'Sauf disposition contraire du présent accord, à la fin de la période de transition, le Royaume-Uni n'est plus autorisé à accéder à tout réseau, à tout système d'information et à toute base de données établis sur la base du droit de l'Union. Le Royaume-Uni prend les mesures appropriées pour s'assurer qu'il n'accède pas à un réseau, à un système d'information ou à une base de données auquel il n'est plus autorisé à accéder.'*

plus poussée entre les services de renseignement des États membres de l'Union européenne 'post-Brexit'. Le *EU Intelligence and Analysis Centre* (EU INTCEN) et l'*Intelligence Directorate* du *EU Military Staff*, qui font partie du Service européen pour l'action extérieure, sont actuellement les seules structures de renseignement au sein des institutions européennes. Ces organes établissent des analyses stratégiques, en s'appuyant sur des informations provenant de sources ouvertes, ainsi que des analyses de renseignements qui sont fournis par les services de renseignement des États membres. Une évolution pourrait être qu'à côté de l'INTCEN, une structure soit établie au sein de l'UE en vue d'échanger des renseignements opérationnels, par exemple en matière de contre-terrorisme, d'activités d'ingérence par des États tiers ou de cybermenaces.

Par ailleurs, les ministres européens de la Défense et des Affaires étrangères ont déjà décidé dès novembre 2018 de créer une *Joint EU Intelligence School*. Ce projet sera coordonné par les autorités grecques.

I.3.5. CONCLUSION

Le Comité permanent P n'a trouvé aucun élément indiquant que le retrait du Royaume-Uni de l'Union européenne impacterait négativement les services de renseignement belges et britanniques. La conclusion est identique outre-Manche. À ce stade, il n'y a pas de raison de mettre en doute les déclarations officielles des instances britanniques, notamment dans le texte de la Déclaration politique qui accompagne l'accord sur le Brexit entre le Royaume-Uni et l'UE.

I.4. L'ÉVENTUELLE INGÉRENCE DE SERVICES/ÉTATS ÉTRANGERS DANS LE PROCESSUS ÉLECTORAL BELGE

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

La cyber-influence en ligne des élections depuis l'étranger peut prendre différentes formes. Il peut s'agit de piratage ('*hacking*'), d'infiltration et de manipulation de la technologie électorale via un accès aux ordinateurs de vote et de l'infiltration de systèmes informatiques en vue d'obtenir des informations sur les stratégies des partis ou des informations sensibles et d'organiser des fuites dans la presse ou les médias sociaux ; ou encore de la diffusion en ligne de '*fake news*'

et la désinformation via des plateformes de médias sociaux et des sites Internet de sociétés de médias.

Les élections de mai 2019[59] ont placé cette problématique au centre de l'actualité. L'organisation d'élections ouvertes, régulières est au cœur de la démocratie. Il incombe à la VSSE d'identifier certaines menaces visant les institutions belges et d'en informer les autorités compétentes. Par conséquent, le Comité a décidé, début 2019, d'ouvrir une enquête de contrôle[60] sur la manière dont les services de renseignement belges ont réagi (collecte de renseignements, avertissements, coopération internationale, possibles entraves, etc.) à l'ingérence éventuelle par des services/des États étrangers dans le processus électoral belge.

I.4.1. UNE PRISE DE CONSCIENCE ACCRUE

En Belgique aussi, il y a eu une prise de conscience accrue sur le thème de l'influence malveillante des processus politiques et des élections.

Une cellule interdépartementale a été créée pour élaborer des feuilles de route ('*roadmaps*') en vue de mener des actions concrètes. Le Gouvernement estimait par ailleurs qu'une approche nationale ne pouvait pas suffire. La Belgique a dès lors collaboré, lors des Conseils européens successifs, à l'accroissement de la résilience de l'Union européenne contre les campagnes de désinformation. Un élément majeur de la contre-stratégie belge dans ce cadre était la collaboration internationale via l'UE et l'OTAN, entre autres via le *NATO Cooperative Cyber Defence Centre of Excellence* (Tallinn). La Belgique a également développé une collaboration avec le Centre d'excellence pour la lutte contre les menaces hybrides (Helsinki).

Une éventuelle coordination de la détection des cyberattaques a encore été confiée au Centre pour la Cybersécurité Belgique (CCB), dont fait également partie le SGRS. Le Centre de crise (DGCC) a prévu la création d'une plateforme de coopération en matière de désinformation et de communication stratégique. Au niveau national, citons encore le projet *stopfakenews.be* du ministre de l'Agenda numérique.

En outre, la problématique de la désinformation digitale a été discutée à diverses reprises par le CCB précité et les services de renseignement au sein du Comité de coordination du renseignement et de la sécurité (CCRS). Le CCB a également collaboré avec le SPF Intérieur sur la sécurisation du système de vote électronique.

---

59 Il s'agissait des élections du 26 mai 2019 du Parlement européen, de la Chambre des représentants et des Parlements des Régions et des Communautés.

60 L'intitulé complet de l'enquête est le suivant : 'Enquête de contrôle sur la manière dont les services de renseignement suivent les risques liés à une éventuelle ingérence d'acteurs étrangers dans le processus électoral belge, sur la manière dont ils tentent de contrer les menaces potentielles et sur la manière dont ils font rapport aux autorités, en particulier en ce qui concerne le risque de cyber-ingérence et de cyber-attaques'. Le rapport a été finalisé début 2020.

Enfin, le Gouvernement a annoncé la création, au sein du SGRS, d'un *Cyber Security Operations Center*. Ce service est responsable de la détection et de la lutte contre les cyber-incidents et devait se concentrer sur la protection des réseaux et des systèmes d'armement de la Défense, mais devait aussi apporter une assistance technique aux enquêtes du CCB ou du Parquet fédéral (*infra*).

I.4.2. LE RÔLE ATTRIBUÉ À LA VSSE

En vertu des articles 7, 1° et 8 L.R&S, la VSSE est compétente pour rechercher des renseignements sur une éventuelle influence des élections via des cyber-moyens, puisqu'une telle influence est couverte par les notions d''espionnage', et d''ingérence'.[61] Étant donné que la désinformation et les '*fake news*' font souvent partie d'opérations qui sont menées par des services de renseignements étrangers offensifs, la VSSE se considérait comme un *'partenaire naturel dans la lutte contre cette problématique*'.

La VSSE estimait que son rôle était de rechercher et d'analyser les renseignements relatifs à ces problématiques pour ensuite sensibiliser les autorités, administrations, entreprises et autres organismes. En revanche, la VSSE affirmait ne pas développer une politique active d'information des citoyens pour leur permettre de séparer le bon grain de l'ivraie en matière d'information. Le service estimait qu'il ne lui incombait pas non plus de suivre les médias sociaux et les entreprises de technologie pour évaluer leur approche des '*fake news*', ni d'en élaborer une définition.

Le Comité a pu constater que le service avait déjà émis des instructions en août 2018 concernant les élections de 2019 et confié le suivi à trois de ses sections. L'accent était mis sur les menaces émanant de la Russie. Deux acteurs majeurs des médias sociaux étaient suivis de près et une répartition des tâches a été décidée avec le SGRS. L'intention n'était pas de vérifier la véracité des faits ou de détecter des '*fakes news*', mais bien de tenter de déterminer quels profils spécifiques étaient actifs, et ce sans contrôle automatisé. En novembre 2018, la VSSE est allée plus loin en constituant, en interne, un Groupe de Travail – Elections. Ce Groupe de Travail a élaboré un plan d'action pour examiner de plus près ce que pouvait être la contribution du service à cette *Joint Intelligence Task Force (JITF)* (*infra*).

---

[61] Dans un souci d'exhaustivité, il peut être mentionné que la VSSE est également compétente pour suivre la matière via l'article 7, 3° L.R&S qui prévoit que la VSSE a pour mission *'de rechercher, analyser et traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge.*'

I.4.3. LE RÔLE ATTRIBUÉ AU SGRS

À première vue, la compétence du SGRS en la matière semblait moins évidente que celle de la VSSE. En effet, le SGRS est en premier lieu un service de renseignement militaire qui doit se concentrer sur les matières militaires. Cependant, le SGRS s'est penché sur le phénomène de cyber-ingérence dans les élections, vu que l'influence clandestine de processus politiques a généralement une origine militaire. Ainsi, il est de notoriété publique que, par exemple, le service de renseignement militaire russe GRU utilise une stratégie d'*'hybrid warfare'*. En ce sens, cela relève de la compétence du SGRS, même si la menace ne vise pas *stricto sensu* les systèmes ICT militaires. Un second point d'ancrage figure à l'article 9 L.R&S : '*à la requête de la Sûreté de l'État, le Service Général du Renseignement et de la Sécurité prête son concours à celle-ci pour recueillir les renseignements lorsque des militaires sont impliqués dans des activités visées à l'article 7, 1°et 3°'*. Vu qu'il existait de fortes présomptions que la menace émanait souvent de services militaires étrangers, il était légitime, dans cette optique, que le SGRS assiste la VSSE en la matière.

Dès novembre 2017, le SGRS avait rédigé une note sur d'éventuelles cyber-menaces lors des élections communales de 2018 et le scrutin fédéral de 2019 pour son ministre de tutelle.[62] Il a également été décidé de créer, en interne, une 'Projectteam Elections 2019' (PTE19) provisoire, constituée de réservistes et de collaborateurs issus de quatre directions différentes. Leur mission se limitait à la période s'étendant jusqu'au jour des élections, se concentrait uniquement sur la Fédération de Russie et ne suivait que 'l'influence extérieure' et/ou la 'manipulation'. Le fonctionnement de cette équipe provisoire était indépendant de la structure des directions existantes au sein du SGRS. Un plan de collecte a néanmoins été discuté avec ces directions. Par ailleurs, l'initiative a été prise de lancer une étude concernant l'éventuelle menace.

I.4.4. LA COLLABORATION AU SEIN DE LA *JOINT INTELLIGENCE TASK FORCE* (JITF)

Fin 2018, la VSSE et le SGRS[63] ont constitué une *Joint Intelligence Task Force* (JITF), qui avait comme périmètre d'action spécifique l'influence en ligne des élections fédérales et régionales en Belgique par des acteurs étatiques russes. La task force était active sur quatre terrains distincts, c'est-à-dire (1) la sensibilisation et la '*resilience building*', (2) l'analyse stratégique (de phénomènes), (3) la détection des risques et incidents et (4) la gestion de crise sous la forme, entre autres, de la

62 *Doc. parl.* Chambre, 2017-18, 54-3267/1, 13 septembre 2018, 9.

63 Le SGRS s'est limité à utiliser ses capacités de collecte pour mener des activités de détection et livrer une sorte de '*primary assessment*'.

communication et de l'alerte rapide, pour lesquelles un pilote a été désigné au sein de chaque service.

La task force a pris plusieurs initiatives en matière de sensibilisation et d'accroissement de la résilience.[64] En outre, douze projets de détection ont été développés pour détecter les tentatives d'influence. La JITF a par ailleurs collaboré avec différents partenaires internationaux, parmi lesquels l'*East StratCom Task Force* du Service d'action extérieure européen[65], qui dispose d'une banque de données reprenant les propagateurs de désinformation sur l'Union européenne. Une collaboration a également été mise en place avec la *Transatlantic Commission on Election Integrity*.

Sur la base des projets précités et des risques et incidents détectés, la JITF a établi des analyses opérationnelles qui se sont retrouvées dans les dénommés *Joint Detection Reports* (JDR), dans lequel il était notamment fait référence à diverses situations prévalant en Belgique relatées par les médias russes, à l'origine de comptes Twitter, à la diffusion d'une désinformation bien déterminée concernant la Belgique, ou encore aux premiers constats des grandes sociétés Internet présentes.

Outre l'analyse opérationnelle, des analyses stratégiques ont été réalisées en s'appuyant sur la collecte d'informations des deux services.

Le dernier pilier de l'approche de la JITF se situait au niveau de la coopération nationale et internationale dans le domaine de la cybersécurité. L'initiative n'a pas été prise par les services de renseignement eux-mêmes, mais par d'autres instances, à savoir la Direction générale du centre de crise du SPF Intérieur et le Centre pour la Cybersécurité Belgique.

I.4.5. LA COLLABORATION DES SERVICES DE RENSEIGNEMENT AVEC D'AUTRES ACTEURS

Les services de renseignement ne travaillaient évidemment pas sur une île.

On peut par exemple citer diverses initiatives qui ont été prises avec d'autres institutions publiques. Une concertation a eu lieu entre la VSSE et la Direction générale Institutions et Population du SPF Intérieur afin d'anticiper les éventuelles menaces dirigées contre les élections. Une concertation a également été organisée entre les deux services de renseignement et le Centre pour la Cybersécurité Belgique.[66] Le CCB a constitué un guide de sensibilisation pour les partis

---

64 Comme, par exemple, le briefing du ministre de la Justice et des représentants des médias belges fin janvier 2019.

65 La *EEAS East StratCom Task Force* a été créée par le Conseil européen en mars 2015, spécifiquement en vue de contrer la diffusion de désinformation émanant de la Russie.

66 Le Centre pour la Cybersécurité Belgique (CCB du SPF Chancellerie du Premier ministre) était chargé en premier lieu de contrer d'éventuelles menaces techniques extérieures.

et le personnel politiques[67], et ce en collaboration avec les deux services de renseignement. Par la suite, une concertation a eu lieu avec le Centre de crise. Les acteurs se sont accordés sur la stratégie de communication et ont défini le rôle des services de renseignement, qui consistait essentiellement à identifier l'éventuelle diffusion de désinformation en vue d'influencer les résultats des élections.

Dans les premiers mois de 2019, la VSSE a également étudié l'approche adoptée par plusieurs pays européens. Certains services partenaires ont été interrogés. La VSSE a aussi établi des contacts avec Facebook, qui a expliqué avoir élaboré un plan d'action à la suite d'expériences malheureuses lors de scrutins précédents, notamment aux États-Unis. Facebook a expliqué le traitement réservé aux fausses informations visant à influencer l'opinion publique et a exposé ses constats quant aux élections européennes.

Pour soutenir ses analyses, le 'Projectteam Elections 2019' (PTE19) du SGRS pouvait s'appuyer sur les bons contacts précédemment établis avec le *NATO Strategic Communications Centre of Excellence* (NATO StratCom COE).[68] Cette expertise a permis au PTE19 d'avoir une bonne vue sur les techniques utilisées par les Russes ou par des acteurs sponsorisés par la Russie pour influencer des publics cibles étrangers. La JTIF a également pris contact avec la *Transatlantic Commission on Election Integrity* (TCEI), un projet de l'*Alliance of Democracies*, une organisation à but non lucratif qui compte parmi ses fondateurs l'ancien secrétaire général de l'OTAN Anders Fogh Rasmussen. Le TCEI utilisait un logiciel *ad hoc* pour détecter un comportement anormal sur Twitter, logiciel qu'il avait déjà utilisé lors de différentes campagnes électorales. Enfin, des représentants de la VSSE et/ou du SGRS ont participé à une série de forums de concertation, séminaires et conférences sur la thématique.

I.4.6. CONCLUSIONS

À l'issue de l'enquête, le Comité permanent R a estimé que les deux services de renseignement avaient pris les mesures nécessaires pour contrer les éventuelles menaces visant les élections belges et européennes de mai 2019. Les services :

– avaient reconnu et assimilé la problématique ;
– avaient examiné et identifié les risques et les menaces ;
– s'étaient organisés comme il se doit ;

---

67 'Surfer en toute sécurité pendant la campagne électorale – Recommandations pour une campagne cybersécurisée', CCB, VSSE, SGRS, février 2019, 9 pages. Cette brochure peut être consultée depuis février 2019 sur le site internet de la VSSE (www.vsse.be).

68 Le *NATO StratCom COE* (https://www.stratcomcoe.org), établi à Riga (Lettonie), est devenu opérationnel en janvier 2014 après la signature d'un mémorandum par sept pays membres de l'OTAN. Il s'agit d'une organisation internationale et militaire accréditée par l'OTAN qui réunit des experts internationaux.

– avaient développé la collaboration qui s'imposait entre eux et avec d'autres acteurs ;
– avaient sensibilisé et informé le Gouvernement et d'autres parties intéressées pour leur permettre, le cas échéant, de prendre les mesures nécessaires.

Selon les services, les actions à grande échelle redoutées n'ont pas eu lieu, tandis qu'il a été constaté que les tactiques de désinformation étaient toujours plus sophistiquées.

I.5. LE MEMORANDUM OF UNDERSTANDING (MOU) ENTRE LE SGRS ET LES SERVICES DE RENSEIGNEMENT RWANDAIS

Le Comité permanent R a décidé de procéder à une enquête sur la portée du MoU conclu entre le Service Général du Renseignement et de la Sécurité (SGRS) et les services de renseignement rwandais en octobre 2016, en particulier, et plus généralement, sur la conclusion d'une collaboration entre un service de renseignement belge et un de ses partenaires étrangers.[69]

I.5.1. CADRE JURIDIQUE

I.5.1.1. La Loi organique des services de renseignement et de sécurité (L.R&S)

Dès 1998, le législateur a encouragé la collaboration des services de renseignement, d'une part, avec les services belges de police, les autorités administratives et judiciaires et, d'autre part, avec des services de renseignement et de sécurité étrangers. L'article 20 L.R&S attribue à la VSSE et au SGRS la compétence générale d'établir des relations de collaboration avec des services de renseignement et de sécurité d'autres pays.

La loi ne précise ni la nature de la collaboration ni ses modalités pratiques, mais confie au Conseil national de sécurité (CNS) le soin d'en définir les conditions.

[69] L'enquête a été initiée par la Commission de suivi. Voir *Doc. parl.*, Chambre, 2019-20, 55-888/001, 11.

I.5.1.2. L'application de la loi et la directive ministérielle de 2016

En septembre 2016, les ministres de la Justice et de la Défense ont adressé une directive classifiée 'confidentiel Loi 11.12.1998' au Conseil national de sécurité[70] concernant les relations des services de renseignement belges avec des services de renseignement étrangers. Cette directive a pour objet de procéder à une évaluation desdits services étrangers en vue de déterminer la nature de ces relations. Il s'agit d'un outil d'appui stratégique à la coopération bilatérale/multilatérale.

La directive décrit les mécanismes que la VSSE et le SGRS doivent respecter. Elle précise la manière d'objectiver et de structurer les choix des partenaires étrangers, la nécessité de déterminer la portée des collaborations et, enfin, l'obligation de les évaluer régulièrement.[71]

La directive ne précise cependant pas de manière univoque si la VSSE et le SGRS doivent obtenir ou pas l'aval ministériel préalable ou l'aval d'une autre autorité.[72] Pourtant, le Comité estimait déjà en 2014 *'que les services de renseignement doivent faire preuve d'une plus grande ouverture concernant les accords de coopération bilatéraux ou multilatéraux existants, et ce en premier lieu à l'égard des ministres compétents. En effet, ces accords de coopération peuvent renfermer des engagements ou des choix qui requièrent une vérification et une couverture politiques. En d'autres termes, les ministres compétents doivent être suffisamment informés afin d'être toujours en mesure de prendre leurs responsabilités politiques. Il convient de remarquer à cet égard que ce qui est « politiquement pertinent », ou ce qui ne l'est pas, peut évoluer avec le temps*'.[73] En 2017, la nécessité d'une couverture politique a fait une nouvelle fois l'objet d'une recommandation du Comité.[74]

---

70 MITS 16-007498 du 26.09.2016. Le 30 septembre 2016, le CNS a approuvé cette directive. Le Comité avait déjà insisté sur ce point à maintes reprises. Dans COMITÉ PERMANENT R, *Rapport d'activités 2012* ('I.1.2. Modalités particulières de la collaboration avec des services étrangers'), *Rapport d'activités 2013* ('IX.1.1. Exécution des articles 19 et 20 L.R&S') et *Rapport d'activités 2014* ('IX.1.2. Directives concernant la collaboration avec des services étrangers').

71 La Directive ne répondait toutefois que partiellement aux recommandations du Comité : '*La transmission d'informations/de données à caractère personnel à des services étrangers n'y est cependant traitée que de manière sommaire. Le Comité maintient dès lors ses recommandations antérieures et juge l'initiative prioritaire. Il convient, de toute façon, de prêter attention au principe de prudence, que les services de renseignement sont tenus respecter dans le cadre des échanges d'informations*', COMITÉ PERMANENT R, *Rapport d'activités 2016*, 166.

72 Voir dans ce sens : Proposition de loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité en vue d'instaurer des notes d'évaluation pour la collaboration avec les services de renseignement et de sécurité étrangers, *Doc. parl.* Chambre 2019-20, n° 55-956/001 (23 janvier 2020).

73 COMITÉ PERMANENT R, *Rapport d'activités 2014*, 113.

74 COMITÉ PERMANENT R, *Rapport d'activités 2017*, 107 ('XII. Couverture politique des accords de coopération').

I.5.1.3. Un Memorandum of Understanding du SGRS avec les services de renseignement rwandais

Un mémorandum d'entente (*Memorandum of Understanding*[75]) est un document décrivant un accord ou une convention bilatérale ou multilatérale entre ses parties. Il déclare une convergence d'intention entre les différentes parties, indiquant une ligne d'action commune. Il est souvent utilisé dans les cas où les parties n'ont pas impliqué un engagement juridique ou bien dans des situations où les parties ne peuvent pas créer une entente ayant force exécutoire. Il est une alternative plus formelle à un 'gentlemen's agreement'. En droit international public, les mémorandums d'entente tombent dans la catégorie générale des traités. D'un point de vue juridique, ils ne présupposent pas de caractère contraignant, mais expriment une intention *politique* des signataires.

S'agissant de la conclusion d'un MoU ou de toute autre forme de collaboration avec un partenaire étranger, le Comité estime que celle-ci revêt un caractère politique indéniable, même si, de l'avis du SGRS, un tel accord n'a pas de portée juridique. En effet, le service de renseignement partenaire peut volontairement ou non utiliser cet accord dans la défense de ses intérêts personnels et mettre à mal la Belgique dans ses relations diplomatiques.[76]

Au moment de l'enquête, le SGRS avait développé des collaborations[77] avec diférents partenaires étrangers. Seules 15 % de ces collaborations ont fait l'objet d'un MoU, dont celle conclue le 14 octobre 2016 avec les services rwandais.

Ce MoU a été signé par le Chef du SGRS à l'époque, et le secrétaire général du Service de renseignement rwandais (NISS). Il s'agissait d'un document non classifié[78] visant : *'to regulate the terms and conditions of exchange of national classified information, to define areas of bilateral cooperation in the field of intelligence and to formalize the procedure regarding the meetings between the two Participants*'.[79] Dans ce document, trois domaines de partenariat sont abordés, mais la manière dont celui-ci doit se réaliser concrètement n'est pas précisée.

---

75 Foreign and Commonwealth Office, Legal directorate, Treaty section, *Treaties and memoranda of understanding (mou's) guidance on practice and procedures*, actualisé en mars 2014.

76 Dans ses rapports sur l'affaire Edward Snowden et la plainte déposée par un collaborateur du SGRS, le Comité avait déjà relevé ce risque. COMITÉ PERMANENT R, *Rapport d'activités 2014* (II.1. Les révélations d'Edward Snowden et la position des services de renseignement belges') et COMITÉ PERMANENT R, *Rapport d'activités 2017* ('II.1. Une plainte concernant trois opérations du SGRS').

77 Le Comité a constaté une absence de corrélation entre ce type de collaboration et le Plan directeur du Renseignement établi par le SGRS et signé par le ministre de la Défense.

78 Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (L.C&HS).

79 '*de réglementer et définir les conditions d'échange d'informations nationales classifiées, de définir les domaines d'une collaboration bilatérale en termes de renseignements et de formaliser la procédure concernant les réunions entre les participants*' (traduction libre).

Nonobstant l'obligation stipulée à l'article 33 L.Contrôle de transmettre *« d'initiative au Comité permanent R les règlements et directives internes ainsi que tous les documents réglant le comportement des membres de ces services »*[80] et les multiples recommandations du Comité, force a été de constater, une nouvelle fois, qu'en 2016, le SGRS n'avait pas pris l'initiative d'envoyer le MoU conclu avec le Rwanda.

I.5.2. ANALYSE

I.5.2.1. Quant à l'évaluation du partenaire et la signature du MoU

Au cours de l'enquête, le SGRS a précisé que les accords qu'il conclut avec un partenaire ne sont pas juridiquement contraignants et comportent peu d'intentions. Il précise également que ses actions sont développées en adéquation avec les activités et la position politique de la Belgique.

Le SGRS affirmait que compte tenu de l'impact très limité de cet accord, l'aval du ministre de la Défense – préalable à la signature – n'avait pas été demandé.

Le Comité a pu constater que le partenaire rwandais n'avait pas fait l'objet d'une évaluation préalable à la conclusion du MoU, conformément à la directive ministérielle du 26 septembre 2016. Le SGRS a indiqué n'avoir effectué cette évaluation que postérieurement, et ce dans le courant du deuxième semestre 2018.

Après analyse, le SGRS a catégorisé le service rwandais. Le Comité a relevé, après examen, que cette analyse était non datée, trop sommaire et insuffisamment documentée. En outre, elle ne constituait pas une évaluation globale du SGRS, mais résultait de l'analyse de deux de ses directions. De surcroît, une de ces directions n'utilisait pas les critères d'évaluation de la directive précitée. Enfin, certains incidents n'étaient pas mentionnés.

I.5.2.2. Quant au contenu technique du MoU

Le Comité a pu constater que le MoU contenait des dispositions pour les deux parties concernant :

- l'exécution du MoU, qui se fera toujours dans le respect des normes nationales et internationales des pays respectifs ;
- la règle du tiers service devant être respectée ;
- la concordance et les niveaux de classification ;

---

[80] COMITÉ PERMANENT R, *Rapport d'activités 2014*, 125 ('IX.3. Recommandation relative à l'efficacité du contrôle : application stricte de l'article 33, § 2 L.Contrôle'). *'Cette obligation s'applique également aux conventions, Memorandums of Understanding (MoUs) ou accords conclus au niveau international, qu'ils soient bilatéraux ou multilatéraux ».*

– les mesures de conservation et de sécurité en ce qui concerne les documents classifiés ;
– les procédures en cas d'incident et de compromission ;
– les procédures d'organisation de réunions.

Le MoU ne contenait pas de dispositions relatives aux domaines de collaboration, à la gestion et à la transmission de données à caractère personnel.

I.5.3. CONCLUSIONS

Le Comité reste convaincu que les services de renseignement belges doivent continuer à investir dans une collaboration avec les services étrangers, et ce tant au niveau bilatéral que multilatéral.[81] Néanmoins, cette collaboration doit être d'une totale transparence et d'une totale traçabilité compte tenu de son caractère politique indéniable.

Malgré l'obligation stipulée à l'article 33 L. Contrôle de transmettre « *d'initiative au Comité permanent R les règlements et directives internes ainsi que tous les documents réglant le comportement des membres de ces services* » et les multiples recommandations du Comité, le SGRS continuait de pas envoyer les documents précités, dont les MoU, au Comité permanent R.

En ce qui concerne la collaboration avec un partenaire étranger, le Comité a réitéré son constat que ses recommandations n'avaient pas été suivies quant à la nécessité de disposer d'un accord politique préalable à la conclusion d'accords bilatéraux/internationaux. Il relève que la directive ministérielle ne porte aucune mention univoque selon laquelle les services de renseignement doivent obtenir l'accord du Ministre préalablement à la conclusion d'un accord, formel ou informel, de coopération avec un service étranger, alors que sa responsabilité politique pourrait être engagée.

En ce qui concerne plus particulièrement le partenariat avec les services rwandais, le Comité estimait que le SGRS n'avait pas respecté la directive ministérielle, que ce soit lors de sa conclusion, ou actuellement dans le cadre de sa mise en œuvre.

Le Comité a constaté une fois encore un défaut de prudence dans le chef du SGRS, dans la mesure où il n'y avait pas de classification uniforme de ce type de document.

Malgré l'existence de la directive, le Comité a constaté :
– une évaluation tardive du partenaire (deux ans après la signature du MoU) ;
– une évaluation non datée, trop sommaire, insuffisamment documentée ;

[81] Voir également : COMITÉ PERMANENT R, *Rapport d'activités 2013,* ('IX.1.1. Exécution des articles 19 et 20 L.R&S').

– l'application non uniforme des critères d'évaluation prescrits par la directive[82] ;
– l'absence de notification des incidents ;
– l'absence d'évaluation bisanuelle.

Malgré ses précédentes recommandations, le Comité permanent R a constaté que les points de vue des différentes directions sur ce sujet divergeaient au sein du SGRS et qu'il n'existait pas de position commune.

I.6. LES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION DANS LE PROCESSUS DE RENSEIGNEMENT AU SGRS

I.6.1. LE CORE BUSINESS D'UN SERVICE DE RENSEIGNEMENT

Les technologies de l'information et de la communication (TIC ou ICT en anglais) jouent un rôle de plus en plus important dans les processus de renseignement, aussi bien dans la collecte et l'analyse des informations de base que dans la diffusion des renseignements. Les informations peuvent notamment provenir de sources humaines (HUMINT), de sources digitales, telles que les '*open sources*' ou sources ouvertes (OSINT), les écoutes (SIGINT) ou encore les prises d'images (GEOINT). L'augmentation constante des flux de données nécessite des systèmes adéquats, prêts à absorber ces flux et permettant une analyse correcte, rapide et efficace. L'environnement informatique doit donc être un outil stable et orienté vers l'avenir, et ce afin de donner du support aux différents acteurs intervenant dans le cycle du renseignement. Cet environnement, aussi bien matériel ('*hardware*') que logiciel ('*software*') doit se conformer aux standards en la matière, aux bonnes pratiques IT, tout en tenant compte des évolutions technologiques[83], telles que le '*big data*'.[84]

Dans des enquêtes antérieures, le Comité permanent R a constaté que les services de renseignement étaient confrontés à des défis majeurs dans ce domaine. Surtout pour le SGRS, il est déjà apparu par le passé que l'ICT était un point d'attention. Le Comité a relevé que les activités de renseignement n'étaient pas (ou

---

82 Les anciennes directions 'Intelligence' (I) et 'Contre ingérence' (CI) n'utilisent pas les mêmes critères d'évaluation.

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

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

plus) suffisamment soutenues par l'ICT. Les conditions d'une bonne gestion de l'information n'étaient pas (ou plus) complètement remplies.[85] [86]

Aussi, le Comité permanent R a initié, en mai 2019, une 'enquête de contrôle sur les moyens informatiques utilisés par les services de renseignement belges pour la collecte, le traitement, l'analyse et la communication de l'information dans le cadre du cycle du renseignement'. L'enquête se concentrait sur les moyens informatiques spécifiquement utilisés pour appuyer les éléments du cycle du renseignement. Il s'agit des systèmes qui sont utilisés, par exemple, pour effectuer la collecte, ou encore des outils d'analyse et bases de données spécifiques.[87] Le Comité permanent R ne s'est pas penché sur les facilités bureautiques (génériques/standard) utilisées par les services (par ex. Windows, Word, Excel, etc.), dans la mesure où elles ne sont pas spécifiques aux services de renseignement. Le Comité n'a pas non plus examiné en détail le matériel informatique ('*hardware*') à la disposition des services, à moins qu'il ne soit spécifique au service de renseignement concerné. L'enquête visait à identifier les risques[88] auxquels les services étaient confrontés en formulant des recommandations adaptées.

Le premier volet de l'enquête portait sur le SGRS, et ce en raison de l'impact de la restructuration de ce service en matière d'outils ICT et de méthodes de travail.[89] Les questions d'enquête étaient les suivantes :

- Quelles sont les technologies et quels sont les outils utilisés par le SGRS pour soutenir ses activités ?
- Dans quelle mesure les instruments sont-ils développés en interne ou fournis par des partenaires externes ?

---

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

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

87 Au SGRS, ces systèmes sont appelés '*weapon systems*', par analogie avec, par exemple, des systèmes intégrés aux plateformes de défense à la Défense (par ex. les logiciels pour les systèmes radar ou pour le '*battle management*').

88 Un 'risque' a été défini comme étant l'éventualité de l'existence d'une défaillance ou d'une menace plus ou moins prévisible pouvant influencer la réalisation des objectifs d'une organisation ou l'accomplissement efficiente de ceux-ci, associé à la probabilité que survienne un événement nuisible suite à cette défaillance.

89 En ce qui concerne le SGRS, l'enquête a été finalisée en mai 2020. Le volet de l'enquête 'ICT-VSSE' s'est poursuivi en 2020-2021.

- Les 'bonnes pratiques' usuelles (ci-après 'ITIL')[90] sont-elles appliquées correctement ? (plus précisément : *'change management'*, *'inventory management'*, *'business continuity'*, *'incident management'*, *'problem management'*, etc.)?
- Existe-t-il une politique de *'business continuity plan'* (BCP) ainsi que des procédures *'disaster recovery plan'* (DRP) incluant les backups et sont-elles actualisées ?[91]

L'enquête visait donc à identifier les risques auxquels sont confrontés les services de renseignement et, par le biais de recommandations, à réduire ces risques. C'est le modèle dit 'CIA'[92] qui a été appliqué. On distingue trois types de risques :

- *Confidendiality* : le risque de prise de connaissance de données, classifiées ou non ;
- *Integrity* : le risque de modification non autorisée de données, classifiées ou non ;
- *Availability* : le risque que les données ne soient pas disponibles, ce qui empêcherait de mener à bien les missions du service.

À cet égard, les instruments ICT utilisés spécifiquement pour le SIGINT n'ont pas été analysés.[93] Les moyens ICT utilisés par la Direction Cyber n'ont été étudiés que dans la mesure où ils se rapportent au cycle du renseignement. En effet, les attributions de cette direction comprennent également (et d'ailleurs principalement) des activités qui ne concernent pas (ou pas directement) le cycle du renseignement (article 11, § 1er, 1° et 5° L.R&S), mais plutôt la cyberdéfense et, le cas échéant, les cyberattaques (article 11, § 1er, 2° L.R&S).[94]

---

90 ITIL est l'acronyme de '*Information Technology Infrastructure Library*', qui se traduit par 'Bibliothèque pour l'infrastructure des technologies de l'information'. Il s'agit des bonnes pratiques pour la gestion des services IT les plus utilisés au monde (source : www.heflo.com/fr/blog/technologie/definition-itil).

91 Il existe de bonnes pratiques généralement acceptées sur la meilleure manière d'effectuer des sauvegardes et sur les procédures à appliquer en cas de désastre. La gestion des backups s'inscrit, tout comme les procédures DRP ('*disaster recovery plan*') dans un '*business continuity plan*' (BCP) global.

92 L'utilisation du modèle dit 'CIA' est préconisée comme base d'analyse de risques selon les normes internationales ISO 270 relatives à la sécurité de l'information. Ce modèle est également utilisé par de nombreuses autres normes telles TCSEC – Orange Book (1983 – VS) ou encore Common Criteria (1994 – international).

93 Il s'agit d'une matière portant le niveau de classification 'TRÈS SECRET' qui fait l'objet d'une enquête de contrôle (en cours).

94 C'est-à-dire de '*veiller au maintien de la sécurité militaire (…) et, dans le cadre des cyberattaques de systèmes d'armes, de systèmes informatiques et de communication militaires ou de ceux que le Ministre de la Défense nationale gère, de neutraliser l'attaque et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit des conflits armés*'.

I.6.2. CONTEXTE

I.6.2.1. Équipe, personnel et réseaux

L'informatique au SGRS est principalement gérée par le service d'appui J6 du service. Cette section est divisée en deux piliers : le premier gère les parties logicielles (analystes, développeurs, administrateurs de bases de données), tandis que le second pilier s'occupe surtout de la gestion des aspects les plus matériels, tels que le réseau, les serveurs, le magasin et le helpdesk. Le service d'appui J6 est responsable de plusieurs réseaux (en fonction de la nature des informations qui y transitent) et également de la gestion des utilisateurs. Chaque collaborateur peut avoir accès à plusieurs comptes d'utilisateur en fonction de ses attributions, de ses missions et du '*need to know*'. Ces réseaux peuvent être disponibles tant sur le territoire belge qu'à l'étranger.

I.6.2.2. Bases de données

En ce qui concerne les bases de données et leurs systèmes de gestion, on peut distinguer au sein du SGRS :

- les 'grandes' bases de données : il existe plusieurs types de bases de données au SGRS. Il s'agit pour la plupart de bases de données de type SQL en mode relationnel (*Structured Query Language*). La majorité des bases de données fonctionnent avec la technologie MS-SQL de Microsoft, même s'il y a encore d'autres types. L'ancienne Direction I disposait (et dispose toujours) d'un système de 'logiciel de groupe' (*groupware*). Ce système permet de placer des documents dans une bibliothèque ('référentiel' of '*repository*'), où ils sont 'publiés' (via un portail) afin d'être accessibles à plusieurs personnes ou groupes.
- les 'petites' bases de données : à côté des bases de données destinées aux applications principales, il existe des petites bases de données individuelles ou des bases de données par service.

Ce qui démontre l'importance des bases de données, c'est souvent l'augmentation de leur taille au fil du temps, à un point tel qu'il devient presque impossible de retrouver de manière efficace les données pertinentes dans les quantités astronomiques de données qu'elles contiennent. Le Comité permanent R a suggéré trois solutions pour y remédier[95]:

[95] Par analogie, une base de données SQL serait, par exemple, un fichier clients d'un magasin. Le '*data warehouse*' serait alors la consolidation des fichiers clients et achats de tous les magasins de Belgique. Une base de données de type *'no sql'* serait alors, par exemple, un moteur de recherche tel que Google.

- une consolidation et une réorganisation des bases de données de type SQL par l'adjonction d'index de recherche. Cette méthode est peu onéreuse et fournit des résultats pour les opérations les plus courantes ;
- l'utilisation de '*data warehouses*' ('*big data*'), où toutes les données des différentes bases de données sont dupliquées pour pouvoir effectuer des analyses à grande échelle. Ceci permet d'établir des tendances ou de découvrir des informations qui, au départ, n'étaient pas évidentes lorsque chaque base de données était consultée séparément. Cette méthode nécessite une puissance de calcul et un stockage considérables, ainsi qu'une connaissance du sujet à traiter, afin de réaliser une modélisation de données correcte ;
- l'utilisation de nouveaux types de bases de données qui ne se fondent plus sur des relations structurées (SQL), mais plutôt sur la présence d'éléments (données, tags) permettant d'établir un score de pertinence de l'information. Il s'agit de bases de données *'no-sql'* qui ont structure beaucoup plus simple et permettent des recherches sur des contenus de fichiers ou de tags.

Le Comité a par ailleurs établi une série de constatations concernant la sécurité du matériel physique ou la sécurité des communications ICT. C'est un service de la Direction Cyber qui effectue des tests de sécurité avant tout déploiement d'applications au sein de la Défense et du SGRS.

I.6.3. ÉVALUATION DES RISQUES

Une série de points d'attention ont été énumérés pour chaque section de l'organisation ICT du SGRS. Au cours de cette enquête, le Comité a mis en évidence certains risques, leur probabilité ainsi que les pistes d'atténuation ('*mitigation*') afin de réduire ces risques. Un aperçu a été donné des problèmes constatés au SGRS, répertoriés par catégorie.[96] Parmi les risques les plus importants encourus par le service, l'attention s'est portée sur :

- la vitesse du réseau, compte tenu de son utilité pour toutes les applications et donc pour la bonne exécution des missions du service ;
- le monitoring du réseau, mais également de toute l'infrastructure digitale visant une détection proactive des signes avant-coureurs de pannes ou de lenteurs ;
- la journalisation (*'logging'*) des activités afin de se prémunir d'abus, mais aussi dans le but de pouvoir fournir des preuves légales concernant les activités des utilisateurs ;

[96] La confidentialité ne permet pas de détailler cette analyse de risques dans ce rapport d'activités public.

- la gestion de l'*'Active Directory'* afin de limiter la possibilité de *'privilege creeping'*[97] (correspondant au fait d'accumuler des droits d'accès à chaque changement de fonction sans que les anciens accès soient supprimés) ;
- le *'change management'*, pour que chaque changement (mise à jour, nouvelle installation) se déroule selon une procédure stricte comprenant une méthode qui permet un retour à la situation antérieure.

Enfin, la question du manque de personnel ICT a été soulevée. Il était important de régler de toute urgence ce problème et de lancer sans tarder la procédure d'engagement, étant donné qu'il s'agit d'une procédure assez longue. En effet, si le manque de personnel venait à perdurer ou à s'aggraver, toutes les missions sous-jacentes risquent/risquaient d'être impactées dans l'éventualité d'une panne ou tout simplement pour la maintenance de l'infrastructure physique ou logicielle.

I.7. LE SUIVI DE L'EXTRÊME DROITE PAR LES SERVICES DE RENSEIGNEMENT BELGES

I.7.1. OBJETS DE L'ENQUÊTE : LE CYCLE DU RENSEIGNEMENT ET L'ANALYSE DES RISQUES

Compte tenu de l'augmentation du nombre d'incidents terroristes dans le monde, qui sont liés à des individus aux idées extrémistes, et compte tenu aussi de la montée des mouvements identitaires et du reportage controversé sur Schild & Vrienden[98], le Comité permanent R a jugé opportun d'ouvrir une enquête de contrôle sur la manière dont les services de renseignement suivent la menace qui émane (du phénomène) de l'extrême droite en Belgique et de faire rapport aux autorités.

Le Comité souhaitait examiner si et comment les services de renseignement s'acquittent de leur mission légale de suivi de l'extrémisme, et plus particulièrement de l'extrémisme de droite en Belgique. Dans cette optique, une 'approche du risque' a été intégrée au cycle du renseignement, ce qui s'est traduit comme suit :

---

97 Une accumulation progressive (souvent dans le cadre de changements d'affectation) de droits d'accès qui vont au-delà de ce dont une personne a besoin pour faire son travail. Dans le domaine des TIC, le terme 'privilège' désigne un droit d'accès particulier dont dispose un utilisateur final à un fichier ou à une machine virtuelle.

98 https://www.vrt.be/vrtnws/nl/2018/09/05/pano-wie-is-schild-vrienden-echt/

Phase du cycle du renseignement	Risque	Questions d'enquête
Déterminer les objectifs de renseignement (stratégiques ou au niveau de la politique du renseignement)	Le phénomène n'est pas reconnu ou attire trop peu l'attention : – Il n'est pas bien décrit (au niveau juridique ou stratégique), si bien que les services ne peuvent pas se concentrer sur ce phénomène (délimitation qualitative) – Il n'est pas quantifié, si bien qu'on ne peut pas évaluer ce qu'il représente effectivement (délimitation quantitative)	Qui doit procéder à la délimitation et quel est le contexte juridique et stratégique ? Quelles sont les instructions données aux services par les ministres compétents, le CNS ou d'autres instances ? Les services de renseignement et de sécurité belges utilisent-ils une définition commune dans le cadre du Plan Radicalisme ? Le phénomène est-il quantifiable ?
Déterminer les objectifs de renseignement, les planifier et s'organiser (d'un point de vue opérationnel et tactique au niveau des services)	Le phénomène est reconnu mais il n'est pas suffisamment traduit dans l'organisation et dans la planification interne des services (pas proportionnellement).	Comment les services de renseignement intègrent-ils eux-mêmes le phénomène de 'l'extrême droite' dans leur organisation et leur planification ? Comment détermine-t-on quels groupes et situations font l'objet d'un suivi actif ? Comment les services sont-ils organisés pour effectuer ce suivi ? Quelles priorités ont été fixées ? L'utilisation des moyens (personnel, méthodes, etc.) est-elle proportionnelle à l'objectif visé ?
Collecte et traitement	La collecte est insuffisante : – Trop peu de sources pour suivre le phénomène ; – Les sources et les instruments ne sont pas bien utilisés ; – Le traitement des données pose problème.	Quelles méthodes sont mises en œuvre ? (méthodes ordinaires, MRD, HUMINT, etc.) ? Comment les informations sont-elles traitées ?
Analyse et diffusion/ coopération	L'analyse est insuffisante, voire inexistante. Les renseignements ne sont pas diffusés, si bien que le phénomène ne reçoit pas l'attention du monde politique. La coopération est insuffisante.	Quelles évaluations ont été effectuées (analyses) ? Comment en a-t-on fait rapport aux autorités ? Comment coopère-t-on et avec quels partenaires ?
Feedback	Le niveau politique ne reçoit pas de feedback, si bien qu'il n'est pas possible d'affiner ou d'orienter les objectifs de renseignement.	Quel feedback les services reçoivent-ils des utilisateurs ?

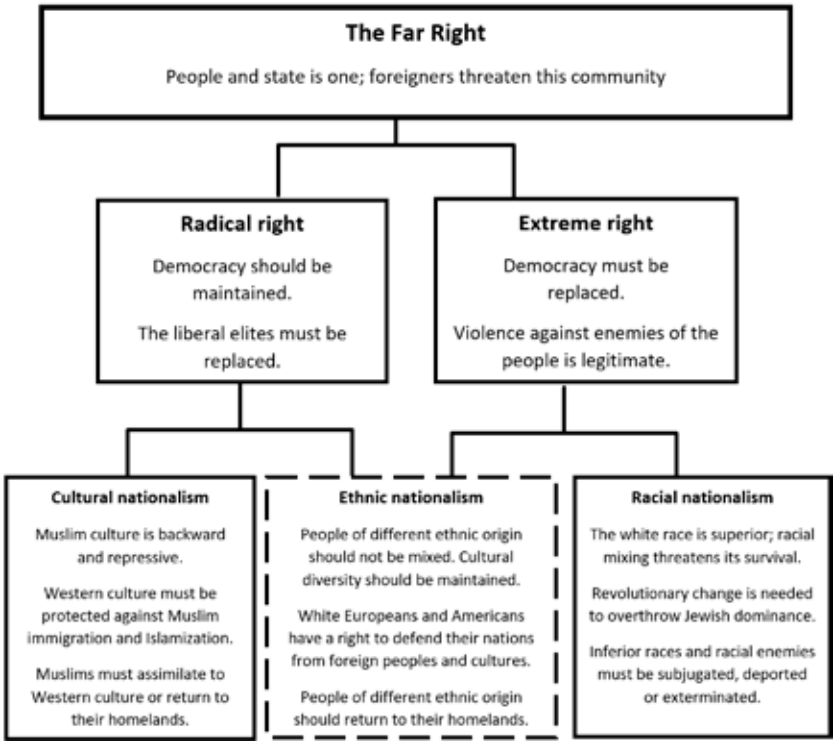
I.7.2. L'EXTRÊME DROITE : CADRE CONCEPTUEL ET REPRÉSENTATION DU PHÉNOMÈNE

I.7.2.1. Du point de vue académique

Il apparaît que les avis sur l'interprétation précise des notions d''extrême droite' et d''extrémisme de droite' divergent fortement. Il est clair qu'il n'y aucun consensus sur la définition exacte de ces concepts. Un article du politologue néerlandais Mudde (1995) constituait la base d'une nouvelle conceptualisation de l'extrême droite en Europe.[99] Dans le spectre politique de droite, Mudde opérait une distinction entre la droite modérée et l'extrême droite. Ensuite, une distinction était l'extrême droite, entre la droite radicale, qui opère dans un cadre démocratique, et l'extrémisme de droite, qui favorise le recours à la force ou à d'autres moyens non conventionnels pour provoquer un changement politique.

[99] C. MUDDE, 'Right-Wing Extremism Analyzed. A Comparative Analysis of the Ideologies of Three Alleged Right-Wing Extremist Parties (NPD, NDP, CP'86)', E*uropean Journal of Political Research*, 1995, Vol.27, Issue 2, pp. 203-224.

Les Norvégiens Bjørgo et Ravndal[100] (2019) ont élaboré certains de ces concepts et développé un modèle conceptuel dans lequel se trouvent trois 'familles' de l'extrême droite contemporaine :[101]



Concernant les chiffres, un jeu de données[102] relatif à la violence et/ou au terrorisme d'extrême droite ayant causé des décès en Europe occidentale et aux

---

100 T. BJØRGO & J.A. RAVNDAL, *Extreme-Right Violence and Terrorism: Concepts, Patterns, and Responses*, International Centre for Counter-Terrorism, September 2019, 22 p.

101 Cette classification est non seulement importante d'un point de vue académique, mais également d'un point de vue pratique. La distinction établie entre trois familles d'extrême droite permet d'avoir une perspective sur les groupes et individus les plus susceptibles de recourir à la violence. La définition a donc toute son importance d'un point de vue opérationnel. On retrouve les auteurs d'actes de violence essentiellement dans l'extrémisme de droite. Dans ce mouvement, la violence est considérée comme une manière d'agir légitime, nécessaire et souvent louable. Les partisans du nationalisme racial, tels que les néonazis, les fascistes et les suprémacistes blancs, sont classés plutôt en haut de la liste des auteurs de violences d'extrême droite.

102 J.A. RAVNDAL, 'Right-wing terrorism and violence in Western Europe', *Perspectives on Terrorism*, 2016, Vol.X, Issue 3. Les chiffres ont été actualisés dans J.A. RAVNDAL, S. LYGREN, A.R. JUPSKAS et T. BORGJO, RTV *Trend Report. Right wing terrorism and violence in Western Europe (1990-2019)*. On peut y lire que : *"To sum up the year 2019, we may conclude that right-wing terrorism and violence still constitute significant problems in Western Europe"*.

États-Unis a montré que l'Europe occidentale a connu un pic au début des années 1990 et au début du millénaire. Il y a eu une tendance à la baisse depuis lors, avec un pic plus faible en 2016, qui pourrait être dû à la crise des réfugiés en Europe. Il ressort des chiffres recueillis par le service de renseignement allemand *Bundesamt für Verfassungsschutz* (BfV) une augmentation constante du nombre d'extrémistes de droite en Allemagne depuis 2013, de même qu'une augmentation du nombre d'infractions commises par des extrémistes de droite de 2014 à 2018, avec un pic en 2015-2016.[103]

I.7.2.2. Représentation du phénomène de l'extrême droite par les services belges

a) L'Organe de coordination pour l'analyse de la menace (OCAM)[104]

Dans une note, l'OCAM dresse un tableau général du phénomène de 'l'extrémisme de droite'.[105] Selon l'organe de coordination, le processus de radicalisation extrémiste de droite violente est très similaire à d'autres processus de radicalisation (par ex. le djihadisme). Dans son analyse, l'OCAM fait référence aux travaux du chercheur norvégien Tore Bjørgo, qui soutient que l'idéologie joue un rôle secondaire dans la radicalisation de la jeunesse extrémiste de droite. Les sentiments diffus et hostiles, en revanche, jouent un rôle majeur.

L'OCAM relève essentiellement trois terreaux qui alimentent l'extrême droite : certains événements déclencheurs, un contexte social spécifique et des motifs (socio-) psychologiques. Internet apparaît comme étant un facteur de plus en plus important dans la propagation des idéologies et de la propagande radicales et violentes. Il s'agit, en effet, d'un moyen de communication bon marché et largement utilisé. Il permet de créer des réseaux à travers le monde et, grâce à un (relatif) anonymat, permet l'expression d'opinions souvent plus radicales que si l'auteur pouvait être identifié ; les opinions radicales ou la propagande peuvent également se propager rapidement ou devenir 'virales' en utilisant des profils automatisés ou ce que l'on appelle les '*bots*'. L'OCAM soutient que les extrémistes de droite tentent de créer un sentiment de 'nous-eux' à partir duquel les partisans d'une idéologie d'extrême droite assument soit un sentiment de supériorité, soit un rôle de victime, ce qui, dans les deux cas de figure, implique une menace. Souvent, tout cela va de pair avec les théories du complot, alléguant qu'un complot du gouvernement – représenté par des partis démocratiques libéraux – et les médias traditionnels tentent de cacher et de manipuler 'la vérité'. Une autre tactique préconisée par

---

103 EUROPOL, 'Terrorism Situation and Trend Report 2019 (TE-SAT)', 27 juin 2019, p.61.

104 Bien que cette enquête ne porte pas sur le suivi de l'extrême droite par l'OCAM, contact a été pris avec ce service, notamment parce qu'il agit en tant que service pilote du Groupe de travail Extrême droite dans le cadre du Plan d'action Radicalisme (Plan R).

105 ORGANE DE COORDINATION POUR L'ANALYSE DE LA MENACE, '*Note sur le phénomène de l'extrémisme de droite*', 14 février 2020, 39 p.

les mouvements d'extrême droite est, toujours selon l'OCAM, une soi-disant 'marche à travers les institutions'. Cette stratégie consiste à gagner en influence grâce à la participation aux mouvements sociaux et à la participation aux processus démocratiques et politiques, dans le but de pouvoir, à long terme, faire avancer sa propre idéologie anti-démocratique.

b) La VSSE et le SGRS

La VSSE constate que le milieu de l'extrême droite en Belgique a subi une 'transformation fondamentale' au cours de ces dernières années. Les formes traditionnelles de l'extrême droite, telles que le néonazisme et la culture Skinhead, sont en déclin, alors que l'activisme anti-islam et anti-migrants – surtout depuis la crise migratoire de 2015-2016 – sont devenus les sujets principaux pour l'extrême droite. Là où, auparavant, les groupements extrémistes faisaient appel aux sentiments nationalistes de leurs partisans, le curseur s'est déplacé vers la défense d'opinions xénophobes. Ceci concerne à la fois les 'plus anciens' groupements d'extrême droite et les nouveaux mouvements. La VSSE constate également, chez les extrémistes de droite en Belgique, un intérêt croissant pour les armes et les formations au maniement des armes. Le service estime qu'en Belgique, la principale menace est constituée par les '*lone actors*', qui se radicalisent et planifient des attaques violentes en solo.[106]

Le législateur a explicitement confié le suivi des activités extrémistes à la VSSE (articles 7 et 8, 1°, c) L.R&S). Mais ceci n'empêche pas le SGRS de suivre légitimement l'extrémisme parmi les militaires ou parmi le personnel civil, pour autant qu'ils représentent une menace pour le département ou pour son fonctionnement.[107] Le SGRS n'a cependant pas développé sa propre vision sur cette thématique[108] ; il prend appui sur le travail de la VSSE et de l'OCAM.

---

106 SÛRETE DE L'ÉTAT, *Rapport annuel 2019*, 20 (https://www.vsse.be/fr/rapportannuel-2019).

107 En outre, différentes dispositions relatives au statut du personnel militaire et civil prescrivent qu'ils doivent respecter la Constitution et défendre les intérêts moraux et matériels de l'État. Certains actes ou certaines déclarations à caractère extrémiste, tant dans le contexte professionnel qu'en dehors, sont punissables parce qu'ils sont en contradiction avec le statut disciplinaire, la déontologie et les règlements militaires.

108 En 2012, le Comité permanent R avait déjà ouvert une enquête de contrôle sur la détection et le suivi des éléments extrémistes au sein du personnel de la Défense. L'enquête a montré qu'au cours de cette période, un nombre assez limité d'individus au sein de la Défense étaient impliqués dans des activités extrémistes. Au cours de l'enquête, le SGRS a dit constater que le nombre de militaires qui attirent l'attention en raison d'une éventuelle implication dans des activités d'extrême droite est limité.

I.7.3. PREMIÈRE ÉTAPE DANS LE CYCLE DU RENSEIGNEMENT : LA DÉLIMITATION DE L'OBJECTIF DE RENSEIGNEMENT 'EXTRÊME DROITE'

I.7.3.1. Délimitation qualitative : la définition du phénomène

Organiser la fonction de renseignement et déterminer où l'attention d'un service de renseignement est d'une importance capitale pour définir le phénomène avec précision et pouvoir ensuite se le représenter.

La VSSE se réfère à l'article 8 de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) pour déterminer si un individu ou un groupement doit être considéré comme étant d'extrême droite. Toutefois, la loi ne mentionne pas explicitement ce qu'il y a lieu d'entendre par 'extrême droite' ou 'extrémisme de droite'.[109] Le service se réfère également au modèle conceptuel de l'universitaire norvégien Tore Bjørgo (*supra)* et se base sur la définition utilisée par le service de renseignement néerlandais (AIVD).

À la question du Comité sur les définitions et concepts du service de renseignement militaire, il n'y a pas eu de réponse différente de celle d'autres acteurs. Dans la pratique, l'attention du SGRS se concentre sur les militaires qui se rendent éventuellement coupables de propos ou d'un comportement raciste, négationniste ou discriminatoire, ou qui font partie de groupements qui tiennent de tels propos ou adoptent un tel comportement. Compte tenu du fait que le SGRS focalise son attention sur la sauvegarde des intérêts militaires, le suivi de l'extrême droite par ce service est moins étendu que celui de la VSSE. Le SGRS s'appuie dès lors sur les analyses de la VSSE pour mieux cerner la problématique et se base donc logiquement sur les définitions et concepts utilisés par la VSSE.

Mais à qui incombe la délimitation ? Il revient avant tout au législateur de déterminer ce sur quoi les services de renseignement doivent se concentrer et de délimiter le champ d'action (cf. la Loi organique des services de renseignement et de sécurité). Viennent ensuite les ministres compétents : les articles 4 et 10 L.R&S stipulent que la VSSE et le SGRS accomplissement leurs missions à l'intervention, respectivement, du ministre de la Justice et du ministre de la Défense. Le Conseil national de sécurité (CNS) intervient en parallèle, en établissant la politique générale

---

[109] Plusieurs de ces notions ont été précisées dans J. SEGERS en D. PEETERS, 'Inlichtingendiensten en extremisme', in M. COOLS, K. DASSEN, R. LIBERT, P. PONSAERS (eds.), *De Staatsveiligheid – Essays over 175 jaar Veiligheid van de Staat*, Politeia, 2005, pp. 281-302). C'est surtout l'apparition du terme 'nationalisme' dans la définition légale de l'extrémisme qui requiert une explication complémentaire: *'Pour le service (VSSE), le nationalisme en tant que phénomène en relation avec l'extrémisme ne revêt une importance que dans la mesure où il rejoint les notions précitées de racisme et/ou xénophobie. En d'autres termes, des mouvements qui, de manière démocratique, aspirent à un degré élevé d'autonomie par rapport à une communauté (populaire), ou qui ont une préférence certaine pour leur propre peuple, tout en respectant les droits humains, ne peuvent pas être considérés comme extrémistes.'* (traduction libre).

du renseignement et de la sécurité et en fixant les priorités. L'opérationnalisation des missions incombe aux deux services de renseignement, si nécessaire en coordination avec d'autres services de sécurité (par ex. l'OCAM).

a) La Loi organique des services de renseignement (1998)

La Loi organique des services de renseignement et de sécurité (pas plus que la Loi OCAM) ne définit les termes 'extrême droite' ou 'extrémisme de droite'. L'article 8, 1°, c) L.R&S mentionne uniquement cette définition de l'"extrémisme' : *'les conceptions ou les visées racistes, xénophobes, anarchistes, nationalistes, autoritaires ou totalitaires, qu'elles soient à caractère politique, idéologique, confessionnel ou philosophique, contraires, en théorie ou en pratique, aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'État de droit en ce compris le processus de radicalisation*'. Avec la Loi du 30 mars 2017, cette définition a été complétée par ce qui suit : *'En ce compris le processus de radicalisation*'.[110]

Une réserve est de mise, en ce sens que le législateur lui-même indique que, de toute manière, les définitions sont relativement vagues. Lors des discussions préalables à l'introduction de la L.R&S, les membres du pouvoir législatif affirmaient que les définitions *'ne sont pas aussi précises que les définitions du Code pénal'* ou entouraient les termes menace extrémiste de guillemets (L. OCAM).

b) Le Conseil national de sécurité (CNS) et les ministres de tutelle

Le Conseil national de sécurité, pas plus que les ministres de tutelle, n'ont ajouté d'éléments ou de spécifications à la terminologie qui est utilisée par le législateur, que ce soit en qui concerne le concept général de l'extrémisme ou les notions spécifiques d'extrême droite ou d'extrémisme de droite.

c) Les services de renseignement et le Plan d'action Radicalisme (Plan R)

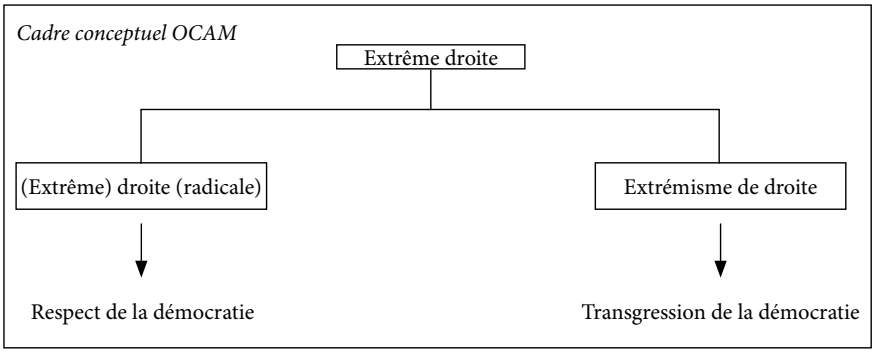
Ni la VSSE ni le SGRS n'ont élaboré leur 'propre' terminologie concernant l'extrême droite. Ceci n'est pas illogique : le faire, c'était risquer de sortir ou d'outrepasser les normes en vigueur (donc, en premier lieu, la L.R&S). Il convient néanmoins

[110] La notion de 'processus de radicalisation' est définie à l'article 3, 15° L.R&S : *'un processus influençant un individu ou un groupe d'individus de telle sorte que cet individu ou ce groupe d'individus soit mentalement préparé ou disposé à commettre des actes terroristes*'. Le terme a également été expliqué dans l'Exposé des motifs de l'élargissement de la Loi MRD : *'[…] un processus, […] la progression d'un individu dans un contexte déterminé, en l'occurrence radical. Au point 0 du processus, l'individu commence à partager des idées radicales qui sont en rupture avec les valeurs démocratiques de notre société. Cela correspond à l'extrémisme, au sens de la loi des services de renseignement et de sécurité. L'individu n'est pas encore et n'atteindra peut-être jamais le stade de poser des actes terroristes. Le processus de radicalisation couvre en réalité les deux phénomènes : l'extrémisme et le terrorisme, en fin de parcours*'.

d'attirer l'attention sur une initiative importante, dans laquelle il est également question de l'extrême droite : le Plan d'action Radicalisme (Plan R) qui a été établi en 2006 et actualisé en 2015. Le Plan R offre aux différents partenaires, via la National Task Force et divers de groupes de travail, des plateformes leur permettant d'échanger des informations et de l'expertise. Cela leur donne donc la possibilité de se représenter le plus correctement possible les phénomènes qui constituent une menace, et ce pour en réduire l'impact.

Le 'Groupe de travail Extrême droite' du Plan R, a travaillé sur une étude dont le premier objectif est de tenter de clarifier le cadre conceptuel.[111] Le second objectif du texte est de préciser ce que doit être le '*scope*' des services concernant le suivi de l'extrême droite ou de l'extrémisme de droite. Il convient de noter que la terminologie utilisée pour le phénomène n'est pas homogène et que différents concepts sont utilisés de manière interchangeable.

L'OCAM a proposé d'employer les termes 'radical de droite' ou 'extrême droite' pour les acteurs qui respectent la démocratie, et le terme 'extrémisme de droite' pour ceux dont les actes et les opinions transgressent les limites de la démocratie.



La VSSE a fait savoir au Comité qu'elle n'est pas d'accord avec la terminologie proposée par l'OCAM, qui établit une distinction entre l'extrême droite et l'extrémisme de droite.

I.7.3.2. Délimitation quantitative : l'ampleur du phénomène

Lorsqu'il est clair pour les services de renseignement qu'un phénomène se manifeste, il est important d'en évaluer l'ampleur. C'est ce qui permet, en effet, de définir l'importance des moyens à mobiliser pour contrer cette menace ainsi que le degré de priorité approprié.

Nonobstant la masse de données internationales sur des événements et des incidents liés à l'extrême droite, le Comité a dû constater une absence manifeste de

111 ORGANE DE COORDINATION POUR L'ANALYSE DE LA MENACE, '*Note sur le phénomène de l'extrémisme de droite*', 14 février 2020, 39 p. Dans sa note, l'OCAM distingue cinq catégories de recommandations sur les politiques à mener pour lutter plus efficacement contre l'extrême droite.

données quantitatives sur l'ampleur de la menace émanant de l'extrême droite en Belgique. Le Comité n'a pas pu obtenir de chiffres clairs de la part des deux services de renseignement.

L'OCAM[112] a fait remarquer que les crimes de haine et les incidents inspirés par l'extrême droite sont, dans une large mesure, sous-rapportés. Ils ne sont pas toujours reconnus ni enregistrés en tant que tels par les services de sécurité. Contrairement à l'Allemagne, entre autres, la Belgique n'a pas pour habitude d'indiquer, dans les procès-verbaux, une mention spéciale des motifs idéologiques, par exemple en cas de violence. Ceci complique la quantification du phénomène et *mutatis mutandis* l'obtention par les services de renseignement d'informations complètes (correctes). L'ampleur effective et l'évolution du phénomène restent dès lors difficile à évaluer, ce qui rend les moyens pour le suivre souvent difficiles à définir.[113] [114]

I.7.4. LA RÉORGANISATION ET LA PLANIFICATION DES SERVICES

I.7.4.1. Réorganisation

En 2016, la VSSE a mené une réforme interne qui s'est traduite, pour certaines matières, par la fusion des sections des services internes (d'analyse) et des services extérieurs. Les sections chargées de l'extrémisme idéologique (extrême droite et extrême gauche) étaient donc également concernées. Les effectifs de cette section ont été renforcés en 2020.

En janvier 2020, une nouvelle structure a également été mise en place au SGRS. Cette réorganisation a notamment donné lieu à la création d'une plateforme d'analyse 'Non-Religious ideological threats'. Tout comme à la VSSE, cette plateforme suit à la fois l'extrémisme de droite et l'extrémisme de gauche. L'attention se porte également sur les bandes de motards criminels. Après la mise

---

112 *Ibid.*

113 En France également, une commission parlementaire a constaté le même problème de l'absence de quantification : *'La commission ne dispose pas d'éléments permettant de chiffrer l'évolution des diverses infractions commises par les groupuscules (…) L'État n'effectue aucun suivi des infractions en fonction des motivations idéologiques de leurs auteurs.',* 'Rapport fait au nom de la commission d'enquête sur la lutte contre les groupuscules d'extrême droite en France', Assemblée Nationale, n°2006, 6 juin 2019.

114 Il est important que les services de police, les Parquets, les autorités locales et les secouristes, entre autres, captent les premiers signaux. Une meilleure compréhension de certains symboles, logos et autres éléments spécifiques de la culture de l'extrémisme de droite par les autorités locales, la police, les services sociaux, etc. peut, selon l'OCAM, aider à identifier la problématique. Même les participants aux LTF et aux CSIL (Plan R) qui se concentraient jusqu'à présent sur l'extrémisme islamiste, n'ont pas toujours une connaissance suffisante de l'extrémisme de droite. Une sensibilisation complémentaire est donc nécessaire.

en place de la nouvelle structure au SGRS début 2020, le personnel de cette équipe, qui traite l'extrémisme idéologique a été renforcé. Il s'agissait principalement de stagiaires analystes qui avaient besoin d'une certaine période de rodage.

I.7.4.2. Planification et orientation

Dans le Plan d'action 2019-20 de la VSSE, les objectifs stratégiques du service sont traduits en objectifs opérationnels. L'accent est mis sur la détection d'individus ou de groupes qui soutiennent et/ou diffusent un comportement extrémiste, et sur la minimalisation de l'impact d'un tel comportement. À cet égard, une attention particulière est accordée à la propagande qui fait l'apologie d'actions violentes et du passage à l'acte. Une attention particulière a également été portée aux individus qui expriment des idées extrémistes, tout en manifestant une fascination pour les armes, et/ou qui ont participé à des entraînements paramilitaires.

Le Plan directeur du renseignement de sécurité détermine les éléments de la politique en matière de renseignement et de sécurité du SGRS au profit de la Défense et du pays. Ce plan est établi pour une période de cinq ans et a pour objectif de définir les objectifs primaires et secondaires pour les activités de contre-espionnage du SGRS. La collecte et l'analyse des menaces et des risques d'ingérence et d'espionnage émanant d'organisations extrémistes, radicales et subversives contre les intérêts de la Défense font partie des priorités décrites dans ce plan directeur. L'*Intelligence Collection Plan* (ICP) est la mise en œuvre concrète des priorités en matière de renseignement qui sont définies dans le plan directeur. Il s'agit en substance d'indicateurs qui sont utiles pour évaluer des comportements et des formes d'expression susceptibles d'être liés à l'extrémisme de droite. Cet ICP, qui sert de fil conducteur pour les services de collecte, doit permettre au SGRS de récolter des informations sur qui adhère résolument aux thèses défendues par l'extrême droite ou sur quels groupements sont actifs au sein de la Défense. Il doit également permettre de déterminer si un recrutement actif est organisé au sein de la Défense, si une menace émane de l'extrême droite contre la Défense ou ses collaborateurs, ou encore si des incidents inspirés par l'extrême droite se sont produits.

I.7.5. LA COLLECTE ET LE TRAITEMENT DES DONNÉES

I.7.5.1. HUMINT

L'exploitation de sources humaines (HUMINT), occupe une place très importante dans la collecte d'informations relatives à l'extrême droite. En 2019 et 2020, un effort notable a été fait en matière de recrutement de sources humaines supplémentaires. Au cours de la période 2016-2018, la VSSE s'était essentiellement

concentrée sur la lutte contre le terrorisme (islamiste). La VSSE estime que la position d'information du service au sein du milieu de l'extrême droite peut être qualifiée de bonne, et qu'il est donc en mesure de réaliser une analyse correcte de la menace. En 2019 et 2020, les services de collecte qui assurent le suivi de l'extrémisme idéologique ont été renforcés, ce qui a donné lieu à une augmentation considérable du nombre de rapports d'information.

Au cours de l'enquête, il a pu être constaté que le nombre de sources humaines pouvant fournir des informations au SGRS sur le milieu de l'extrême droite est très restreint. Par ailleurs, le nombre relativement limité de rapports de collecte indiquait une lacune : la position d'information 'indépendante' du service sur l'extrême droite était limitée, indépendamment des rapports militaires traditionnellement établis. Le service pouvait difficilement détecter lui-même les cas d'infiltration de l'extrême droite au sein des Forces armées.

I.7.5.2. SOCMINT

En ce qui concerne la menace concrète qui émane de l'extrémisme de droite, le rôle des individus et des '*lone actors*', ne cesse de gagner en intérêt. La détection de tels individus est cependant compliquée, d'une part, en raison de leur isolement et, d'autre part en raison de leur absence des activités menées par des groupements. Ils trouvent souvent leur inspiration sur Internet, auquel ils limitent leur action. La VSSE considère comme très importante l'utilisation de moyens SOCMINT supplémentaires pour suivre les activités en ligne des extrémistes (de droite).

Bien que le SOCMINT gagne en importance dans la collecte d'informations, les rapports d'information sur la base du HUMINT sont encore les principales sources d'informations. En 2019, le service d'analyse compétent pour l'extrême droite a reçu peu de rapports de la Cellule SOCMINT du SGRS. Cette cellule établit toujours ses rapports après avoir été questionné par les services d'analyse via un *Request for Collect* (RFC) ; elle n'agit que de manière proactive. La situation en matière de SOCMINT s'est déjà sensiblement améliorée à l'automne 2020. En septembre 2020, la Cellule SOCMINT a ainsi établi dix rapports concernant l'extrême droite. Toutefois, elle ne dispose encore actuellement que de 50 % de la capacité prévue et elle ne peut pas compter sur un logiciel performant.

I.7.5.3. Méthodes de recueil de données (MRD)

En 2017, 2018 et 2019, respectivement 82, 52 et 62 méthodes de recueil de données ont été mises en œuvre dans le cadre du suivi de l'extrême droite. Selon la VSSE, la contribution du HUMINT à la collecte d'informations sur l'extrémisme idéologique est plus importante que pour certaines autres menaces suivies par le service, ce qui fait que le nombre de MRD était relativement plus limité que dans le contexte de certaines autres menaces.

Pour la période 2015-2019, le SGRS n'a mis en œuvre qu'une seule méthode de recueil de données dans le cadre du suivi de l'extrême droite (sur un total de 216 méthodes). En 2020, une évolution positive a également été constatée par rapport à l'année précédente en ce qui concerne l'utilisation de MRD. Ainsi, cinq MRD ont été mises en œuvre jusqu'au mois de septembre en rapport avec la problématique de l'extrême droite.

I.7.5.4. Traitement des informations

La VSSE reprend les données relatives à l'extrême droite, comme d'ailleurs les données relatives à toutes les autres matières, dans une banque de donnée centrale.[115] II est apparu, au cours de l'enquête, qu'il était impossible de demander de manière automatique des données chiffrées sur les matières suivies. Le service affirmait que ces données devaient être *'exfiltrées manuellement de la banque de données'*.

Au SGRS, il a pu être constaté, une fois encore, que le laps de temps entre la rédaction d'un rapport de collecte et l'exploitation de celui-ci par le service d'analyse était en moyenne très long. Ceci s'expliquait tant par le fait que les services de collecte étaient en sous-effectifs que par le flux d'informations défaillant au sein du SGRS. Compte tenu d'un nombre insuffisant de documentalistes, la saisie dans les temps des informations dans les banques de données constituait un problème. Par conséquent, des analystes étaient, eux aussi, mis à contribution pour la saisie et la mise à disposition des informations dans les banques de données, et ce au détriment de leurs propres missions de base.

I.7.6. L'ANALYSE, LA DIFFUSION ET LA COOPÉRATION

I.7.6.1. Analyse par les services de renseignement

En 2019, la VSSE a constaté que le nombre de messages entrants et sortants relatifs à l'extrême droite avait sensiblement augmenté par rapport aux deux années précédentes. Cette hausse concernait la communication avec les partenaires belges et les partenaires étrangers. Ces dernières années, la VSSE s'est en grande partie limitée à des analyses ponctuelles sur certains groupements et courants dans les milieux d'extrême droite, mais n'a pas rédigé d'analyses générales de phénomène. Des briefings généraux ont néanmoins été donnés à certaines autorités. Dans des enquêtes antérieures, le Comité permanent R avait déjà établi que produire ce que l'on appelle des renseignements prédictifs, définir des scénarios et formuler des

[115] Un projet est actuellement en cours à la VSSE pour remplacer cette banque de données par une nouvelle banque de données qui doit offrir davantage de possibilités.

hypothèses faisaient partie de l'essence même d'un service de renseignement. La VSSE avait affirmé ne pas disposer du personnel nécessaire pour pouvoir produire des renseignements prédictifs.

La VSSE utilise un instrument d'analyse doté d'une cinquantaine d'indicateurs lui permettant d'évaluer le degré de radicalisation d'un individu, ou le degré de risque que cet individu verse dans la violence extrémiste. Cet instrument doit ainsi permettre de collecter des informations plus ciblées et de mieux détecter les plus grandes menaces. Au moment de l'enquête, l'instrument ne s'appliquait qu'aux individus faisant l'objet de dossiers d'enquête liés au terrorisme islamiste et à l'extrémisme, et pas à l'extrémisme idéologique. Les effectifs n'étaient pas suffisants pour permettre un déploiement de l'instrument à plus large échelle.

Le SGRS a fourni une série de chiffres pour 2019 sur la charge de travail de la plateforme d'analyse 'menaces idéologiques non religieuses', et plus précisément les analystes qui traitent l'extrême droite. Ce qui le plus frappant dans ces chiffres, c'est le nombre peu élevé de *Requests for Collection* (RFC), qui orientent la collecte d'informations. Selon les collaborateurs de la plateforme, l'effectif actuel est encore insuffisant pour assurer un suivi suffisant de la matière. Les analystes ont trop de tâches complémentaires à remplir (donner des briefings, assister à des réunions, etc.), ce qui fait qu'il leur reste très peu de temps à consacrer à leur '*core business*', c'est-à-dire l'analyse de la problématique qui leur a été confiée. Par manque de temps, les analystes doivent nécessairement adopter une attitude réactive concernant les dossiers *ad hoc* de militaires extrémistes de droite qu'ils reçoivent de partenaires internes ou externes. Comme le Comité a pu constater, on n'en est pas à la réalisation d'analyses propres sur l'évolution éventuelle du phénomène, spécifiquement au sein de la Défense.

Certes, il y a lieu de mentionner que l'OCAM est le service pilote du Groupe de travail Extrême droite dans le cadre du Plan R, qui rédige des analyses générales. Compte tenu de la mission de l'OCAM, ce sont en principe surtout des 'analyses de la menace', mais elles peuvent aussi entrer dans la catégorie des analyses générales de phénomène.[116] En ce sens, l'éventuelle lacune en matière d'analyses de phénomène à la VSSE peut aussi être (en partie) comblée.

I.7.6.2. Diffusion/coopération

La VSSE partage les renseignements sur l'extrême droite avec divers partenaires. Au niveau national, une coopération existe au sein du Groupe de travail Extrême droite (Plan Radicalisme). Depuis 2018, des efforts supplémentaires ont néanmoins été consentis en matière de sensibilisation à la problématique, et des briefings ont été donnés à des journalistes, à des membres du milieu académique, etc. Enfin, il y a la sensibilisation ('*outreach*') des différents acteurs de la société. Concernant l'extrême

[116] En exécution de l'article 8, 1° L.OCAM : *'une évaluation commune qui doit permettre d'apprécier si des menaces, visées à l'article 3 et, le cas échéant, quelles mesures s'avèrent nécessaires (…)'.*

droite, le service affirme avoir jusqu'ici lancé moins d'initiatives en matière de sensibilisation de la société en rapport avec l'extrémisme de droite qu'en matière d'islamisme, par exemple.[117] En ce qui concerne la coopération internationale, il y a, outre la coopération bilatérale principalement avec les partenaires européens, la coopération au sein de la plateforme multilatérale du Club de Berne.

Ces dernières années, la plateforme d'analyse du SGRS a rédigé quelques notes stratégiques sur l'extrême droite à l'attention du ministre de la Défense. L'enquête montre que le service s'est toutefois plutôt concentré sur les renseignements ponctuels qui sont de nature opérationnelle. Des briefings sont régulièrement donnés sur des matières pour lesquelles ils sont compétents, entre autres à l'ERM pour les chefs de corps des unités et à l'École de Renseignement et Sécurité (ERS) à Heverlee, pour le public cible des officiers S2 des différentes unités opérationnelles des Forces armées. Au niveau de la coopération internationale, le SGRS n'a conclu que des accords de coopération bilatéraux sur l'extrême droite. Il n'y a pas de plateformes multilatérales pour ces matières. En 2019, une concertation sur l'extrême droite a eu lieu avec quatre services partenaires européens.

I.7.7. LE FEEDBACK

La VSSE reçoit rarement, voire jamais, de feedback à propos des renseignements qu'elle envoie aux destinataires, à moins d'une éventuelle demande de renseignements complémentaires – de partenaires étrangers – dont on peut déduire que les renseignements ont suscité un intérêt. Malgré le peu d'informations disponibles sur le feedback spécifique des partenaires externes concernant le suivi de l'extrême droite par le service, le Comité permanent R se réfère à l'évaluation générale des besoins réalisée par le service entre mars et juin 2019. Ce questionnaire a montré que le travail de la VSSE est considéré par les partenaires externes du service comme globalement positif : la grande majorité des répondants estiment que les collaborateurs du service sont professionnels et transparents (dans la mesure du possible) et que le service démontre une grande expertise. La plupart du temps, l'impression qui ressort des contacts directs avec le service est plus positive que l'image qui en est donnée dans les médias. Le contenu des produits de la VSSE est généralement apprécié, et les renseignements fournis sont qualifiés d'utiles. Bien que de nombreux clients indiquent qu'il leur est difficile de déterminer si la VSSE

[117] Il n'en va pas de même pour le salafisme, par exemple, qui est un thème sur lequel la VSSE a publié une brochure. Celle-ci a été diffusée largement dans la société civile et dans toutes sortes d'organisations qui entrent en contact avec le phénomène. La VSSE indique même que, par exemple, le service de renseignement allemand BfV communique régulièrement sur la menace de l'extrême droite à différents groupes dans la société. Le service néerlandais AIVD a lui aussi publié en octobre 2018 une brochure intitulée *'Rechts-extremisme in Nederland, een fenomeen in beweging'*.

détecte les menaces à temps, la plupart d'entre eux précisent qu'ils ont confiance en la capacité du service de le faire.

Avant l'introduction de la nouvelle structure du SGRS en janvier 2020, seul un feedback des destinataires était demandé pour les produits de l'ancienne Direction I.

Depuis l'introduction de la nouvelle structure organisationnelle, des efforts supplémentaires ont été consentis à ce niveau. Pour tout produit sortant, un feedback des partenaires est demandé. De plus, un service de '*quality control*' a été créé. Outre le contrôle de la qualité de tous les produits de renseignement, la mission du service consiste à voir, avec les différents partenaires, comment mieux adapter les produits à leurs besoins.

I.7.8. CONCLUSIONS

Au début de l'enquête, le Comité a identifié un certain nombre de risques et les a associés au cycle du renseignement.

Le Comité permanent R partage l'avis de l'OCAM. D'une part, la terminologie utilisée pour la menace n'est pas homogène et, d'autre part, divers concepts sont utilisés indistinctement, sans souvent se référer au même contenu. En effet, même si l'on peut affirmer que le législateur a bien décrit la notion d"extrémisme', les termes 'extrême droite' ou 'extrémisme de droite' (et donc aussi 'extrémisme de gauche') ne sont pas définis. Le Conseil national de sécurité ou les ministres de tutelle ne donnent pas non plus d'orientation en la matière.

La seconde étape – si nécessaire, en parallèle – consiste à délimiter quantitativement la menace et à recueillir les informations sur les politiques menées et la gestion des informations. De telles données permettent d'évaluer l'évolution de la menace, mais permettent aussi aux services de renseignement de déterminer ce à quoi ils affectent quels moyens. Au moment où l'enquête a été menée, ce genre d'informations n'existaient pas en Belgique, ni au sein des deux services.

En ce qui concerne la VSSE, le Comité permanent R a pu constater qu'après un recul pendant la crise terroriste de 2015-2016, le service a réinvesti dans le suivi de l'extrémisme idéologique, duquel l'extrême droite fait partie. Du personnel a été affecté et des objectifs tactiques et opérationnels ont été définis. Le nombre de sources (HUMINT) qui fournissent des informations sur l'extrême droite a augmenté en 2019-2020 ; il est question d'un mouvement de rattrapage, cette matière ayant fait l'objet de moins d'attention au cours de la période 2015-2016 (attentats terroristes). En l'absence d'une description claire de la menace et de son ampleur, il est difficile de déterminer si les moyens sont proportionnels à l'objectif. Le Comité permanent R constate que la VSSE effectue des analyses, mais que celles-ci se concentrent principalement sur la détection d'éventuelles menaces de violence par des milieux d'extrême droite. Il est donc rarement question d'analyses

générales de phénomène, qui donnent lieu à des hypothèses, des scénarios et à des 'renseignements prédictifs'. Le Comité estime néanmoins que ceci fait partie de l'essence même d'un service de renseignement.

En ce qui concerne le SGRS, après une réorganisation intervenue début 2020, une nouvelle plateforme mixte a été créée afin de suivre l'extrémisme (de droite) au sein des Forces armées. Du personnel a été mobilisé et des objectifs ont été fixés. Des éléments indiquent cependant que le soutien est trop limité, ce qui se traduit par un laps de temps relativement long pour certains rapports ainsi qu'un problème en matière de saisie des données dans la banque de données. De plus, le Comité a constaté que la position d'information était limitée. En ce qui concerne le SGRS, les analystes se limitent, par manque de temps, à adopter une attitude réactive dans les dossiers *ad hoc* qu'ils reçoivent de partenaires internes ou externes à propos de militaires extrémistes de droite. Aucune analyse de phénomène n'est réalisée sur l'extrême droite à la Défense, alors que cela semble nécessaire.

Le Comité permanent R estime qu'une coopération étroite s'impose entre la VSSE et le SGRS concernant la menace de l'extrémisme de droite, qu'une concertation régulière doit être organisée et que des renseignements doivent être échangés sur la problématique.

Enfin, le Comité a constaté un manque de feedback à la VSSE et au SGRS de la part des destinataires des renseignements des deux services de renseignement. Ceci était également vrai au niveau politique. Il était dès lors difficile pour les services d'affiner et d'orienter les objectifs de renseignement.

I.8. LE CORONAVIRUS ET LA QUESTION DE LA COMPÉTENCE DES SERVICES DE RENSEIGNEMENT BELGES

I.8.1. PRÉAMBULE

L'impact considérable du coronavirus et son contrôle sur la vie sociale, socio-économique et personnelle ont plongé le monde et continuent de le plonger dans l'inconnu. La nature de la crise a eu pour conséquence que le coronavirus a dominé l'agenda national et international pendant un certain temps.

À chaque crise, il est légitime de se demander si les événements auraient pu être évités. Les questions sur la réponse à la crise, en particulier sur la prudence dans sa gestion, font également partie intégrante du traitement des événements.

Les médias nationaux et internationaux se sont intéressés au rôle (éventuel) des services de renseignement dans la prévention et la lutte contre les pandémies, et à certains aspects et certaines conséquences de la crise du coronavirus en particulier. Ainsi, il a été clairement indiqué que dans certains pays, la communauté du renseignement mettait en garde contre la menace d'une pandémie depuis des années

déjà. Ces avertissements sont pris en compte dans les perspectives stratégiques que les services de renseignement présentent à leurs gouvernements et qui répondent à la question de savoir quelles tendances peuvent, à moyen et à long terme, menacer la sécurité nationale. Aux États-Unis, par exemple, des avertissements ont été émis dès 2004 sur le risque mondial posé par les pandémies.[118] En ce qui concerne la crise sanitaire, les rapports internationaux ont montré également que certains services de renseignement s'occupent d'aspects spécifiques de la gestion des maladies de la crise du coronavirus. En Israël, par exemple, les enquêteurs numériques du service de renseignement militaire, en soutien aux médecins et aux enquêteurs du ministère de la Santé, sont chargés de collecter toutes les informations disponibles sur le virus et de les mettre à la disposition du gouvernement, des autorités sanitaires et des responsables de la défense. Dans d'autres pays, les services de renseignement ne fournissent pas d'informations médicales concrètes, mais ils fournissent des connaissances et une expérience de la gestion des crises et des menaces à la sécurité nationale. Ainsi, au Royaume-Uni, un officier supérieur de lutte contre le terrorisme a été temporairement chargé du nouveau 'Joint Biosecurity Centre' dont la mission est de déterminer le niveau de menace posé par le coronavirus et de coordonner son approche. Enfin, divers articles de presse nationaux et internationaux font état des préoccupations des services de renseignement du monde entier face aux menaces pour la sécurité découlant de la menace sanitaire que représente le coronavirus (terrorisme, extrémisme, propagande et désinformation, etc.). Par exemple, le coordinateur de l'UE pour la lutte contre le terrorisme au Conseil européen a mis en garde, entre autres, contre une crise sécuritaire due à la crise du coronavirus et ses implications pour les activités des autorités de sécurité.[119]

I.8.2. LE CORONAVIRUS COMME MENACE

Le Sars-CoV2 est un virus appartenant à la famille des coronavirus. Chez l'homme, il provoque une maladie appelée 'Covid-19'. Le haut degré de contagiosité de ce coronavirus, le manque d'anticorps chez l'homme, l'absence de vaccin et le comportement humain (mobilité élevée, contacts sociaux, urbanité de la moitié de la population mondiale) semblent être à l'origine de sa propagation rapide. L'Organisation mondiale de la santé a caractérisé cette épidémie comme une pandémie.

---

118 National Intelligence Council (NIC), Mapping the Global Future. Report of the National Intelligence Council's 2020 Project, December 2004. Dans deux rapports ultérieurs, NIC Global Trends 2025 (publ. 2008) et NIC Global Trends 2030 (publ. 2012), le risque posé par une pandémie faisait l'objet d'une attention croissante.

119 https://www.zeit.de/gesellschaft/zeitgeschehen/2020-05/terrorismus-coronavirus-extremismus-sicherheit-krise-eu

Le coronavirus représente clairement une menace sanitaire, tant au niveau national que mondial. Toutefois, la nuisibilité ne se mesure pas uniquement en matière de santé ; elle constitue également une menace économique, sociale et psychologique.

I.8.3. LA QUESTION DES ACTIVITÉS DU SERVICE DE RENSEIGNEMENT CIVIL DANS LE CADRE DU CORONAVIRUS

I.8.3.1. La question de la compétence

Conformément aux articles 7 et 8 L.R&S, la compétence de la VSSE dans la mission de renseignement est déterminée par les intérêts à protéger combinés aux menaces à maîtriser. En d'autres termes, pour savoir si le service de renseignement civil est compétent dans un cas concret, il convient d'examiner si un point d'ancrage peut être trouvé avec au moins un intérêt[120] et au moins une menace.[121] Cela signifie que le service peut enquêter sur des événements, groupes ou personnes susceptibles de mettre en danger les intérêts fondamentaux susmentionnés uniquement si cette enquête vise à détecter et à suivre les menaces énumérées dans la loi.[122] Ce 'principe de finalité' est énoncé à l'article 13 L.R&S et à l'article 75, 2 ° LPD.

Le choix du législateur d'établir une liste bien déterminée de menaces en matière de sécurité a pour conséquence que la VSSE ne peut être tenue pour responsable de ne pas avoir informé d'autres autorités publiques, de sa propre initiative ou pas, de risques qui ne sont pas repris dans liste légale. Le principe de finalité dans le cadre de la communication de renseignements, énoncé à l'article 19, alinéa 1er L.R&S, ne laisse planer aucun doute à cet égard. La VSSE ne peut communiquer

---

120 Les 'intérêts' à protéger sont : (a) la sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel, (b) la sûreté extérieure de l'État et les relations internationales et (c) la sauvegarde des éléments essentiels du potentiel économique et scientifique du pays. Ce sont les seuls intérêts que la VSSE peut protéger. Il importe néanmoins de souligner que le législateur a donné au Gouvernement le pouvoir d'étendre cette liste par arrêté royal. Le Gouvernement n'en a pas fait usage jusqu'à présent, ce qui n'a rien d'étonnant compte tenu de la description légale, déjà large, des intérêts précités.

121 Les 'menaces' à maîtriser sont : l'espionnage, l'ingérence, l'extrémisme, le terrorisme, la prolifération, les organisations sectaires nuisibles et, enfin, les organisations criminelles. Ce sont les seuls risques que la VSSE peut détecter et suivre.

122 L'Exposé des motifs de la Loi du 30 mars 2017 précise que '*la finalité de la mission de renseignement consiste en l'identification et le contrôle de phénomènes, groupements et personnes qui présentent ou pourraient présenter une menace de sécurité spécifique. En d'autres mots, il s'agit tant de la détection, du suivi et de la maîtrise de menaces (ou risques) potentielles que du suivi et de la maîtrise de menaces (ou dangers) déjà détectées.*' (*Doc. parl.* Chambre 2015-2016, n°54-2043/001, 59). Pour réaliser ce que l'on appelle la 'finalité du renseignement', la VSSE doit opérer dans les limites légales de la mission de renseignement (art. 7, 1 ° L.R&S), et le service ne dispose que des compétences (d'enquête) que le législateur a définies dans la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

des renseignements à des tiers qu'en fonction de la finalité de ses missions (lisez : la détection, le suivi et la maîtrise des menaces en matière de sécurité énumérées dans la loi).

Enfin, contrairement aux intérêts fondamentaux, la loi relative aux services de renseignement ne prévoit pas d'étendre la liste des menaces à suivre par arrêté royal. Si les responsables politiques jugent la mission assignée à la VSSE insuffisante, la loi précitée devra être adaptée.

I.8.3.2. Détection et suivi dans le cadre du coronavirus

À la question posée par le Comité permanent R à la VSSE concernant les compétences dont ce service disposerait dans le cadre du coronavirus, l'Administrateur général de la VSSE a répondu :

> « *dat de enige juridische grondslag voor de werking van de VSSE i.h.k.v. de "Covid-19-pandemie" zich bevindt in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (WIV). Daarin staat immers vermeld dat het onze primaire opdracht is om inlichtingen in te winnen, te analyseren en te verwerken die betrekking hebben op elke activiteit die de inwendige veiligheid van de staat en het voortbestaan van de democratische orde, de uitwendige veiligheid van de staat en de internationale betrekkingen, het wetenschappelijk en economisch potentieel of elk ander fundamenteel belang van het land bedreigt of zou kunnen bedreigen. Wij dienen deze drie domeinen te beschermen tegen diverse bedreigingen (spionage, inmenging, terrorisme, extremisme, proliferatie, schadelijke sektarische organisaties en criminele organisaties). Dit is dan ook wat wij onverkort doen d.m.v. de nota's die wij overmaken aan de bevoegde politieke en administratieve overheden (…)* ».[123]

La VSSE a pour mission de protéger la « *sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel* ». Cet intérêt est, entre autres, décrit comme étant « *la sécurité et la sauvegarde physique et morale des personnes* » (art. 8, 2°, b) L.R&S). Sévissant à l'échelle nationale, le coronavirus met clairement en danger la sauvegarde physique des Belges et des étrangers résidant en Belgique.

---

[123] 'que la seule base juridique pour le fonctionnement de la VSSE dans le cadre de la « pandémie Covid-19 » figure dans la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S). Il est en effet mentionné que notre mission première est de collecter, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'Etat et les relations internationales, le potentiel scientifique ou économique ou tout autre intérêt fondamental du pays. Nous devons protéger ces trois domaines contre diverses menaces (espionnage, ingérence, terrorisme, extrémisme, prolifération, organisations sectaires nuisibles et organisations criminelles). Nous nous y employons sans réserve en transmettant des notes aux autorités politiques et administratives compétentes'. (traduction libre)

Toutefois, la détection et la lutte contre la menace sanitaire du coronavirus ne relèvent pas de la compétence de la VSSE. En effet, le service de renseignement civil est seulement responsable de la détection des sept menaces à la sécurité susmentionnées et de leur examen. Le '*Medical intelligence*' (MEDINT) ou renseignement médical, c'est-à-dire la collecte, l'analyse et la diffusion d'informations médicales importantes, notamment pour la prise de décision politique (définition plus approfondie, infra), ne relève pas des compétences de la VSSE. Les menaces en matière de sécurité pour lesquelles la VSSE est compétente sont, au demeurant, des menaces dont la source est l'homme. Les phénomènes sanitaires, et plus généralement les phénomènes naturels, qui constituent une menace pour les intérêts fondamentaux susmentionnés du pays, ne relèvent pas en soi de la sphère d'intérêt légale de la VSSE.

En revanche, la collecte et l'analyse d'informations médicales peuvent relever de la sphère d'intérêt légale de la VSSE, mais uniquement si une enquête est menée à ce sujet dans le cadre de la détection des menaces en matière de sécurité énumérées dans la loi. La question centrale est ici de savoir dans quelle mesure le phénomène sanitaire du coronavirus conduit à l'extrémisme, aux interférences, etc. Une brochure[124] intitulée 'Le danger caché derrière le COVID-19' et publiée le 21 avril 2020 conjointement par la VSSE et le SGRS, se situe dans ce contexte. Cette publication se concentre sur l'extrémisme de droite, l'extrémisme de gauche, l'ingérence (potentielle) par le biais de reportages pro-russes et par le biais de campagnes de désinformation menées par des puissances étrangères, ainsi que sur les matières PES.

Enfin, il convient de mentionner qu'il existe un consensus au sein de la communauté médicale sur l'absence d'intention dommageable dans la propagation du coronavirus. Cependant, si le VSSE avait obtenu des indices sérieux de sources ouvertes ou fermées que le coronavirus était ou avait été utilisé comme arme biologique, sa propagation aurait dû être considérée comme une prolifération de matériel CBRN.[125] Si de telles informations étaient avérées, la VSSE serait saisie d'une enquête plus approfondie.

[124] Le 21 avril 2020, les deux services de renseignement ont publié la brochure intitulée 'Le danger caché derrière le Covid-19' (https://vsse.be/fr/le-danger-cache-derriere-le-covid-19).

[125] CRBN est l'acronyme anglais de 'Chemical, Biological, Radiological and Nuclear' et fait référence aux biens et instruments chimiques, biologiques, radiologiques et nucléaires.

I.8.4. LA QUESTION DES ACTIVITÉS DU SERVICE DE RENSEIGNEMENT MILITAIRE DANS LE CADRE DU CORONAVIRUS

I.8.4.1. La question de la compétence

La mission de renseignement du SGRS est décrite à l'article 11, § 1er, 1° L.R&S. Sur la base de cette disposition, le SGRS a pour attributions :

(1) le recueil, l'analyse et le traitement du renseignement relatif à toute activité qui menace ou pourrait menacer les intérêts suivants :
   a. l'intégrité du territoire national ou la survie de tout ou partie de la population ;
   b. les plans de défense militaires ;
   c. le PES en rapport avec la défense ;
   d. l'accomplissement des missions des Forces armées ;
   e. la sécurité des ressortissants belges à l'étranger ;

et il convient d'en informer sans délai les ministres compétents.

Comme pour la VSSE, le domaine de compétences du SGRS dans ce segment de la mission de renseignement est déterminé par les intérêts à protéger combinés aux menaces à maîtriser. En d'autres termes, pour déterminer si le service de renseignement militaire est compétent dans un cas concret, il convient ici aussi d'examiner s'il est possible de trouver un point d'ancrage avec au moins un intérêt et au moins une menace.

Il existe toutefois des différences avec la description des compétences de la VSSE. La principale différence réside dans l'existence requise d'un aspect militaire, soit dans l'intérêt à protéger (par exemple, les plans de défense militaire, l'accomplissement des missions militaires), soit dans la manière dont les intérêts à protéger peuvent être touchés, c'est-à-dire par des moyens de nature militaire.

Il est important à cet égard que, tout comme pour la VSSE, l'homme soit la source de la menace qui relève de la compétence du SGRS.[126] Les sources de menaces autres que les activités humaines, par exemple les phénomènes naturels, n'entrent dans le champ des compétences que dans la mesure où leur suivi engendre ou peut engendrer une menace pour les intérêts fondamentaux susmentionnés.

(2) le recueil, l'analyse et le traitement du renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à

[126] L'article 11, § 2, 1° à 4° L.R&S reprend chaque fois la phrase « *toute manifestation de l'intention de*'. Une telle expression de volonté n'est possible que chez l'homme.

leurs éventuelles opérations à venir. Il convient d'en informer sans délai les ministres compétents.

Ce segment de la mission de renseignement est appelé 'appui en renseignement aux opérations militaires'. L'objectif est de protéger les troupes et de soutenir les opérations proprement dites, en collectant et en traitant des données sur des puissances étrangères, des (éléments des) forces armées régulières hostiles ou potentiellement hostiles, des forces combattantes irrégulières et sur des zones et circonstances dans lesquelles une intervention est requise ou pourrait l'être à l'avenir.

Il s'agit de l'identification et du suivi des facteurs pouvant constituer un risque pour la sécurité des opérations militaires en cours (ou éventuelles) sur le sol belge ou à l'étranger et, le cas échéant, la transmission des informations pertinentes aux autorités et services militaires compétents. Les facteurs qui affectent (ou peuvent affecter) la sécurité nationale et internationale peuvent être à la fois des activités humaines et des phénomènes non humains. Dans ce contexte, cependant, détecter et combattre activement tous les risques imaginables ne fait pas partie des missions attribuées au SGRS. Comme indiqué, la finalité ultime de ce travail de renseignement militaire est de protéger les troupes et d'appuyer l'opération proprement dite. Ce n'est qu'à partir du moment où une activité, un phénomène ou un 'risque identifié' est susceptible de mettre en danger une opération militaire particulière ou les troupes impliquées que la collecte et le traitement des informations pertinentes relèvent de la compétence du SGRS.

L'appui en renseignement aux opérations militaires ne relève pas de la responsabilité exclusive du SGRS. Au sein des Forces armées, les instances S2, c'est-à-dire les personnes et les services chargés de la fonction militaire 'renseignement et sécurité', jouent également un rôle important dans la collecte et le traitement des renseignements militaires pertinents. En outre, diverses instances publiques, au sein et en dehors des Forces armées, sont également chargées de collecter et d'étudier activement des informations et des risques spécifiques qui, le cas échéant, peuvent être importants pour les opérations militaires en cours ou les opérations qui pourraient être menées dans le futur.

I.8.4.2. Le contexte élargi : le renseignement médical ('medical intelligence')

La question s'est posée de savoir dans quelle mesure le '*medical intelligence*' (MEDINT ou MEDINTEL) relève du domaine de compétences du SGRS. Afin d'y apporter une réponse adéquate, il convenait de déterminer au préalable en quoi consiste exactement cette activité.

La notion de renseignement médical ('*medical intelligence*') est peu connue en Belgique, tant au sein de la communauté du renseignement qu'au sein de la Défense. Mais au niveau international, cette notion, entre autres, a été définie dans le 'Glossary of terms and definitions' du '*NATO Standardization Office' (NSO)* :

> « *'medical intelligence'* is *'(i)ntelligence derived from medical, bio-scientific, epidemiological, environmental and other information related to human or animal health. Note: This intelligence, being of a specific technical nature, requires medical expertise throughout its direction and processing within the intelligence cycle* ».[127]

Cela signifie que pour les États membres de l'OTAN, la fonction MEDINT est une fonction de défense.[128]

Dans certains pays, la fonction MEDINT est créée au sein d'un (ou du) service de renseignement et de sécurité militaire. C'est le cas, par exemple, aux États-Unis, où cette activité est exercée par le *National Center for Medical Intelligence* (NCMI), qui est une section de la *Defense Intelligence Agency* (DIA).[129]

La question se pose de savoir si le renseignement médical, en particulier si détecter et suivre la menace sanitaire du coronavirus et ensuite informer les autorités et services militaires compétents, relève de la compétence du SGRS. Il s'agit d'une réponse à une question juridique, à savoir si le SGRS est légalement autorisé à mener de telles activités de renseignement.

Une question connexe est la suivante : au sein des Forces armées belges, d'autres composantes peuvent-elles être (partiellement) chargées d'une fonction MEDINT ? À cet égard, on peut penser en premier lieu à la composante médicale.

La question de la compétence, c'est-à-dire si le renseignement médical peut effectivement être considéré comme une activité du SGRS, doit également être distinguée de la question politique de savoir si le domaine fonctionnel militaire 'renseignements et sécurité' doit être mis en place au sein de la composante médicale de la défense, ou s'il est préférable – comme à la DIA américaine – que le renseignement médical soit une section d'un service de renseignement et de sécurité militaire. Le Comité s'est limité à étudier l'étendue des compétences du SGRS.

---

127 AAP-06, ed. 2019, NATO Glossary of terms and definitions.

128 À noter également que l'OTAN organise un cursus spécifique en la matière, à savoir le 'M4-87 NATO Medical Intelligence Course (MEDINTEL)'. L'OTAN affirme à ce propos : *'(m)edical intelligence is a crucial element of medical support and has undergone considerable changes. NATO's concept of joint and multinational missions and NATO's ability to respond outside of traditional areas of operation (whenever and wherever) has added to a growing importance attached to (medical) force protection. This has led to increased demands for comprehensive, integrated, timely, and cohesive medical intelligence.'*.

129 Le US Department of Defense (DoD) décrit le renseignement médical ('*medical intelligence*') comme suit : « *that category of* intelligence *resulting from collection, evaluation, analysis, and interpretation of foreign* medical*, bio-scientific, and* environmental *information that is of interest to* strategic planning *and to military medical planning and operations for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both* military *and* civilian *sectors.*» Voir : U.S. Department of Defense, Feb. 15, 2013, Joint Publication 1-02, Department of Defense Dictionary of Military and Associates Terms.

I.8.4.3. Détection et suivi dans le cadre du coronavirus

À la question posée par le Comité permanent R au SGRS concernant les compétences dont ce service disposerait dans le cadre du coronavirus, le Chef du SGRS a répondu comme suit :

> *'(…) je peux vous dire que le SGRS n'est pas compétent pour « la détection et/ou le suivi de la pandémie proprement dite ».*
> *Si le SGRS est bien compétent pour faire du renseignement relatif à toute activité qui menace ou pourrait menacer les intérêts visés à l'article 11 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, il est néanmoins évident qu'il n'a pas de compétence en matière médicale et qu'il appartient à d'autres autorités publiques belges de détecter des pandémies et de suivre les conséquences directes des maladies sur la santé des citoyens.*
> *Dès lors, la compétence du SGRS se limite aux conséquences 'indirectes' de la pandémie et du contexte qui l'entoure sur le potentiel économique et scientifique dans le secteur de la Défense, sur la sécurité des systèmes informatiques de la Défense, sur les plans et missions de la Défense, sur la sécurité des ressortissants belges à l'étranger, … et est orientée essentiellement sur les menaces de type espionnage, ingérence, extrémisme, …'.*

Comme déjà indiqué, le Comité permanent R s'est concentré sur l'étendue des compétences de la mission de renseignement du SGRS, et non sur l'organisation de la gestion des activités de renseignement, ni sur les priorités politiques qui leur sont assignées.

À l'instar de la VSSE, le SGRS n'est pas habilité à détecter et à combattre activement les risques médicaux pouvant constituer une menace pour la santé publique. Le SGRS est un service de renseignement et de sécurité militaire ; il n'a aucune compétence en matière de prévention et de contrôle des maladies. Tout comme la VSSE, le SGRS dispose d'une compétence de gestion des conséquences du risque sanitaire, dans la mesure où ces conséquences relèvent du domaine de compétences légal. La publication conjointe avec la VSSE en est une illustration claire.[130]

Le Covid-19 constitue une menace pour la santé publique en Belgique. Il représente également une menace pour la santé publique à l'étranger, y compris dans les zones de conflits militaires (potentiels). Le renseignement médical trouve sa raison d'être essentiellement dans le recueil d'informations sur les pathologies auprès de la population dans une zone d'opération existante ou future. Il s'agit, entre autres, de la recherche d'éventuelles maladies et épidémies qui impactent ou peuvent impacter le personnel militaire présent et la relation du personnel militaire

[130] Voir également en ce sens la création récente par le SGRS d'une *Information Warfare Platform* (en collaboration avec la VSSE) qui entend lutter contre la désinformation, y compris sur le Covid-19.

avec la population locale, ainsi que des facteurs qui peuvent avoir une influence sur la mission à l'étranger. D'un point de vue juridique, le renseignement médical ne relève pas de la compétence du SGRS. La question de savoir dans quelle mesure le renseignement médical a été ou devrait être une thématique à suivre au sein des Forces armées ne relève pas de la compétence du Comité permanent R.

Enfin, dans le cadre de la discussion sur les compétences du SGRS, il y a également lieu de mentionner que la propagation du coronavirus n'est pas considérée comme un acte humain intentionnel. La même considération s'applique ici aussi : si le SGRS, par des sources ouvertes ou fermées, obtenait de sérieux indices que le coronavirus est ou était utilisé comme une arme biologique, il relèverait alors de son domaine de compétences.

I.8.5. CONCLUSIONS

Un ensemble complexe de mesures très variées a pour but de gérer la crise du coronavirus dans tous ses aspects. Les services de renseignement du monde entier sont eux aussi impliqués par leurs gouvernements dans la gestion de cette crise. Traditionnellement, cette catégorie d'instances publiques est active dans la détection et la lutte contre les menaces à la sécurité nationale. Toutefois, la pratique diffère d'un pays à l'autre. Les rapports internationaux sur le rôle des services de renseignement dans le contexte de la crise du coronavirus montrent clairement que les tâches assignées aux différents services de renseignement en la matière diffèrent parfois fortement.

Au niveau belge, les activités de la Sûreté de l'État et du Service Général du Renseignement et de la Sécurité constituent un maillon dans l'endiguement et la lutte contre certaines menaces à la sécurité résultant de la crise actuelle. Les services belges de renseignement et de sécurité sont guidés par la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Il est établi que ni la VSSE ni le SGRS ne disposent de compétences légales pour détecter et combattre activement les risques médicaux pouvant constituer une menace pour la santé publique. Ce sont des services de renseignement, et ils n'ont aucun rôle légal à jouer dans la prévention et le contrôle des maladies. Le renseignement médical ne fait pas partie des missions des deux services.

Les deux services de renseignement ont un rôle à jouer dans la gestion de certaines conséquences du risque sanitaire lorsque ces conséquences relèvent du domaine de compétences des services. La brochure intitulée 'Le danger caché du Covid-19' a clairement montré que les deux services ont rempli leur rôle juridique consciencieusement et de manière proactive. Par ailleurs, cela a aussi montré que, dans ce cadre, la loi est suffisamment claire et ne nécessite aucun ajustement.

I.9. CONCERTATION SOCIALE AU SEIN DE LA SÛRETÉ DE L'ÉTAT

La Sûreté de l'État est composée du personnel des services intérieurs et des services extérieurs. Historiquement, il existe deux statuts du personnel. L'Arrêté royal du 2 octobre 1937 portant le statut des agents de l'État règle le statut du personnel du service intérieur (en l'occurrence, appartenant à la Direction de l'Analyse, à la Direction d'Encadrement, au Staff de la Direction générale et à la Direction des Opérations). Les agents des services extérieurs (en l'occurrence, appartenant à la Direction des Opérations, à la Direction d'Encadrement et au Staff de la Direction générale) ont un statut spécifique, prévu par l'Arrêté royal du 13 décembre 2006 'portant le statut des agents des services extérieurs de la Sûreté de l'État'. Cet A.R. prévoit un statut pécuniaire 'particulier' et un système d'allocations, d'indemnités et de bonus.

Le Gouvernement, qui souhaitait adapter le statut du personnel des agents de la Sûreté de l'État, a présenté à cet effet un projet d'arrêté royal modifiant l'A.R. du 13 décembre 2006 pour la concertation sociale. La proposition (l'A.R. 'petite intégration') visait à faire converger le statut du personnel qui est d'application au sein de la VSSE et, en particulier, à intégrer partiellement le personnel des services intérieurs au statut administratif et pécuniaire applicable au personnel des services extérieurs. Il s'agissait d'une première mesure dans le cadre d'une réforme plus générale au sein de la VSSE et dans le prolongement de la création d'un 'statut unique', telle que recommandée par la Commission d'enquête parlementaire 'Attentats terroristes'.[131]

Les représentants syndicaux n'ont cependant pas soutenu cette proposition et en ont informé la Commission parlementaire de suivi ainsi que le Comité permanent R.

Conformément à sa loi organique, le Comité est resté attentif à ce dossier, dans la mesure où un conflit social affecte l'efficacité du fonctionnement de la Sûreté de l'État. Le Comité considérait ne pas être compétent en matière de conflits sociaux, estimant que tout différend devait être réglé au sein des comités de négociation et de consultation et, si nécessaire, devant le médiateur social.[132]

Une réunion a néanmoins eu lieu en août 2020 entre le Comité permanent R et deux représentants d'une organisation syndicale, tous deux membres des services extérieurs de la Sûreté de l'État. Le Comité leur a rappelé les limites de sa compétence au niveau social, l'esprit de la Loi de 2004, la nécessité de maintenir

---

131 Une réunion du Comité de négociation a eu lieu dans cette optique en août 2020. Les services extérieurs de la Sûreté de l'État, l'OCAM et les Cabinets de la Justice et de la Défense se sont rencontrés en vue d'élaborer un projet de statut unique.

132 C'est la Loi du 17 mars 2004 organisant les relations entre les autorités publiques et les organisations syndicales du personnel des services extérieurs de la Sûreté de l'État qui fixe les règles des négociations et de la concertation avec les services extérieurs. *M.B.* 2 avril 2004, avec une entrée en vigueur le 12 avril 2004.

le dialogue social avec les autorités et, enfin, l'importance du bon fonctionnement de la Sûreté de l'État et de la garantie du bien-être des employés. L'Administrateur général de la Sûreté de l'État a été informé de cette rencontre, et ce avec l'assentiment de l'organisation syndicale.

L'Arrêté royal du 24 septembre 2020 modifiant l'arrêté royal du 13 décembre 2006 portant le statut des agents des services extérieurs de la Sûreté de l'État est paru au Moniteur belge le 1er octobre 2020 et est entré en vigueur le 1er janvier 2021.

I.10. INCIDENTS DANS UNE ZONE D'OPÉRATION À L'ÉTRANGER

Une partie importante du travail du SGRS vise la production de renseignements sur la situation politico-militaire à l'étranger. En 2018, le Comité s'est penché sur le déploiement du SGRS dans une zone d'opération donnée.[133] [134] Le SGRS fournit un appui aux commandants militaires belges sur place et est responsable de la '*force protection*' des militaires belges. Le service mène également des missions d'appui pour l'ambassade belge et contribue à la sécurité des expatriés. Au cours de l'enquête, le Comité a détecté quelques vulnérabilités qui comportaient des risques éventuels pour la sécurité des opérations ou du personnel.

Depuis lors, le Comité a de nouveau reçu des informations relatives à une série d'incidents graves, qui représentaient un risque au niveau de la sécurité. Un rapport classifié a été adressé au Chef du SGRS, avec le CHOD et le ministre de la Défense en copie. Dans ce rapport, la SGRS était invité à prendre de toute urgence des mesures afin de protéger les hommes déployés.

Le Comité a regretté de devoir constater que les incidents de sécurité n'ont donné lieu qu'à une procédure de retrait d'une habilitation de sécurité et que le service n'a pas lancé la moindre procédure disciplinaire. De plus, le Comité a dû constater que lorsque le SGRS était confronté à un délit ou un crime commis par un de ses collaborateurs, l'article 29 CIC n'était pas appliqué et que les infractions n'étaient pas dénoncées aux autorités judiciaires. Enfin, la nécessité de la rédaction d'un rapport complet par le SGRS en cas d'incident de sécurité a une fois encore[135] été rappelée. Il convient d'examiner et d'analyser, dans ce rapport, toutes les dimensions, qu'elles soient techniques ou comportementales.

---

133 Pour des raisons de sécurité, le Comité a décidé de ne pas mentionner le lieu.

134 COMITÉ PERMANENT R, *Rapport d'activités 2018*, 18-21 ('I.2. Les activités du SGRS dans une zone d'opération à l'étranger').

135 COMITÉ PERMANENT R, *Rapport d'activités 2015*, 109 ('IX.2.8. Un rapport circonstancié en cas d'incident de sécurité').

I.11. ENQUÊTES DE CONTRÔLE POUR LESQUELLES DES DEVOIRS D'ENQUÊTE ONT ÉTÉ EFFECTUÉS EN 2020 ET ENQUÊTES QUI ONT DÉBUTÉ EN 2020

I.11.1. L'APPLICATION DE NOUVELLES MÉTHODES (PARTICULIÈRES) DE RENSEIGNEMENT

Dès 2010, les possibilités de recueil d'informations du SGRS et de la VSSE ont été considérablement élargies. Depuis lors, les services peuvent recourir à des méthodes ordinaires, spécifiques et exceptionnelles, qui devraient refléter le degré d'intrusion des mesures.[136] Les modifications de loi intervenues entre-temps ont modifié la portée de plusieurs méthodes (lisez : élargi). Ainsi, certaines méthodes 'particulières' sont devenues 'ordinaires' et de nouvelles méthodes ordinaires ont été ajoutées.

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

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

En 2020, l'accent a été mis sur l'élaboration d'une méthodologie dans le cadre du contrôle de l'identification de l'utilisateur de télécommunications (art. 16/2 L.R&S), ainsi que l'accès aux données PNR (art. 16/3). Vers la fin de l'année 2020 et le début de l'année 2021, le volet méthodologique relatif au contrôle préalable aux interceptions, intrusions dans un système informatique et la prise d'images animées (art. 44/3 L.R&S) a été finalisé. En l'absence d'arrêt d'exécution,[137] la dernière nouvelle méthode ordinaire d'observation, c'est-à-dire laisser les services de renseignement accéder aux images des caméras utilisées par les services police (art. 16/4 L.R&S), n'a pas encore pu entrer en vigueur.

---

136 À l'occasion des dix ans d'existence de la 'Loi BIM', le Comité a organisé un colloque à la Chambre (*infra*). Voir à ce propos : J. VANDERBORGHT, (ed.), *Les méthodes particulières de renseignement : de l'ombre à la lumière*, Antwerpen, Intersentia, 2020, 70 et suiv.

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

I.11.2. LES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION DANS LE PROCESSUS DE RENSEIGNEMENT À LA VSSE

En mai 2019, le Comité permanent R a informé le Président de la Chambre de l'ouverture d'une enquête de contrôle intitulée 'Enquête de contrôle sur les moyens informatiques utilisés par les services de renseignement belges pour la collecte, le traitement, l'analyse et la communication de l'information dans le cadre du cycle du renseignement'. La portée de l'enquête a été balisée dès le départ. L'enquête se concentre sur les moyens informatiques spécifiquement utilisés pour soutenir les éléments du cycle du renseignement. L'enquête vise à identifier les risques auxquels sont confrontés les services et à réduire ces risques par le biais de recommandations adaptées.

Un premier module (SGRS) a été finalisé mi-2020.[138] Les résultats de l'enquête concernant la VSSE sont attendus pour début 2021.

I.11.3 LE SUIVI PAR LA VSSE DES CONDAMNÉS POUR TERRORISME QUI ONT ÉTÉ LIBÉRÉS

Ces cinq dernières années (2015-2020), les tribunaux belges ont prononcé un total de 464 condamnations pour des infractions liées à des activités terroristes.[139] Certains condamnés l'ont été par contumace et n'ont donc pas pu être placés en détention. Une série d'autres ont obtenu une permission de sortie de prison, ont entre-temps purgé leur peine ou ont été libérés sous condition suite à une décision du tribunal d'application des peines.

Compte tenu du danger potentiel de récidive, le Comité a décidé, à la mi-2019, d'ouvrir une enquête de contrôle sur *'le suivi par les services de renseignement et de sécurité belges, d'une part des inculpés en Belgique pour infractions terroristes perpétrées en Belgique ou ailleurs et bénéficiant d'une modalité visée par la loi du 20 juillet 1990 et d'autre part, des condamnés en Belgique pour infractions terroristes qui sortent de prisons belges, soit dans le cadre d'une des modalités visées dans le cadre de la loi du 17 mai 2006, soit qui sont libérés définitivement (art. 71 de ladite loi)'*.

Le Comité a examiné la manière dont les deux services de renseignement (VSSE et SGRS) suivent cette thématique, quels moyens et quelles méthodes sont

---

138 Voir à ce propos 'I.6. Les technologies de l'information et de la communication dans le processus de renseignement au SGRS' (*supra*).

139 M. VANDERSMISSEN, *Knack*, 19 janvier 2021 ('Belgische rechtbanken veroordeelden de voorbije vijf jaar 464 terroristen'). Aux presque 500 individus condamnés, il y a lieu d'ajouter 200 djihadistes qui se trouvaient ou se trouvent encore en Syrie ou en Irak. On ignore le nombre exact de ces individus encore en vie.

employés, la manière dont se déroule la coopération avec les partenaires (entre autres l'OCAM, la Direction générale des Établissements pénitentiaires, la Police fédérale et locale, etc.) et au sein de quelles structures (Local Task Forces, Joint Intelligence and Decision Committees, etc.). Enfin, le benchmarking a été utilisé pour étudier l'approche française et anglaise. L'enquête sera finalisée au premier semestre 2021.

I.11.4. LE RISQUE D'INFILTRATION AU SEIN DES DEUX SERVICES DE RENSEIGNEMENT

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

Plusieurs réunions de travail ont été organisées avec le SGRS et la VSSE sur la thématique 'cartographie et évaluation du risque d'infiltration au sein des services de renseignement'. À cet égard, le processus de gestion du risque, telle que reprise dans la norme ISO 31000, constituait une base de départ.[140] L'enquête sera finalisée courant 2021.

I.11.5. MENACES ÉVENTUELLES POUR LE POTENTIEL ÉCONOMIQUE ET SCIENTIFIQUE : ENQUÊTE DE SUIVI

En 2016, une enquête de contrôle relative à la protection du potentiel économique et scientifique, dans la foulée desdites 'révélations de Snowden', a été finalisée.[141] Ces révélations ont notamment donné un aperçu de l'existence du programme PRISM, au travers duquel la NSA américaine récoltait des (méta)données de télécommunication. Elles ont également révélé les opérations de renseignement montées par les services américains, mais aussi britanniques, contre certaines institutions internationales et structures de coopération (ONU, UE et G20). Des pays dits 'amis' étaient eux aussi visés. L'enquête portait sur les implications

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

141 COMITÉ PERMANENT R, *Rapport d'activités 2016*, 52 et suiv. L'intitulé complet de l'enquête est le suivant : 'Enquête de contrôle sur l'attention que les services de renseignement belges portent (ou non) sur les menaces que peuvent représenter pour le potentiel scientifique et économique de la Belgique des programmes de surveillance électroniques sur les systèmes de communication et d'information mis en œuvre à grande échelle par des puissances et/ou services de renseignement étrangers'.

éventuelles des programmes étrangers sur la protection du potentiel économique et scientifique du pays. Il s'agissait de vérifier si les services de renseignement belges étaient attentifs à ce phénomène ; s'ils avaient détecté une menace réelle ou potentielle contre le potentiel économique et scientifique belge ; s'ils avaient informé les autorités compétentes et leur avaient suggéré des mesures de protection et, enfin, s'ils disposaient de moyens suffisants et adéquats pour suivre cette problématique. Le Comité a par ailleurs examiné les conséquences du programme PRISM et/ou de systèmes analogues sur le potentiel économique et scientifique du pays.

Fin novembre 2019, la Commission parlementaire de suivi a demandé au Comité permanent R de reprendre l'enquête de contrôle et de l'actualiser.

I.11.6. ESPIONNAGE VIA DU MATÉRIEL DE CRYPTAGE : L'OPÉRATION RUBICON

Mi-février 2020, des révélations ont été faites sur l'"'Operation Rubicon'[142] ou l'opération de renseignement par laquelle les services de renseignement américains et allemands ont, des décennies durant, écouté des communications cryptées émanant d'autorités dans des dizaines de pays, en utilisant la société suisse Crypto AG comme couverture.[143] Les Pays-Bas, la France, la Suède et le Danemark (les 'pays Maximator'), entre autres, étaient '*cognescenti*', c'est-à-dire initiés aux détails cryptologiques de certains appareils. La Belgique, notamment, "*waardevol voor de verheldering die zijn rapporten bood over diplomatieke gebeurtenissen*"[144] et surtout intéressante comme centre diplomatique de l'OTAN et de ce qui était à l'époque la Communauté économique européenne, aurait été visée.

Le lendemain de la publication (12 février 2020), le SGRS a réagi dans un communiqué adressé à l'agence Belga : *'De ADIV is op de hoogte van de Rubicon-affaire en onderzoekt momenteel de mogelijke omvang van de gemelde afluisterpraktijken. Daarin wordt niet expliciet aangegeven of België al dan niet geviseerd zou geweest zijn door de operatie, die eerst 'Thesaurus' en later 'Rubicon' werd genoemd. Meer in het algemeen is de ADIV zich ten volle bewust van de*

---

142 La revue *Intelligence and National Security* (Volume 35, August 2020, Issue 5) y a consacré un numéro thématique. Voir notamment : 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" et B. JACOBS, 'Maximator: Europan signals intelligence cooperation from a Dutch perspective'.

143 Les rapports d'évaluation des services de renseignement américains et allemands ont été publiés par la chaîne de télévision allemande ZDF et le Washington Post. La plateforme de recherche néerlandaise Argos a pu consulter les rapports, qui ont notamment été repris par De Tijd (L. BOVÉ, *De Tijd*, 13 février 2020, ('Geheime documenten onthullen spionage van België door CIA en Duitse BND')).

144 *« était précieuse pour les éclaircissements que ses rapports apportaient sur les événements diplomatiques »*. (traduction libre)

vooruitgang, maar ook van de gevaren en/of potentiële misbruiken in verband met het gebruik van crypto hardware ».[145] Le SGRS « *doet er alles aan om zich tegen hen te wapenen en maakt er vooral een erezaak van om enerzijds het wettelijk kader op dit gebied te respecteren en anderzijds een morele 'code' te hanteren ten opzichte van zijn partners/bondgenoten in een wereld waar, zonder naïef te zijn, vertrouwen vaak met voorzichtigheid gepaard gaat* ».[146]

Le Comité a ensuite décidé d'ouvrir une enquête de contrôle, tentant d'apporter une réponse à des questions telles que [147]: dans quelle mesure les services de renseignement belges étaient-ils au courant (ou dans quelle mesure devaient-ils l'être) de ces opérations compte tenu de leurs missions légales ? Des renseignements ont-ils été recueillis à ce propos ou cela n'a-t-il pas été jugé souhaitable ? Mais plus important encore : les services offrent-ils actuellement une protection suffisante en la matière ? Des analyses de risques ont-elles été effectuées ? En cas d'utilisation avérée de matériel du cryptage, quelles mesures de précaution ont alors été prises ? Comment cette problématique de cryptage est-elle gérée aujourd'hui ? Fin septembre 2020, il a été décidé de fusionner cette enquête avec l'enquête de suivi PRISM/PES (cf. I.11.5).

I.11.7. MOYENS DE RENSEIGNEMENT OFFENSIFS POUR LES SERVICES DE RENSEIGNEMENT ?

Compte tenu de la mission de renseignement décrite par le législateur, les informations pertinentes pour les services de renseignement se trouvent à la fois en Belgique et à l'étranger. Par conséquent, une enquête de contrôle a été ouverte en 2019 sur les besoins en moyens de renseignements offensifs (supplémentaires) des services de renseignement belges'. Cette enquête poursuit divers objectifs :

– Vérifier si la VSSE/le SGRS procèdent actuellement à un recueil opérationnel d'informations à l'étranger, et dans l'affirmative, sous quelle forme et par le biais de quelles activités de renseignement ;
– Examiner les activités menées à l'étranger sous l'angle du cadre réglementaire en vigueur ;

---

145 *'Le SGRS est au courant de l'affaire Rubicon et se penche à l'heure actuelle sur l'ampleur potentielle des écoutes ainsi dénoncées. Il n'est pas explicitement indiqué si la Belgique a pu être visée par l'opération, initialement baptisée 'Thesaurus' et ensuite 'Rubicon'. Plus généralement, le SGRS est pleinement conscient des progrès, mais aussi des dangers et/ou abus potentiels liés à l'utilisation de matériel de cryptographie'.* (traduction libre)

146 *'met tout en œuvre pour s'en protéger et, surtout, met un point d'honneur à respecter le cadre légal en la matière, d'une part, et à appliquer un 'code' moral à ses partenaires/alliés, d'autre part, dans un monde où, sans être naïf, la confiance s'accompagne souvent de prudence».*(traduction libre)

147 Mais par exemple aussi : quelle est la signification/valeur de la notion d'"État ami' dans le contexte des services de renseignement et dans quelle mesure cette notion détermine-t-elle la position de nos propres services de renseignement ?

– Vérifier si les services ont besoin de moyens supplémentaires, parmi lesquels des moyens juridiques (en d'autres termes, des compétences d'enquête) pour pouvoir recueillir des informations à l'étranger.

En 2020, des devoirs d'enquête concrets n'ont pas pu être effectués en raison d'autres priorités. Cependant, les compétences d'enquête à effet extraterritorial ont déjà été esquissées. Cette étude constitue le cadre juridique de référence et d'évaluation si le Comité devait, le cas échéant, constater que les deux services développent effectivement des activités opérationnelles de renseignement à l'étranger.

I.11.8. L'OCAM ET LES SERVICES D'APPUI (SUIVI)

En juin 2020, le Comité permanent R a, conjointement avec le Comité permanent P, finalisé un enquête de contrôle sur les service d'appui de l'Organe de coordination pour l'analyse de la menace (OCAM).[148] Cette enquête portait sur quatre services d'appui : le SPF Intérieur (Office des étrangers), le SPF Affaires étrangères, le SPF Mobilité et Transports et le SPF Finances (Douanes et Accises).[149] L'enquête visait à examiner les relations entre les services d'appui précités et l'OCAM en ce qui concerne la coopération et l'échange d'informations. Une attention particulière a été accordée à la légalité, à l'efficacité et à la coordination de cette coopération et de cet échange d'informations.

Afin de pouvoir répondre aux questions posées par la Commission parlementaire de suivi concernant l'état d'avancement de la mise en œuvre des recommandations formulées dans le cadre de cette enquête, les Comités permanents R et P ont ouvert une enquête de suivi début juin 2020. Les résultats de cette enquête ont été présentés à la Commission de suivi en avril 2021.

I.11.9. L'OCAM ET LES SERVICES D'APPUI 'SUPPLÉMENTAIRES'

Comme susmentionné, l'OCAM peut faire appel à divers 'services d'appui', à savoir les services de police et de renseignement, mais aussi l'Office des étrangers (SPF Intérieur), le SPF Affaires étrangères, le SPF Mobilité et Transports, et l'Administration des Douanes et Accises du SPF Finances.

---

148 Voir I.1. Les services d'appui de l'OCAM' (*supra*).

149 Les services de police et de renseignement ont déjà fait l'objet d'une enquête de contrôle commune portant sur les services d'appui de l'OCAM. Voir à ce propos : COMITÉ PERMANENT R, *Rapport d'activités 2010*, 45-46 ('II.12.6. Communication de renseignements à l'OCAM par les services d'appui') et plus en détail : COMITÉ PERMANENT R, *Rapport d'activités 2011*, 25-33 ('II.4. Les flux d'informations entre l'OCAM et ses services d'appui').

L'A.R. du 17 août 2018 a élargi cette liste des services d'appui de l'OCAM à quatre autres services, que sont la Direction générale Centre de crise, l'Administration générale de la Trésorerie, la Direction générale des Établissements pénitentiaires et le Service Laïcité et Cultes de la Direction générale de la Législation et des Libertés et Droits fondamentaux du SPF Justice. Bien que cette décision remonte à août 2018, l'enquête ne portait pas encore sur ces services car il était prématuré d'effectuer une analyse du flux d'informations et des processus mis en œuvre dans ce cadre. Une nouvelle enquête de contrôle, menée conjointement avec le Comité permanent P, s'imposait. Les résultats ont également été discutés avec la Commission parlementaire de suivi en avril 2021.

I.11.10. L'ÉCHANGE D'INFORMATIONS SUR UN COLLABORATEUR ENTRE LES SERVICES DE RENSEIGNEMENT ET UN EMPLOYEUR PRIVÉ OU PUBLIC

En août 2019, le Comité permanent R a reçu une plainte d'une personne qui travaillait pour une institution publique. L'intéressé se plaignait que son employeur avait demandé des informations le concernant à un service de renseignement qui, sur cette base, entendait entreprendre des démarches disciplinaires.

Au cours du traitement de la plainte, le Comité a décidé de commencer par effectuer une analyse juridique de la question plus générale des cas et des conditions dans lesquels une instance privée ou publique peut adresser une demande à l'un des deux services de renseignement sur un collaborateur (ou un candidat à un emploi). Le Comité s'est en outre demandé dans quels cas le service de renseignement concerné peut ou doit y répondre et, le cas échéant, à quelles exigences cette réponse doit satisfaire. Cette analyse juridique a été discutée avec la Commission de suivi au premier trimestre 2021.

I.11.11. CONTRÔLE DES FONDS SPÉCIAUX : ENQUÊTE DE SUIVI

À l'instar de tout service public, les services de renseignement se voient également allouer des fonds publics pour exercer leurs missions légales. La règle normale pour l'utilisation de ces fonds doit être une transparence parfaite et un contrôle total. Cependant, comme certaines tâches de la VSSE et du SGRS sont imprévisibles ou doivent être tenues secrètes, une partie de leur budget échappe à cette 'règle normale'. Cette partie est mieux connue sous le nom de 'fonds spéciaux'. Bien que le montant de ces fonds soit intégré dans le budget alloué aux services, des règles

particulières s'appliquent à leur gestion, leur utilisation et leur contrôle. En 2015[150], le Comité s'est notamment attaché à déterminer la nature de ces 'fonds spéciaux', leur montant et leur répartition. Il a également contrôlé l'utilisation des moyens et les interactions entre ces 'fonds spéciaux' et les budgets dits 'normaux'. Enfin, le Comité s'est penché sur le cadre réglementaire et a examiné les mécanismes de contrôle, et ce tant en interne (au sein des services) qu'en externe (Cour des comptes, Inspection des Finances, Comité permanent R, etc.). Différentes recommandations ont été formulées.

Depuis 2018 (VSSE) et 2020 (SGRS), la Cour des comptes a exprimé son intention de réaliser un contrôle périodique de ces fonds.[151] Dans ce contexte, la Cour des comptes a pu recourir à une assistance technique, telle que proposée par le Comité permanent R.[152] Le Comité pouvait à son tour '*exercer sa mission avec plus d'attention sur l'utilisation de ces dits fonds*'. Une enquête de suivi a été ouverte en 2020 sur la gestion, l'utilisation et le contrôle des fonds spéciaux.

I.11.12. ENQUÊTE SUR LE SUIVI DES MANDATAIRES POLITIQUES

Lors de débats (parlementaires)[153], une question a déjà été posée à maintes reprises, à savoir si et dans quelle mesure les services de renseignement belges suivaient (ou étaient autorisés à suivre) des mandataires politiques, et quelles règles devaient être observées à cet égard. Depuis début janvier 2018, une nouvelle note de service classifiée 'confidentiel', datée du 13 décembre 2017, est d'application au sein de la VSSE.[154] Ce service envoie deux types de rapports au ministre de la Justice et au Premier ministre, avec copie au Comité permanent R. Il s'agit, d'une part, de rapports ponctuels sur des mandataires politiques qui contribuent à l'apparition

---

150 COMITÉ PERMANENT R, *Rapport d'activités 2015*, 11-16 ('La gestion, l'utilisation et le contrôle des fonds spéciaux').

151 En 2020, le Comité a reçu une copie du contrôle effectué en 2019 par la Cour des comptes à la VSSE pour l'exercice comptable 2018, COUR DES COMPTES, *Sûreté de l'État. Contrôle 2019 des fonds spéciaux. Rapport adressé au ministre de la Justice*, 20 mai 2020.

152 '*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*'.

153 Voir encore récemment : Question de S. Creyelman au ministre de la Justice sur les 'dossiers politiques à la VSSE' (*Q&R.* Chambre 2019-20, 16 juillet 2020, QRVA 23, 33, Q. n° 351).

154 La note de service a été actualisée en juin 2020 en vue d'améliorer les rapports destinés à la direction sur les activités disruptives. Malgré ses demandes répétées, le Comité n'a reçu, en 2019, aucune information du SGRS. Le Comité avait pourtant exhorté le SGRS, comme la VSSE d'ailleurs, à adopter une directive uniforme, assortie de règles claires et univoques quant au recueil, au traitement, à la consultation, au stockage et à l'archivage des informations relatives aux mandataires politiques. Le SGRS ne dispose pas d'une procédure spécifique (SOP) pour traiter cette thématique, pas plus qu'il n'a défini de procédure pour informer le Comité permanent R.

d'une menace et, d'autre part, d'un aperçu trimestriel de l'ensemble des documents dans lesquels des mandataires politiques sont mentionnés.[155] Le ministre de la Justice avait marqué son accord sur le *'principe de vérifications par le Comité R qui s'avèrent nécessaires conformément à la loi organique du 18 juillet 1991'*.[156]

Étant donné qu'il n'est mentionné nulle part ce qu'il est censé faire des informations précitées, le Comité permanent R a pris l'initiative de développer une méthodologie autour de la 'problématique du suivi des mandataires politiques par les services de renseignement et le rôle du Comité permanent R'. Cette méthodologie a été approuvée par la Commission parlementaire de suivi en 2020. Sur la base de cette méthodologie, une enquête de contrôle (périodique) a été initiée en 2020.

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

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

CHAPITRE II

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

L'année 2020 a marqué le dixième anniversaire de la Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité (Loi MRD[157]). Cet événement méritait d'être célébré. Aussi, le Comité a organisé, le 31 janvier 2020, sous les auspices de la Chambre des représentants, le colloque intitulé 'Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulières de renseignement : de l'ombre à la lumière'.[158]

Avec l'entrée en vigueur de cette loi, que la Loi du 30 mars 2017[159] (la 'Loi d'actualisation MRD') a profondément modifiée, les possibilités de recueil d'informations par les deux services de renseignement ont été considérablement élargies.

Lorsque le législateur en 2010 a finalement décidé de doter les services de renseignement de nouvelles compétences, une mission importante a, par la même occasion, été confiée au Comité permanent R. Le Comité devait, conjointement avec la Commission BIM, contrôler l'exécution de ces MRD, lesquelles sont par définition très intrusives pour les droits et libertés individuels. L'article 35 L. Contrôle impose une transparence au Comité dans les activités qu'il mène dans ce contexte.

Le présent chapitre reprend donc les chiffres détaillés de la mise en œuvre par la Sûreté de l'État (VSSE) et par le Service Général du Renseignement et de la Sécurité (SGRS) des méthodes spécifiques et exceptionnelles (regroupées en 'méthodes particulières de renseignement') et de certaines méthodes ordinaires, pour

---

157 *M.B.* 10 mars 2010.

158 Y étaient représentés : le ministre de la Justice, différents Députés, membres des services de renseignement et de sécurité, des représentants du milieu académique, des journalistes, des membres d'institutions des droits de l'homme, du barreau et du monde judiciaire, des organes de contrôle ainsi que des contacts internationaux. Un compte-rendu, sous la forme d'un livre, a été publié à ce propos : J. VANDERBORGHT (ed.), *Bijzondere inlichtingenmethoden in de schijnwerpers - Les méthodes particulières de renseignement: de l'ombre à la lumière,* Intersentia, Antwerpen, 2020, 151 p.

159 *M.B.* 28 avril 2017.

lesquelles le Comité s'est vu confier une mission de contrôle supplémentaire. De plus, il est fait rapport sur la manière dont le Comité assure sa mission de contrôle juridictionnelle sur ces méthodes. Outre une série de chiffres sur le nombre de décisions et la manière dont le Comité a été saisi, la substance des décisions finales du Comité permanent R est également reprise. La jurisprudence a été expurgée des données opérationnelles ; seuls sont mentionnés les éléments qui présentent un intérêt d'un point de vue juridique.

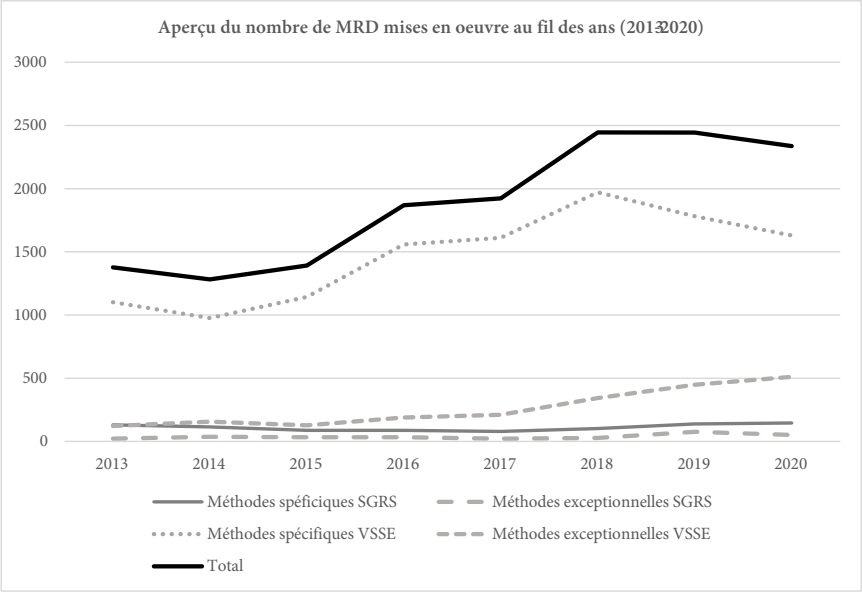
II.1. LES CHIFFRES RELATIFS AUX MÉTHODES PARTICULIÈRES ET À CERTAINES MÉTHODES ORDINAIRES

Entre le 1er janvier et le 31 décembre 2020, 2337 autorisations ont été émises par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de renseignement : 2140 par la VSSE (1629 spécifiques et 511 exceptionnelles) et 197 par le SGRS (146 spécifiques et 51 exceptionnelles). Selon les responsables MRD de la VSSE et du SGRS, la pandémie de COVID n'a eu aucun impact sur le nombre de méthodes particulières de renseignement mises en œuvre.

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

	SGRS		VSSE		TOTAL
	Méthodes spécifiques	**Méthodes exceptionnelles**	**Méthodes spécifiques**	**Méthodes exceptionnelles**	
2013	131	23	1102	122	1378
2014	114	36	976	156	1282
2015	87	34	1143	128	1392
2016	88	33	1558	189	1868
2017	79	22	1612	210	1923
2018	102	28	1971	344	2445
2019	138	76	1781	449	2444
2020	146	51	1629	511	2337

Cela donne schématiquement :



Après une augmentation constante du nombre de MRD mises en œuvre ces dernières années et une stagnation en 2019, on remarque pour la première fois une diminution (négligeable) : le nombre total de méthodes utilisées est resté plutôt stable en 2020. Il convient néanmoins de noter que plusieurs targets (tels que des personnes, des organisations, des lieux, des objets, des moyens de communication, etc.) peuvent être visés dans une même autorisation.

La VSSE se taille la part du lion, avec 91,5 % des méthodes mises en œuvre.

Une ventilation de ces chiffres permet de constater que l'augmentation du nombre de méthodes spécifiques par le SGRS se poursuit, passant de 138 à 146. Le nombre de méthodes exceptionnelles mises en œuvre connaît toutefois une forte diminution d'environ un tiers, passant de 76 à 51.[160]

À la VSSE, on observe la tendance inverse, c'est-à-dire une diminution remarquable de l'utilisation des méthodes spécifiques (de 1781 en 2019 à 1629 en 2020) et une nouvelle hausse sensible de l'utilisation des méthodes exceptionnelles (de 449 en 2019 à 511 en 2020, soit une hausse d'environ 14 %). Le Comité se limite ici à reprendre les chiffres bruts.

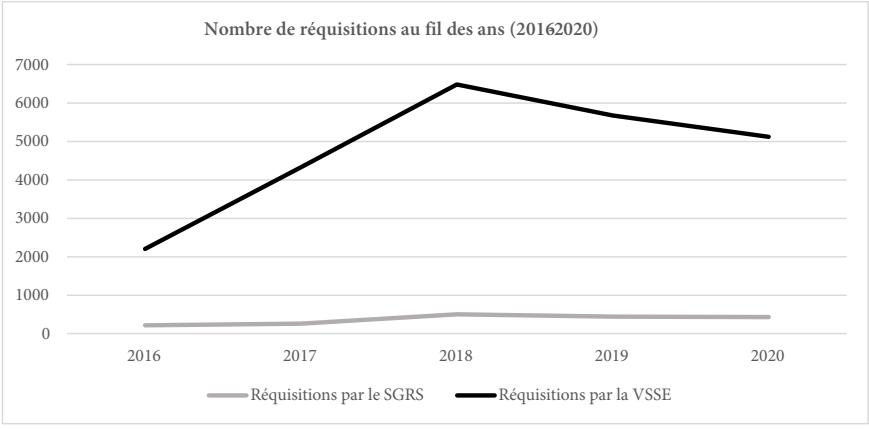
En ce qui concerne les méthodes ordinaires qui consistent à adresser une réquisition à des opérateurs et fournisseurs ('*providers*')

160 Ce qui est important dans ce contexte, c'est que le SGRS dispose également de compétences particulières pour le recueil d'informations, telles que réglées dans les articles 44 et suiv. L.R&S. Voir à ce propos 'Chapitre III. Le contrôle des interceptions à l'étranger, des prises d'images et des intrusions dans des systèmes informatiques'.

de télécom afin d'identifier certains moyens de communication (cf. art. 16/2 L.R&S), on note de nouveau une diminution (environ 10 %). On dénombre une dizaine de réquisitions de moins au SGRS par rapport à 2019, contre plus de 550 réquisitions de moins du côté de la VSSE).

	Réquisitions par le SGRS	**Réquisitions par la VSSE**
2016	216	2203
2017	257	4327
2018	502	6482
2019	442	5674
2020	433	5123

Cela donne schématiquement :



Le Comité avait déjà indiqué[161] qu'« *[il] ne [pouvait] nier qu'un nombre beaucoup plus élevé d'identifications ont été effectuées depuis l'introduction de la procédure assouplie visée à l'article 16/2 L.R&S* ». Le nombre de réquisitions en 2020, bien que toujours en baisse, demeure assez important. Dans l'exercice de sa compétence de contrôle générale, le Comité en a examiné les motifs ; les résultats ont été repris dans l'enquête de contrôle ouverte en 2019 et intitulée *'enquête de contrôle sur l'application et le contrôle interne des services de renseignement des méthodes et instruments récemment insérés ou adaptés par le législateur et dont un rôle de contrôle spécifique a été attribué au Comité permanent R'* (cf. I.11.1).

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

II.1.1. LES MÉTHODES UTILISÉES PAR LE SGRS

II.1.1.1. Les méthodes ordinaires 'plus'

Identification de l'utilisateur de télécommunications

L'identification de l'utilisateur de télécommunications (par ex. d'un numéro de GSM ou d'une adresse IP) ou d'un moyen de communication utilisé est considérée comme une méthode ordinaire, dans la mesure où elle a lieu via une réquisition auprès les opérateurs et fournisseurs (*providers*) de télécom ou via un accès direct aux fichiers des clients.[162] La réglementation prévoit une obligation pour les services de renseignement de tenir un registre de toutes les identifications requises et de toutes les identifications obtenues par accès direct.[163] Conformément à cette même réglementation, le Comité doit recevoir, sur une base mensuelle, une liste des identifications requises et de chaque accès. Le SGRS a, quant à lui, enregistré une légère diminution du nombre de réquisitions, passant de 442 en 2019 à 433 en 2020. Cette thématique a également fait l'objet d'une enquête de contrôle ouverte en 2019 (*supra*).

Identification du détenteur d'une carte prépayée

L'article 16/2 L.R&S mentionne ce qui suit : '*§ 2. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'une banque ou d'une institution financière pour procéder à l'identification de l'utilisateur final d'une carte prépayée visée dans l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques, sur la base de la référence d'une transaction bancaire électronique qui est liée à la carte prépayée et qui a préalablement été communiquée par un opérateur ou un fournisseur en application du paragraphe 1er.*' Comme en 2018 et en 2019, les deux services de renseignement n'ont pas encore employé cette méthode.

Accès aux données PNR

Début 2017,[164] une loi a introduit la possibilité pour les services de renseignement d'avoir accès aux informations détenues par l'Unité d'information des passagers, et ce par le biais de recherches ciblées (art. 16/3 L.R&S et art. 27 Loi PNR du

---

162 Lorsque l'identification a lieu à l'aide d'un moyen technique (et donc pas via une réquisition à un opérateur), la collecte reste une méthode spécifique (art. 18/7 § 1er L.R&S).

163 La possibilité pour les services de renseignement de demander de telles données d'identification via un accès direct à des fichiers clients des opérateurs et fournisseurs de télécommunications, créée à l'article 16/2, § 1er, dernier alinéa L.R&S, est restée sans effet à ce jour.

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

25 décembre 2016). Le Comité est informé de l'utilisation de cette méthode et peut l'interdire le cas échéant.[165]

La réglementation PNR permet également de réaliser ce que l'on appelle une 'évaluation préalable', qui consiste à vérifier automatiquement la correspondance entre les données PNR et les listes ou fichiers de noms des services de renseignement et à envoyer des informations sur la base de '*hits*' validés (art. 24 Loi PNR). Le nombre de recherches effectuées dans les données PNR a diminué, passant de 38 en 2019 à 28 en 2020.

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

La Loi du 30 novembre 1998 organique des services de renseignement et de sécurité a été adaptée par la Loi du 21 mars 2018 (*M.B.* 16 avril 2018) pour permettre aux services de renseignement d'utiliser des images enregistrées par les caméras des services de police. Une nouvelle méthode ordinaire a été introduite à cet effet (art. 16/4 §2 L.R&S).[166] [167]

Les chiffres

Méthodes ordinaires (SGRS)	Nombre d'autorisations
Identification de l'utilisateur de télécommunications	433
Identification du détenteur d'une carte prépayée	0
Recherches ciblées de données PNR	28
Transmission de données PNR sur la base de hits	Non communiqué
Utilisation d'images enregistrées par les caméras des services de police	Pas en vigueur[168]

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

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

167 Début 2019, le Conseil des ministres a approuvé un projet d'arrêté royal en application de l'art. 16 § 4 L.R&S, qui a été soumis à l'avis du Comité permanent R. Cet avis 002/CPR-ACC/2019 du 9 avril 2019 peut être consulté sur le site internet du Comité (www.comiteri.be).

168 Le champ d'application de l'article 16/4 L.R&S (par exemple en ce qui concerne les consultations de la Direction de l'information policière et des moyens ICT (DRI) de la Police fédérale) fait l'objet d'une analyse juridique (2021).

II.1.1.2. Les méthodes spécifiques

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

Méthodes spécifiques (SGRS)	Nombre d'autorisations
Observer, à l'aide d'un moyen technique, dans des lieux accessibles au public ou observer, à l'aide ou non d'un moyen technique, dans un lieu non accessible au public qui n'est pas soustrait à la vue (art. 18/4 L.R&S)169	6
Inspecter des lieux accessibles au public, à l'aide d'un moyen technique, inspecter le contenu d'objets verrouillés ou les emporter (art. 18/5 L.R&S)	0
Prendre connaissance de données d'identification d'un trafic postal et requérir le concours d'un opérateur postal (art.18/6 L.R&S)	0
Requérir des données de transport et de voyage auprès de fournisseurs privés de service en matière de transport ou de voyage (art. 18/6/1 L.R&S)	2
Identifier, à l'aide d'un moyen technique, les services et de moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée (art. 18/7 §1, 1° L.R&S)	2
Requérir le concours de l'opérateur d'un réseau de communications électroniques afin d'obtenir les données relatives à la méthode de paiement, identifier le moyen de paiement et le moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques (art. 18/7 §1, 2° L.R&S)	0
Prendre connaissance des données d'appel d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 §1, 1°L.R&S)	69
Prendre connaissance des données de localisation d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 §1, 2° L.R&S)	67
TOTAL	**146**

En ce qui concerne la mise en œuvre des méthodes spécifiques, ce sont le repérage des données d'appel d'un trafic de communications électroniques' (art. 18/8 L.R&S) et la 'prise de connaissance de données de localisation' (art. 18/8 L.R&S), tous deux assortis d'une réquisition du concours d'un opérateur, qui se hissent clairement en tête du classement (136 des 146 méthodes spécifiques mises en

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

œuvre). L'observation dans des lieux accessibles au public à l'aide d'un moyen technique a diminué de moitié, passant de 12 en 2019 à 6 en 2020.

II.1.1.3. Les méthodes exceptionnelles

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

Méthodes exceptionnelles (SGRS)	Nombre d'autorisations
Observer, à l'aide ou non de moyens techniques, des lieux non accessibles au public qui sont soustraits à la vue et pénétrer dans des lieux non accessibles au public qui sont soustraits ou non à la vue pour exécuter une observation, installer un moyen technique, ouvrir un objet ou l'emporter (art. 18/11 L.R&S)170	2
Inspecter, à l'aide ou non de moyens techniques, des lieux non accessibles au public, ainsi que l'inspection du contenu d'objets verrouillés ou non qui s'y trouvent (art. 18/12 L.R&S)	0
Recourir à une personne morale visée à l'article 13/3, § 1er L.R&S afin de collecter des données	0
Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S)	0
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	6
S'introduire dans un système informatique (article 18/16 L.R&S)	4
Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	39
TOTAL	**51**

La forte diminution en pourcentage (plus de 30 %) du nombre de méthodes exceptionnelles mises en œuvre par le SGRS se situe principalement au niveau de la 'collecte de données concernant les comptes bancaires et les transactions bancaires' (art. 18/15 L.R&S) : si cette méthode avait encore été employée à 20 reprises en 2019, elle ne l'a été qu'à 6 reprises en 2020. La même tendance à la baisse s'observe pour les intrusions dans un système informatique (18/16 L.R&S) ; il y en a eu deux fois moins par rapport à 2019 (de 8 à 4).

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

II.1.1.4. Les missions et les menaces justifiant le recours aux méthodes ordinaires et particulières [171]

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

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

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

4. La recherche, l'analyse et le traitement du renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge (art. 11, 5°, L.R&S).

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

Environ deux tiers des méthodes spécifiques et exceptionnelles sont utilisés par le SGRS dans le cadre de la mission de recherche, d'analyse et de traitement du renseignement relatif aux activités des services de renseignements étrangers sur le territoire belge (art. 11, 5° L.R&S).[172] On ne peut cependant pas en déduire que, depuis 2017, le SGRS suit un 'nouveau genre' de menace. En effet, le suivi de services étrangers était auparavant plus vite associé à la mission de renseignement dans le contexte de la lutte contre l'espionnage. On peut encore noter que le nombre de MRD mises en œuvre dans le cadre des menaces 'terrorisme' et 'extrémisme' ont connu une hausse sensible, au détriment de la menace 'ingérence', qui a diminué de moitié.

NATURE DE LA MENACE	NOMBRE EN 2020
Espionnage	139
Ingérence	19
Extrémisme	20
Terrorisme	19
Organisations criminelles	-
Autre	-
TOTAL	**197**

Contrairement à la mise en œuvre de méthodes particulières, le Comité ne dispose pas de données chiffrées relatives à la menace visée et aux intérêts à défendre en ce qui concerne les méthodes ordinaires dont il est question dans le présent chapitre. Dans son précédent rapport d'activités, le Comité recommandait aux services de consigner ces données et de les tenir à disposition.[173] Étant donné que ce n'est pas encore le cas, le Comité réitère sa recommandation.

172 Aucune méthode particulière de renseignement n'a été utilisée à l'étranger par le SGRS en 2020.
173 COMITÉ PERMANENT R, *Rapport d'activités 2017*, 43.

II.1.2. LES MÉTHODES UTILISÉES PAR LA VSSE

II.1.2.1. Les méthodes ordinaires 'plus'

Méthodes ordinaires (VSSE)	Nombre d'autorisations
Identification de l'utilisateur de télécommunications	5123
Identification du détenteur d'une carte prépayée	0
Recherches ciblées de données PNR	30
Transmission de données PNR sur la base de '*hits*'	Non communiqué
Utilisation d'images enregistrées par les caméras des services de police	Pas en vigueur[174]

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

II.1.2.2. Les méthodes spécifiques

Méthodes spécifiques (VSSE)	Nombre d'autorisations
Observer, à l'aide d'un moyen technique, dans des lieux accessibles au public ou observer, à l'aide ou non d'un moyen technique, dans un lieu non accessible au public qui n'est pas soustrait à la vue (art. 18/4 L.R&S)	245
Inspecter des lieux accessibles au public, à l'aide d'un moyen technique, inspecter le contenu d'objets verrouillés ou les emporter (art. 18/5 L.R&S)	0
Prendre connaissance de données d'identification d'un trafic postal et requérir le concours d'un opérateur postal (art.18/6 L.R&S)	1
Requérir des données de transport et de voyage auprès de fournisseurs privés de service en matière de transport ou de voyage (art. 18/6/1 L.R&S)	70
Identifier, à l'aide d'un moyen technique, les services et de moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée (art. 18/7 §1, 1° L.R&S)	46
Requérir le concours de l'opérateur d'un réseau de communications électroniques afin d'obtenir les données relatives à la méthode de paiement, identifier le moyen de paiement et le moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques (art. 18/7 §1, 2° L.R&S)	0
Prendre connaissance des données d'appel d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 L.R&S)	650

[174] Le champ d'application de l'article 16/4 L.R&S (par exemple en ce qui concerne les consultations de la Direction de l'information policière et des moyens ICT (DRI) de la Police fédérale) fait l'objet d'une analyse juridique (2021).

Méthodes spécifiques (VSSE)	Nombre d'autorisations
Prendre connaissance des données de localisation d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 L.R&S)	617
TOTAL	**1629**

Comme susmentionné, le nombre de méthodes spécifiques mises en œuvre en 2020 par rapport à 2019 a clairement diminué, passant de 1781 à 1629 méthodes. On constate que cette diminution est graduelle pour pratiquement toutes les méthodes spécifiques, à l'exception de la réquisition des données de transport et de voyage auprès de fournisseurs privés de service en matière de transport ou de voyage, qui a considérablement augmenté, passant de 48 en 2019 à 70 en 2020.

II.1.2.3. Les méthodes exceptionnelles

Méthodes exceptionnelles (VSSE)	Nombre d'autorisations
Observer, à l'aide ou non de moyens techniques, des lieux non accessibles au public qui sont soustraits à la vue et pénétrer dans des lieux non accessibles au public qui sont soustraits ou non à la vue pour exécuter une observation, installer un moyen technique, ouvrir un objet ou l'emporter (art. 18/11 L.R&S)	9
Inspecter, à l'aide ou non de moyens techniques, des lieux non accessibles au public, ainsi que l'inspection du contenu d'objets verrouillés ou non qui s'y trouvent (art. 18/12 L.R&S)	8
Recourir à une personne morale visée à l'article 13/3, § 1er L.R&S afin de collecter des données	0
Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S)	11
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	186
S'introduire dans un système informatique (article 18/16 L.R&S)	74
Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	223
TOTAL	**511**

Contrairement à la mise en œuvre des méthodes spécifiques, le nombre de méthodes exceptionnelles mises en œuvre par la VSSE est en constante augmentation (+ 14 % par rapport à 2019). Cette hausse s'explique entièrement par l'utilisation de la méthode 'Collecte des données concernant des comptes bancaires et des transactions bancaires' (art. 18/15 L/R&S) qui a plus que doublé, passant de 95 en 2019 à 186 en 2020) et de la méthode 'Intrusion dans un système informatique' (art 18/16 L.R&S), qui est passé de 48 en 2019 à 74 en 2020). Toutes les autres méthodes exceptionnelles ont été moins utilisées qu'en 2019.

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

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

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

criminelles qui se rapportent intrinsèquement aux activités visées dans des menaces précédentes ou qui peuvent avoir des conséquences déstabilisantes sur le plan politique ou socio-économique.

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

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

NATURE DE LA MENACE	NOMBRE EN 2020
Espionnage	816
Ingérence	27
Extrémisme	296
Prolifération	3
Organisations sectaires nuisibles	0
Terrorisme	998
Organisations criminelles	0
Suivi des activités des services étrangers en Belgique	(inclus dans les chiffres ci-dessus)
TOTAL	**2140**

Les chiffres repris ci-dessus montrent que le 'terrorisme', pour ce qui est de la mise en œuvre de MRD en 2020, a certes diminué (de 1118 à 998), mais que cette menace demeure la priorité absolue de la VSSE en 2020, suivie de près par la menace 'espionnage' (816). On peut constater à la VSSE, tout comme au SGRS, une forte diminution du nombre de 'dossiers d'ingérence' (de 87 en 2019 à 27 en 2020). Étant donné que les organisations sectaires nuisibles et les organisations criminelles ne font plus l'objet d'un suivi actif depuis 2015, il ne faut pas s'étonner que ces menaces ne figurent pas dans les chiffres.

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

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

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

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

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

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

II.2.1. LE CONTRÔLE DE CERTAINES MÉTHODES ORDINAIRES

II.2.1.1. Généralités

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

En ce qui concerne l'identification de l'utilisateur de télécommunications (et l'identification de l'utilisateur d'une carte prépayée qui y est associée), la loi n'a pas instauré de contrôle spécifique. À l'article 16/2 § 4 L.R&S, il est seulement stipulé que la liste des identifications requises et de tous les accès directs doit être communiquée chaque mois au Comité. Comme déjà indiqué, le Comité reçoit uniquement le nombre de réquisitions. Il a toutefois proposé de contrôler annuellement une sélection de réquisitions.[175] Ce contrôle a débuté en 2020. Le Comité a décidé de reprendre cette thématique dans l'enquête qu'il a initiée en 2019 et qui est intitulée *'enquête de contrôle sur l'application et le contrôle interne des services de renseignement des méthodes et instruments récemment insérés ou adaptés par le législateur et dont un rôle de contrôle spécifique a été attribué au Comité permanent R.'*

En ce qui concerne l'accès aux données PNR, qui sont détenues par l'Unité d'information des passagers, l'article 16/3 L.R&S dispose que c'est le dirigeant du service qui doit décider de tout accès, et ce *'de façon dûment motivée'*. Le Comité doit

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

en être informé *et* '*interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les conditions qui ne respectent pas les conditions légales*'. Le Comité a prononcé une seule interdiction de ce genre en 2020 (*infra*).

Enfin, le Comité s'est vu attribuer des modalités de contrôle particulières dans le cadre de la possibilité pour les services de renseignement d'avoir accès à des informations provenant d'images enregistrées par des caméras utilisées par les services de police (article 16/4 L.R&S): un contrôle *a priori* [176] et un contrôle *a posteriori*.[177]

II.2.1.2. Les décisions correctives

L'essentiel des décisions correctives prises par le Comité permanent R dans le cadre de son contrôle de l'utilisation des méthodes ordinaires précitées figurent ci-dessous.

En ce qui concerne la VSSE, deux cas ont donné lieu à une décision de demander un complément d'information, et aucune interdiction d'exploitation n'a été prononcée. Concernant le SGRS, par contre, quatre décisions ont été prises en 2020 dans ce cadre ; dans trois cas, un complément d'information a été demandé et une décision d'interdiction d'exploitation a été prononcée. À ce propos, le Comité permanent R fait remarquer que l'article 16/3 le mentionne effectivement, mais qu'interdire l'exploitation sans ordonner une destruction a peu de sens. Une ordonnance de destruction est cependant toujours possible sur la base de la Loi relative à la protection des données. Il semble dès lors indiqué de combiner l'article 16 L.R&S et l'article 51/3 L. Contrôle.

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

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

II.2.2. LE CONTRÔLE DES MÉTHODES PARTICULIÈRES

II.2.2.1. Les chiffres

Cette section reprend les activités du Comité permanent R relatives aux méthodes de renseignement spécifiques et exceptionnelles. L'attention se focalise ici sur les décisions juridictionnelles prises en la matière, et non sur les données opérationnelles. Il convient toutefois de souligner au préalable que le Comité soumet *toutes* les autorisations de mise en œuvre de méthodes particulières à une enquête *prima facie*, et ce en vue de décider d'une éventuelle saisine. Par ailleurs, un membre du Service d'Enquêtes participe à une réunion de quinzaine, au cours de laquelle la VSSE informe la Commission BIM sur l'exécution des méthodes exceptionnelles. Un rapport en est fait à l'intention du Comité, ce qui lui permet d'avoir une meilleure vue sur ces méthodes.[178]
L'article 43/4 L.R&S stipule que le Comité permanent R peut être saisi de cinq manières :

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

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

---

178 En 2017, le Comité a recommandé au SGRS d'organiser lui aussi de telles réunions de quinzaine. Il s'agit en effet d'une obligation légale (art. 18/10 § 1er, alinéa 3, L.R&S et art. 9 A.R. du 12 octobre 2010). Depuis fin janvier 2018, en raison du nombre restreint de méthodes particulières de renseignement mises en œuvre, une réunion est organisée sur une base mensuelle et, en principe, un rapport est établi sur une base bimensuelle.

TYPE DE SAISINE	2013	2014	2015	2016	2017	2018	2019	2020
1. D'initiative	16	12	16	3	1	1	4	2
2. Commission Vie Privée/ Autorité de protection des données	0	0	0	0	0	0	0	0
3. Plainte	0	0	0	1	0	0	0	0
4. Interdiction d'exploitation par la Commission BIM[179]	5	5	11	19	15	10	12	9
5. Autorisation du ministre	2	1	0	0	0	0	0	0
6. Auteur d'avis préjudiciel	0	0	0	0	0	0	0	0
TOTAL	**23**	**18**	**27**	**23**	**16**	**11**	**16**	**11**

Le nombre de décisions prises par le Comité a continué à diminuer. En outre, toutes les saisines, à deux exceptions près, résultent d'une suspension décidée par la Commission BIM.

Une fois saisi, le Comité peut prendre plusieurs types de décisions et de décisions intermédiaires.

1. Constater la nullité de la plainte pour cause de vice de forme ou absence d'un intérêt personnel et légitime (art. 43/4, alinéa 1er, L.R&S) ;
2. Ne pas donner suite à une plainte qui est manifestement non fondée (art. 43/4, alinéa 1er, L.R&S) ;
3. Suspendre la méthode contestée dans l'attente d'une décision définitive (art. 43/4, dernier alinéa, L.R&S) ;
4. Demander des informations complémentaires à la Commission BIM (43/5 § 1er, alinéa 1er à 3, L.R&S) ;
5. Demander des informations complémentaires au service de renseignement concerné (43/5 § 1er, alinéa 3, L.R&S) ;
6. Ordonner une mission d'enquête pour le service d'Enquêtes R (art. 43/5 § 2 L.R&S). Dans cette rubrique, il est fait référence à la fois aux multiples informations complémentaires recueillies de manière plutôt informelle par le Service d'Enquêtes R avant la saisine proprement dite et aux informations recueillies par le Comité après la saisine ;
7. Procéder à l'audition des membres de la Commission BIM (art. 43/5 § 4, alinéa 1er, L.R&S) ;
8. Procéder à l'audition du dirigeant du service de renseignement ou des membres du service de renseignement concerné (art. 43/5 § 4, alinéa 1er, L.R&S) ;

179 Elles découlent, par exemple, de problèmes d'enregistrement ou d'enlèvement d'appareillages.

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

NATURE DE LA DÉCISION	2014	2015	2016	2017	2018	2019	2020
Décisions préalables à la saisine							
1. Plainte frappée de nullité	0	0	0	0	0	0	0
2. Plainte manifestement non fondée	0	0	0	0	0	0	0
Décisions intermédiaires							
3. Suspension de la méthode	3	2	1	0	0	0	1
4. Information complémentaire de la Commission BIM	0	0	0	0	0	0	0
5. Information complémentaire du service de renseignement	1	1	4	0	0	0	1
6. Mission d'enquête confiée au Service d'Enquêtes R[180]	54	48	60	35	52	52	24

180 Le Comité demande au Service d'Enquêtes d'effectuer des recherches complémentaires et/ou de contacter le service concerné ou la Commission BIM.

NATURE DE LA DÉCISION	2014	2015	2016	2017	2018	2019	2020
7. Audition membres de la Commission BIM	0	2	0	0	0	0	0
8.Audition membres des services de renseignement	0	2	0	0	0	1	1
9. Décision relative au secret de l'instruction	0	0	0	0	0	0	0
10. Informations sensibles lors de l'audition	0	0	0	0	0	0	0
Décisions finales							
11. Cessation de la méthode	3	3	6	9	4	11	10
12. Cessation partielle de la méthode	10	13	4	6	6	4	0
13. Levée (partielle) de l'interdiction de la Commission BIM	0	4	11	0	0	0	0
14. Non compétent	0	0	0	0	0	0	0
15. Autorisation légale/Non-cessation de la méthode/Non-fondement51	4	6	2	1	1	0	0
Avis préjudiciels							
16. Avis préjudiciel	0	0	0	0	0	0	

II.2.2.2. La jurisprudence

La substance des décisions finales prises en 2020 par le Comité permanent R dans le cadre de son rôle juridictionnel est reprise ci-après.[181] Les synthèses sont expurgées des données opérationnelles. Seuls sont mentionnés les éléments qui présentent un intérêt d'un point de vue juridique.
Les décisions ont été regroupées en trois rubriques :
- Les exigences légales (de forme) préalables à la mise en œuvre d'une méthode ;
- La légalité d'une méthode concernant les techniques employées, des données recueillies, la durée de la mesure et la nature de la menace ;
- La légalité de l'exécution d'une méthode légale.

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

Question préjudicielle posée à la cour constitutionnelle

En 2020, pour la première fois depuis l'entrée en vigueur de la Loi MRD du 4 février 2010, le Comité permanent R a posé une question préjudicielle à la Cour constitutionnelle concernant la législation MRD (dossier

[181] Dans certains dossiers, le Comité a été saisi en 2019, mais n'a rendu sa décision finale qu'en 2020.

2020/9606).[182] Cette démarche faisait suite à la décision prise par un service de renseignement d'employer des méthodes spécifiques visées à l'article 18/8, § 1er, 1° et 2° L.R&S à l'égard d'un médecin. L'autorisation du dirigeant du service concerné portait plus particulièrement, d'une part, sur le repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées et, d'autre part, sur la localisation de l'origine ou de la destination de communications électroniques. Cette méthode devait viser le numéro de téléphone utilisé par le médecin en question, et ce pour une période de quatre mois précédant la décision du dirigeant du service ainsi que pendant deux mois à compter de la notification de la décision à la Commission BIM. Une méthode ordinaire a permis de découvrir que le numéro de téléphone visé était enregistré en Belgique au seul nom du médecin. Bien que le service de renseignement n'ait pas contesté la qualité de médecin de l'intéressé, le service de renseignement a suivi la procédure d'autorisation normale pour les méthodes spécifiques. Le dirigeant du service a donc pris une 'décision' et l'a ensuite notifiée à la Commission BIM (en l'occurrence le même jour). Dès le lendemain, la Commission a ordonné la suspension de la méthode concernée en raison de son caractère illégal.

Selon la Commission, la procédure ordinaire pour les méthodes spécifiques a été utilisée à tort. Compte tenu de la qualité de la personne visée, à savoir celle de médecin, la Commission a estimé qu'il convenait d'appliquer la procédure prévue à l'article 18/3, § 5 L.R&S, à savoir *'(l)es méthodes spécifiques ne peuvent être mise en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de moyens de communication que ceux-ci utilisent à des fins professionnelles qu'à la condition que le service de renseignement et de sécurité dispose au préalable d'indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle et après que la commission a rendu, conformément à l'article 18/10, un avis conforme sur le projet de décision du dirigeant du service*'. Cette procédure particulière implique que si un service de renseignement souhaite utiliser une méthode spécifique à l'égard de certaines catégories professionnelles protégées, la procédure des méthodes exceptionnelles doit être suivie, et que toute méthode est soumise, avant sa mise en œuvre, à un contrôle préalable de la Commission BIM. Selon la Commission, il s'agit également d'une exigence en vue de répondre à la procédure visée à l'article 18/2, § 3 L.R&S qui prescrit que si une méthode spécifique ou exceptionnelle *'est mise en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de leurs locaux ou de moyens de communication qu'ils utilisent à des fins professionnelles, ou de leur résidence, ou de leur domicile, cette méthode ne peut être exécutée sans que, suivant le cas, le président de l'Ordre des barreaux francophones et germanophone ou le président de l'Orde van Vlaamse balies, le président du Conseil national de*

182 La Cour constitutionnelle s'était déjà prononcée sur cette législation dans deux arrêts d'annulation (n° 145/2011 et n° 41/2019).

l'Ordre des médecins ou le président de l'Association des journalistes professionnels, ou leur suppléant en cas de maladie ou d'empêchement du président, en soit averti au préalable par le président de la commission visée à l'article 3, 6°. Le président de la commission est tenu de fournir les informations nécessaires au président de l'Ordre ou de l'association des journalistes professionnels dont fait partie l'avocat, le médecin ou le journaliste. Le président concerné et son suppléant sont tenus au secret. (…).' Si une méthode spécifique ou exceptionnelle '*est mise en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de leurs locaux ou de moyens de communication qu'ils utilisent à des fins professionnelles, ou de leur résidence ou de leur domicile, le président de la commission vérifie si les données obtenues grâce à cette méthode, lorsqu'elles sont protégées par le secret professionnel de l'avocat ou du médecin ou par le secret des sources du journaliste, sont directement liées à la menace potentielle. Si aucun lien direct n'est démontré, la Commission interdit aux services de renseignement et de sécurité d'exploiter ces données.*'. Outre la suspension de la méthode concernée, la Commission BIM a imposé une interdiction d'exploitation pour les données déjà recueillies le cas échéant. La Commission a par ailleurs ordonné une conservation spécifique temporaire de ces données.

Conformément à l'article 43/4 L.R&S, le Comité permanent R est saisi de plein droit chaque fois que la Commission BIM a suspendu l'utilisation d'une méthode spécifique ou d'une méthode exceptionnelle pour cause d'illégalité et a interdit l'exploitation des données pour cause d'illégalité d'une méthode spécifique ou d'une méthode exceptionnelle. Compte tenu de l'importance du régime de protection particulier dont jouissent les catégories professionnelles précitées et en sa qualité d'organe juridictionnel[183] dans le cadre du contrôle des méthodes spécifiques et exceptionnelles mises en œuvre par les services de renseignement, le Comité a décidé de poser une question préjudicielle à la Cour constitutionnelle. Cette question était motivée comme suit : '*Le Comité permanent R relève que le prescrit de l'article 18/2, § 3, alinéas 1 & 2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) restreint la protection accordée aux avocats, médecins et journalistes par rapport aux moyens de communication qu'ils utilisent à des fins professionnelles. Il en découlerait du texte actuel que les moyens de communication à des fins non professionnelles ne seraient pas couverts par la protection légale. Le Comité permanent R se pose la question de savoir comment les services de renseignement peuvent-ils (sic), préalablement, s'assurer de la finalité, professionnelle ou non professionnelle, du moyen de communication concerné (téléphone, GSM…). Est-il possible, a priori, de déterminer dans l'historique des appels téléphoniques d'un avocat, médecin ou journaliste, qu'un numéro présente un caractère exclusivement professionnel. Le législateur n'a pas procédé à cette distinction dans la procédure pénale et plus particulièrement dans les articles 90ter à 90decies du Code d'instruction criminelle. Le législateur a déterminé les conditions strictes auxquelles les services de renseignement, sous le contrôle préalable de la*

183 Cour constitutionnelle, 22 septembre 2011, n° 145/2011, cons. B.38.1

commission BIM, peuvent légalement prendre connaissance des communications conformément à l'article 8, § 2 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH). (…) Le Comité permanent R constate que l'article 90octies du Code d'instruction criminelle en matière d'interception de communications ou télécommunications, pour les mêmes méthodes et pour les mêmes professions protégées, prévoit une protection indépendamment de la finalité (professionnelle ou non professionnelle) de l'usage de moyen de communication. Cette protection est, donc, différente de celle prévue dans la loi du 30 novembre 1998 sans qu'une justification objective n'apparaisse et semble, dès lors contraire aux principes d'égalité de traitement et de non-discrimination et/ou à l'article 8 de la CEDH.'.

Le Comité permanent R a décidé de poser la question suivante à la Cour constitutionnelle: *'L'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité viole-t-il les articles 10 et 11 de la Constitution, lus seuls ou conjointement avec l'article 22 de la Constitution et/ou combinés ou non avec l'article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 et approuvée par la loi du 13 mai 1955, en tant qu'il ne prévoit pas en faveur de l'avocat, du médecin ou du journaliste de protection particulière pour les moyens de communication qu'ils utilisent à des fins autre que professionnelles ?*'.[184]

Notification tardive de la commission BIM

Conformément à l'article 18/3, § 1er, alinéa 2 L.R&S, une méthode spécifique ne peut être mise en œuvre qu'après une décision écrite et motivée du dirigeant du service et après la notification de cette décision à la Commission BIM. Dans le dossier 2020/10.218, le dirigeant du service concerné avait autorisé le recours à un opérateur de télécommunication en vue d'obtenir des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées. Cependant, cette décision n'a été notifiée à la Commission BIM qu'un bon mois plus tard. Les données que le service de renseignement a obtenues de l'opérateur de télécommunication pour cette notification avaient donc été obtenues illégalement. Elles devaient par conséquent être détruites par le Comité.

Dans le dossier 2019/8968, un service de renseignement souhaitait prolonger une observation en cours (méthode spécifique). Conformément à l'article 18/3, § 4 L.R&S, l'utilisation de la méthode spécifique ne peut être prolongée (ou renouvelée) que moyennant une nouvelle décision du dirigeant du service et après notification

184 En avril 2021, la Cour constitutionnelle a rendu sa décision : *« Sous réserve de l'interprétation mentionnée en B.15.2, l'article 18/2, § 3, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ne viole pas les articles 10, 11 et 22 de la Constitution, lus en combinaison avec l'article 8 de la Convention européenne des droits de l'homme »* (Cour constitutionnelle, Arrêt n° 64/2021 du 22 avril 2021 (numéro du rôle 7416).

à la Commission BIM. La première méthode spécifique courait du 25 du mois X au 24 du mois Y inclus. Mais ce n'est que le 27 du mois Y que la décision du dirigeant du service de prolonger l'observation a été notifiée à la Commission BIM. À l'instar de l'interdiction d'exploitation prononcée par la Commission BIM, le Comité a décidé que les données recueillies pendant la période non couverte ne pouvaient pas être exploitées et qu'elles devraient être détruites.

Dans le dossier 2020/9595 également, un service de renseignement souhaitait prolonger une observation en cours (méthode spécifique). La première méthode courait jusqu'au 19 du mois X inclus. L'observation en cours devait par conséquent prendre fin à cette date, mais pour des raisons techniques, le recueil d'informations s'est finalement prolongé jusqu'au 26 du mois X inclus. Le dirigeant du service a autorisé la prolongation jusqu'au 26 du mois X, décision qui a été notifiée le 27 à la Commission BIM. Entre le 19 et le 27, les données n'ont donc pas été recueillies légalement. De plus, étant donné que la première observation a pris fin le 19 et que la décision de prolongation n'a été prise par le dirigeant du service que le 26, il ne s'agissait pas *de iure* d'une prolongation de la méthode mais d'un renouvellement. Bien que l'article 18/3, § 4 L.R&S n'établisse pas de distinction entre une prolongation et un renouvellement en ce qui concerne les conditions d'application (en l'occurrence la décision du dirigeant du service et la notification à la Commission BIM), un service de renseignement qui gère la méthode en question doit se montrer plus attentif en cas de prolongation. Sinon, le risque existe qu'il y ait des périodes pendant lesquelles une méthode spécifique n'est pas couverte par une décision notifiée. Dans ce cas, des données sont recueillies en toute illégalité.

Motivation insuffisante

Dans le cadre d'une méthode spécifique, il était question d'une absence de motivation solide de la décision prise par le dirigeant du service (dossier 2019/8768). Le service de renseignement souhaitait obtenir des données de communications téléphoniques d'une personne déterminée pour une période de douze mois précédant la date de la décision du dirigeant du service. Le Comité a cependant jugé que la motivation figurant dans la décision MRD ne permettait pas '*te beslissen of de in toepassing gebrachte BIM voldoet aan de door de wet gestelde vereisten, inzake bevoegdheid van de dienst en proportionaliteit van de methode*'.[185] Comme mentionné dans le rapport d'activités 2019, le Comité s'est saisi et a posé une série de questions complémentaires au service de renseignement concerné.[186] À la suite d'un entretien avec le service de renseignement et une note additionnelle de ce dernier reprenant des informations complémentaires, le Comité a décidé, en

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

186 Voir à ce propos : COMITÉ PERMANENT R, *Rapport d'activités 2019*, 56-57.

2020, de procéder au retrait de sa saisine, et donc que le service de renseignement était compétent en la matière et que la méthode était proportionnelle.

Dans le dossier 2020/9805, il était aussi question d'une absence de motivation solide. Dans le cas d'espèce, un service de renseignement voulait capturer les enregistrements vidéo et audio d'une conversation qui s'était déroulée dans un lieu non accessible au public et soustrait à la vue (cf. article 18/11, §§ 1er et 2 et article 18/17, §§ 1er et 2 L.R&S). Le Comité n'a cependant pas pu déduire du dossier administratif, principalement constitué de l'autorisation du dirigeant du service et de l'avis conforme de la Commission BIM, pourquoi le service de renseignement a voulu appliquer un tel procédé, ni la finalité exacte de l'opération. Dans ce dossier également, le Comité s'est saisi d'office et a demandé un complément d'information au service de renseignement. Après avoir reçu une note du service de renseignement qui *'op omstandige wijze de werkwijze en de finaliteit van de kwestieuze BIM uiteenzette'*[187] le Comité a décidé que la méthode exceptionnelle était légale.

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

Objet imprécis de la méthode

Dans les dossiers 2020/10.023 et 2020/10.180, il est apparu que le service de renseignement avait mentionné par erreur dans son autorisation un numéro de téléphone qui n'était pas visé par la méthode spécifique en question (en l'occurrence la demande de données de trafic de moyens de communication électronique visés à l'article 18/8, § 1er, 1° L.R&S). La réquisition adressée à l'opérateur de télécommunication mentionnait également ce numéro d'appel erroné. Le service l'a lui-même constaté dans les deux dossiers, mais seulement après l'obtention des données réclamées. Le service de renseignement a systématiquement pris l'initiative de placer les données reçues en quarantaine électronique et a informé la Commission BIM de son erreur. La Commission a interdit l'exploitation des données recueillies illégalement, a averti le Comité permanent R, qui a alors ordonné la destruction des données obtenues illégalement.

La légalité de l'exécution d'une méthode légale

Moyens techniques

La Loi organique des services de renseignement décrit un moyen technique comme étant *'une configuration de composants qui détecte des signaux, les transmet, active leur enregistrement et enregistre les signaux'* (art. 3, 14° L.R&S). Un appareil

187 *'a expliqué en détail le procédé et la finalité de la MRD litigieuse.'* (traduction libre)

photo et, seulement dans des cas très limités, une caméra mobile[188] ne sont pas considérés comme un moyen technique. Différentes MRD peuvent être mises en œuvre à l'aide de moyens techniques. Dans le dossier 2019/8987, il a été fait usage d'une caméra munie d'un microphone, et le dirigeant du service a donné son autorisation après l'avis conforme de la Commission BIM (en l'occurrence pour la méthode prévue à l'article 18/11 L.R&S – observation comme méthode exceptionnelle – en combinaison avec la méthode prévue à l'article 18/17 L.R&S – écoute téléphonique). L'autorisation courait jusqu'au 3 du mois, mais l'appareil a continué à faire des enregistrements vidéo et audio après cette date, et ce *'om technische redenen, omdat de camera met microfoon niet van op afstand kon bediend worden.'*[189] Ainsi, *'(bleef) de geplaatste camera (…) beelden maken en de microfoon verder geluid (opnemen)'*[190] même s'il n'y avait plus d'autorisation. Le Comité a suivi l'interdiction d'exploitation prononcée par la Commission BIM pour les données recueillies après cette date et a ordonné leur destruction.

Dans le dossier 2020/9595 mentionné précédemment, il n'a pas été mis fin à une observation (méthode spécifique) pour des raisons techniques et le Comité, après intervention de la Commission BIM, a ordonné la destruction des données recueillies illégalement.

Différence entre l'autorisation du dirigeant du service et la réquisition

Dans trois décisions, l'autorisation du dirigeant du service en vue de mettre en œuvre une méthode spécifique ou exceptionnelle s'avérait parfaitement légale, mais un problème s'est posé au niveau de l'exécution, en ce sens que la réclamation des données ne correspondait pas au mandat initial. Soit le délai de mise sur écoute figurant dans la réquisition ne correspondait avec celui qui était repris dans l'autorisation (dossier 2020/9204), soit un numéro de téléphone erroné a été communiqué au fournisseur de télécommunication (dossier 2019/8964), ou encore *'(werd) per vergissing aan de uitvoerende telecommunicatiedienst niet alleen een eenmalige intrusie (…) gevraagd'*[191], plus précisément un *'eenmalige toegang (…) tot het mailverkeer'* [192] du target (cf. art. 18/16 L.R&S), *'maar (…) werd (ook) gevraagd*

---

188 Est plus particulièrement exclu *'un appareil mobile utilisé pour la prise d'images animées lorsque la prise de photographies ne permet pas de garantir la discrétion et la sécurité des agents et à la condition que cette utilisation ait été préalablement autorisée par le dirigeant du service ou son délégué'*. Dans un tel cas, *'seules les images fixes jugées pertinentes sont conservées. Les autres images sont détruites dans le mois qui suit le jour de l'enregistrement'* (art. 3, 14°, b L.R&S).

189 *'pour des raisons techniques, car la caméra munie d'un microphone ne pouvait pas être contrôlée à distance'.*'(traduction libre)

190 '*la caméra qui était installée a continué à produire des images et le microphone, à enregistrer des sons*'. (traduction libre)

191 '*Ce n'est pas seulement* une intrusion ponctuelle qui a été demandée à tort au service de télécommunications concerné par la réquisition' (traduction libre)

192 '*un accès ponctuel (...) aux échange d'e-mails*' (traduction libre)

om een live acces te voorzien'[193] (dossier 2020/9829). Un élément qui mérite d'être mentionné dans ce dernier cas est le fait que le service de renseignement a lui-même constaté cette erreur et a ensuite pris l'initiative, conformément à l'article 18/10, § 1er, alinéa 4 L.R&S de mettre fin au '*live access*'. Le service de renseignement a décidé de conserver à part les données recueillies illégalement. La Commission BIM a dès lors prononcé une interdiction d'exploitation et a également prévu une conservation spécifique temporaire. Enfin, le Comité a confirmé l'interdiction d'exploitation prononcée par la Commission BIM et a ordonné la destruction des données obtenues via le '*live access*'.

Données erronnées fournies par l'opérateur ou le fournisseur de télécommunication

Dans trois cas distincts, un service de renseignement avait réquisitionné légalement l'opérateur de réseau concerné, mais la transmission des données réclamées posait un problème dans la mesure où les données transmises par l'opérateur n'avaient aucun rapport avec les données réclamées. Dans les dossiers 2020/9167 et 2020/9225, il s'agissait chaque fois d'"*een telefonie-onderzoek en een afluistermaatregel*'[194], portant respectivement sur trois et deux numéros de téléphone. Dans le dossier 2019/8934, il était uniquement question d'une réquisition dans le cadre du repérage de données de trafic et de localisation de moyens de communication électronique. Dans les trois cas, *'(werden) de betreffende data op wederrechtelijke wijze (…) meegedeeld aan*'[195] service de renseignement concerné. Cela s'est donc produit '*buiten de wil van*'[196] service de renseignement *'om*'[197]. Dans tous les cas, la Commission BIM a prononcé une interdiction d'exploitation, suivie par une ordonnance de destruction du Comité.

II.3. CONCLUSIONS

Le Comité permanent R formule les conclusions générales suivantes :

- Entre le 1er janvier 2020 et le 31 décembre 2020, 2337 autorisations ont été émises par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de renseignement : 2140 par la VSSE (1629 spécifiques et 511 exceptionnelles) et 197 par le SGRS (146 spécifiques et 51 exceptionnelles). Après une augmentation constante du nombre de MRD mises en œuvre ces dernières années et une stagnation observée l'année dernière, on remarque

193 '*mais il a aussi été demandé de prévoir un 'live access*" (traduction libre)
194 '*une enquête de téléphonie et d'une opération de mise sur écoute*' (traduction libre)
195 '*les données concernées ont été communiquées illégalement au*' (traduction libre)
196 '*indépendamment de la volonté du*' (traduction libre)
197 '*pour*' (traduction libre)

pour la première fois une légère diminution. Selon les responsables MRD de la VSSE et du SGRS, la pandémie de COVID n'a eu aucun impact sur le nombre de méthodes particulières de renseignement mises en œuvre.

- La VSSE continue de se tailler la part du lion, avec 91,5 % des méthodes mises en œuvre. En d'autres termes, moins d'1 méthode sur 10 est mise en œuvre par le SGRS.
- Une ventilation de ces chiffres permet de constater que l'augmentation du nombre de méthodes spécifiques par le SGRS se poursuit, passant de 138 à 146. Le nombre de méthodes exceptionnelles mises en œuvre connaît toutefois une forte diminution d'environ un tiers, passant de 76 à 51. À la VSSE, on observe la tendance inverse, c'est-à-dire une diminution remarquable de l'utilisation des méthodes spécifiques (de 1781 en 2019 à 1629 en 2020) et une nouvelle hausse sensible de l'utilisation des méthodes exceptionnelles de 14 % par rapport à 2019.
- En ce qui concerne les méthodes ordinaires qui consistent à adresser une réquisition à des opérateurs afin d'identifier certains moyens de communication, on note de nouveau une diminution d'environ 9 %, que soit pour la VSSE ou le SGRS.
- On peut encore noter que les MRD mises en œuvre dans le cadre des menaces 'terrorisme' et 'extrémisme' ont connu une hausse sensible, au détriment de la menace 'ingérence', qui a diminué de moitié.
- Dans le contexte de la mise en œuvre des méthodes particulières de renseignement, le SGRS s'est surtout concentré sur les menaces 'terrorisme' et 'extrémisme', au détriment de la menace 'ingérence', qui a diminué de moitié. La VSSE a, quant à elle, focalisé son attention sur le 'terrorisme', suivi par la menace 'espionnage'.
- Le Comité a été saisi dans 11 dossiers, à savoir 2 saisines d'initiative et 9 saisines de plein droit, après la suspension décidée par la Commission BIM pour illégalité (art. 43/4 L.R&S). Les illégalités concernaient notamment une motivation insuffisante, une notification tardive de la Commission BIM, ou encore un objet imprécis.
- En 2020, pour la première fois depuis l'entrée en vigueur de la Loi MRD du 4 février 2010, le Comité permanent R a posé une question préjudicielle à la Cour constitutionnelle concernant la législation MRD.

CHAPITRE III

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

III.1. LES COMPÉTENCES DU SGRS ET LA MISSION DE CONTRÔLE DU COMITÉ PERMANENT R[198]

Dès 2017, la compétence du Service Général du Renseignement et de la Sécurité (SGRS) a été élargie dans le cadre des interceptions de sécurité.[199] Les interceptions pouvaient alors porter sur des communications *'émises ou reçues à l'étranger'*. Cette possibilité vaut pour presque toutes les missions du SGRS. Il est d'ailleurs intéressant d'observer que les descriptions des missions ont, elles aussi, été élargies. Le législateur a en même temps introduit deux autres méthodes, à savoir l'intrusion dans un système informatique' (art.44/1 L.R&S) et la prise d'images animées' (art.44/2 L.R&S). Par ailleurs, la manière dont le Comité peut contrôler ces méthodes a été modifiée.

Le contrôle *préalable* aux interceptions, prises d'images fixes ou animées s'effectue sur la base d'une liste établie annuellement.[200] Cela signifie qu'en plus du plan annuel d'interceptions, le SGRS doit également élaborer un plan d'intrusions et d'images.[201] Le SGRS doit envoyer ces listes au ministre de la Défense au mois de décembre pour autorisation. Le ministre prend une décision endéans les dix

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

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

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

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

jours ouvrables et doit la communiquer au SGRS[202], qui transmet à son tour les listes pourvues de l'autorisation ministérielle au Comité permanent R.[203]

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

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

Que peut faire le Comité permanent R en cas d'irrégularité ? L'article 44/4 L.R&S stipule que, '*le Comité permanent de contrôle des services de renseignement, sans préjudice des autres compétences attribuées à ce Comité par la loi du 18 juillet 1991, a le droit de faire cesser des interceptions, intrusions ou prises d'images en cours lorsqu'il apparaît que celles-ci ne respectent pas les dispositions légales ou l'autorisation [ministérielle]. Il ordonne l'interdiction d'exploiter les données recueillies illégalement et leur destruction, selon les modalités à fixer par le Roi.*' Malgré la recommandation pressante du Comité[204], un tel arrêté d'interception n'a toujours pas été pris.[205] Aussi, le Comité recommande une nouvelle fois de le faire au plus vite.

---

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

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

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

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

III.2. LES CONTRÔLES EFFECTUÉS EN 2020

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

Le Comité permanent R a reçu, de manière fractionnée, l'ensemble des plans relatifs aux interceptions, intrusions et prises d'images. Ainsi, même si le plan relatif aux interceptions et à la prise d'image a fait l'objet d'une approbation du ministre de la Défense début janvier 2020, ceux-ci n'ont été transmis au Comité permanent R qu'en juin 2020, et ce après plusieurs rappels. Quant au plan relatif aux intrusions, il n'avait pas été transmis au ministre pour approbation à la suite d'un oubli. En réponse à l'interpellation du Comité permanent R, le SGRS a régularisé la situation.

Si le plan relatif aux interceptions n'a fait l'objet que de remarques mineures, le Comité permanent R a insisté pour que les plans futurs relatifs aux prises d'images et aux intrusions soient conformes aux prescrits légaux. Le Comité a suggéré que les sections concernées s'inspirent du plan d'interceptions.

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

En 2020, le Comité a visité les installations d'où sont effectuées les interceptions. Lors de la visite, la conformité du '*logbook*' avec les lois et les directives en la matière a notamment été vérifiée. Le Comité permanent R a constaté à cette occasion que le SGRS avait ouvert un nouveau registre et que celui-ci ne correspondait plus aux recommandations du Comité. Le Comité permanent R a également pu constater que le SGRS poursuivait la mise en œuvre des projets relatifs à l'application de l'article 44 L.R&S.

Malgré les restrictions imposées par la crise sanitaire, le Comité permanent R a poursuivi, en 2020, ses démarches vis-à-vis du SGRS dans le cadre du contrôle des activités liées à l'article 44 L.R&S. Ainsi, en fin d'année, une réunion de travail a été organisée au SGRS avec l'ensemble des acteurs impliqués dans la mise en œuvre dudit article. Cette réunion a permis de clarifier certains points d'attention et de tendre vers une standardisation des différents plans.

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

Le Comité a reçu douze '*listes mensuelles des pays ou des organisations ou institutions ayant effectivement fait l'objet d'une écoute, d'une intrusion ou d'une prise d'images durant le mois écoulé*' et qui justifient '*la raison pour laquelle l'écoute, l'intrusion ou*

la prise d'images a été effectuée en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5°.

Le Comité permanent R a donc reçu l'ensemble des listes légalement prévues. La forme et le contenu de ces listes font l'objet d'une enquête de contrôle qui a été ouverte en 2019.

CHAPITRE IV
MISSIONS PARTICULIÈRES

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

IV.1. CONTRÔLE DES ACTIVITÉS DU BATAILLON ISTAR

La création du Bataillon ISTAR *(Intelligence Surveillance Target Acquisition and Reconnaissance)* répondait à un besoin sans cesse croissant de capacités *battlefield intelligence* lors des opérations à l'étranger. La Loi organique du 30 novembre 1998 ne reconnaît cependant que deux services de renseignement (art. 2 L.R&S). Par conséquent, le Comité permanent R a signalé au Parlement, au ministre de la Défense et au Chief of Defence (CHOD) que ce bataillon développait, ne serait-ce qu'en partie, des activités de renseignement. La Commission d'enquête parlementaire 'Attentats' avait, elle aussi, insisté sur ce point : '*Bien que la commission d'enquête estime que les missions du Bataillon ISTAR sont importantes pour la sécurité de nos militaires, elle considère que les relations entre celui-ci et le SGRS devraient être réglées formellement par le biais d'un protocole de coopération décrivant clairement de quelle façon et à quelles conditions le Bataillon ISTAR pourrait contribuer à renforcer la position d'informations du SGRS. Il s'indiquerait également dans ce cadre de charger le Comité permanent R du contrôle de cette mission de soutien au Bataillon ISTAR*'.[206]

En l'absence de solutions légales ou structurelles à court terme, une solution provisoire a été trouvée fin mai 2018. Il s'agit en l'occurrence d'un protocole d'accord entre le SGRS et le CHOD[207] qui définit les attributions et les compétences du Bataillon ISTAR en matière de HUMINT et de capacité d'analyse. L'organisation

[206] *Doc. parl.*, Chambre, 2016-17, n° 54-1752/008, 306.

[207] Protocole d'Accord du 24 mai 2018 entre le CHOD et le SGRS concernant la capacité HUMINT et la capacité d'analyse du Bn ISTAR.

d'un contrôle technique et juridique a également été élaborée.[208] Ces missions relèvent du SGRS.

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

Le protocole d'accord initial a été conclu pour une période de deux ans. Mi-avril 2020, une réunion de staff a été organisée en interne à la Défense afin d'envisager une prolongation de deux ans. Le CHOD et le Chef du SGRS ont signé cette prolongation le 19 mai 2020.

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

En 2020, le Comité a reçu plusieurs rapports de contrôle, qui ont montré que le Bataillon ISTAR déployait peu d'activités entrant dans le champ d'application du protocole d'accord susmentionné. Selon le SGRS, les activités de renseignement développées par le Bataillon ISTAR répondaient aux réglementations et directives.[209]

IV.2. CONTRÔLE DES FONDS SPÉCIAUX

La Cour des comptes contrôle la légalité, la légitimité et l'efficacité de toutes les dépenses, y compris, en principe, de toutes les dépenses des services de renseignement. Cependant, vu le caractère sensible de la matière, une partie du budget de la VSSE et du SGRS (à savoir les 'fonds spéciaux' avec des dépenses destinées, par exemple, aux opérations et aux informateurs) n'est pas examinée par la Cour des comptes. Pour la VSSE, le contrôle de ces dépenses est effectué par le directeur de la Cellule politique générale du ministre la Justice. Mi-2018, la Cour des comptes a exprimé son intention de réaliser un contrôle périodique de ces fonds à partir de la clôture des comptes de 2018.[210]

Depuis 2020, le contrôle formel des comptes du SGRS est également effectué par la Cour des comptes, qui peut recourir à l'appui technique du Comité permanent

---

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

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

210 En 2020, le Comité a reçu une copie du contrôle de l'exercice 2018 effectué par la Cour des comptes en 2019. COUR DES COMPTES, *Sûreté de l'État. Contrôle 2019 des fonds spéciaux. Rapport adressé au ministre de la Justice*, 20 mai 2020.

R.[211] Le Comité a ainsi pu « *exercer sa mission avec plus d'attention sur l'utilisation de ces dits fonds* ». Par conséquent, il a été décidé de démarrer une enquête de suivi sur la gestion, l'utilisation et le contrôle des fonds spéciaux (cf. Chapitre I.11.11).[212]

IV.3. CONTRÔLE DU SUIVI DE MANDATAIRES POLITIQUES

La question de savoir si et dans quelle mesure les services de renseignement belges suivent (ou sont autorisés à suivre) des mandataires politiques, et selon quelles règles, conserve toute son actualité.[213]

Depuis début janvier 2018, une nouvelle note de service classifiée 'confidentiel' du 13 décembre 2017 est d'application au sein de la VSSE.[214] Ce service envoie deux types de rapports au ministre de la Justice et au Premier ministre, avec copie au Comité permanent R. Il s'agit, d'une part, de rapports ponctuels sur des mandataires politiques qui contribuent à l'apparition d'une menace et, d'autre part, d'un aperçu trimestriel de l'ensemble des documents dans lesquels des mandataires politiques sont mentionnés.[215] Le ministre de la Justice avait précédemment marqué son accord sur le *'principe de vérifications par le Comité R qui s'avèrent nécessaires conformément à la loi organique du 18 juillet 1991'*.[216]

En exécution des principes figurant dans la note de service susmentionnée, le Comité permanent R a effectivement été le destinataire de deux types de rapports en 2020.

À l'instar de la VSSE, le SGRS a été exhorté à adopter une directive uniforme, assortie de règles claires et univoques quant au recueil, au traitement, à la

---

211 *« 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 ».*

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

213 Question de S. Creyelman au ministre des Affaires étrangères sur 'les dossiers politiques traités par le SGRS' (*Q.R.* Chambre 2019-2020, 24 février 2020, n°12, p. 352, Q. n° 143) ; Question de S. Creyelman au ministre des Affaires étrangères sur 'les dossiers politiques et la Sûreté de l'État' (*Q.R.* Chambre 2019-2020, 24 février 2020, n° 12, p. 352, Q. n° 145).

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

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

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

consultation, au stockage et à l'archivage des informations relatives aux mandataires politiques. Mais en 2020, le Comité n'a toujours reçu aucune information en ce sens. Malgré les demandes répétées, le SGRS ne disposait pas d'une procédure spécifique (SOP) pour traiter cette thématique, pas plus qu'il n'avait défini de procédure pour informer le Comité permanent R.

Étant donné qu'il n'est mentionné nulle part ce que le Comité permanent R est censé faire des informations reçues de la VSSE, il a pris l'initiative d'élaborer une méthodologie autour de la 'problématique du suivi des mandataires politiques par les services de renseignement et le rôle du Comité permanent R'. Cette méthodologie a été approuvée par la Commission parlementaire de suivi en 2020. Toujours en 2020, le suivi de mandataires politiques a fait l'objet d'une enquête de contrôle (périodique) (cf. Chapitre I.11.12).

CHAPITRE V

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

V.1. INTRODUCTION

Le Règlement Général sur la Protection des Données 2016/679 (RGPD)[217] et la Directive 2016/680 (Directive)[218] règlent la manière dont les acteurs publics et privés doivent opérer lorsqu'ils collectent, sauvegardent, conservent et communiquent des données à caractère personnel. Les deux instruments européens ont donné lieu à quelques modifications de loi substantielles au niveau national : en décembre 2017, l'Autorité de protection des données (APD)[219] – qui a succédé à la Commission Vie privée – a été créée et en juillet 2018, une nouvelle Loi relative à la protection des données (LPD) a été votée.[220] Cette loi modifie à son tour la L.Contrôle du 18 juillet 1991. Le Comité permanent R a, en effet, été désigné comme autorité de contrôle compétente pour les traitements de données à caractère personnel qui relèvent de la 'sécurité nationale'.

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

---

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

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

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

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

et de renseignement et de l'Organe de contrôle pour l'analyse de la menace (L.Contrôle).[221]

En 2019-2020, le Comité a développé diverses activités pour pouvoir assumer cette mission et ces obligations supplémentaires. Dès 2018, un *Data Protection Officer* (DPO) a été désigné pour tous les traitements effectués par le Comité qui ne relèvent pas de la 'sécurité nationale' (par ex., les traitements dans le cadre de la gestion du personnel et de la logistique)(*infra* XI.2). En outre, différentes réunions ont été organisées avec les trois autres autorités de contrôle compétentes (*infra* V.2.). Les Comités permanents R et P se sont mis d'accord pour élaborer une proposition de modification de la L.Contrôle. En effet, diverses dispositions ne sont pas adaptées à la nouvelle compétence des deux Comités. Pour le surplus, le Comité a également poursuivi ses discussions en interne, et ces réflexions ont donné lieu à un premier commentaire général, qui pourra contribuer à l'exercice prochain d'évaluation de la LPD[222] (*infra* V.7). Enfin, le Comité poursuit l'élaboration de plusieurs processus de travail internes dans le cadre de sa fonction d'avis et en ce qui concerne l'examen des requêtes introduites par des citoyens. Quant à ces dernières, d'ailleurs, il a pu constater une augmentation de sa charge de travail.

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

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

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

221 Pour plus de détails, voir COMITÉ PERMANENT R, *Rapport d'activités 2018*, 75-86.
222 Voir l'article 286 LPD.

banques de données communes visées à l'article 44/11/3*bis* de la Loi sur la fonction de police (LFP) (article 44/11/3*quinquies* LFP).

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

Les autorités de contrôle compétentes ont l'obligation de coopérer étroitement, et coopèrent effectivement, entre autres en ce qui concerne le traitement des plaintes, les avis et les recommandations qui touchent aux compétences de deux ACC ou plus, et ce par souci de cohérence dans l'application de la réglementation nationale, européenne et internationale en matière de protection des données (art. 54/1 § 1er Loi APD). Cette disposition prévoit aussi que le traitement conjoint des plaintes, des avis et des recommandations doit se faire sur la base du principe du guichet unique qui sera assumé par l'Autorité de protection des données. Par ailleurs, les ACC doivent conclure un protocole afin de réaliser la coopération requise. En 2019, les différents services ont élaboré et négocié un protocole, qui a été adopté en 2020 et publié.[223]

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

V.3.1. LE CADRE DU CONTRÔLE DE BELPIU

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

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

223 Voir https://www.comiteri.be/images/pdf/publicaties/samenwerkingsprotocol_DPAS_FR_2020_11_24.pdf.

visés les traitements effectués par la VSSE et le SGRS dans le cadre de leur mission de renseignement régulière. Le Comité est uniquement compétent pour contrôler le fonctionnement de l'IUP dans la mesure où cette unité prête son concours aux demandes d'informations et de renseignements émanant d'un des deux services de renseignement, et ce indépendamment de la forme de ces demandes (recherches ciblées, '*watchlists*' ou profils).

V.3.2. RÉSULTAT DU CONTRÔLE CONCOMITANT

Compte tenu de leurs compétences respectives en leur qualité d'autorité de contrôle compétente en matière de traitement de données par l'Unité d'Information des Passagers, l'Organe de contrôle de l'Information policière (C.O.C.) et le Comité permanent R ont pris l'initiative d'effectuer une visite de contrôle concomitante à ce service. En effet, si les compétences des deux services ne sont pas tout à fait identiques, au moins elles se recoupent.[224] La visite ne faisait pas suite à une plainte (individuelle) ni à des indications (concrètes) de non-respect de la loi et de la réglementation.

Son approche mettait l'accent sur le '*compliance based*' : le traitement de données des passagers est-il conforme à la loi et une norme de sécurité élevée est-elle appliquée ? La visite se concentrait plus sur la sécurité de l'information que sur les aspects juridiques.[225]

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

Le rapport d'enquête a été finalisé en juin 2020 et présenté à la Commission parlementaire de suivi. Le Comité s'attellera en 2021 à la vérification, avec le C.O.C., du suivi qui aura été donné par BELPIU aux recommandations émises à l'issue de cette enquête.

Les principales conclusions, en ce qui concerne la compétence du Comité permanent R, ressortent de l'exercice concomitant des compétences du Comité et du C.O.C. en matière de sécurité de l'information. Les éléments essentiels relatifs au traitement de données s'inscrivant dans le cadre d'une finalité de renseignement seront traités dans le cadre de l'enquête de contrôle initiée en 2018 sur '*l'application*

---

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

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

et le contrôle interne des services de renseignement des méthodes et instruments récemment insérés ou adaptés par le législateur et dont un rôle de contrôle spécifique a été attribué au Comité permanent R'.

En substance, pour ce qui concerne la sécurité de l'information, le Comité et le C.O.C. ont globalement apprécié l'approche structurée de la protection des données et de la sécurité de l'information, en particulier pour les initiatives et conseils du *Data Protection Officer*. Le Comité et le C.O.C. ont néanmoins pu identifier une série de points d'attention ayant trait à l'organisation de la sécurité de l'information (finalisation et validation d'une analyse d'impact relative à la protection des données et d'un plan d'action liés, élaboration d'un processus adéquat de gestion des incidents, etc.). Une attention particulière a également été réservée à un incident lié à la création et à l'usage d'utilisateurs privilégiés, nécessitant une enquête plus approfondie. Le Comité et le C.O.C. ont également mis en lumière un problème lié au respect du principe de '*closed-box*'[226] bien que juridiquement, ce concept n'ait pas été compromis par BELPIU. Ces constatations ont fait l'objet de recommandations qui seront reprises dans le chapitre XII du présent rapport d'activités.

V.4. LES AVIS

Le Comité peut rendre un avis *'sur un projet de loi, d'arrêté royal, de circulaire, ou sur des documents de toutes natures exprimant des orientations politiques des ministres compétents'* dans deux cas : lorsque la loi impose son avis ou à la demande de la Chambre des représentants ou du Ministre compétent (art. 33, alinéa 8 L. Contrôle). Ce genre d'avis porte spécifiquement sur la problématique du traitement de données et doit donc être distingué de la compétence d'avis générale qui porte, par exemple, sur l'efficacité et la coordination (cf. Chapitre VII. Avis). Cette compétence d'avis générale est, en ce sens, plus large, tout en étant plus restreinte puisque limitée au fonctionnement des services de renseignement et de l'OCAM.

En 2020, le Comité a rendu quatre avis en cette qualité, dont deux portent sur l'échange d'informations classifiées[227] et deux autres sur l'approche administrative et la création d'une Direction chargée de l'évaluation de l'intégrité des pouvoirs

---

226 Ce principe renvoie à l'*Operational Travel Intelligence Room* (OTIR), à savoir un espace confiné du SPF Intérieur où les membres détachés ont accès à la banque de données des passagers. Il s'agit d'un espace hermétiquement fermé aux tiers et aux personnes non autorisées, qui n'est accessible qu'à un nombre limité de personnes spécifiquement désignées. L'accès à la banque de données passagers est lié à l'exécution d'une mission spécifique par le membre détaché de l'UIP. Ce dernier n'a accès qu'aux données des passagers relatives à la ou aux affectations de son service, et ce sur la base de profils d'accès individuels.

227 Des avis en ce sens avaient déjà été rendus en 2019 sur l'échange d'informations classifiées avec la République de Chypre, la Hongrie, la République de Finlande et le Royaume d'Espagne.

publics, soit en tant qu'autorité de contrôle exclusivement compétente, soit en tant qu'autorité conjointement compétente avec le Comité permanent P[228] :

— Avis 001/CPR-ACC/2020 du 26 août 2020 portant sur une demande d'avis du président de l'Autorité nationale de sécurité concernant le '*projet de loi portant assentiment à l'accord entre le Royaume de Belgique et la République italienne sur la protection mutuelle des informations classifiées, fait à Rome le 31 janvier 2017*'.
— Avis 002/CPR-ACC/2020 du 26 août 2020 portant sur une demande d'avis du président de l'Autorité nationale de sécurité concernant le '*projet de loi portant assentiment à l'accord entre le Royaume de Belgique et la République française sur la protection mutuelle des informations classifiées, fait à Paris le 11 juillet 2017*'.
— Avis 001/CPR-ACC/2020 du 30 octobre 2020 concernant une '*proposition de loi modifiant diverses dispositions concernant l'approche administrative et portant création d'une Direction chargée de l'évaluation de l'intégrité des pouvoirs publics*', VSSE et SGRS ;
— Avis commun 003/CPR-CPP-ACC/2020 du 17 septembre 2020 concernant une '*proposition de loi modifiant diverses dispositions concernant l'approche administrative et portant création d'une Direction chargée de l'évaluation de l'intégrité des pouvoirs publics*', OCAM.

V.5. LES INFORMATIONS DES SERVICES CONTRÔLÉS

Les services contrôlés par le Comité permanent R doivent tenir ou mettre à sa disposition toute une série de données[229]. Le responsable du traitement doit, par exemple, notifier toute brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques dans les meilleurs délais et si possible, 72 heures après en avoir pris connaissance (articles 89, 122, 155 et 180 LPD). En 2020, aucune brèche de sécurité ('*data breach*')[230] n'a été signalée au Comité.

Le Comité a mis à disposition via son site internet un formulaire permettant de notifier avec la précision nécessaire les brèches de sécurité.[231] Ce formulaire

228 Voir *in extenso* sur le site du Comité permanent R.

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

230 Article 26, 11° LPD : « *"brèche de sécurité" : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données* ». En pratique et en droit hors du contexte de la LPD, il est plutôt fait référence à des « violations de données » ou « *data breaches* ».

231 https://www.comiteri.be/images/pdf/FormDB_fr.pdf.

souligne notamment que les notifications qui ne sont pas effectuées par son intermédiaire ne sont pas enregistrées comme une notification d'une brèche de sécurité, mais tout au plus comme une question ou une réclamation.[232]

V.6. LE TRAITEMENT DES REQUÊTES INDIVIDUELLES

Le Comité permanent R traite également les requêtes individuelles relatives aux traitements de données à caractère personnel par les personnes et les services susmentionnés ainsi que leurs sous-traitants (art. 34 L.Contrôle et articles 79, 113, 145 et 173 LPD). Le requérant est en droit de demander la rectification ou la suppression de données à caractère personnel inexactes le concernant. Et il peut demander à ce que le respect des règles qui sont d'application en matière de protection des données soit vérifié. Il peut encore se plaindre de l'éventuel non-respect des règles de protection des données par un responsable du traitement relevant de la compétence du Comité.

Pour être recevable, une requête doit être écrite, datée, signée et motivée (art. 51/2 L.Contrôle).[233] Si la requête est manifestement non fondée, le Comité peut décider de ne pas y donner suite. Cette décision doit être motivée et communiquée par écrit au requérant.[234]

Le tableau suivant donne un aperçu des dossiers traités (ouverts et/ou clôturés) en 2020. Les colonnes du tableau ventilent les requêtes selon que la compétence du Comité permanent R est exclusive ou conjointe avec d'autres autorités de contrôle.[235]

---

232 Il n'existe par conséquent aucune garantie que la communication d'informations par des canaux alternatifs sera enregistrée et examinée en tant que notification d'une brèche de sécurité.

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

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

235 Le tableau n'indique donc pas les hypothèses dans lesquelles une coopération a pu se réaliser avec une autre autorité de contrôle, le C.O.C. par exemple, lorsque les compétences de chaque autorité de contrôle sont distinctes.

Le traitement des requêtes individuelles[236]

2020	Comité permanent R	Comités permanent R et P	Comités permanents R et P, et C.O.C.	Total
1. Dossier ouvert en 2018	1	0	0	1
2. Dossiers ouverts en 2019	4	0	0	4
3. Dossiers ouverts en 2020	17	1	3	21
4. Interférence concrète alléguée avec les droits et libertés	15	1	2	17
5. Pas d'interférence concrète alléguée avec les droits et libertés	7	0	1	8
6. Dossiers en cours	7	1	3	11
7. Dossiers clôturés	15	0	0	15
8. Requête irrecevable	1	0	0	1
9. Traitement conforme à la LPD	14	-	-	14
10. Traitement non conforme à la LPD	-	-	-	0
11. Total des requêtes	22	1	3	26

En bref, le tableau concerne au total 26 dossiers. Parmi ceux-ci, 11 dossiers sont toujours en cours et 15 dossiers ont été clôturés. Un de ces dossiers a été considéré comme irrecevable et les 14 autres ont donné lieu au constat que le traitement de données était réalisé conformément à la LPD. Dans les dossiers recevables et clôturés, les plaignants ont systématiquement été informés que les vérifications requises avaient été effectuées.

[236] Les lignes 1 à 3 établissent le décompte des dossiers selon l'année de leur ouverture. Les lignes 4 et 5 les répartissent selon que la personne concernée allègue ou pas une interférence concrète liée au traitement de données par le responsable du traitement, dans ses droits et libertés. Il en serait par exemple ainsi dans le cadre d'une procédure de déclaration de nationalité à l'occasion de laquelle un service de renseignement communique des informations au Ministère public, lorsque la personne concernée allègue faire l'objet de contrôles régulier de police, lorsqu'elle constate que l'accès à un territoire lui est refusé, lorsque des données d'un service de renseignement ont été utilisées dans une procédure judiciaire pénale, etc. Les lignes 6 et 7 précisent l'état d'avancement des dossiers en 2020 (clôturés ou toujours en cours). Enfin, les lignes 8 à 10 organisent les dossiers clôturés selon leur résultat (constatation de conformité ou non à la LPD – nb : l'absence de traitement de données à caractère personnel est comptabilisée comme un traitement de données conforme à la LPD).

Il peut être relevé que dans 70 % des requêtes, les personnes concernées allèguent[237] une interférence concrète dans leurs droits et libertés causée par, ou en tout cas liée à, un traitement de données d'un responsable du traitement relevant de la compétence du Comité permanent R. Une telle interférence existerait par exemple dans le cadre d'une procédure de déclaration de nationalité à l'occasion de laquelle un service de renseignement communique des informations au Ministère public, lorsque la personne concernée allègue faire l'objet de contrôles réguliers de police, lorsqu'elle constate que l'accès à un territoire lui est refusé, lorsque des données d'un service de renseignement ont été utilisées dans une procédure judiciaire pénale, etc.

Les 30 % restant de requêtes se composent de demandes d'exercice indirect de droits, sans précision particulière ou grief concret. Typiquement, la personne concernée se demande si des données sont traitées à son sujet et si le traitement de celles-ci est conforme à la réglementation applicable (accès indirect).

Ce constat n'est pas surprenant dès lors que la réponse fournie à la personne concernée exerçant ses droits ne lui apprend rien sur ce qu'il en est du traitement (éventuel) des données à caractère personnel la concernant par les services relevant de la compétence du Comité. Ce n'est que lorsque la personne concernée suspecte ou subit concrètement l'effet d'un tel traitement de données qu'elle verra un intérêt à s'adresser au Comité permanent R pour qu'il réalise les vérifications nécessaires, dans l'espoir d'obtenir une amélioration de sa situation.

V.7. ÉVALUATION DE LA LOI RELATIVE À LA PROTECTION DES DONNÉES

L'article 286 LPD dispose que la Loi relative à la protection des données doit être soumise à une évaluation conjointe des ministres compétents dans le courant de la troisième année après son entrée en vigueur. Dans ce contexte et compte tenu de l'expérience nouvelle qu'il vient d'acquérir en tant qu'autorité de contrôle, le Comité formule les recommandations suivantes à l'égard du législateur.

Le Comité permanent R est conscient du rôle clé qu'il joue, en tant qu'autorité de contrôle, dans domaine de la protection des données au sein de celui de la sécurité nationale. Ce dernier jouissant d'un cadre législatif moins contraignant dans lequel les droits de personnes concernées sont particulièrement limités, le Comité en devient un acteur incontournable de l'effectivité des règles de protection des données.

---

237 Il est à noter que dans plusieurs dossiers, ces interférences ne sont pas seulement alléguées par les personnes concernées mais bien étayées par elles et avérées (s'agissant par exemple, de la communication de notes d'analyse dont dispose les personnes concernées dans le cadre des procédures où ces notes sont utilisées par les autorités publiques). Dans d'autres cas, ces allégations sont des suspicions, plus ou moins, voire non, étayées en fait.

C'est principalement dans l'optique d'une telle effectivité que ont été formulées ces recommandations.

V.7.1. COMMUNIQUER UTILEMENT VERS LES PERSONNES CONCERNÉES

Force est de constater que quelle que soit l'ampleur et le résultat du contrôle opéré par le Comité, la personne qui introduit une plainte ou exerce ses droits de manière indirecte auprès du Comité doit systématiquement se satisfaire d'une réponse sibylline : « *il a été procédé aux vérifications nécessaires* ».[238]

Or il ne peut être exclu, *a prioiri* et en toute hypothèse, qu'il puisse être légitime et indiqué de communiquer malgré tout certaines informations à la personne concernée.

Le législateur s'est, par exemple, déjà prononcé en ce sens dans le domaine de compétence originel du Comité. Ainsi, dans le cadre du traitement des plaintes et dénonciations, le Comité, lorsqu'une enquête est clôturée, peut (voire *doit*) communiquer le résultat de celle-ci 'en termes généraux'.[239] Quant au C.O.C., qui exerce également sa compétence d'autorité de contrôle dans le domaine de l'information policière, nécessitant une certaine confidentialité, il *peut*, dans le cadre de l'exercice indirect de leurs droits par les personnes concernées, « *communiquer à la personne concernée certaines informations contextuelles* ».[240]

Le Comité permanent R recommande au législateur de prévoir, dans certains cas, la possibilité d'une communication de certaines informations à l'attention de la personne concernée dans le cadre du Titre 3 de la LPD.

V.7.2. VÉRIFIER L'APPLICATION DES RÈGLES DE PROTECTION DES DONNÉES AU MOMENT OPPORTUN

Le Comité permanent R fait remarquer qu'il peut être consulté par des personnes impliquées ou en phase d'être impliquées dans des procédures civiles judiciaires ou administratives (par ex., processus de naturalisation, mesures d'ordre, etc.) au cœur de la résolution desquelles peuvent se trouver des analyses ou données émanant d'un service de renseignement ou de l'OCAM.

Le Comité considère que dans de telles hypothèses, lorsque les différends entrent dans une phase contentieuse, le législateur pourrait envisager que le juge compétent, confronté à une contestation sérieuse des données utilisées devant

238 Article 80, al. 2 LPD ; article 34, al. 6 L.Contrôle.
239 Article 34, al. 6 L.Contrôle.
240 Articles 42, al. 3, et 43, al. 3 LPD. Un arrêté royal est toutefois attendu afin de déterminer les catégories d'informations contextuelles qui peuvent être communiquées à la personne concernée.

lui, puisse, s'il l'estime nécessaire (et le cas échéant, à la demande de la personne concernée uniquement), suspendre sa cause. Le juge compétent peut ensuite interroger le Comité permanent R via un mécanisme juridique du type de la question préjudicielle, afin que le Comité puisse réaliser les vérifications nécessaires et lui transmettre un avis.

V.7.3. UNE MEILLEURE COORDINATION DES COMPÉTENCES CONJOINTES OU CONCOMITANTES ENTRE AUTORITÉS DE CONTRÔLE COMPÉTENTES

Dans la manière dont il a défini le champ d'application des règles de protection des données belges ainsi que les compétences des ACC belges, le législateur a choisi d'utiliser principalement un critère organique. En termes simplifiés, on peut dire que l'Organe de contrôle de l'information policière est compétent pour la police intégrée, l'APD pour le secteur privé et le Comité permanent R pour la VSSE et le SGRS.

À côté de ces hypothèses plutôt claires de répartition des compétences, le législateur a aussi prévu, pour ce qui concerne le Comité permanent R, des hypothèses de compétences conjointes : l'une à propos de l'OCAM (compétence conjointe avec le Comité permanent P),[241] et l'autre à propos des banques de données communes (compétence conjointe avec le C.O.C.).[242] Cela conduit parfois à ce qu'une même demande d'un citoyen concernant le fonctionnement de l'OCAM donne lieu à deux vérifications distinctes : une première conjointement au C.O.C. sur le rôle de l'OCAM dans le cadre des banques de données communes, et une seconde conjointement au Comité permanent P sur les autres aspects du fonctionnement de l'OCAM.

Les compétences peuvent aussi être concomitantes, en ce que la compétence de chaque autorité de contrôle séparément est juridiquement exclusive mais, en pratique, s'exerce au moins pour partie concomitamment, de telle sorte que l'une pourrait difficilement agir sans l'autre (notamment au risque de soumettre un responsable du traitement à des injonctions contradictoires). La visite concomitante de BELPIU effectuée par le C.O.C. et le Comité permanent R en est une illustration (*supra* V.3.2.).

Ces compétences conjointes ou concomitantes découlent du caractère hybride des institutions (OCAM, BELPIU) ou systèmes d'information concernés (banques de données communes et banque de données passagers), qui impliquent à la fois, le cas échéant à des degrés divers de responsabilité, des entités constitutives relevant en principe de la compétence (organique) de l'une ou l'autre autorité de contrôle.

---

241 Voir l'article 161 LPD ainsi que le Sous-titre 4 du Titre 3 LPD.

242 Voir les articles 44/11/3*bis* à 44/11/3*quinquies*/2 LFP.

Cette situation illustre qu'une « logique organique » de l'applicabilité des règles de protection des données, comporte aussi sa part de complexité et en conséquence, de possibles lourdeurs administratives qui pourraient être une source réelle d'inefficacité. Autrement dit, un critère organique n'est pas plus la panacée que ne l'est un critère de finalité auquel le législateur aurait également pu recourir et dont il sera encore question plus loin.

Par souci d'efficacité, le Comité permanent R recommande au législateur de n'attribuer aux autorités de contrôle compétentes que des compétences exclusives claires et cohérentes.

V.7.4. CLARIFIER LES RÈGLES DE PROTECTION DES DONNÉES APPLICABLES AUX AUTORITÉS DE CONTRÔLE COMPÉTENTES DANS LE SECTEUR DE LA SÉCURITÉ NATIONALE

L'intention du législateur était clairement que le Titre 3 de la LPD régit le secteur de la sécurité nationale (VSSE, OCAM, SGRS, etc.) et consacre en son sein, de manière autonome et exclusive, les règles de protection des données applicables à ce secteur. Ces règles sont définies sur la base du standard international que constituent la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son Protocole additionnel, récemment modernisés en « Convention 108+ » (signée le 10 octobre 2018 par la Belgique mais pas encore ratifiée).[243]

Le Sous-titre 6 du Titre 3 de la LPD, qui vise les règles de protection des données notamment applicables au Comité permanent R et la Commission BIM en tant que responsables du traitement, est excessivement lacunaire.

À cet égard, le Comité permanent R recommande au législateur de définir clairement le régime de protection des données applicable au Comité et à la Commission BIM dans l'exercice de leurs fonctions dans le domaine de la sécurité nationale. Ce régime juridique devrait être ancré dans le Titre 3 de la LPD et adapté aux spécificités des institutions susmentionnées. À ce propos, le législateur peut s'inspirer des règles de protection des données applicables aux services de renseignement et de sécurité. C'est dans cet esprit que l'actuel Sous-titre 6 du Titre 3 du CPC a été rédigé.

---

243 Voir à ce sujet : https://www.coe.int/fr/web/data-protection/convention108-and-protocol. Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 128e Session du Comité des Ministres, Elseneur, Danemark, 17-18 mai 2018.

V.7.5. PERMETTRE AU COMITÉ PERMANENT R D'ADOPTER DES AVIS D'INITIATIVE

Le législateur n'a pas permis au Comité de pouvoir adopter des avis d'initiative, contrairement aux possibilités qui sont ouvertes à l'APD et le C.O.C.[244] Sauf si la loi l'impose, le Comité permanent R ne peut rendre un avis que lorsqu'il est sollicité par la Chambre des représentants ou par le Ministre compétent. Alors qu'il ne peut être exclu qu'à l'occasion de l'exercice de sa compétence, le Comité permanent R identifie des textes ou pratiques surannés au sujet desquels il souhaiterait pouvoir attirer l'attention par voie d'avis, indépendamment de l'existence ou non, d'un processus législatif les impliquant.

V.7.6. AMÉLIORER LA SÉCURITÉ JURIDIQUE DANS LE RÉGIME DE PROTECTION DES DONNÉES APPLICABLE AU DOMAINE DE LA SÉCURITÉ NATIONALE

Le droit belge de la protection des données à caractère personnel est rédigé d'une manière complexe, ce qui nuit à sa lisibilité. Or il s'agit d'un domaine où la clarté des textes est une exigence constitutionnelle et conventionnelle.

Le Comité permanent R souhaite tout d'abord mettre en évidence le caractère déterminant qui pourrait, selon lui, être reconnu à la finalité des traitements de données, dans la détermination des règles applicables en matière de protection des données. En droit positif, pour partie du moins, le législateur régit en effet la compétence des autorités de contrôle sur la base d'un critère organique. Or c'est la finalité d'un traitement de données qui devrait déterminer si celui-ci tombe ou pas dans le champ d'application d'un Titre 3 complet, en ce qu'il concerne la sécurité nationale, notamment compte tenu du fait que d'autres acteurs que les services de renseignement sont également impliqués dans le cycle du renseignement.

Ensuite, dans un même objectif de clarté et de sécurité juridique, le Comité permanent R relève que les critères prévus pour identifier le responsable du traitement sont une source d'insécurité juridique. Pour ce qui concerne le domaine de la sécurité nationale, le législateur pourrait, dans la LPD, identifier le ou les responsables du traitement conjoints[245] compte tenu de leurs responsabilités concrètes au regard de ces missions et de leur relative autonomie, voire de leur indépendance.

---

244 Voir l'article 23, § 1er Loi APD et l'article 236, § 2 LPD.

245 Dans le domaine des banques de données communes, le législateur a, par exemple, réparti les responsabilités entre entités concernées, voir notamment l'article 44/11/3*bis* LFP.

V.7.7. DIMENSION INTERNATIONALE DES TRAITEMENTS DE DONNÉES

Dans la déclaration commune de Berne,[246] le Comité permanent R et certains de ses homologues ont souligné les limites de leurs mandats de contrôles respectifs *nationaux*. S'en est suivie l'adoption d'une *Charter of the Intelligence Oversight Working Group* et la création d'un *Oversight Working Group*.[247]

Mutatis mutandis, un constat similaire vaut dans le cadre de la protection des personnes physiques à l'égard du traitement de données à caractère personnel.

Dans ce contexte, le Comité permanent R attire l'attention du législateur sur la ratification prochaine de la Convention 108+ qui met en place un mécanisme de coopération et d'entraide entre Parties. Contrairement aux mécanismes de coopération de droit européen (de l'Union européenne), cet instrument international couvrira les traitements à finalité sécurité nationale. Afin de mettre en œuvre ce mécanisme, l'article 16, 2., a) prévoit que chaque Partie désigne une ou plusieurs autorités de contrôle au sens de l'article 15 de la Convention 108+.

Or en l'état du droit, l'article 55, § 1er, de la loi APD dispose que « *(l)'Autorité de protection des données peut collaborer avec toute instance ou autre autorité de protection des données d'un autre État en faisant usage des pouvoirs qui lui sont conférés soit en vertu du Règlement 2016/679 soit par la législation nationale* ».

Eu égard à l'indépendance des deux institutions, l'APD et le Comité permanent R, en tant qu'autorité de contrôle compétente, le Comité recommande au législateur d'attribuer au Comité, compte tenu des règles régissant son activités (y compris la L.C&HS), une compétence exclusive et propre en matière de coopération internationale dans le domaine de la protection des données dans le secteur du renseignement.[248]

Au-delà de cette question de la coopération internationale en tant que telle, la dimension internationale des flux de données entraîne également *au niveau des services belges*, une perte de maîtrise des données qui sortent de la juridiction belge, suite à des flux de données transfrontières.

---

246 Renforcement du contrôle des échanges internationaux de données entre les services de renseignement et de sécurité », 22 octobre 2018.

247 Voir https://www.comiteri.be/images/pdf/Charter_Intelligence_Oversight_Working_Group_signed_12_December_2019.pdf.

248 Dans le « Protocole de coopération entre les autorités de contrôle fédérales belges en matière de protection des données », les Comités permanents R et P, le C.O.C. et l'APD ont relevé que « *chaque A est libre – dans le cadre de ses compétences spécifiques (par exemple la police, les services de renseignement et de sécurité,…) et sans préjudice de l'article 116 LCA – d'adhérer à un forum/ une institution déterminé(e) ou d'en devenir membre ou de réclamer via l'APD des documents qui correspondent à sa compétence* », considérant n° 36. Toutefois, la L.Contrôle, lorsqu'elle régit dans la section 4 de son chapitre III (« Contrôle des services de renseignement »), les compétences du Comité permanent R en tant qu'autorité de protection des données, n'y prévoit aucune compétence du Comité sur le plan international.

Sur ce point, si le législateur n'a pas choisi de rendre contraignant le principe d' '*accountability*' (de « responsabilité ») à charge des services de renseignement,[249] le Comité permanent R est néanmoins d'avis que certaines modifications des règles relatives aux flux de données transfrontaliers dans le sens d'une '*accountability*' plus grande des services, pourraient renforcer l'effectivité de la protection des données.

Le Comité insiste sur l'importance de ce volet des règles de protection des données. Il convient en effet d'éviter que les données à caractère personnel, une fois transférées par les services de renseignement belges, échappent complètement à leur maîtrise et aient des effets injustifiés (ou qui ne sont plus justifiés) sur les droits et libertés des personnes concernées, à l'étranger. Dans un monde interconnecté où les individus circulent plus facilement et librement, la nécessité de mettre des données à jour par exemple, doit pouvoir être effectivement mise en œuvre dans un contexte international. Bref, la nécessité d'échanger sur la scène internationale, des données en matière de sécurité nationale, va de pair avec la nécessité de mettre en œuvre dans ce contexte aussi, des règles de protection des données efficaces pour les personnes concernées.

[249] À propos de ce principe, voir notamment les articles 5, 2. et 24, 1. RGPD, ainsi que l'article 10, 1. de la Convention 108+.

CHAPITRE VI

LE CONTRÔLE DE BANQUES DE DONNÉES COMMUNES

Les ministres de l'Intérieur et de la Justice ont créé, en 2016, la banque de données commune '*foreign terrorist fighters*' (BDC FTF). Ils lui ont assigné la finalité de contribuer à l'analyse, à l'évaluation et au suivi de personnes en lien avec cette problématique. Cette banque de données commune (BDC) a été modifiée en 2018 : on parle désormais de la banque de données commune '*terrorist fighters*' (BDC TF). Celle-ci comprend, outre la catégorie générale existante des '*foreign terrorist fighters*', une catégorie visant les '*homegrown terrorist fighters*'. Toujours en 2018, une (nouvelle) banque de données commune distincte a été créée pour 'les propagandistes de haine' (BDC PH).[250]

Par un Arrêté royal pris fin décembre 2019[251], deux nouvelles catégories ont été ajoutées à la BDC TF, à savoir les 'extrémistes potentiellement violents' (EPV) ainsi que les 'personnes condamnées pour terrorisme' (PCT).

VI.1. LES PRINCIPALES MODIFICATIONS DE LA RÉGLEMENTATION

L'Arrêté royal du 20 décembre 2019, paru en janvier 2020, poursuit un triple objectif. Le premier est d'ajouter de nouvelles catégories à la banque de données commune TF, à savoir les 'extrémistes potentiellement violents' ainsi que les 'personnes condamnées pour terrorisme'. Le deuxième objectif est d'apporter des 'modifications techniques' aux AR TF et PH suite à la modification de la Loi du 5 août 1992 par la Loi du 22 mai 2019. Enfin, le troisième objectif est de prévoir un accès direct pour l'Administration générale de la Trésorerie du SPF Finances aux banques de données TF et PH.

---

250 L'article 44/6 LFP assigne le contrôle du traitement des informations et des données à caractère personnel contenues dans les BDC à l'Organe de contrôle de l'information policière (C.O.C.) et au Comité permanent R (par la suite, 'les autorités de contrôle').

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

VI.1.1 L'AJOUT DES EXTRÉMISTES POTENTIELLEMENT VIOLENTS (EPV) DANS LA BDC TF

L'extrémiste potentiellement violent est défini comme toute personne physique ayant un lien avec la Belgique qui répond aux critères cumulatifs suivants :

a) elle a des conceptions extrémistes qui justifient l'usage de la violence ou de la contrainte comme méthode d'action en Belgique ;
b) il existe des indications fiables qu'elle a l'intention de recourir à la violence, et ce en relation avec des conceptions extrémistes mentionnées en a) ;
c) en outre, l'EPV doit répondre au minimum à l'une des trois conditions suivantes qui sont considérées comme étant des facteurs de risque quant à l'utilisation de la violence:
   - il entretient systématiquement des contacts sociaux au sein des milieux extrémistes ;
   - il a des problèmes psychiques constatés par un professionnel compétent en la matière ;
   - il a commis des actes ou il présente des antécédents qui peuvent être considérés comme soit a) un crime ou un délit portant atteinte à ou menaçant l'intégrité physique ou psychique de tiers ; soit b) des instructions ou des formations relatives à la fabrication ou l'utilisation d'explosifs, d'armes à feu ou d'autres armes ou substances nocives ou dangereuses, ou pour d'autres méthodes et techniques spécifiques en vue de commettre des infractions terroristes ; soit c) des agissements en connaissance de cause constituant un soutien matériel en faveur d'une organisation d'un réseau terroriste/extrémistes ; soit d) des agissements dont la nature indique un niveau de vigilance préoccupant de l'individu à l'égard de la sécurité.

VI.1.2. L'AJOUT DES PERSONNES CONDAMNÉES POUR TERRORISME (PCT) DANS LA BDC TF

En plus de la catégorie des 'extrémistes potentiellement violents', une seconde catégorie a été ajoutée dans la BDC TF, à savoir les 'personnes condamnées pour terrorisme'. Il s'agit des personnes qui, cumulativement :
- ont un lien avec la Belgique ;
- ont été condamnées ou ont reçu une décision judiciaire d'internement ou, dans le cas de mineurs, fait l'objet d'une mesure de protection pour des infractions terroristes, telles que décrites au Livre II Titre I Ter du Code pénal (en Belgique) ou des faits qualifiés comme tels ou par une infraction équivalente à l'étranger ;

– et des personnes à l'égard desquelles l'OCAM a estimé que le niveau de menace qu'elles représentent se définit comme moyen (niveau 2), grave (niveau 3) ou très grave (niveau 4)

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

VI.1.3. L'ACCÈS DIRECT EN FAVEUR D'UN NOUVEAU SERVICE DANS LES BDC TF ET PH

L'Administration générale de la Trésorerie se voit accorder un accès direct à la BDC TF et PH.[252] Il s'agit de l'autorité compétente en matière de sanctions financières pour le gel des fonds et des ressources économiques des personnes ou entités qui commettent, ou tentent de commettre, des infractions terroristes, les facilitent ou y participent.

VI.2. LA MISSION DE CONTRÔLE ET L'OBJET DU CONTRÔLE

Pour l'année 2020, le Comité permanent R et le C.O.C. ont décidé d'axer leur contrôle conjoint, d'une part, sur la vérification de l'accès direct prévu en faveur de l'Autorité nationale de sécurité (ANS) et, d'autre part, sur le suivi réservé à certaines recommandations formulées dans les rapports des années précédentes.
Par ailleurs, les organes de contrôle ont procédé à un examen approfondi de la coordination du traitement des informations dans la BDC TF et PH, avec notamment une attention particulière pour le rôle du *Data Protection Officer* (DPO). À cet égard, il également a été tenu compte du nombre croissant de services disposant d'un accès à la BDC TF et PH.

Sur le plan méthodologique, compte tenu de la crise sanitaire et afin de permettre aux services de disposer d'un recul suffisant pour la mise en œuvre des recommandations formulées au terme du rapport relatif au contrôle pratiqué en 2019, il a été décidé de prévoir le déroulement de l'enquête durant le quatrième trimestre de l'année 2020. Plusieurs services ont été questionnés, parmi lesquels l'ANS, l'OCAM (responsable opérationnel des banques de données communes), la Police fédérale (gestionnaire technique) ainsi que le *Data Protection Officer* (DPO). L'enquête s'est clôturée par une rencontre avec le Directeur f.f. de l'OCAM ainsi que

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

le DPO des banques de données communes. Le rapport est planifié pour le premier semestre de 2021.

VI.3. LA MISSION D'AVIS

La Loi sur la fonction de police (LFP) prévoit l'obligation de recueillir l'avis conjoint du Comité permanent R et du C.O.C. dans différentes hypothèses.

Ainsi, préalablement à sa création, les ministres de l'Intérieur et de la Justice doivent déclarer la banque de données commune, ainsi que les modalités de traitement, dont celles relatives à l'enregistrement des données, et les différentes catégories et types de données à caractère personnel et d'informations traitées, au Comité permanent R et au C.O.C. À leur tour, le Comité et le C.O.C. doivent émettre conjointement un avis dans les 30 jours à partir de la réception de la déclaration (art.44/11/3*bis* § 3 LFP). Par ailleurs, pour chaque banque de données commune, un arrêté royal délibéré en Conseil des ministres détermine, après avis des deux instances précitées, les règles de responsabilités en matière de protection des données à caractère personnel des organes, services, autorités et organismes traitant des données, les règles en matière de sécurité des traitements, les règles d'utilisation, de conservation et d'effacement des données (art.44/11/3*bis* § 4 LFP). En outre, des modalités complémentaires de gestion des banques de données communes peuvent être déterminées par un arrêté royal délibéré en Conseil des ministres, toujours après un avis du Comité permanent R et du C.O.C. (art.44/11/3*bis* § 8 LFP). Enfin, la fonction d'avis s'exerce également en ce qui concerne tout projet d'Arrêté royal instaurant ou modifiant les accès aux banques de données communes (art.44/11/3*ter* §§ 2 à 4).

Le Comité permanent R et le C.O.C. n'ont pas été sollicités en 2020 dans ce contexte.[253]

[253] Un avis conjoint avait été rendu en 2019 concernant l'A.R. du 20 décembre 2019, paru au Moniteur belge le 27 janvier 2020 (www.comiteri.be).

CHAPITRE VII
AVIS

L'article 33, alinéa 7, L. Contrôle stipule que le Comité *'ne peut rendre un avis sur un projet de loi, d'arrêté royal, de circulaire, ou sur des documents de toutes natures exprimant les orientations politiques des ministres compétents, qu'à la demande de la Chambre des représentants ou du Ministre compétent.*' En 2020, l'avis du Comité a été sollicité à plusieurs reprises.

Par ailleurs, le Comité doit rendre des avis en tant qu'autorité de contrôle compétente (ACC) dans le cadre des traitements de données à caractère personnel ainsi que dans le cadre de la réglementation légale relative aux banques de données communes, et ce conjointement avec l'Organe de contrôle de l'information policière (C.O.C.). Ces deux compétences d'avis sont traitées respectivement au Chapitre V et au Chapitre VI.

VII.1. AVIS CONCERNANT LA PROPOSITION DE LOI RELATIVE À LA DÉCLASSIFICATION AUTOMATIQUE ET AU TRANSFERT DES PIÈCES AUX ARCHIVES DU ROYAUME

En novembre 2019, une proposition de loi visant à fixer des règles générales de déclassification pour les pièces classifiées a été déposée.[254] Cette proposition de loi déterminait de quelle manière et dans quelles circonstances les pièces classifiées doivent être déclassifiées. Ce faisant, elle comble une lacune importante de la législation sur la classification, qui a de lourdes répercussions pour les recherches historiques et pour la transparence des décisions des pouvoirs publics. En effet, la Belgique est l'un des rares pays occidentaux dépourvus d'une procédure de déclassification, les pièces classifiées n'y étant en principe jamais déclassifiées.

En principe, une date de déclassification est d'emblée fixée au moment de la rédaction d'une pièce classifiée. Les pièces déclassifiées des services de renseignement devraient être transférées plus rapidement aux Archives du Royaume. À l'instar des services de renseignement, le Comité permanent R a pu,

254 *Doc. parl.* Chambre 2019-2020, 55-0732/001.

début janvier 2020, donner son avis sur la proposition de loi à Commission de l'Intérieur de la Chambre.[255]

La proposition de loi renfermait deux réglementations qui étaient certes liées, mais qu'il y avait lieu de distinguer clairement : la déclassification automatique et le transfert des pièces aux Archives du Royaume. Les deux réglementations sont indépendantes l'une de l'autre en ce sens que l'archivage ou non des informations peut concerner à la fois des renseignements classifiés et non classifiés, ou inversement, que la déclassification d'une pièce ne signifie pas nécessairement qu'elle peut être archivée. Ce n'est pas parce qu'une pièce n'est plus sensible, qu'elle n'est plus utile à des fins de renseignement. Ce dernier aspect est également très important à retenir : tant qu'une pièce est utile au renseignement, elle ne peut être archivée au sens de la Loi relative aux archives, même si elle a plus de trente ans.

VII.1.1. DÉCLASSIFICATION AUTOMATIQUE

Par le passé, le Comité s'était déjà prononcé en faveur d'une déclassification automatique.[256] Il avait cependant opté pour des délais plus longs que la proposition de loi : pour un document 'SECRET', il avait proposé une déclassification après trente ans ; pour un document 'TRÈS SECRET', après cinquante ans. Ces délais plus longs sont plus réalistes pour les services de renseignement. Selon le Comité, ceci n'empêche pas ce que l'on appelle « l'autorité d'origine » de déclassifier une pièce plus tôt, sur demande ou de sa propre initiative. En outre, il a été suggéré de prévoir un système par lequel le Comité permanent R est désigné comme organe qui, de sa propre initiative ou sur demande, pourrait annuler une classificiation si elle ne répond manifestement pas ou plus aux finalités d'une classification.[257] En tout cas, le Comité ne peut être investi que d'un pouvoir de contrôle marginal, c'est-à-dire un contrôle limité à la question de savoir si la classification même ou sa durée n'est pas manifestement illégale ou déraisonnable. Le Comité ne peut en effet se substituer au pouvoir exécutif, ni mener sa propre politique en la matière.

VII.1.2. ARCHIVAGE

Le Comité a souligné qu'il n'avait aucune observation particulière à formuler concernant la proposition de loi lorsqu'elle prévoit de transférer, sous trois conditions cumulatives, des documents aux Archives du Royaume : il s'agit de documents créés il y a plus de trente ans (au lieu de cinquante ans), non classifiées et qui ont perdu leur utilité administrative.

---

255 L'avis complet est disponible sur www.comiteri.be.
256 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 81 et suiv.
257 COMITÉ PERMANENT R, *Rapport d'activités 2006*, 133.

Mais là n'est pas le plus important. Ainsi, la proposition de loi ne tient pas compte de l'arsenal juridique existant en matière de protection de données à caractère personnel. Qu'il s'agisse de données relatives à des targets, à des citoyens lambda ou encore à des sources, un débat fondamental s'impose sur ces questions. Le Comité estimait dès lors que la proposition de loi devait prendre en considération successivement l'article 21 de la Loi organique des services de renseignement qui prévoit la destruction obligatoire de certaines données à caractère personnel, une disposition similaire de la Loi relative à la classification en ce qui concerne les données à caractère personnel issues des enquêtes de sécurité, avec l'obligation de protéger les sources des services de renseignement à tout moment, mais certainement aussi les (nouvelles) règles de traitement de données à caractère personnel à des fins historiques, scientifiques ou statistiques contenues dans la Loi relative à la protection des données (articles 99 LPD et suiv.).

Enfin, il convenait également d'examiner dans quelle mesure le règlement proposé de déclassification et d'archivage de données sensibles constitue un ensemble logique avec les possibilités offertes par la Loi relative à la publicité de l'administration (LPA). Le Comité insiste dans ce cadre sur l'instauration d'un délai de déclassification suffisamment long, sur la possibilité d'*'overruling'* d'une classification initiale ou prolongée et sur une cohérence avec les réglementations précitées.

VII.2. AVIS RELATIF AU 'RAPPORT DU COMITÉ DE CONCERTATION SUR LA CRÉATION D'UNE BANQUE-CARREFOUR DE LA SÉCURITÉ'

Début février 2020, le Comité a rendu un avis au ministre de la Justice et au ministre de la Sécurité et de l'Intérieur concernant le rapport du comité de concertation sur la création d'une Banque-Carrefour de la Sécurité'.[258] Ce rapport contenait une série d'orientations majeures à prendre par les décideurs politiques concernant la 'Banque Carrefour de la Sécurité' initiée par la Commission d'enquête parlementaire 'Attentats'. La commission d'enquête considérait qu'il était urgent de disposer d'une vision et d'une stratégie globales de l'organisation intégrée de la gestion de l'information, ainsi que d'une coopération loyale de tous les services de police, de justice, de renseignement et de sécurité concernés.[259]

Il était proposé, dans le cadre l'architecture de sécurité, de recourir au système d'une banque-carrefour en tant qu'instrument de gestion intégrée des informations de coordination entre les différents services et instances. Cette banque-carrefour,

---

258 La demande d'avis date du 24 octobre 2019. La demande portait sur un rapport du 'comité de concertation' et ne constituait pas, en tant que tel, un texte réglementaire ou un texte à portée normative.

259 *Doc. parl.* Chambre 2016-2017, 54-1752/008, 251.

à l'instar de la Banque-Carrefour de la Sécurité Sociale et de la plate-forme *e-health*, doit constituer un système efficace de partage électronique et sécurisé de données entre les banques de données électroniques (existantes), qui relèvent de la responsabilité de différentes instances.[260]

Dans son avis, le Comité estimait que ce projet ne pourrait être mis en oeuvre que si l'investissement financier, technologique et humain était garanti de manière pérenne et sans devoir remettre en question les budgets limités des services de renseignement. La création d'une telle banque-carrefour doit répondre à une double garantie : d'une part, la mise en oeuvre d'un système répondant effectivement aux problèmes de gestion de l'information (stockage, traitement et exploitation) et de l'échange de celle-ci, tels que rencontrés préalablement aux attentats de Zaventem et Maelbeek ; d'autre part, la mise en œuvre d'un système garantissant la protection des droits et libertés fondamentaux, la protection des données à caractère personnel, ainsi que d'autres intérêts essentiels tels que la règle du tiers service ou les normes de classification.

VII.3. AVIS CONCERNANT LA PROPOSITION DE LOI EN VUE D'INSTAUTER DES NOTES D'ÉVALUATION POUR LA COLLABORATION AVEC DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ÉTRANGERS

Le cadre juridique de la collaboration (inter)nationale et de l'échange d'informations est uniquement constitué par les articles 19, alinéa 1er et 20 § 3 L.R&S. L'article 19, alinéa 1er L.R&S règle la compétence générale de communication et de transfert de renseignements à des instances tierces.[261] Cependant, en 1998, le législateur lui-même jugeait cette réglementation insuffisante. Aussi, l'article 20 § 3 L.R&S dispose que le Conseil national de sécurité (CNS), entre autres, doit poursuivre l'élaboration de la collaboration et de l'échange d'informations. Par l'adoption de

260 L'objectif n'est pas de dupliquer ou de centraliser les banques de données existantes, mais bien de rendre accessibles les informations pertinentes disponibles.

261 Article 19, alinéa 1er L.R&S : « *Les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 13, deuxième alinéa, qu'aux ministres et autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes conformément aux finalités de leurs missions ainsi qu'aux instances et personnes qui font l'objet d'une menace visée aux articles 7 et 11.* ».

la Directive du 30 septembre 2016, le CNS a (en partie) rempli cette obligation légale.[262]

Mi-juin 2020, le Président de la Commission de l'Intérieur, de la Sécurité, de la Migration et des Matières Administratives a demandé au Comité permanent R de rendre un avis sur la proposition de loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité en vue d'instaurer des notes d'évaluation pour la collaboration avec les services de renseignement et de sécurité étrangers.[263]

La proposition de loi entend conférer un fondement juridique formel à la collaboration de la Sûreté de l'État et du Service Général du Renseignement et de la Sécurité avec d'autres pays. L'évaluation de l'intérêt de la relation de collaboration par rapport aux risques qu'elle implique revêt une importance primordiale. L'évaluation des risques sera consignée dans une 'note d'évaluation', qui constitue la base sur laquelle repose la collaboration des services. Ce fondement juridique est non seulement nécessaire pour de nouvelles relations de collaboration, mais aussi pour celles qui existent déjà et sont poursuivies.

Le Comité permanent R ne pouvait que saluer la proposition de loi car depuis plusieurs années déjà, il plaidait en faveur d'une réglementation légale pour la collaboration internationale des services de renseignement et de sécurité belges.[264] Le Comité a dès lors formulé un avis particulièrement détaillé.[265] Une proposition de texte a été ajoutée dans les cas où une précision textuelle de la proposition de loi était susceptible d'apporter une valeur ajoutée à la protection du citoyen ou à l'application pratique de la réglementation par les services de renseignement et de sécurité.

---

262 La Directive du 30 septembre 2016 du Conseil national de sécurité concernant les relations de la Sûreté de l'État (VSSE) et du Service Général du Renseignement et de la Sécurité (SGRS) avec les services de renseignement étrangers). Il a été décidé de classifier (au niveau 'Confidentiel') cette directive (de qualité) du CNS. Le Comité ne comprend pas pourquoi ce document doit être classifié. En effet, il ne contient ni des données et méthodologies opérationnelles ni d'autres types de données sensibles. En outre, vu que la directive du CNS fait partie du cadre juridique d'évaluation de l'action internationale des services de renseignement et de sécurité, le Comité estime qu'il n'y a aucune raison de classifier un tel document de manière permanente. Une autre question était de savoir si une adpatation et une actualisation s'imposaient comme suite à l'entrée en vigueur de Loi du 30 juillet 2018 relative à la protection des données. Vu que la directive du CNS ne faisait pas l'objet de l'avis, la question n'a pas été approfondie.

263 *Doc. parl.* 2019-20, DOC 55-0956/001. L'avis du Comité a été envoyé fin août au Président de la Commission de l'Intérieur, de la Sécurité, de la Migration et des Matières Administratives de la Chambre des représentants. À la clôture du rapport d'activités, la proposition était toujours pendante à la Chambre.

264 COMITÉ PERMANENT R, *Rapport d'activités 1997*, 163 ; COMITÉ PERMANENT R, *Rapport d'activités 2007*, 51 ; COMITÉ PERMANENT R, *Rapport d'activités 2008*, 105-106; COMITÉ PERMANENT R, *Rapport d'activités 2009*, 4, 106-107; COMITÉ PERMANENT R, *Rapport d'activités 2012*, 2 et 97; et COMITÉ PERMANENT R, *Rapport d'activités 2016*, 119.

265 L'avis intégral et les propositions de textes coordonnées peuvent être consultés sur www.comiteri.be.

Si la présente proposition de loi est adoptée par le Parlement, la directive du CNS nécessite une adaptation et une actualisation. Le Comité estimait néanmoins que la proposition législative et la directive du CNS pouvaient coexister, à condition que la directive soit modifiée sur un certain nombre de points en tant que norme juridique subordonnée.

VII.4. BRUXELLES PRÉVENTION & SÉCURITÉ, L'ACCÈS À LA BANQUE DE DONNÉES *TERRORIST FIGHTERS* ET LA COMMUNICATION DE LISTES À DES TIERS

Le Comité permanent R a répondu, dans une analyse juridique, à la demande d'avis de la Commission de suivi[266] quant à la communication d'informations issues de la banque de données *Terrorist Fighters* (GGB TF) au service Bruxelles Prévention & Sécurité (BPS), un organisme d'intérêt public (OIP).[267] Le Comité a fait remarquer à cet égard qu'il convenait de distinguer d'une part, l'accès (direct ou indirect) à la BDC TF et, d'autre part, la communication de listes à des tiers (c'est-à-dire ceux qui ne disposent pas d'un accès à la BDC TF).

VII.4.1. ACCÈS (IN)DIRECT À LA BDC TF

L'article 7 de l'arrêté royal du 21 juillet 2016 relatif à la banque de données *terrorist fighters* (AR TF)[268] prévoit une gradation des accès aux banques de données : un accès direct pour les services dits 'de base' (parmi lesquels les services de renseignement et de sécurité) ainsi que pour certains 'services partenaires' (parmi lesquels le Ministère public), et un accès direct mais limité aux données relatives aux TF dans le cadre de leurs missions (par ex. l'accompagnement et la surveillance judiciaires).

266 Question posée par la Commission parlementaire de suivi le 3 juin 2020.

267 Bruxelles Prévention & Sécurité (BPS), organisme créé par l'Ordonnance du 28 mai 2015 (*M.B.* 10 juin 2015), coordonne la prévention et la sécurité sur le territoire de la Région de Bruxelles-Capitale, d'une part, et assiste tous les acteurs concernés pour garantir au mieux la sécurité des Bruxellois et de toutes celles et ceux qui visitent la Région, d'autre part (www.bps-bpv.brusselsfr/home-fr).

268 Arrêté royal du 21 juillet 2016 relatif à la banque de données commune *Terrorist Fighters*, *M.B.* 22 septembre 2016.

L'article 44/11/3*ter*, § 3 LFP permet une extension à d'autres services[269], et ce par arrêté royal délibéré en Conseil des ministres, après avis du Comité permanent R et du C.O.C.

Début août 2019, le C.O.C. et le Comité permanent R ont rendu un avis[270] sur un projet d'A.R. modifiant l'AR TF. Un des éléments de ce projet portait sur l'extension du droit d'interrogation[271] directe à Bruxelles Prévention & Sécurité à la BDC TF. Pour les deux instances de contrôle, le contexte dans lequel cet organisme était désigné comme service partenaire n'était absolument pas clair. La mission attribuée à BPS par la loi ne pouvait nullement être lue comme une mission (claire) dans les chaînes pénales ou comme une mission de protection de la sécurité publique. Aussi, il n'était pas acceptable, selon le Comité et le C.O.C. *« qu'un nouvel organisme soit ajouté à la liste existante, déjà large, des destinataires de données très sensibles sur le plan de la vie privée, sans qu'en soit démontrées la pertinence et la plus-value pour la société.* »

Par conséquent, cet organisme d'intérêt public n'a pas été inclus en tant que service bénéficiaire dans l'A.R.

VII.4.2. LA COMMUNICATION DE LISTES À DES INSTANCES TIERCES

L'extraction et la communication de listes sont ensuite réglées à l'article 11, § 2 AR TF. L'extraction est autorisée uniquement aux services qui ont un accès direct ; la communication des listes n'est pas autorisée, sauf moyennant le respect de plusieurs conditions cumulatives.[272] [273]

Depuis 2017, le C.O.C. et le Comité permanent R ont cependant pu constater que des listes étaient communiquées à Bruxelles Prévention & Sécurité, ce qui s'est confirmé en 2019 :

---

269 Autres autorités publiques belges, organes ou organismes publics ou d'intérêt public chargés par la loi de l'application de la loi pénale ou qui ont des missions légales de sécurité publique, qui, lorsqu'ils sont chargés de compétences dans les domaines prévus à l'article 44/2, § 2, peuvent accéder, sur la base du besoin d'en connaître, notamment au niveau stratégique, tactique ou opérationnel aux banques de données communes.

270 Avis 001/CPR-C.O.C/2019 du 1er août 2019 (www.comiteri.be).

271 Sous la forme de 'hit/no hit'.

272 Le cas échéant, la transmission est effectuée par un service de base ; elle a lieu après une évaluation par le gestionnaire (Police fédérale), le responsable opérationnel (l'OCAM) et les (autres) services de base (Police locale et services de renseignement) ; le destinataire est une autorité publique ou un service public ; la finalité de la liste s'inscrit dans la mission légale du destinataire, etc.

273 L'article 44/11/3*quater* LFP permet une communication de listes à une autorité ou une entité tierce à une double condition : d'une part, le respect des modalités fixées par arrêté royal et d'autre part, une évaluation conjointe par la police intégrée, l'OCAM et les services de renseignement.

« (…) Selon les informations fournies par l'OCAM le 6 février 2020, la pratique consiste actuellement à envoyer chaque mois par e-mail une liste des données et informations à caractère personnel figurant dans la BDC TF et PH, notamment au SPF Emploi, à l'AFCN et à Bruxelles Prévention & Sécurité. […] [i]l est d'autant plus discutable que la même institution, en l'absence de toute évaluation ou notification claire des conditions de communication, figure dans une liste de diffusion extensive qui va à l'encontre de la délimitation de la transmission des données de la police, telle que précisée dans la LFP. »

VII.4.3. CONCLUSIONS

Le Comité permanent R a dès lors conseillé ce qui suit :

— Si la volonté du gouvernement était de voir Bruxelles Prévention & Sécurité bénéficier d'un accès aux banques de données communes, le Comité permanent R recommandait la rédaction d'un arrêté royal accompagné d'un rapport au Roi détaillé.[274]
— Si la volonté du gouvernement était de voir BPS continuer à bénéficier de listes transmises par l'OCAM, le Comité réitérait les recommandations prises (avec le C.O.C.) et sollicitait que les autorités compétentes prennent incessamment l'ensemble des mesures préconisées.

Enfin, le Comité a indiqué que l'OCAM était entre-temps chargé de respecter et de faire respecter le prescrit légal.

274 Conformément à l'art. 44/11/3*ter* § 3 LFP, ce projet d'AR doit être soumis pour avis au C.O.C. et au Comité permanent R. Ensuite, la déclaration de traitement visée à l'art. 44/11/3*bis*, § 3 LFP devra, le cas échéant, être complétée.

CHAPITRE VIII

LES INFORMATIONS ET INSTRUCTIONS JUDICIAIRES

Parallèlement à sa collaboration aux enquêtes de contrôle, le Service d'Enquêtes R du Comité effectue également des enquêtes sur les membres des services de renseignement suspectés d'avoir commis un crime et/ou un délit.[275] Il s'agit de missions confiées au Service d'Enquêtes par les autorités judiciaires. Cette compétence est décrite à l'article 40, alinéa 3 de la Loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace. La Loi du 10 juillet 2006 relative à l'analyse de la menace a élargi cette compétence aux crimes et délits commis par des membres de l'Organe de coordination pour l'analyse de la menace (OCAM).[276]

Lorsqu'ils remplissent une mission de police judiciaire, les membres et le directeur du Service d'Enquêtes R sont soumis à l'autorité du procureur général près la cour d'appel ou du procureur fédéral (art. 39 L.Contrôle). Le Comité permanent R n'a aucune autorité sur eux. Le président du Comité doit cependant veiller à ce que l'exécution des missions de police judiciaire n'entrave pas l'exécution des enquêtes de contrôle. La raison en est évidente : le Comité a beaucoup d'autres missions légales. Celles-ci pourraient être mises en péril si les dossiers judiciaires nécessitaient un investissement trop conséquent. Le président peut, le cas échéant, se concerter avec les autorités judiciaires quant à la participation des membres du Service d'Enquêtes R à des enquêtes pénales (art. 61*bis* L.Contrôle).

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

---

275 Dans son courrier du 13 janvier 2020 adressé au Collège des procureurs généraux, le président du Comité permanent R a rappelé l'application de l'art. 38 L. Contrôle ainsi que la COL 8/2014 (version du 11 janvier 2018). Il y est notamment stipulé qu'une copie des jugements et ordonnances relatifs aux crimes et délits commis par des membres des services de renseignement et de l'OCAM doit d'office être envoyée au Comité permanent R.

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

En 2020 également, le Service d'Enquêtes R a effectué des devoirs d'enquête dans le cadre de missions judiciaires, en l'occurrence de trois dossiers répressifs. Ce ne sont pas moins de 25 procès-verbaux qui ont été dressés.

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

À la demande d'un juge d'instruction, un collaborateur d'un service de renseignement a fait l'objet d'une enquête pour des faits de violation du secret professionnel. L'intéressé aurait contacté la Police fédérale sous de faux prétextes en vue de transmettre les informations ainsi obtenues à des personnes étroitement liées au milieu criminel.

À la suite d'une plainte introduite auprès du Comité permanent R par un collaborateur d'un service de renseignement concernant 'quelques questions d'ordre professionnel', le Service d'Enquêtes R a décidé de dresser un procès-verbal (art. 29 CIC), et donc d'informer les autorités judiciaires d'éventuelles infractions pénales dans le chef d'un ou de plusieurs membres d'un service de renseignement. En 2020, le Service d'Enquêtes R a effectué plusieurs missions dans ce cadre.

Enfin, un juge d'instruction bruxellois a demandé l'avis du Service d'Enquêtes R dans le cadre d'une enquête portant sur une affaire d'espionnage. Le juge d'instruction a ensuite décidé que l'enquête serait menée par la Police fédérale, avec l'appui du Service d'Enquêtes R. Cependant, aucun devoir d'enquête n'a encore été effectué.

Par ailleurs, l'article 50 L. Contrôle dispose que *'[t]out membre d'un service de police qui constate un crime ou un délit commis par un membre d'un service de renseignements rédige un rapport d'information et le communique dans les quinze jours au chef du Service d'enquêtes R'*. En 2020, le Service d'Enquêtes R n'a reçu aucun signalement en ce sens.

CHAPITRE IX
EXPERTISE ET CONTACTS EXTERNES

IX.1. COLLOQUE À L'OCCASION DES DIX ANS DE LA LOI MRD

L'année 2020 a marqué le dixième anniversaire de la Loi MRD, un événement qui ne pouvait pas passer inaperçu. Depuis l'entrée la Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité, la VSSE et le SGRS utilisent ce que l'on appelle les 'méthodes particulières de renseignement'. En 2010, lorsque le législateur a décidé de doter les services de renseignement de nouvelles compétences, une mission importante a, par la même occasion, été confiée au Comité permanent R : il devait, conjointement avec la Commission BIM, contrôler l'exécution de ces MRD, lesquelles sont, par définition, très intrusives pour les droits et libertés individuels.

Le Comité permanent R a jugé opportun, une décennie après l'entrée en vigueur de la Loi MRD, de procéder à une évaluation critique et de se tourner vers l'avenir avec des spécialistes du domaine.

Le Comité a ainsi organisé, le 31 janvier 2020, sous les auspices de la Chambre des représentants, le colloque intitulé 'Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulières de renseignement : de l'ombre à la lumière' pour le monde du renseignement au sens large. Entre autres le président de la Chambre, le ministre de la Justice, des représentants du SGRS et de la VSSE, des représentants d'institutions des droits de l'homme, des médias et du barreau, mais aussi du milieu académique et des organes de contrôle sont intervenus, et ce sous l'angle de leur expérience, de leur expertise et de leur intérêt respectifs. Le *United Nations Special Rapporteur for the Protection and Promotion of Human Rights while Countering Terrorism* ne pouvait pas ne pas être présent.

Le compte-rendu du colloque, publié sous la forme d'un livre[277], reprend les interventions. Quelques contributions internationales des Pays-Bas, de Suisse et de France sont venues l'enrichir à cette occasion.

---

277 J. VANDERBORGHT (ed.), *Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulières de renseignement : de l'ombre à la lumière*, Lefebvre Sarrut Belgium, Brussel, 2020, 151 p.

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

Avec la Loi du 12 mai 2019, l'Institut fédéral pour la protection et la promotion des droits humains (IFDH) a été créé.[278] La création d'un institut national des droits de l'homme, qui est un engagement pris lors de la signature du Protocole dans le cadre de la convention des Nations Unies contre la torture, s'est fait attendre longtemps.

Des réunions – et compte tenu des mesures strictes dictées par la crise sanitaire, des vidéoconférences – ont été organisées à intervalles réguliers avec les différentes institutions dotées d'un mandat en matière de droits de l'homme.[279] Par le biais d'un protocole de coopération[280], toutes les institutions participantes ont accepté d'échanger des pratiques et des méthodes, d'examiner des questions communes et de promouvoir la coopération mutuelle. L'attention s'est ainsi portée sur la circulaire 'violence contre la police', la reconnaissance faciale pour les services de police et l'utilisation de '*bodycams*'. Ont également fait l'objet d'une concertation les préoccupations et les points d'attention liés à la COVID-19, tels que les caméras déployées à la Côte et dans les villes afin de mesurer l'animation, la '*contact tracing app*', l'utilisation des données de télécommunication anonymisées pour évaluer la mobilité, etc. En termes de contenu, la contribution du Comité permanent R lors de ces réunions est particulièrement limitée.

Entre-temps, l'institut nouvellement créé s'est vu confier différentes missions : rendre, sur demande ou d'initiative, des avis et des recommandations sur des questions en rapport avec la promotion et la protection des droits fondamentaux, suivre la mise en œuvre des obligations internationales que les autorités belges se sont engagées à respecter et stimuler la ratification des nouveaux instruments internationaux en matière de droits humains. En 2020, la Chambre a constitué un conseil d'administration en nommant douze personnes indépendantes issues du milieu académique, du monde judiciaire, de la société civile ainsi que des partenaires sociaux.

Le Comité permanent R a participé à une recherche menée par les étudiants de la *Legal Clinic Mensenrechten en Migratierecht* de l'UGent sur les compétences de l'Institut fédéral pour la protection et la promotion des droits humains.[281]

---

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

279 Comme l'Unia, le Centre fédéral de la migration, l'Institut pour l'égalité des femmes et des hommes, l'Autorité de protection des données, le Médiateur fédéral, le Conseil supérieur de la Justice, les Comités permanents R et P. En 2021, c'est le Service de lutte contre la pauvreté, la précarité et l'exclusion sociale qui a succédé à Unia à la présidence.

280 Protocole d'accord du 13 janvier 2015 entre les institutions exerçant partiellement ou entièrement un mandat d'institution chargée du respect des droits de l'homme.

281 J. BREMS et al., *De bevoegdheden van het Federaal Instituut voor de Rechten van de Mens*, Legal Clinic Mensenrechten en Migratierecht, UGent, 2020-2021.

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

L'inévitable multiplication des échanges de données au niveau international entre les services de renseignement et de sécurité pose naturellement un certain nombre de défis aux organes de contrôle nationaux. Les organes de contrôle de (au départ) cinq pays européens (la Belgique, le Danemark, les Pays-Bas, la Norvège[282] et la Suisse)[283] collaborent depuis quelques années afin de relever ces défis, en identifiant des méthodes de travail qui leur permettraient de limiter le risque de lacunes dans le contrôle. Après un certain temps, un nouveau partenaire a été impliqué dans ce projet, à savoir l'*Investigatory Powers Commissioner's Office (IPCO)* du Royaume-Uni. Le groupe a été rebaptisé '*Intelligence Oversight Working Group*' (IOWG) et, en 2019, a été élargi à trois observateurs, à savoir le *Swedisch Foreign Intelligence Inspectorate (Statens inspektion av försvarunderättelse-verksamhet (SIUN))*, le *Swedish Board of Inventions (Statens uppfinnarnämnd, (SUN))* et la Commission G10 allemande.

En raison des restrictions liées à la crise sanitaire, les activités internationales sont restées très limitées en 2020.

Mi-janvier 2020 – et donc avant le déclenchement de la pandémie de COVID-19 — une '*expert meeting*' s'est tenue à Oslo (Norvège) avec les représentants des différents organes de contrôle en vue d'échanger leurs expériences et de discuter de leurs méthodes, de leurs meilleures pratiques ainsi que des écueils juridiques auxquels ils sont confrontés. Les thèmes qui ont été abordés lors de cette réunion étaient notamment les '*tools for log analysis*', l'organisation du contrôle de la '*bulk collection*' et la possibilité de partager des informations entre les différents organes de contrôle participants. En outre, le Comité permanent R a expliqué son intention de procéder, avec l'Autorité de surveillance indépendante des activités de renseignement (AS-Rens) suisse, à un échange de personnel dans le cadre d'un stage, même de courte durée. Après une suspension en raison de la crise sanitaire, cet échange est fixé au quatrième trimestre 2021.

La réunion suivante, qui devrait se tenir à Berne (Suisse), a elle aussi été reportée *sine die* pour les raisons déjà mentionnées.

La *Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten* néerlandaise a pris à son tour l'initiative d'étudier les règles établies sur la base de la norme internationale constituée par la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son protocole additionnel,

---

282 L'organe de contrôle norvégien a informé les participants à la réunion de l'existence de la nouvelle loi (*Intelligence Service Act)* pour le service de renseignement norvégien. Celle-ci remplace la loi de 1998 et est entrée en vigueur le 1er janvier 2021. Une attention particulière y est accordée à la '*bulk collection of metadata that crosses Norwegian borders*'.

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

récemment modernisés dans la Convention 108+ (signée par la Belgique le 10 octobre 2018 mais pas encore ratifiée)[284], en sollicitant la contribution des autres autorités de contrôle.

IX.4. CONTACTS AVEC DES ORGANES DE CONTRÔLE ÉTRANGERS

Les conférences organisées annuellement par et pour les organes de contrôle nationaux ont repris depuis 2018. Après la première conférence à Paris en 2018, co-organisée par le CNCTR français et le Comité permanent R, une deuxième conférence s'est tenue en décembre 2019. En 2020, l'organe de contrôle italien, la *Procura Generale della Corte di Cassazione*, devait accueillir, à Rome, la *European Intelligence Oversight Conference*. La conférence, qui avait dû être annulée, doit finalement se tenir en octobre 2021. En juillet 2020, des délégations de la CTIVD, du CNCTR et de l'IPCO ont rencontré, à Rome, l'organe de contrôle italien afin de planifier cette conférence et de discuter du programme.

Dans le prolongement de la *European Intelligence Oversight Conference 2019* à La Haye, la Commission nationale de contrôle des techniques de renseignement (CNCTR) a préparé un questionnaire sur l'*ex ante oversight*, auquel les organes de contrôle de tous les pays participants ont été invités à répondre. Cette initiative vise à améliorer la connaissance des meilleures pratiques en matière de contrôle *ex ante* appliquées en Europe. Le questionnaire a été conçu pour servir de base à la discussion et à l'échange d'expériences au cours de la réunion suivante. Le Comité permanent R a rempli ce questionnaire en étroite concertation avec la Commission BIM. En juillet 2020, l'organe de contrôle néerlandais CTIVD a lancé une initiative similaire. Il s'agissait d'un questionnaire portant sur le '*complaint handling*' (traitement des plaintes). L'objectif de cette initiative est semblable (*supra*) : recueillir et analyser les meilleures pratiques en Europe en matière de traitement des plaintes à des fins d'amélioration. Ces initiatives ont toutefois dû être mises entre parenthèses.

Enfin, en mars 2020, le *National Special Intelligence Devices Control Bureau* bulgare a mis en place un projet '*for strenghtening the capacities of the oversight bodies to protect the rights and freedoms of citizens against unlawful use of special intelligence devices*'. Pour l'heure, aucune suite n'y a été donné.

---

284 Voir à ce propos : https://www.coe.int/fr/web/data-protection/convention108-and-protocol. Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 128ème Session du Comité des Ministres, Helsingør, Danemark, 17-18 mai 2018.

CHAPITRE X

L'ORGANE DE RECOURS EN MATIÈRE D'HABILITATIONS, D'ATTESTATIONS ET D'AVIS DE SÉCURITÉ[285]

X.1. INTRODUCTION

L'Organe de recours est la juridiction administrative compétente pour les contentieux portant sur des décisions administratives dans quatre domaines : les habilitations de sécurité, les attestations de sécurité qui doivent permettre l'accès à des lieux où se trouvent des documents classifiés, les attestations de sécurité qui permettent l'accès à des lieux précis faisant l'objet de menaces et, enfin, les avis de sécurité. L'Organe de recours intervient également en tant que 'juge d'annulation' contre des décisions d'autorités publiques ou administratives, lorsqu'elles imposent des avis ou des attestations de sécurité pour un secteur, un lieu ou un événement donné.[286]

L'Organe de recours est composé du président du Comité permanent R, du président du Comité permanent P et du président de la Chambre contentieuse de l'Autorité de protection des données. Les trois présidents peuvent être remplacés en cas d'empêchement par un membre-conseiller effectif de l'institution à laquelle appartient le président concerné.

Le président du Comité permanent R assure la présidence de l'Organe de recours. La fonction de greffier est exercée par le greffier du Comité permanent R et le personnel du greffe est le personnel affecté par le Comité. Les activités de l'Organe de recours constituent depuis plus de vingt ans l'exemple parfait de synergie au sein de certaines institutions satellitaires du Parlement. La composition collégiale de l'Organe de recours apporte en outre une contribution multidisciplinaire à la délibération de chaque dossier.

---

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

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

Le fonctionnement de l'Organe de recours est supporté intégralement par le Comité permanent R. Il s'agit, d'une part, de la mise à disposition du président et de ses membres suppléants, de son greffier mais aussi des juristes comme '*greffiers assumés*' et du personnel administratif qui forment le greffe de cette juridiction administrative. D'autre part, le Comité permanent R prend en charge, sur son budget, les frais de locaux comme de fonctionnement de l'Organe de recours. C'est ainsi que contrairement au Comité permanent R et au Comité permanent P, il ne bénéficie pas de la franchise postale, alors que tous ses envois se font par lettre recommandée avec accusé de réception.

Les décisions sont délibérées collégialement.

Cette juridiction se caractérise par sa totale gratuité. En effet, contrairement à la plupart des autres juridictions administratives ou de l'ordre judiciaire, le dépôt de la requête est sans frais. En outre, la partie qui perd son litige ne sera condamnée à aucun dépens, en vertu de la loi.

Enfin, l'année 2020 a vu la création du site internet de la juridiction administrative www.organederecours.be. Le site entend offrir aux citoyens, justiciables et avocats une série d'informations nécessaires et utiles pour leur permettre d'introduire une action et soutenir le procès devant la juridiction collégiale.

X.2. UNE JURIDICTION CONFRONTÉE À LA PANDÉMIE

L'Organe de recours a vu son fonctionnement affecté par la pandémie du COVID-19. Outre les problèmes de confinement dès le mois de mars 2020, le greffe ne recevra plus les envois recommandés des requérants ni certains dossiers en raison des problèmes de la poste. L'Organe de recours devra annuler certaines audiences entre le 13 mars et le 27 mai 2020 en raison du confinement, la fermeture des bâtiments de la Chambre des représentants empêchant l'accès à la salle d'audience.

Toutefois, en vue de garantir le bon fonctionnement du service public de la justice et ne pas créer d'arriéré, l'Organe de recours a multiplié les audiences après le confinement. Il en a tenu en moyenne plus de trois par mois en juin, juillet, septembre et octobre 2020 au lieu des deux audiences habituelles.

X.3. UNE PROCÉDURE PARFOIS LOURDE ET COMPLEXE

Nonobstant la diminution des recours introduits en 2020 (de 196 en 2019 à 144 en 2020), il apparaît que le nombre de décisions rendues en 2020 a augmenté (de 166 en 2019 à 176 en 2020) (*infra*). L'Organe de recours constate à nouveau une croissance de la charge de travail. En effet, la gestion administrative des dossiers,

des audiences et des décisions demeure davantage complexe. La préparation des dossiers de l'Organe de recours nécessite des capacités qui sont aujourd'hui insuffisantes. Un renfort pour assurer certaines tâches est souhaitable à l'avenir pour garantir un meilleur fonctionnement pour la jurisdiction.

L'Organe de recours relève les problèmes suivants :

- Le non-respect du délai légal de transmission du dossier administratif par l'autorité de sécurité à l'Organe de recours. Il en résulte une impossibilité pour l'Organe de recours de rendre ses décisions dans les délais impartis.
- Les dossiers administratifs transmis par les différentes autorités de sécurité ne sont pas toujours complets. Le greffe doit effectuer des démarches supplémentaires ou la juridiction prononce des décisions avant dire droit quant au fond en vue de le voir compléter.
- L'application de l'article 5 § 3 L. Org. recours est souvent problématique. Cette disposition permet à l'Organe de recours, à la demande d'un service de renseignement ou d'un service de police, de décider de soustraire certaines pièces à la consultation du requérant ou de son avocat lorsque la divulgation de ces pièces est susceptible de porter préjudice à la protection des sources, à la vie privée de tiers ou à l'accomplissement des missions légales des services de renseignement, ou encore au secret de l'information ou de l'instruction judiciaire. Toutefois, il est rare que la demande soit (correctement) motivée, ou bien elle émane d'une autorité qui n'est pas légalement compétente en la matière, ce qui oblige parfois le greffe, ici aussi, à recueillir des informations complémentaires. En outre, il arrive souvent que ces autorités restent attachées à l'idée erronée que le requérant et son avocat ne peuvent pas consulter des données classifiées sans motivation supplémentaire, et ce en dépit de la jurisprudence constante de l'Organe de recours selon laquelle la L. Org. recours est une *lex specialis* par rapport à la Loi Classification. Enfin, il y a aussi des cas où le président de l'Organe de recours doit soustraire d'office des éléments du dossier parce que le service concerné a manifestement omis d'invoquer l'article 5 § 3 L. Org. recours aux fins de protection de la vie privée de tiers.
- Les décisions des autorités de sécurité ne sont pas suffisamment motivées et, contrairement à ce que la loi exige, aucune décision pleinement motivée n'est établie dans les cas où l'article 22, alinéa 5 L.C&HS permet de ne pas reprendre certains éléments dans la décision qui est communiquée à l'intéressé. En outre, dans la motivation, il incombe à l'autorité de sécurité de spécifier quels faits concrets constituent une contre-indication compte tenu de la finalité réglementairement établie d'une vérification de sécurité déterminée. Il s'agit de la seule manière pour l'Organe de recours de vérifier la proportionnalité d'une décision.
- Par ailleurs, l'Organe de recours relève encore que diverses autorités de sécurité ne respectent pas les principes formels de droit administratif (décisions dépourvues de dates ou de l'identité du fonctionnaire qui les a adoptées,

problème de délégation de pouvoir, absence d'audition de l'intéressé, emploi de la langue en matière administrative).

- Enfin, sans motivation circonstanciée, les autorités de sécurité ne suivent pas la jurisprudence de l'Organe de recours (par exemple, en ce qui concerne la problématique des enquêtes ou des vérifications à propos de personnes qui n'ont pas la nationalité belge).

Relevons que si la qualité du dossier qui est constitué est un souci récurrent, l'intervention de plus en plus fréquente d'avocats a aussi un impact non négligeable sur le fonctionnement de la juridiction. En effet, l'Organe de recours est contraint, à juste titre, de motiver ses décisions en répondant aux arguments pertinents soulevés par les conseils dans la défense des intérêts de leur client.

Pour l'Organe de recours, la loi et ses arrêtés royaux ne sont plus en phase avec les exigences modernes d'accès à la justice. En effet, les articles 2 et 3 de l'AR Org. recours, stipulent respectivement que '*l'envoi à l'organe de recours de toutes pièces de procédure se fait sous pli recommandé à la poste*' et que '*le recours est signé et daté par le requérant ou par son avocat*'. De nombreux justiciables confrontés à l'accès à la justice ne respectent pas ces règles. Le plus souvent en raison d'une maîtrise imparfaite et compréhensible des règles de procédure. C'est le sens de la proposition de loi rédigée à destination de la Chambre des représentants. Il y a lieu, en effet, de mieux prendre en compte la qualité, voire la fragilité, de nombreux requérants et de prévoir des dispositions légales qui n'entraînent pas la nullité de plein droit. Le processus de décision même requiert lui aussi davantage de temps qu'il y a plusieurs années, et ce pour deux raisons majeures. D'une part, le nombre élevé de questions procédurales (par ex. la recevabilité, l'emploi des langues, les droits de la défense ou la délégation de compétence de l'autorité qui prend sa décision). D'autre part, l'Organe de recours est plus souvent confronté à des dossiers hautement sensibles. Par ailleurs, il arrive que des mesures de sécurité spécifiques doivent être prises.

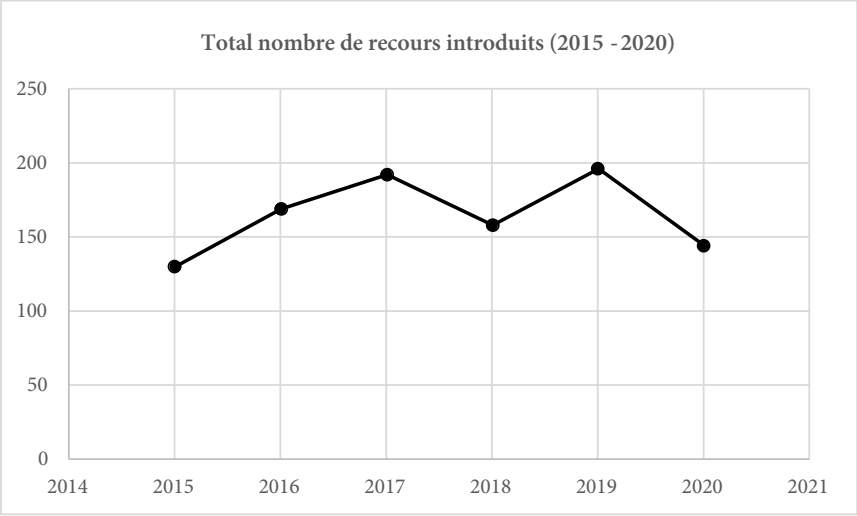
X.4. PAS D'ÉVOLUTION DU CADRE JURIDIQUE

Si en 2018 et 2019, le cadre juridique avait considérablement évolué, tant au niveau de la L.C.&HS que de la L. Org. recours, l'on ne relèvera aucune initiative législative ou réglementaire en 2020.

X.5. LE DÉTAIL DES CHIFFRES

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

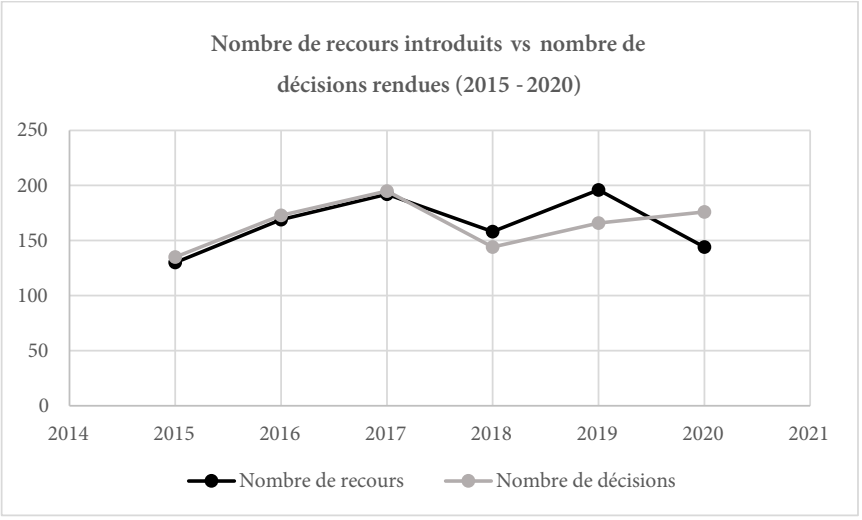
Tableau 1. Nombre de recours introduits (2015-2020)



La tendance globale des chiffres sur les dernières années montre une diminution des recours soumis à l'Organe de recours. Cette diminution s'articule autour de trois axes principaux : tout d'abord, une récession des recours concernant les habilitations de sécurité (de 36 en 2018 à 51 en 2019 et à 32 en 2020). Par ailleurs, après une année en recul, le contentieux en matière d'avis de sécurité est également en nette régression (de 115 en 2019 à 99 en 2020). Enfin, les recours concernant les refus d'attestations de sécurité pour le secteur nucléaire sont également en nette baisse (17 en 2019 à 7 en 2020).

Toutefois, une considération importante s'impose. Nonobstant la diminution des recours introduits en 2020, il apparaît que le nombre de décisions rendues en 2020 a augmenté. Le tableau ci-dessous établit une comparaison entre le nombre de recours introduits et le nombre de décisions rendues.

Tableau 2. Nombre de recours introduits *vs* nombre de décisions rendues (2015-2020)



On relèvera que l'Organe de recours a connu pour la première fois de la question de l'octroi d'une attestation de sécurité à un imam en vue de travailler au sein des établissements pénitentiaires belges sur base du prescrit de l'arrêté royal du 17 mai 2019.[287]

La juridiction a également été saisie de la question de l'octroi de l'avis de sécurité pour les agents des douanes amenés à porter une arme dans le cadre de l'exercice de leur fonction et ce conformément au prescrit de l'arrêté royal du 15 décembre 2013.[288]

De la même manière, pour la première fois, l'Organe de recours a été saisi de la question de l'octroi de l'avis de sécurité pour les fournisseurs, sous-traitants et leur personnel des institutions européennes à la suite d'un protocole conclut entre les Affaires étrangères et les institutions européennes.[289]

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

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

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

289 Voir à ce propos l'arrêté royal du 8 mai 2018 fixant les secteurs d'activités et les autorités administratives compétentes visées à l'article 22*quinquies*, §7 de la L.C.&HS qui attribue au fonctionnaire dirigeant du SPF Affaires étrangères la compétence en ce qui concerne le « secteur d'activités » des institutions internationales. Un 'memorandum of understanding' a été conclu le 21 mai 2019 entre ce dernier et les institutions européennes.

possible que cette nouvelle procédure d'avis de sécurité soit mise en œuvre à ce propos.

Enfin, 26 audiences de l'Organe de recours ont été organisées en 2020.

Tableau 3. Autorités de sécurité concernées (2015-2020)

	2015	2016	2017	2018	2019	2020
Autorité nationale de sécurité	68	92	129	113	114	91
Sûreté de l'État	1	0	0	0	0	0
Service Général du Renseignement et de la Sécurité	47	68	53	32	61	41
Agence fédérale de Contrôle nucléaire	10	8	7	10	17	7
Police fédérale	3	1	3	3	3	4
Police locale	1	0	0	0	1	1
TOTAL	130	169	192	158	196	144

Le graphique figurant ci-dessous visualise la répartition des autorités de sécurité concernées en 2020.

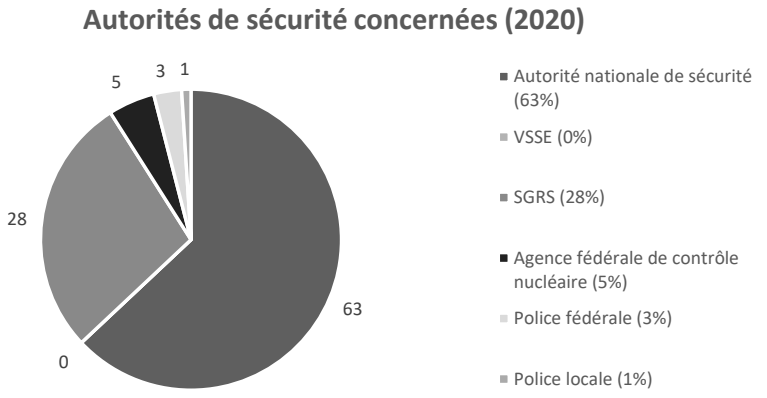


Tableau 4. Nature des décisions contestées

	2015	2016	2017	2018	2019	2020
Habilitations de sécurité (art. 12 et s. L.C&HS)						
Confidentiel	9	5	1	2	5	0
Secret	35	38	33	31	39	27
Très secret	4	7	6	3	7	5
Refus	36	28	30	26	39	23
Retrait	7	9	7	4	16	8
Refus et retrait	0	0	0	0	0	0
Habilitation pour une durée limitée	3	4	1	1	3	0
Habilitation pour un niveau inférieur	0	1	0	0	0	0
Pas de décision dans les délais	2	7	2	5	0	0
Pas de décision dans les nouveaux délais	0	1	0	0	0	0
Autres						1[290]
SOUS-TOTAL HABILITATIONS DE SÉCURITÉ	48	50	40	36	51	32
Attestations de sécurité zone classifiée (art. 22*bis*, al.1 L.C&HS)						
Refus	6	1	3	3	1	0
Retrait	0	0	0	0	0	0
Pas de décision dans les délais	0	0	0	0	0	0
Attestations de sécurité lieu ou événement (art. 22*bis*, al.2 L.C&HS)						
Refus	12	9	20	15	12	6
Retrait	1	0	0	0	0	0
Pas de décision dans le délai	0	0	0	0	0	0
Attestations de sécurité lieu secteur nucléaire (art. 8*bis* L.C&HS)						
Refus	-	7	7	11	17	7
Retrait	-	1	0	0	0	0
Pas de décision dans le délai	-	0	0	1	0	0
Avis de sécurité (art. 22*quinquies* L.C&HS)						
Avis négatif	63	101	122	92	115	99
Pas d'avis	0	0	0	0	0	0

290 'Mise en garde du requérant'. Une personne s'était vue octroyer l'habilitation de sécurité pour cinq ans avec une mise en garde. Il est allé en recours contre cette mise en garde.

	2015	2016	2017	2018	2019	2020
Révocation d'avis positif	0	0	0	0	0	0
Actes normatifs d'une autorité administrative (art. 12 L. Org.recours)						
Décision d'une autorité publique d'exiger des attestations de sécurité	0	0	0	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des attestations de sécurité	0	0	0	0	0	0
Décision d'une autorité administrative d'exiger des avis de sécurité	0	0	0	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des avis de sécurité	0	0	0	0	0	0
SOUS-TOTAL ATTESTATIONS ET AVIS	82	119	152	122	145	112
TOTAL DÉCISIONS CONTESTÉES	130	169	192	158	196	144

Tableau 5. Nature du requérant

	2015	2016	2017	2018	2019	2020
Fonctionnaire	4	2	4	5	4	8
Militaire	29	23	20	8	27	39
Particulier	93	139	164	140	163	95
Personne morale	4	5	4	5	2	2

Le graphique figurant ci-dessous visualise la répartition 'nature du requérant' en 2020.

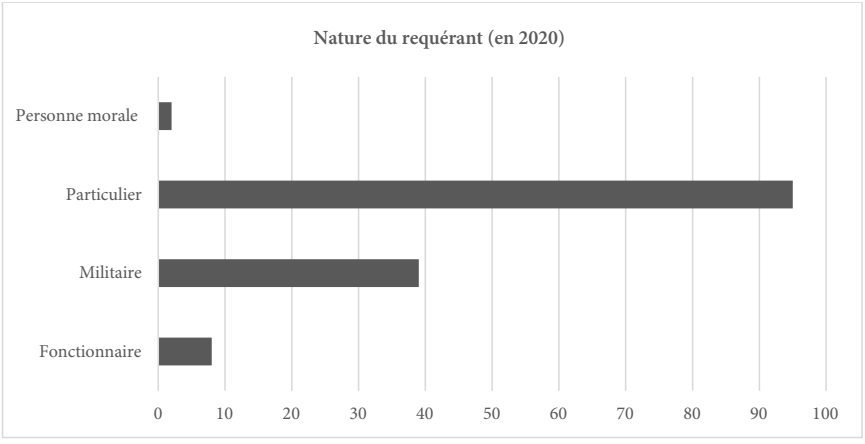


Tableau 6. Langue du requérant

	2015	2016	2017	2018	2019	2020
Français	75	99	115	83	101	83
Néerlandais	54	70	77	75	95	61
Allemand	0	0	0	0	0	0
Autre langue	1	0	0	0	0	0

Tableau 7. Actes du greffe

	2015	2016	2017	2018	2019	2020
Demande du dossier complet (1)	130	167	191	154	191	141
Demande d'informations complémentaires (2) et rappels adressés aux autorités de sécurité (3)	7	23	36	12	39	41

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

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

(3) L'art. 6 de l'AR Org. recours prévoit les délais pour la communication des dossiers par les autorités de sécurité. Ces délais prennent cours lorsque le greffier transmet une copie du recours à l'autorité de sécurité concernée. Ils varient selon la nature de l'acte attaqué. Ainsi, l'autorité de sécurité doit communiquer son dossier dans les 15 jours en ce qui concerne les habilitations de sécurité, dans les 5 jours en matière d'attestations de sécurité et dans les 10 jours si le recours porte sur un avis de sécurité. Lorsque ces délais ne sont pas respectés, le greffe prend les contacts nécessaires. Ces données sont comptabilisées à partir de 2019.

Tableau 8. Actes juridictionnels interlocutoires pris par l'Organe de recours [291]

	2015	2016	2017	2018	2019	2020
Audition d'un membre d'une autorité (1)	7	10	0	1	6	1
Décision du président (2)	0	0	0	0	0	0
Soustraction d'informations du dossier par l'Organe de recours (3)	50	54	80	72	77	50
Décisions avant dire droit (4)	/	/	/	/	9	9

(1) L'Organe de recours peut décider d'entendre les membres des services de renseignement et de police ou des autorités de sécurité qui ont participé à l'enquête ou à la vérification de sécurité.
(2) Le président de l'Organe de recours peut décider de permettre au membre du service de renseignement de garder secrètes certaines données pendant son audition.
(3) Si le service de renseignement ou de police concerné le demande, l'Organe de recours peut décider que certaines informations soient retirées du dossier communiqué au requérant.
(4) Il peut s'agir par exemples d'une décision de jonction de deux dossiers ou de demander un complément d'informations à propos de la situation d'un dossier judiciaire. Ces données sont comptabilisées à partir de 2019.

Tableau 9. Manière dont le requérant fait usage de ses droits de défense

	2015	2016	2017	2018	2019	2020
Consultation du dossier par le requérant et/ou l'avocat	84	87	105	69	96	96
Audition du requérant (assisté ou non d'un avocat)[292]	107	127	158	111	143	135

291 Le nombre d'actes juridictionnels interlocutoires' (tableau 6), les 'manières dont les requérants font usage de leurs droits de défense' (tableau 7), ou encore la 'nature des décisions de l'Organe de recours' (tableau 8) ne correspondent pas nécessairement au nombre de requêtes introduites (voir tableaux 1 à 4). En effet, certains dossiers ont par exemple déjà été ouverts en 2019, alors que la décision n'a été rendue qu'en 2020.

292 La L.Org. recours prévoit l'assistance d'un avocat à l'audience mais pas la représentation par ce dernier. À noter que, dans le cadre de certains dossiers, le requérant (assisté ou non de son avocat) est auditionné à plusieurs reprises. Dans 56 % des cas, le requérant était assisté d'un avocat.

Tableau 10. Nature des décisions de l'Organe de recours

	2015	2016	2017	2018	2019	2020
Habilitations de sécurité (art. 12 et s. L.C&HS)						
Recours irrecevable	4	0	3	0	1	1
Recours sans objet	3	7	0	4	3	3
Recours non fondé	19	18	13	12	12	16
Recours fondé (avec octroi partiel ou complet)	24	24	24	12	25	14
Devoir d'enquête complémentaire par l'autorité	0	2	0	1	1	2
Délai supplémentaire pour l'autorité	1	2	1	1	0	3
Donne acte de retrait de recours	1	0	0	3	2	2
Attestations de sécurité zone classifiée (art. 22*bis*, al.1 L.C&HS)						
Recours irrecevable	0	0	1	0	0	0
Recours sans objet	0	0	1	0	0	0
Recours non fondé	4	1	0	1	1	0
Recours fondé (avec octroi)	2	1	1	0	3	0
Donne acte de retrait de recours	-	-	-	-	1	0
Attestations de sécurité pour lieux ou événements (art. 22*bis*, al.2 L.C&HS)						
Recours irrecevable	0	0	1	2	4	2
Recours sans objet	0	0	1	0	0	0
Recours non fondé	8	2	12	2	4	4
Recours fondé (avec octroi)	10	4	7	3	4	1
Donne acte de retrait de recours	2	0	1	2	0	0
Attestations de sécurité pour le secteur nucléaire (art. 8*bis* §2 L.C&HS)						
Recours irrecevable	-	1	1	0	1	0
Recours sans objet	-	1	0	1	0	0
Recours non fondé	-	0	1	1	5	2
Recours fondé (avec octroi)	-	7	5	6	7	4
Donne acte de retrait de recours	-	-	-	2	0	0

	2015	2016	2017	2018	2019	2020
Avis de sécurité (art. 22*quinquies* L.C&HS)						
Organe de recours non compétent	0	0	20[293]	12	0	0
Recours irrecevable	6	15	10	3	7	8
Recours sans objet	0	0	1	3	1	6
Confirmation de l'avis négatif	28	42	49	46	40	51
Transformation en avis positif	23	46	41	27	43	52
Donne acte de retrait de recours	0	0	1	0	1	5
Recours contre des actes normatifs d'une autorité administrative (art. 12 L. Org. recours)	0	0	0	0	0	0
TOTAL	135[294]	173	195	144	166	176

X.6. UNE PROPOSITION DE RÉFORME

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

C'est dans ce contexte que le 24 novembre 2020, après avoir soumis le texte aux présidents du Comité permanent P et de la Chambre contentieuse de l'Autorité de protection des données, le Comité permanent R, a transmis un texte à la Chambre des représentants.

Ce texte est le fruit d'une réflexion initiée depuis des années par le président de l'Organe de recours. Cette réflexion s'est appuyée sur l'expertise de Monsieur Ivan Verougstraete, ancien Président de la Cour de cassation. Il est proposé d'instituer un Conseil pour les contentieux en matière de sécurité en abrogeant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité. Cette juridiction ferait suite à

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

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

l'Organe de recours car l'idée défendue par les rédacteurs est de créer un 'juge naturel' de la sécurité tant en matière d'habilitations, attestations et avis de sécurité qu'en matière de gardiennage et de détectives privés. Cette juridiction voit son indépendance confortée par la présence de trois membres 'experts': le Comité permanent R pour les aspects « Loi sur habilitations » et « Loi sur le renseignement »; le Comité permanent P en matière de Loi sur la fonction de police et la Chambre contentieuse de l'Autorité de protection des données pour la protection de la vie privé. Le texte[295] propose une simplification des procédures et une plus grande transparence, notamment par l'introduction de la numérisation des dossiers. La proposition de réforme devrait, si elle aboutit, permettre d'introduire les recours par voie électronique. En outre, les parties pourront entrer en contact avec le greffe via cette plateforme au sujet de leur dossier. Des contacts ont été pris avec le barreau pour développer les contacts utiles pour favoriser l'accès du justiciable. Les nouvelles règles de procédure rendront la procédure plus fluide et plus transparente par l'uniformisation des délais de recours au délai unique de trente jours. En effet, actuellement, le délai de huit jours (en matière d'attestations et d'avis de sécurité) est trop court pour permettre au citoyen d'assurer convenablement ses droits de défense. Ainsi, seraient ménagés à la fois les intérêts de l'État et des citoyens. Enfin, la proposition maintient le principe de la gratuité de l'accès pour le justiciable.

Le président de l'Organe de recours examine la possibilité d'accueillir des étudiants ou des avocats afin de leur permettre d'effectuer un stage en son sein.

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

295 Le texte de la proposition sera publié sur le site internet de l'Organe de recours après la présentation de ce rapport à la Commission d'accompagnement du Comité permanent R de la Chambre des représentants.

CHAPITRE XI

LE FONCTIONNEMENT INTERNE DU COMITÉ PERMANENT R

XI.1. COMPOSITION DU COMITÉ PERMANENT R

L'année 2020 a été marquée par de nombreux changements au niveau du personnel. Serge Lipszyc (F), premier substitut de l'auditeur du travail près de l'auditorat du travail de Liège, qui a prêté serment en septembre 2018,[296] a continué à remplir sa mission de président. Pieter-Alexander De Brock (N), dont le premier mandat expirait en mai 2019, a été reconduit dans sa fonction de conseiller mi-janvier 2020.[297] Fin novembre 2020, Laurent Van Doren (F), conseiller francophone du Comité permanent R, a informé la Chambre de sa démission à compter du 31 décembre 2020.[298] Thibaut Vandamme (F), substitut du procureur du Roi de l'arrondissement du Luxembourg, qui avait été désigné lors de la séance plénière du 22 novembre 2018 comme premier suppléant, a accepté, le 1er décembre 2020, d'exercer le mandat de membre.[299]

Début janvier 2020, le greffier Wouter De Ridder a fait valoir ses droits à la retraite. Fin avril 2020, le président du Comité a demandé par courrier à la Chambre de lancer la procédure de désignation d'un nouveau greffier.[300] Un appel

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

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

298 *C.R.I.* Chambre 2020-21 PLEN 074, 47. Le 24 septembre 2020, Linda Schweiger a été désignée comme premier membre suppléant (*C.R.I.* Chambre 2019-20 PLEN055, 85) et le 29 octobre 2020, Wauter Van Laethem a été désigné comme second membre suppléant (*C.R.I.* Chambre 2019-20, PLEN 067, 16)

299 Conformément à l'article 30, alinéa 3 L.Contrôle, la Chambre doit, en cas de vacance d'une place de membre suppléant, procéder sans délai à la nomination d'un nouveau membre suppléant. L'appel à candidatures est paru au Moniteur belge le 18 décembre 2020. Le premier membre suppléant, Thierry Werts, a été désigné lors de la séance plénière du 20 mai 2021 (*C.R.I.* Chambre, 2020-21, PLEN 105, 47). Michel Croquet demeure le second membre suppléant du membre francophone.

300 *C.R.I.* Chambre 2019-20, PLEN 038, 70.

à candidatures pour la désignation du greffier du Comité permanent R est paru au Moniteur belge mi-mai 2020.[301]

Des changements sont également intervenus au sein du Service d'Enquêtes : Frank Franceus a quitté son poste de directeur et a été remplacé par Fabian Poncelet (F), qui remplit également le rôle d'officier de sécurité, et un nouveau commissaire-auditeur néerlandophone a rejoint les rangs du service en septembre 2020.

Enfin, le cadre administratif du Comité permanent R, placé sous la direction du greffier faisant fonction Wauter Van Laethem (N), a lui aussi subi quelques changements. En mars 2020, un juriste néerlandophone statutaire a rejoint les rangs de la Section documentation et analyse juridique, suivi par un juriste statutaire francophone en décembre 2020. Toujours au cours de cette année de référence, les examens de sélection en vue du recrutement d'un(e) secrétaire statutaire néerlandophone et d'un(e) secrétaire statutaire francophone ont été organisés. Fin 2020, le cadre administratif comptait 18 collaborateurs.

XI.2. LE 'DATA PROTECTION OFFICER' AU COMITÉ

Le Comité a pu continuer à faire appel au *Data Protection Officier* (DPO)[302], désigné pour tous les traitements de données qui ne relèvent pas de la 'sécurité nationale'.

Ce délégué à la protection des données tient le registre des activités de traitement qui a été établi en concertation avec les différents services au sein du Comité permanent R et validé par son président et ses conseillers. En outre, le DPO a également offert ses conseils sur le nouveau site internet (par ex. les marchés publics) et sur les procédures de recrutement (par ex. l'obligation d'information à l'égard des intéressés). Entre-temps, le DPO est activement impliqué dans, notamment, l'utilisation et l'accès au (numéro de) Registre national, l'utilisation des caméras de surveillance et l'obligation d'information à l'égard des intéressés (entre autres les collaborateurs internes).

XI.3. RÉUNIONS AVEC LA COMMISSION DE SUIVI

En octobre 2019, la Chambre des représentants a adapté son règlement, ce qui a modifié la composition de la Commission spéciale chargée de l'accompagnement parlementaire du Comité permanent de Contrôle des services de police et du Comité permanent de Contrôle des services de renseignement et de sécurité. Désormais, il est procédé à autant de nominations qu'il est nécessaire pour que chaque groupe

301 À la clôture du présent rapport d'activités, le nouveau greffier n'a toujours pas été désigné. Le 21 juin 2021, une proposition de loi visant à élargir les conditions de nomination des greffiers des Comités permanents R et P a été introduite (*Doc. parl.* Chambre 2021-21, 55-2064/001).

302 Le DPO est commun à plusieurs institutions.

politique représenté dans les commissions permanentes soit représenté par un membre au moins au sein de la commission. Chaque groupe politique qui n'est pas représenté au sein de la commission désigne parmi ses membres un membre qui participera aux activités de la commission, mais sans voix délibérative.[303] Au lendemain des élections fédérales de mai 2019, la composition de la Commission de suivi a subi quelques modifications. Les membres avec voix délibérative étaient les suivants : Peter Buysrogge (N-VA), Joy Donné (N-VA), Cécile Thibaut (Ecolo-Groen), Stefaan Van Hecke (Ecolo-Groen), André Flahaut (PS), Ahmed Laaouej (PS), Ortwin Depoortere (VB), Marijke Dillen (VB), Denis Ducarme (MR), Servais Verherstraeten (CD&V), Nabil Boukli (PVDA-PTB), Patrick Dewael (Open Vld) et Bert Moyaers (Vooruit). Mi-octobre 2020, Eliane Tillieux (PS) a succédé à Patrick Dewael (Open Vld) à la présidence de la Chambre. Georges Dallemagne (cdH) participe en qualité de membre ne disposant pas d'une voix délibérative.

Dans le courant de l'année 2020, et malgré la crise sanitaire, plusieurs réunions ont eu lieu avec la Commission. Juste avant le déclenchement de la crise sanitaire, les membres de la Commission de suivi ont été invités, le 2 mars 2021, à une réunion de travail dans les bureaux du Comité. L'objectif de cette rencontre était de présenter aux nouveaux membres de la Commission les activités du Comité et d'avoir un échange de vues plus approfondi avec les visages connus. Plusieurs enquêtes de contrôle clôturées par le Comité permanent R ont été discutées lors d'autres réunions de la Commission, à huis clos. Du temps a également été consacré au rapport annuel sur l'application des méthodes spécifiques et exceptionnelles par les services de renseignement et au contrôle exercé par le Comité sur la mise en œuvre de ces méthodes (art. 35 L.Contrôle), ainsi qu'au rapport rédigé dans le cadre de sa compétence de contrôle – conjointement à l'Organe de contrôle de l'information policière (C.O.C.) – concernant les banques de données (art. 44/6 LFP). Lors de sa réunion du 16 décembre 2020, le *Rapport d'activités 2019* du Comité permanent R a été discuté.[304] La Commission a souligné *'la grande qualité du rapport annuel qui fournit une image complète des activités du Comité R*'.[305] Une série de thématiques ont particulièrement retenu l'attention des Députés, comme le suivi des sectes, la pénurie de personnel au sein des services de renseignement, les habilitations de

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

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

305 Si les membres du Comité comprennent que la situation politique et les circonstances difficiles ont retardé la présentation du rapport, ils ont demandé au Comité d'accélérer la présentation du prochain rapport d'activités. Le Comité a prêté à ce commentaire toute l'attention qu'il mérite.

sécurité et l'Organe de recours, ou encore le suivi des recommandations.[306] En guise de conclusion, la Commission a pris *'acte du rapport d'activités 2019 du Comité R et souscrit à ses recommandations'*.[307]

XI.4. RÉUNIONS COMMUNES AVEC LE COMITÉ PERMANENT P

En 2020, quelques réunions communes ont été organisées, sans compter les contacts informels. Les articles 52 à 55 L.Contrôle déterminent les cas où le Comité permanent R et le Comité permanent P doivent organiser des réunions communes et la manière dont ils doivent les organiser. La présidence de ces réunions communes est exercée en alternance par les présidents des deux Comités (art. 54 L.Contrôle). Ces rencontres poursuivent un double objectif : d'une part, échanger des informations, et, d'autre part, initier des enquêtes de contrôle communes et discuter des enquêtes en cours.

Deux enquêtes communes ont été effectuées en 2020 : l'enquête de suivi sur la mise en œuvre des recommandations émises par les Comités permanents R et P dans le cadre de l'enquête sur les services d'appui de l'OCAM (cf. I.11.8) et l'enquête de contrôle sur les quatre services d'appui 'supplémentaires' de l'OCAM (cf. I.11.9). Il a été décidé de ne pas démarrer d'autre enquête commune.

Par ailleurs, toute une série de points ont été mis à l'ordre du jour. Ont par exemple été discutés le projet de modification de la Loi Contrôle proposé par le Comité permanent P a été discuté et une proposition visant à étendre la nécessité d'être titulaire d'une habilitation de sécurité de niveau 'TRÈS SECRET' à l'ensemble du personnel administratif des Comités permanents R et P et à tous les membres du Service d'Enquêtes P. L'état d'avancement du développement d'un outil de collecte sur Internet au profit du SGRS, de la VSSE et de la Police fédérale a également

306 En vue d'améliorer le suivi des recommandations des Comités permanents R et P, une proposition de révision du Règlement de la Chambre a été introduite en décembre 2019 par deux membres de la Commission. Il a ainsi été proposé d'adapter l'article 149 du Règlement de la Chambre comme suit : *'Lorsque la Commission constate qu'aucune suite n'a été réservée par les ministres compétents aux recommandations proposées par le Comité permanent P et/ou le Comité permanent R, ou que les mesures prises sont inappropriées ou insuffisantes, elle peut demander aux ministres compétents de faire rapport devant elle. Les ministres compétents rendent, au minimum, un rapport par an à la Commission sur l'état de la mise en œuvre des recommandations. À cet égard, les ministres compétents tiennent un tableau de bord permanent de suivi des recommandations […] qui est communiqué à la Commission*'. *Doc. parl.*, Chambre 2019-20, 55-0868/001, 11 décembre 2019. La proposition n'a cependant pas été retenue.

307 *Doc. parl.* Chambre 2020-21, 55-1689/001, 29 décembre 2020 (Rapport d'activités 2019 du Comité permanent de Contrôle des services de renseignement et de sécurité, Rapport fait au nom de la commission spéciale chargée de l'accompagnement parlementaire du Comité permanent de Contrôle des services de police et du Comité permanent de contrôle des services de renseignement et de sécurité).

été mis à l'ordre du jour[308], une réflexion a été menée sur la demande d'accès au Registre national pour les commissaires-auditeurs, ou encore des idées ont été échangées sur la recherche d'éventuelles synergies entre les deux institutions. En ce qui concerne ce dernier point, la possibilité a été examinée d'acheter un logiciel commun de vidéoconférence (ou appels vidéo) pour organiser des réunions à distance, des réunions internes, des événements, des webinaires ou des conférences.

XI.5. MOYENS FINANCIERS ET ACTIVITÉS DE GESTION

Le budget 2020 du Comité permanent R a été fixé à 4,615 millions d'euros, ce qui représente une augmentation de 9,5 % par rapport à 2019.[309]

Outre les augmentations naturelles (indexation, etc.), cet accroissement a été motivé par deux projets soumis à l'approbation du Parlement : d'une part, un projet de digitalisation des processus de travail et des moyens de communication (site internet) et d'autre part, une refonte du cadre administratif visant à adapter le profil des futurs collaborateurs au développement des missions du Comité exigeant plus de personnel opérationnel au détriment du personnel d'appui.

Les sources de financement attribuées par la Chambre des représentants[310] sont les suivantes : 85,84 % au titre du budget de dotation et 14,16 % de boni de 2018.

L'exécution du budget 2020 a produit un boni comptable de 463,045 euros, représentant la différence entre le budget approuvé et les dépenses constatées.

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

Le dégagement d'un boni comptable considérable provient essentiellement de l'écart temporel existant entre l'approbation des budgets et, notamment, l'entrée effective en service du personnel en raison de la longueur des procédures de recrutement et de l'obtention des habilitations de sécurité requises. Cette

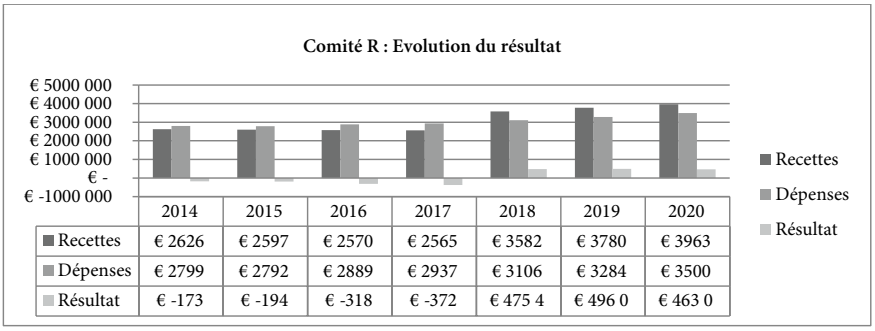
---

308 Cet outil, qui se compose d'une combinaison de modules 'software' et 'hardware', doit permettre aux services de police et de renseignement de rechercher des informations sur les médias sociaux et les sites internet de manière plus rapide et plus ciblée. L'achat a été approuvé au Conseil des ministres dès août 2016.
Cependant, le contrat conclu avec le développeur de logiciels néerlandais BAVAK a été résilié parce que le moteur de recherche ne répondait pas aux attentes. Voir à ce propos : K. CLERIX, Knack, 23 février 2021 ('Nieuwe topman Philippe Boucké zet ADIV op scherp').

309 *C.R.I.* Chambre 2019-20, PLEN 018, 72.

310 *Doc. parl.* Chambre 2019-2020, 55-0867/001, 24-27.

tendance devrait perdurer pendant quelques années encore de par le processus d'engagements découlant des nouvelles missions du Comité, mais aussi compte tenu du remplacement du personnel originel qui fait ou fera valoir ses droits à la retraite. Il s'agira là aussi d'un défi pour le Comité de gérer ces expériences accumulées pour les transmettre aux nouveaux collaborateurs. On peut cependant prédire que lorsque tous les engagements seront finalisés, ils seront à charge de la dotation et qu'il y aura un équilibrage naturel *ceteris paribus* entre les recettes et les dépenses.



	2014	2015	2016	2017	2018	2019	2020
Recettes	€ 2626	€ 2597	€ 2570	€ 2565	€ 3582	€ 3780	€ 3963
Dépenses	€ 2799	€ 2792	€ 2889	€ 2937	€ 3106	€ 3284	€ 3500
Résultat	€ -173	€ -194	€ -318	€ -372	€ 475 4	€ 496 0	€ 463 0

D'autre part, le Comité permanent R reste attentif aux possibilités de synergie qui lui sont offertes par la Chambre des représentants et par les autres institutions satellites de celle-ci. Le Comité y adhère sans retenue lorsque la faisabilité est source d'efficience, d'efficacité et d'économies potentielles sans que cela ne contrarie ses impératifs de sécurité. Concrètement, un contrat de dépôt a été conclu entre le Comité et la bibliothèque du Parlement, en vertu duquel le Comité a confié la conservation de sa collection limitée mais spécialisée de monographies, de périodiques et d'autres publications relatives au fonctionnement, aux compétences et aux domaines de responsabilité des services de renseignement et de sécurité dans un contexte large (international). Dans le courant de l'année 2020, tous les livres et revues ont été transférés physiquement à la bibliothèque du Parlement : cela a permis d'éviter la duplication future des achats, d'offrir un accès plus large à la littérature existante et de créer des bureaux supplémentaires au Comité.

XI.6. MISE EN ŒUVRE DES RECOMMANDATIONS DE L'AUDIT DE LA COUR DES COMPTES

À la demande de la Commission de la Comptabilité de la Chambre des représentants, la Cour des comptes a, dès 2017, initié une enquête sur les institutions à dotation, conjointement à Ernst & Young. Le Comité permanent R était donc concerné. La Cour des comptes s'est surtout concentrée sur les aspects budgétaires (une analyse

des recettes et des dépenses) et sur la délimitation des missions des différentes institutions. De son côté, Ernst & Young était principalement chargé de procéder à une analyse approfondie des processus, des systèmes et de l'organisation de chacune de ces institutions. Le rapport d'audit[311] reprenant des recommandations concernant les 'missions' des neuf institutions à dotation concernées par l'audit a été transmis fin mars 2018. La caractéristique commune des missions de ces institutions *'ligt in het doel om tot een betere rechtsbescherming voor burgers te komen door het uitoefenen van verschillende vormen van toezicht in specifieke beleidsdomeinen*'.[312]

À l'occasion de l'audit de suivi des institutions par la Cour des Comptes, la Commission de la Comptabilité a décidé, mi-novembre 2020, de demander aux services de la Questure de rédiger un état du dossier de l'exécution des recommandations de cet audit. Il a également été demandé d'examiner de quelle manière des synergies supplémentaires pouvaient être implémentées afin de réaliser d'autres économies et gains en efficacité.

XI.7. FORMATIONS

Compte tenu de l'intérêt pour l'organisation, le Comité permanent R encourage ses membres et ses collaborateurs à suivre des formations générales (informatique, management, etc.) ou propres au secteur, ou encore à participer à des conférences.[313]

En raison des mesures adoptées dans le cadre de la crise sanitaire, il n'a pas été possible de suivre des formations externes en 2020. Un nombre limité de briefings internes ont toutefois été organisés, au cours desquels des experts ont informé le Comité sur des thématiques actuelles et importantes au sein de la communauté du renseignement au sens large (par ex. le Professeur Christian Behrendt, associé à l'ULiège et à la KULeuven, expert en questions constitutionnelles au niveau national et international et le Prof. Damien Van Puyvelde, *lecturer in intelligence and international security*, Glasgow).

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

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

313 Les briefings de sécurité auxquels les collaborateurs sont tenus d'assister ont eu lieu.

CHAPITRE XII
RECOMMANDATIONS

À la lumière des enquêtes de contrôle, des contrôles et des inspections clôturés en 2020, le Comité permanent R formule les recommandations reprises ci-après. Ces recommandations portent à la fois sur la protection des droits que la Constitution et la loi confèrent aux personnes, sur la coordination et l'efficacité des services de renseignement, de l'OCAM et des services d'appui et sur l'optimalisation des possibilités d'enquête du Comité permanent R.

XII.1. RECOMMANDATIONS RELATIVES À LA COORDINATION ET À L'EFFICACITÉ DES SERVICES DE RENSEIGNEMENT, DE L'OCAM ET DES SERVICES D'APPUI

XII.1.1. DIVERSES RECOMMANDATIONS RELATIVES À L'ENQUÊTE DE CONTRÔLE COMMUNE SUR L'OCAM ET LES SERVICES D'APPUI[314]

XII.1.1.1. Une meilleure communication interne et des sessions d'information pour les experts détachés

Une meilleure communication en interne, en particulier entre les départements de l'OCAM, permettrait de mieux savoir qui fait quoi, et ce également au niveau des experts détachés. Dans le même ordre d'idée, une actualisation régulière de la liste des membres du personnel avec leurs compétences respectives constituerait une plus-value (avec une diffusion de la liste au sein du personnel).

Il a été constaté que les experts détachés (département Analyse ponctuelle) se déplacent peu – voire pas du tout – au sein de leurs services d'origine, et certains d'entre eux ont même très peu de contacts avec ces services. Une formation ou une session d'information permettant de remettre à jour leur connaissance de leur service d'origine et des changements éventuels, législatifs ou d'ordre interne par exemple, constituerait également une plus-value.

314 Voir 'Chapitre I.1. Les services d'appui de l'OCAM'.

XII.1.1.2. Optimalisation des contacts entre l'OCAM et les services d'appui

Lorsque des contacts directs sont établis entre le service d'appui et l'OCAM, il est important d'informer le point de contact principal du service d'appui via sa boîte fonctionnelle, en le mettant en copie de tout échange d'informations. L'objectif est d'éviter au maximum toute perte d'information.

Dans les cas de contacts bilatéraux développés par un membre du personnel de l'OCAM (ou du service d'appui) avec des membres du service d'appui (ou de l'OCAM), il convient de s'assurer qu'en cas de départ (ou d'absence), une continuité pourra être opérée par un autre membre du personnel. En effet, le départ (ou l'absence) du membre du personnel ayant développé de bons contacts avec certains membres du service d'appui (ou de l'OCAM) fait courir un risque de perte de qualité dans le flux d'informations.

En ce qui concerne les services d'appui dont le flux d'informations est très limité, il serait opportun de développer une synergie entre l'OCAM et le point de contact afin de sensibiliser le personnel aux missions de l'OCAM, et ce, dans la mesure du possible, à travers les différentes composantes du service d'appui (par des séances d'information par exemple). Il appartient aux services d'appui de prendre des initiatives afin de sensibiliser au mieux son personnel.

XII.1.1.3. Le respect des obligations légales par l'Administration des Douanes et Accises

Si l'Administration des Douanes et Accises – section enquêtes et recherche (SPF Finances) ne voit pas d'intérêt dans sa collaboration avec l'OCAM et ne voit pas quelles informations elle pourrait transmettre, il n'en reste pas moins que cette administration demeure le point de contact de l'OCAM tel que désigné par la loi. Dès lors, il revient à ce service de procéder à une analyse en interne afin d'établir quels types d'informations recueillies pourraient s'avérer utiles pour l'OCAM. Sur cette base, un autre point de contact peut éventuellement être désigné au sein des Douanes et Accises.

Par ailleurs, le SPF Finances Douanes et Accises – section enquêtes et recherche doit s'attacher à prendre les mesures adéquates afin de respecter les normes minimales en matière de conservation et de consultation de documents classifiés, ce qui est une obligation légale.

XII.1.2. DIVERSES RECOMMANDATIONS RELATIVES À L'ENQUÊTE DE CONTRÔLE SUR LE SUIVI DE L'EXTRÊME DROITE[315]

XII.1.2.1. Recommandations concernant la délimitation politique de l'objectif de renseignement

Les différents services chargés du suivi de l'extrême droite/de l'extrémisme de droite devraient en arriver à employer une terminologie commune et uniforme. Ils devraient également définir les critères les plus objectifs possibles pour déterminer quels individus et/ou groupes doivent faire l'objet d'un suivi de leur part. L'emploi d'une même terminologie par tous les services concernés aurait un impact positif sur l'échange de données et la coopération.
Plusieurs options s'offrent aux pouvoirs législatif et exécutif :

- le législateur peut envisager de mieux décrire[316] la notion d'‘extrémisme' dans Loi 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) et de préciser le terme 'extrémisme de droite' (et logiquement aussi l'"extrémisme de gauche'). En outre, d'autres notions, comme le 'nationalisme', peuvent être reprises ;
- ou le Conseil national de sécurité (CNS) prend l'initiative, comme c'est d'ailleurs stipulé dans l'Arrêté royal portant création de cet organe ;
- ou encore les ministres compétents prennent l'initiative de donner des instructions claires sur la manière de considérer la menace.

Dans tous ces cas, il peut être demandé aux services qui font partie du Groupe de travail Extrême droite d'adopter une approche commune. D'ailleurs, un paradigme théorique existe déjà à cet égard. L'OCAM est en bonne position pour, avec les services, arriver à une conclusion. Celle-ci pourra ensuite être formalisée à un niveau supérieur.

Il convient par ailleurs de mesurer l'ampleur de la menace. Il n'y a pas que les services de renseignement qui recueillent ou peuvent recueillir des informations à ce sujet. Établir de telles données chiffrées ne relève pas de la seule responsabilité des services de renseignement. Par exemple, une collaboration et une coordination avec les services de police et les Parquets est nécessaire pour recueillir ces données chiffrées relatives aux infractions motivées politiquement et idéologiquement. Le Groupe de travail Extrême droite du Plan d'action Radicalisme peut jouer un rôle central, sous la direction du CNS pour déterminer la contribution de chacun.

---

315 Voir 'Chapitre I.7. Le suivi de l'extrême droite par les services de renseignement belges'.

316 À cet égard, la VSSE fait remarquer, à juste titre, qu'une définition claire comporte des avantages et des inconvénients : elle crée un bon cadre, actuel, mais la définition doit être suffisamment flexible pour englober des phénomènes (nouveaux).

XII.1.2.2. Recommandations concernant l'organisation et la planification

Le Comité permanent R recommande que les services de renseignement évaluent si leur planification interne (opérationnelle, tactique) est adéquate pour atteindre les objectifs stratégiques et si les ressources sont proportionnelles à la menace à suivre. Il y a toutefois une condition préalable : la description claire du phénomène et de son ampleur (voir recommandation ci-dessus).

XII.1.2.3. Recommandations concernant la collecte et le traitement

Le Comité permanent R recommande que lors de la création de sa banque de données, la VSSE rende possible la recherche et le regroupement d'informations via les axes MPG (ou d'une manière comparable puisque la VSSE a l'intention de remplacer la banque de données par une nouvelle solution).

En ce qui concerne le SGRS, le Comité permanent R recommande que le service développe une position HUMINT plus indépendante (des officiers S2) et y affecte plus de gestionnaires de sources. Le service doit en outre examiner les raisons de la lenteur du flux d'informations et du retard en matière d'input dans la banque de données. Il convient de trouver des solutions et de les mettre en œuvre.

XII.1.2.4. Recommandations concernant l'analyse, la diffusion et la coopération

De concert avec l'OCAM, les services doivent examiner comment établir davantage d'analyses générales de phénomène. La VSSE et l'OCAM doivent s'accorder – éventuellement dans le cadre du Plan d'action R – pour se répartir les tâches.

La VSSE dispose d'un instrument qui vise à évaluer le degré de radicalisation et de violence d'une personne. La VSSE ne dispose pas des effectifs lui permettant de déployer complètement cet instrument, qui demande d'ailleurs énormément d'informations (une cinquantaine d'indicateurs). Selon la VSSE, détecter les '*lone actors*' n'est peut-être pas le plus approprié. Il convient dès lors d'examiner si cet instrument peut éventuellement être allégé et si d'autres méthodes permettraient de mieux détecter des '*lone actors*'. Dans d'autres services (notamment à l'OCAM), d'autres instruments encore sont utilisés ou sont à l'étude.

Le Comité permanent R estime qu'une coopération et une coordination accrues sont nécessaires entre les services au niveau du développement et de l'utilisation de tels outils, ainsi qu'au niveau des formations liées à l'utilisation de ceux-ci. Et le Comité d'estimer que de tels outils susceptibles d'aider à la détection et à l'évaluation des menaces doivent systématiquement être utilisés pour le suivi de toutes les formes d'extrémisme, et que les moyens nécessaires en personnel doivent être mobilisés. Ceci, à plus forte raison que les services de renseignement affirment que d'éventuels actes terroristes, perpétrés par des '*lone actors*', constituent pour le moment la principale menace émanant de l'extrême droite.

Enfin, en ce qui concerne la sensibilisation des différents acteurs de la société sur la menace (ou sa gravité), la VSSE, et *a fortiori* le SGRS, ont pris peu d'initiatives. Compte tenu du caractère politique de la menace, il va de soi que l'éventuelle intervention de ces services dans les forums publics doit être couverte par le Conseil national de sécurité ou par les ministres compétents.

XII.1.2.5. Recommandations concernant le feedback

Le Comité permanent R recommande aux deux services de demander explicitement et périodiquement un feedback aux destinataires des renseignements. Il revient à ces destinataires de répondre afin que les services puissent affiner/orienter leurs objectifs en matière de renseignement.

XII.1.3. APPLICATION DE LA '*RICHTLIJN AANGAANDE DE RELATIES VAN BELGISCHE INLICHTINGENDIENSTEN MET BUITENLANDSE INLICHTINGENDIENSTEN*'[317] [318]

Le 26 septembre 2016, la '*Richtlijn aangaande de relaties van Belgische inlichtingendiensten met buitenlandse inlichtingendiensten*' a été prise. Toutefois, la transmission des informations/données à caractère personnel à des services étrangers n'y était traitée que de manière sommaire. Le Comité s'en tient par conséquent aux recommandations qu'il avait formulées et estime qu'une initiative en la matière constitue une priorité. À cet égard, c'est le principe de prudence qui doit certainement prévaloir dans le cadre des échanges d'informations pratiqués par les services de renseignement.

La directive susmentionnée vise à évaluer les services de renseignement étrangers en vue de déterminer la nature de la relation avec chacun de ces services. Elle constitue un instrument de soutien de la politique en matière de coopération bilatérale. Les dispositions reprises dans la directive doivent toujours être respectées.[319] Il convient de prévoir une évaluation conjointe, notamment concernant le critères 'obstacles', lorsque le partenaire étranger collabore avec la VSSE et le SGRS.

---

317 Ces recommandations découlent du 'Chapitre I.3. Le Brexit et la relation entre les services de renseignement belges et britanniques' et du 'Chapitre I.5. Le Memorandum of Understanding (MOU) entre le SGRS et les services de renseignement rwandais'.

318 Directive concernant les relations des services de renseignement belges avec les services de renseignement étrangers (traduction libre)

319 Le 23 janvier 2020, les Députés Meryame Kitir et Kris Verduyckt ont introduit une proposition de loi en vue d'inscrire une telle évaluation de la coopération avec des services étrangers dans la L.R&S. Cette évaluation se baserait sur six critères au moins. Proposition de loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, *Doc. parl.,* Chambre 2019-20, 23 janvier 2020, 0956/001 (www.comiteri.be).

Si à un moment donné, il devait y voir des répercussions sur la protection des données à caractère personnel (parce que le Royaume-Uni aurait dérogé aux règles RGPD), il reviendrait aux services de renseignement qui y seraient confrontés de saisir les différentes instances nationales compétentes (les ministres compétents et les différentes autorités de protection des données).[320]

En outre, il est recommandé que le SGRS invite la ministre de la Défense à adapter la directive du 26 septembre 2016 avec le ministre de la Justice en vue de prévoir dorénavant un accord ministériel préalable à toute collaboration (formelle ou informelle) avec un partenaire étranger (étatique ou non étatique) .

Enfin, le SGRS doit, dans un délai de deux ans, évaluer l'ensemble de ses relations internationales à la lumière de la directive ministérielle du 26 septembre 2016. Cette évaluation doit préciser les éléments concrets ayant conduit à la catégorisation. L'évaluation bisannuelle des services de renseignement étrangers et le suivi de la coopération doivent être systématiquement réalisés, conformément à la directive du 26 septembre 2016.

XII.1.4. ADAPTATION DE L'ARTICLE 20 L.R&S

Il est recommandé que le SGRS invite la ministre de la Défense à déposer, avec le ministre de la Justice, un projet de loi en vue de faire adapter l'article 20 L.R&S afin d'assurer la concordance linguistique français/néerlandais.

XII.1.5. ACCORD MINISTÉRIEL PRÉALABLE POUR LA CONCLUSION D'ACCORDS DE COOPÉRATION ET CLASSIFICATION SYSTÉMATIQUE

Le Comité permanent R recommande que le SGRS veille systématiquement à obtenir un accord ministériel préalable, sans attendre la modification de la directive. Le SGRS s'est d'ores et déjà engagé en ce sens pour les MoU.[321]

Par ailleurs, les nouveaux accords de collaboration avec des partenaires étrangers doivent être systématiquement classifiés conformément à la Loi du 11 décembre 1998.

---

320 Inversement, si des instances nationales avaient connaissance des conséquences du Brexit qui présentent un intérêt pour les services de renseignement, elles devraient idéalement saisir ces services à temps et éventuellement les associer à des discussions.

321 Le Comité permanent R a été informé que le SGRS développait des projets dans le cadre de la conclusion des MoU, du management de ses relations stratégiques et du processus de ses contacts internationaux. Le Comité évaluera l'exécution de ces projets dans l'année qui suit les présentes recommandations.

XII.1.6. CONCLUSION D'UN ACCORD DE COOPÉRATION ENTRE LA VSSE ET LE SGRS

Le Comité permanent R recommande que le Conseil national de sécurité et les deux services de renseignement mettent en œuvre l'obligation, contenue dans l'article 20 § 4 L.R&S[322], d'élaborer respectivement une directive et un accord de coopération. Le Comité permanent R estime que le modèle d'une *Joint Intelligence Task Force* est une initiative réussie qui pourrait être appliquée avec le même succès à d'autres thématiques dans le futur. Les directions des deux services doivent cependant tenir compte des inconvénients du projet, tels qu'identifiés par la VSSE et le SGRS dans leurs évaluations internes.

XII.1.7. OUTILS AUTOMATISÉS POUR LA SURVEILLANCE DES MÉDIAS SOCIAUX

Le Comité permanent R a constaté que la surveillance des médias sociaux par les services de renseignement reste fort laborieuse.[323] Les services disposent actuellement de trop peu d'outils automatisés permettant d'adopter une approche plus efficace. Le Comité permanent R juge nécessaire d'investir dans ce domaine à l'avenir, étant donné l'importance croissante des médias sociaux et alternatifs dans la diffusion de la propagande et de la désinformation visant à influencer l'opinion publique.

XII.1.8. RESPECT DE PROCÉDURES DISCIPLINAIRES ET JUDICIAIRES PAR LE SGRS (LORS DES MISSIONS À L'ÉTRANGER)

À la suite d'incidents survenus dans une zone d'opération non spécifiée à l'étranger[324], le Comité permanent R a recommandé différentes mesures ponctuelles (notamment celles liées à l'utilisation des sources) afin de garantir la sécurité des troupes déployées sur le terrain.

Il est recommandé que le SGRS se conforme scrupuleusement aux procédures disciplinaires et judiciaires en vigueur.

---

322 « Pour les missions décrites à l'article 7, 3° /1 et à l'article 11, § 1er, 5°, la Sûreté de l'État et le Service Général du Renseignement et de la Sécurité concluent un accord de coopération sur la base de directives obtenues du Conseil national de sécurité ». Les missions sont « *de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge* ».

323 Voir 'Chapitre I.6. Les technologies de l'information et de la communication dans le processus de renseignement au SGRS'.

324 Voir 'Chapitre I.10. Incidents dans une zone d'opération à l'étranger'.

Le Comité réitère également une recommandation antérieure[325] selon laquelle le SGRS doit rédiger un rapport détaillé sur chaque incident de sécurité, avec un examen et une analyse de toutes ses dimensions (non seulement techniques, mais aussi comportementales), en particulier lorsqu'une des parties impliquées est titulaire d'une habilitation de sécurité. Ce rapport doit être transmis à l'autorité de sécurité compétente, le cas échéant avec une proposition de décision.

XII.2. RECOMMANDATION RELATIVE À L'EFFICACITÉ DU CONTRÔLE

XII.2.1. UN STRICT RESPECT DE L'ARTICLE 33 L.CONTRÔLE PAR LE SGRS

Le Comité permanent R continue de rappeler que le SGRS est tenu de respecter l'article 33 L.Contrôle. Il est en particulier recommandé que le SGRS transmette systématiquement au Comité tous les protocoles d'accord et les autorisations ministérielles correspondantes, ainsi que les approbations ministérielles en cas de coopération informelle.

XII.2.2. LA MISE EN PLACE D'UN SYSTÈME DE CONTRÔLE INTERNE PAR LE SGRS

Le Comité permanent R recommande que le SGRS mette en place un système de contrôle interne pour assurer le respect de toutes les procédures relatives aux relations internationales.

XII.2.3. RAPPEL DE L'APPLICATION DE L'ARTICLE 38 L. CONTRÔLE

L'article 38 L. Controle prévoit deux formes de communication des autorités judiciaires vers le président du Comité permanent R.

Tout d'abord, il est prévu que le Procureur général et l'Auditeur général adressent d'office président du Comité permanent R une copie des jugements et arrêts définitifs relatifs aux crimes ou délits commis par les membres des services de renseignement et de l'OCAM. Le deuxième alinéa prévoit que le procureur général, l'auditeur du travail, le Procureur fédéral ou le Procureur général près la Cour d'appel, selon le cas, informe le président du Comité permanent R chaque

325 Voir COMITÉ PERMANENT R, Rapport d'activités 2015, 109.

fois qu'une information ou instruction pour crime ou délit est ouverte à charge d'un membre d'un service de renseignement ou de l'OCAM.

La COL 8/2014 apporte une précision, en indiquant qu'il s'agit d'une communication '*systématique*'.

Cette obligation est rappelée étant donné que l'article 38 L.Contrôle (principalement le deuxième alinéa) n'est pas toujours respecté.[326]

[326] La Circulaire du Collège des procureurs généraux (COL 08/2014) portant sur la communication d'informations, poursuites et condamnations à charge de fonctionnaires et personnes exerçant des missions d'intérêt public où les fonctions impliquent une relation d'autorité habituelle avec des mineurs ou des personnes vulnérables a été révisée le 9 janvier 2020.

ANNEXES

ANNEXE A
APERÇU DES PRINCIPALES RÉGLEMENTATIONS RELATIVES AUX COMPÉTENCES, AU FONCTIONNEMENT ET AU CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'OCAM (1ER JANVIER 2020 AU 31 DÉCEMBRE 2020)

Loi du 8 juillet 2020 modifiant la loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, *M.B.* 15 juillet 2020

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

A.R. 24 septembre 2020 modifiant l'arrêté royal du 13 décembre 2006 portant le statut des agents des services extérieurs de la Sûreté de l'État, *M.B.* 1er octobre 2020

A.R. 8 mai 2018 fixant les secteurs d'activités et les autorités administratives compétentes visées à l'article 22*quinquies*, § 7, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité — Traduction allemande, *M.B.* 15 décembre 2020

M.B. 18 avril 2020 portant délégation de la compétence de rejeter une demande de consultation, d'explications ou de communication sous forme de copie d'un document administratif en possession de la Sûreté de l'État, *M.B.* 18 mai 2020

M.B. 27 avril 2020 accordant délégation de pouvoir et de signature en matière de personnel pour la Sûreté de l'État à l'administrateur général de la sûreté de l'État, *M.B.* 18 mai 2020

Sélection comparative de documentalistes néerlandophones Renseignement et Sécurité (m/f/x) (niveau B) pour le ministère de la Défense — Numéro de sélection: ANG19407, *M.B.* 6 janvier 2020

Résultat de la sélection comparative de Spécialistes ICT (m/f/x) (niveau A) francophones pour le Ministère de la Défense — Numéro de sélection : AFG19342, *M.B.* 13 janvier 2020

Sélection comparative de Médias analystes (m/f/x) (niveau A1), francophones, pour le Ministère de la Défense — Numéro de sélection : AFG19394, *M.B.* 13 janvier 2020

Résultat de la sélection comparative de psychologues (m/f/x) (niveau A1), néerlandophones, pour la Sûreté de l'État — Numéro de sélection : ANG19287, *M.B.* 14 janvier 2020

Sélection comparative de juristes data governances (m/f/x) (niveau A2) francophones pour la Sûreté de l'État — Numéro de sélection : MFG20008, *M.B.* 13 février 2020

Sélection comparative de juristes data governances (m/f/x) (niveau A2) néerlandophones pour la Sûreté de l'État — Numéro de sélection : MNG20014, *M.B.* 13 février 2020

Sélection comparative de collaborateurs servicedesk (m/f/x) (niveau C) francophones pour la Sûreté de l'État — Numéro de sélection : AFG20031, *M.B.* 13 février 2020

Nomination du greffier du Comité permanent de contrôle des services de renseignement (Comité R), *M.B.* 13 mai 2020

Recrutement pour l'entrée en service immédiate et constitution d'une réserve de recrutement d'un(e) secrétaire néerlandophone statutaire (niv. B), *M.B.* 2 juin 2020

Sélection comparative de Cyber Securlty Experts A2 (m/f/x) (niveau A2), francophones, pour le Service Général du Renseignement et de la Sécurité (SGRS) de la Défense — Numéro de sélection : AFG20056, *M.B.* 3 juin 2020

Sélection comparative de Cyber Securlty Experts A2 (m/f/x) (niveau A2), néerlandophones, pour le Service Général du Renseignement et de la Sécurité (SGRS) de la Défense — Numéro de sélection : ANG20078, *M.B.* 3 juin 2020

Résultat de la sélection comparative de juristes data govemance (mlf/x) (niveau A2), néerlandophones, pour la Sûreté de l'État — Numéro de sélection : MNG20014, *M.B.* 9 juin 2020

Sélection comparative d'Expert technique en électronique (mlf/x) (niveau B), francophones, pour le Ministère de la Défense — Numéro de sélection: AFG20122, *M.B.* 15 juin 2020

Sélection comparative de Cyber Threat Intelligence Analyst (A2) (mlf/x) (niveau A2), francophones, pour le Ministère de la Défense — Numéro de sélection : AFG20128, *M.B.* 15 juin 2020

Résultat de la sélection comparative de Juristes data governance (m/f/x) (niveau A2), francophones, pour la Sûreté de l'État — Numéro de sélection : MFG20008, *M.B.* 18 juin 2020

Avis prescrit par l'article 74 de la loi spéciale du 6 janvier 1989. Par décision du 1er juillet 2020, dont l'expédition est parvenue au greffe de la Cour le 6 juillet 2020, le Comité permanent de contrôle des services de renseignement et de sécurité a posé la question préjudicielle suivante : « L'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité viole-t-il les articles 10 et 11 de la Constitution, lus seuls ou conjointement avec l'article 22 de la Constitution et/ou combinés ou non avec l'article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 et approuvée par la loi du 13 mai 1955, en tant qu'il ne prévoit pas en faveur de l'avocat, du médecin ou du journaliste de protection particulière pour les moyens de communication qu'ils utilisent à des fins autres que professionnelles ? ». Cette affaire est inscrite sous le numéro 7416 du rôle de la Cour, *M.B.* 31 août 2020

Sélection comparative d'assistant(e)s de direction (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État — Numéro de sélection : ANG20321, *M.B.* 13 novembre 2020

Résultat de la sélection comparative de data officers (m/f/x) (niveau B), francophones, pour la Sûreté de l'État — Numéro de sélection : AFG19290, *M.B.* 1er décembre 2020

Résultat de la sélection comparative de case officers (m/f/x) (niveau B), francophones, pour la Sûreté de l'État — Numéro de sélection : AFG19291, *M.B.* 1er décembre 2020

Résultat de la sélection comparative de data officers (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État — Numéro de sélection : ANG19326, *M.B.* 1er décembre 2020

Résultat de la sélection comparative d'assistants de direction (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État — Numéro de sélection : ANG20321, *M.B.* 31 décembre 2020

ANNEXE B
APERÇU DES PRINCIPALES PROPOSITIONS DE LOIS, DES PROJETS DE LOIS, DES RÉSOLUTIONS ET DES DÉBATS PARLEMENTAIRES RELATIFS AUX COMPÉTENCES, AU FONCTIONNEMENT ET AU CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'OCAM (1ER JANVIER 2020 AU 31 DÉCEMBRE 2020)

Chambre des représentants

Proposition de loi modifiant le Code de la nationalité belge afin de permettre la déchéance de la nationalité pour terrorisme, *Doc. parl.*, Chambre, 2019-2020, n° 55-0068/4

Proposition de résolution relative à la politique des ressources humaines au sein de la Défense, *Doc. parl.*, Chambre, 2019-2020, n° 55-567/6

Rapport d'activités 2018 du Comité permanent de contrôle des services de renseignement et de sécurité, *Doc. parl.*, Chambre, 2019-2020, n° 55-888/1

Proposition de loi modifiant la loi du 30 n°vembre 1998 organique des services de renseignement et de sécurité en vue d'instaurer des notes d'évaluation pour la collaboration avec les services de renseignement et de sécurité étrangers, *Doc. parl.*, Chambre, 2019-2020, n° 55-956/1

Proposition de loi modifiant le Code pénal en vue d'étendre la mise à la disposition du tribunal d'application des peines à l'ensemble des infractions terroristes, *Doc. parl.*, Chambre, 2019-2020, n° 55-969/1

Le déploiement du réseau 5G, audition, rapport, *Doc. parl.*, Chambre, 2019-2020, n° 55-981/1

Rapport annuel 2018 d'Unia, audition, rapport, *Doc. parl.*, Chambre, 2019-2020, n° 55-996/1

Proposition de résolution visant à mettre fin à l'Opération Vigilant Guardian, *Doc. parl.*, Chambre, 2019-2020, n° 55-1004/1

Projet de loi ouvrant des crédits provisoires pour les mois d'avril, mai et juin 2020, *Doc. parl.*, Chambre, 2019-2020, n° 55-1052/1

Projet de loi modifiant la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour, *Doc. parl.*, Chambre, 2019-2020, n° 55-1072/1

Proposition de résolution relative à l'avenir des missions d'aide à la nation de la Défense, *Doc. parl.*, Chambre, 2019-2020, n° 55-1196/1

Comité permanent de contrôle des services de renseignements et de sécurité – remplacement du greffier – appel aux candidats (*C.R.I.*, Chambre, 2019-2020, 30 avril 2020, PLEN 38, p. 70)

Proposition de loi modifiant portant des dispositions diverses en matière de justice, notamment dans le cadre de la lutte contre la propagation du coronavirus, *Doc. parl.*, Chambre, 2019-2020, n° 55-1295/1

Proposition de loi modifiant la loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, *Doc. parl.*, Chambre, 2019-2020, n° 55-1322/1 et 1322/4

Proposition de loi modifiant diverses dispositions concernant l'approche administrative et portant création d'une direction chargée de l'évaluation de l'intégrité des pouvoirs publics, *Doc. parl.*, Chambre, 2019-2020, n° 55-1381/1

Proposition de loi modifiant la loi du 13 juin 2005 relative aux communications électroniques en ce qui concerne la sécurité et l'intégrité des réseaux et des services publics de communications électroniques, *Doc. parl.*, Chambre, 2019-2020, n° 55-1488/1

Comité R – Nomination du premier suppléant et du second suppléant d'un membre effectif néerlandophone (*C.R.I.*, Chambre, 2019-2020, 17 septembre 2020, PLEN 55, p. 84)

Comité permanent de contrôle des services de renseignements et de sécurité – Nomination du premier suppléant d'un membre effectif néerlandophone (*C.R.I.*, Chambre, 2019-2020, 24 septembre 2020, PLEN 56, p. 53)

Projet de loi portant ajustement de la loi du 30 juin 2020 ouvrant des crédits provisoires pour les mois novembre et décembre 2020, *Doc. parl.*, Chambre, 2019-2020, n° 55-1532/1

Échange de vues avec l'amiral Michel Hofman, nouveau chef de la Défense, *Doc. parl.*, Chambre, 2019-2020, n° 55-1544/1

Comité permanent de contrôle des services de renseignements et de sécurité – Nomination du second suppléant de M. Pieter-Alexander De Brock, membre effectif néerlandophone (*C.R.I.*, Chambre, 2020-2021, 29 octobre 2020, PLEN 66, p. 47)

Comité permanent de contrôle des services de renseignements et de sécurité – Nomination du second suppléant de M. Pieter-Alexander De Brock, membre effectif néerlandophone – Résultat du scrutin (*C.R.I.*, Chambre, 2020-2021, 29 octobre 2020, PLEN 67, p. 10)

Projet de loi contenant le budget des Voies et Moyens de l'année budgétaire 2021, *Doc. parl.*, Chambre, 2020-2021, n^{os} 55-1577/1 et 55K1577/4

Projet de loi contenant le Budget général des dépenses de l'année budgétaire 2021, *Doc. parl.*, Chambre, 2020-2021, n^{os} 55-1578/1, 55-1578/3, 55-1578/7, 55-1578/12, 55-1578/16, 55-1578/18, 55K1578/23, 55-1578/33, 55K1578/41 et 55K1578/42

Justification du Budget général des dépenses pour l'année budgétaire 2021, *Doc. parl.*, Chambre, 2020-2021, n^{os} 55-1579/2, 55-1579/6, 55-1579/7, 55-1579/9 et 55-1579/10

Note de politique générale du premier ministre, *Doc. parl.*, Chambre, 2020-2021, n^{os} 55-1580/5 et 55-1580/16

Exposé d'orientation Politique du ministre de la Justice, *Doc. parl.*, Chambre, 2019-2020, n° 55-1610/15

Proposition de loi visant à renforcer la démocratie contre tout acte effectué en lien avec le nazisme et ses idéologies apparentées, *Doc. parl.*, Chambre, 2020-2021, n° 55- 1637/1

Plan d'opérations 2021, Audition, *Doc. parl.*, Chambre, 2020-2021, n° 55- 1706/1

Proposition de modification du Règlement de la Chambre des représentants en ce qui concerne les règles spécifiques applicables aux commissions spéciales afin de permettre à la commission des Achats et des ventes militaires de se réunir publiquement lorsqu'elle le décide (1319/1-2) (*C.R.I.*, Chambre, 2020-2021, 3 décembre 2020, PLEN 73, p. 48)

Comité permanent de contrôle des services de renseignements et de sécurité – Remplacement d'un membre francophone – Appel aux candidats (*C.R.I.*, Chambre, 2020-2021, 10 décembre 2020, PLEN 74, p. 31)

Comité permanent de contrôle des services de renseignement et de sécurité – Comptes de l'année budgétaire 2019 (1676/1-4) (*C.R.I.*, Chambre, 2020-2021, 17 décembre 2020, PLEN 81, p. 68)

ANNEXE C
APERÇU DES INTERPELLATIONS, DES DEMANDES D'EXPLICATIONS ET DES QUESTIONS ORALES ET ÉCRITES RELATIVES AUX COMPÉTENCES, AU FONCTIONNEMENT ET AU CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'OCAM (1ER JANVIER 2020 AU 31 DÉCEMBRE 2020)

Sénat

Question écrite de C. Van Cauter au ministre de la Justice sur la 'extrême droite et extrême gauche — menace de violences — augmentation — contacts internationaux des groupements d'extrême droite — nécessité d'enquêter' (Sénat, 2019-2020, 8 janvier 2020, Q. nº 7-271)

Question écrite de C. Van Cauter au ministre de l'Intérieur sur la 'extrême droite et extrême gauche — menace de violences — augmentation — contacts internationaux des groupements d'extrême droite — nécessité d'enquêter' (Sénat, 2019-2020, 8 janvier 2020, Q. nº 7-272)

Question écrite de C. Van Cauter au ministre de la Justice sur la 'cybercriminalité — cybersécurité — entreprises — Sûreté de l'État — coopération' (Sénat, 2019-2020, 31 janvier 2020, Q. nº 7-331)

Question écrite de C. Van Cauter au ministre de l'Intérieur sur la 'cybercriminalité — cybersécurité — entreprises — Sûreté de l'État — coopération' (Sénat, 2019-2020, 31 janvier 2020, Q. nº 7-332)

Question écrite de C. Van Cauter au ministre de la Justice sur la 'cybercriminalité — cybersécurité — entreprises – standards sécurisés de courriels' (Sénat, 2019-2020, 31 janvier 2020, Q. nº 7-334)

Question écrite de C. Van Cauter au ministre de la Justice sur la 'cybercriminalité — cybersécurité — entreprises — Sûreté de l'État — cyberattaques — conseils pour la sécurisation des données' (Sénat, 2019-2020, 31 janvier 2020, Q. nº 7-337)

Question écrite de C. Van Cauter au ministre de l'Intérieur sur la 'cybercriminalité — cybersécurité — entreprises — Sûreté de l'État — cyberattaques — conseils pour la sécurisation des données' (Sénat, 2019-2020, 31 janvier 2020, Q. nº 7-338)

Question écrite de C. Van Cauter au ministre de l'Intérieur sur l''extrême droite et extrême gauche — menace de violences — Allemagne — forums de discussion en ligne' (Sénat, 2019-2020, 9 mars 2020, Q. nº 7-385)

Question écrite de C. Van Cauter à la première ministre sur la 'cybercriminalité — cybersécurité — entreprises — Sûreté de l'État — coopération' (Sénat, 2019-2020, 25 mars 2020, Q. nº 7-419)

Question écrite de C. Van Cauter à la première ministre sur la 'cybercriminalité — cybersécurité — entreprises — Sûreté de l'État — cyberattaques offensives — conseils pour la sécurisation des données' (Sénat, 2019-2020, 25 mars 2020, Q. nº 7-420)

Question écrite de S. D'Hose au ministre de l'Intérieur sur la 'Crise du coronavirus — campagne de déstabilisation — fake news — déstabilisation de la démocratie' (Sénat, 2019-2020, 31 mars 2020, Q. nº 7-422)

Question écrite de S. D'Hose au ministre des Affaires étrangères sur la 'crise du coronavirus — campagne de déstabilisation — fake news — déstabilisation de la démocratie' (Sénat, 2019-2020, 31 mars 2020, Q. nº 7-423)

Question écrite de B. De Brabandere au ministre de l'Intérieur sur les 'groupements violents d'extrême gauche — Groupements actifs en Belgique' (Sénat, 2019-2020, 5 juin 2020, Q. nº 7-589)

Question écrite de R. Daems au ministre de la Justice sur les 'services de renseignements — conséquences du Brexit — sécurité — terrorisme — mandat d'arrêt européen' (Sénat, 2020-2021, 9 novembre 2020, Q. nº 7-757)
Question écrite de G. D'haeseleer au ministre de la Justice sur les 'personnes condamnées pour terrorisme — personnes suivies pour radicalisme — chiffres' (Sénat, 2020-2021, 9 novembre 2020, Q. nº 7-763)
Question écrite de G. D'haeseleer au ministre de la Justice sur les 'personnes condamnées pour terrorisme — personnes suivies pour radicalisme — chiffres' (Sénat, 2020-2021, 9 novembre 2020, Q. nº 7-764)
Question écrite de S. D'Hose au ministre de la Justice sur 'l'extrême droite et extrême gauche — menace de violences — Allemagne — forums de discussion en ligne' (Sénat, 2020-2021, 9 novembre 2020, Q. nº 7-769)
Question écrite de S. D'Hose au secrétaire d'État à la Digitalisation sur 'cybercriminalité — cybersécurité — entreprises — Sûreté de l'État — cyberattaques — conseils pour la sécurisation des données' (Sénat, 2020-2021, 9 novembre 2020, Q. nº 7-803)

Chambre des représentants
Question de M. Freilich à la Première ministre sur la '5G — risques de sécurité' (*Q.R.*, Chambre, 2019-2020, 7 janvier 2020, nº 8, p. 80, Q. nº 11)
Question de J. Chanson au ministre de l'Intérieur sur la 'lutte contre les dérives sectaires' (*Q.R.*, Chambre, 2019-2020, 7 janvier 2020, nº 8, p. 150, Q. nº 269)
Question de J. Arens au ministre de l'Intérieur sur la 'situation des cinq PJF de la police fédérale' (*Q.R.*, Chambre, 2019-2020, 7 janvier 2020, nº 8, p. 164, Q. nº 279)
Question de M. Freilich au ministre des Télécommunications sur la '5G — risques de sécurité' (*Q.R.*, Chambre, 2019-2020, 7 janvier 2020, nº 8, p. 227, Q. nº 44)
Débat d'actualité sur la problématique des FTF et questions jointes de K. Jadin, M. Ben Achour, G. Dallemagne, E. Samyn et S. Cogolati au ministre des Affaires étrangères sur 'les ingérences des services de renseignement rwandais en Belgique' (*C.R.I.*, Chambre, 2019-2020, 8 janvier 2020, COM 83, p. 38, Q. nºs 1550, 1563, 1566, 1646, 1565, 1681 et 2239)
Questions jointes de S. Cogolati, W. De Vriendt et E. Van Hoof au ministre des Affaires étrangères sur 'les ingérences des services de renseignement rwandais en Belgique' (*C.R.I.*, Chambre, 2019-2020, 21 janvier 2020, COM 91, p. 19, Q. nºs 1884, 1895 et 2305)
Questions jointes de S. Cogolati et W. De Vriendt au ministre des Affaires étrangères sur 'les cyberattaques contre la délégation belge en Chine' (*C.R.I.*, Chambre, 2019-2020, 21 janvier 2020, COM 91, p. 28, Q. nºs 1890 et 1897)
Question de M. Freilich au ministre de l'Intérieur 'la recrudescence de l'antisémitisme' (*Q.R.*, Chambre, 2019-2020, 22 janvier 2020, nº 9, p. 153, Q. nº 284)
Question de B. Pas au ministre de l'Intérieur 'le personnel de la police fédérale' (*Q.R.*, Chambre, 2019-2020, 22 janvier 2020, nº 9, p. 169, Q. nº 293)
Question de S. Rohonyi au au ministre de la Justice sur 'le suivi des détenus condamnés pour terrorisme pendant et après leur incarcération' (*C.R.I.*, Chambre, 2019-2020, 29 janvier 2020, COM 99, p. 13, Q. nº 2666)
Questions jointes de B. Pas, J.-M. Dedecker et P. De Roover à la première ministre sur 'le rapatriement d'enfants de combattants de l'EI' (*C.R.I.*, Chambre, 2019-2020, 30 janvier 2020, PLEN 22, p. 1, Q. nºs 394, 401 et 411)
Question de T. Vandenput au ministre de l'Intérieur sur 'l'étude du Vias Institute sur la collecte de données biométriques' (*C.R.I.*, Chambre, 2019-2020, 30 janvier 2020, PLEN 22, p. 11, Q. nº 405)

Question d'O. Depoortere au ministre de la Justice sur 'l'enquête sur les activités des Loups gris en Belgique' (*C.R.I.*, Chambre, 2019-2020, 5 février 2020, COM 103, p. 8, Q. nº 2778)

Débat d'actualité sur la 5G et questions jointes de M. Freilich, L. Dierick, V. Matz et K. Verhelst au ministre des Télécommunications sur 'la lettre d'avertissement des autorités américaines sur la sécurité des réseaux 5G' (*C.R.I.*, Chambre, 2019-2020, 5 février 2020, COM 104, p. 1, Q. nºs 2594, 2822, 2978, 3075, 3076 et 3085)

Question de D. Van Langenhove au ministre de la Justice sur 'le salafisme en Belgique' (*C.R.I.*, Chambre, 2019-2020, 6 février 2020, PLEN 23, p. 13, Q. nº 421)

Questions jointes de P. De Roover, B. Pas et S. Cogolati à la Première ministre sur 'les actions du gouvernement à la suite du jugement concernant les enfants de combattants de l'EI' (*C.R.I.*, Chambre, 2019-2020, 6 février 2020, PLEN 23, p. 20, Q. nºs 423, 433 et 442)

Question de J. Soors au ministre de la Justice sur le 'partage d'informations sur le terrorisme et la radicalisation avec les États-Unis' (*Q.R.*, Chambre, 2019-2020, 13 février 2020, nº 11, p. 48, Q. nº 234)

Échange de vues avec le ministre des Affaires étrangères et de la Défense suite à sa récente visite en Jordanie, en Irak et au Liban et questions jointes de K. Jadin, M. Ben Achour, S. Cogolati, J. Soors, E. Samyn, P. De Roover, G. Dallemagne et W. De Vriendt au ministre des Affaires étrangères sur 'la situation en Irak' (*C.R.I.*, Chambre, 2019-2020, 18 februari 2020, COM 113, p. 1, Q. nºs 2129, 2173, 2564, 2686, 2711, 2840, 2887, 3103, 3132, 3183, 3184, 3197, 3404 et 3442)

Question d'E. Samyn au ministre des Affaires étrangères sur les 'djihadistes belges détenus en Syrie et en Irak' (*Q.R.*, Chambre, 2019-2020, 24 février 2020, nº 12, p. 326, Q. nº 99)

Question de S. Cogolati au ministre des Affaires étrangères sur les 'escadrons de la mort rwandais en Belgique' (*Q.R.*, Chambre, 2019-2020, 24 février 2020, nº 12, p. 331, Q. nº 107)

Question de S. Creyelman au ministre des Affaires étrangères sur 'les dossiers politiques traités par le SGRS' (*Q.R.*, Chambre, 2019-2020, 24 février 2020, nº 12, p. 352, Q. nº 143)

Question de S. Creyelman au ministre des Affaires étrangères sur 'les dossiers politiques et la Sûreté de l'État' (*Q.R.*, Chambre, 2019-2020, 24 février 2020, nº 12, p. 353, Q. nº 145)

Question d'A. Ponthier au ministre des Affaires étrangères sur 'le recours aux réseaux sociaux par les militaires' (*Q.R.*, Chambre, 2019-2020, 24 février 2020, nº 12, p. 368, Q. nº 165)

Question de M. Freilich au ministre des Affaires étrangères sur le 'réseaux 5G – incidence sur la Défense et sur la sécurité nationale' (*Q.R.*, Chambre, 2019-2020, 24 février 2020, nº 12, p. 373, Q. nº 182)

Question d'Y. Van Camp au ministre des Affaires sociales sur 'le point de contact « radicalisation » de Fedasil' (*C.R.I.*, Chambre, 2019-2020, 3 mars 2020, COM 123, p. 43, Q. nº 2633)

Question de V. Scourneau au ministre de la Justice sur 'l'utilisation illégale du GSM en prison' (*Q.R.*, Chambre, 2019-2020, 10 mars 2020, nº 13, p. 148, Q. nº 186)

Question de V. Matz au ministre de l'Intérieur sur le 'plan d'Action Radicalisme – actualisation' (*Q.R.*, Chambre, 2019-2020, 10 mars 2020, nº 13, p. 225, Q. nº 337)

Question de M. Depraetere au ministre des Télécommunications sur 'les mesures de sécurité dans le cadre du développement des réseaux 5G' (*Q.R.*, Chambre, 2019-2020, 24 mars 2020, nº 14, p. 367, Q. nº 110)

Question de T. Van Grieken au ministre des Affaires étrangères sur 'les militaires islamistes' (*Q.R.*, Chambre, 2019-2020, 24 mars 2020, nº 14, p. 417, Q. nº 204)

Question de V. Scourneau au ministre de la Justice sur le 'recensement des imams' (*Q.R.*, Chambre, 2019-2020, 9 april 2020, nº 15, p. 115, Q. nº 181)

Question de C. Thibaut au ministre de l'lntérieur sur la 'manifestation antifasciste à Gilly' (*Q.R.*, Chambre, 2019-2020, 9 april 2020, nº 15, p. 211, Q. nº 389)

Question de S. Cogolati au ministre de la Justice sur 'la protection de la communauté kurde en Belgique' (*C.R.I.*, Chambre, 2019-2020, 22 april 2020, COM 156, p. 43, Q. nº 5102)

Question de Ch. Lacroix au ministre des Affaires étrangères sur 'la réforme du SGRS' (*C.R.I.*, Chambre, 2019-2020, 29 april 2020, COM 162, p. 19, Q. nº 3923)

Questions jointes de Ch. Lacroix et B. Delvaux au ministre des Affaires étrangères sur 'la lutte contre les 'fake news' et l'extrême droite' (*C.R.I.*, Chambre, 2019-2020, 29 avril 2020, COM 162, p. 45, Q. nºs 5339 et 5524)

Question de K. Metsu au ministre de l'lntérieur sur 'Daesh sur les réseaux sociaux' (*Q.R.*, Chambre, 2019-2020, 4 mai 2020, nº 17, p. 153, Q. nº 444)

Débat d'actualité sur les rapatriements depuis le Maroc et questions jointes d'A. Van Bossuyt, S. Cogolati, G. Daems, N. Boukili, M. Ben Achour, F. De Smet, M. De Maegd, J. Crombez, et N. Lanjri sur 'les rapatriements au départ du Maroc' (*C.R.I.*, Chambre, 2019-2020, 19 mai 2020, COM 179, p. 1, Q. nºs 5511, 5645, 5695, 6238, 5761, 5842, 6066, 6073, 6224, 6236 et 6249)

Interpellation et questions jointes d'A. Van Bossuyt, G. Dallemagne, T. Francken, M. Bihet et A. Ponthier au ministre des Affaires étrangères et Défense sur 'la désinformation de la part de la Chine' (*C.R.I.*, Chambre, 2019-2020, 19 mai 2020, COM 179, p. 44, Q. nºs 5788, 5876, 5997, 6045, 6051 et 12I)

L'impact du COVID-19 sur la justice: débat d'actualité et questions jointes de S. Cogolati, S. Van Hecke, L. Hennuy, Ph. Pivin, O. Ozan, S. Thémont, V. Matz, B. Segers, K. Gabriëls, N. Boukili, K. Aouasti et N. Gilson sur 'l'espionnage chinois en Belgique durant la crise du COVID-19' (*C.R.I.*, Chambre, 2019-2020, 19 mai 2020, COM 182, p. 1, Q. nºs 5867, 5885, 5935, 6041, 6062, 6078, 6079, 6148, 6159, 6191, 6228, 6247 et 6242)

Questions jointes de K. Metsu, B. Segers et Ph. Pivin au ministre de la Justice sur 'le suivi des terroristes libérés' (*C.R.I.*, Chambre, 2019-2020, 19 mai 2020, COM 182, p. 16, Q. nºs 5863, 6005 et 6063)

Question de M. Freilich au ministre des Affaires étrangères sur 'les aides d'État en faveur de Huawei' (*Q.R.*, Chambre, 2019-2020, 27 mai 2020, nº 19, p. 370, Q. nº 283)

Questions jointes de S. De Wit, K. Bury et B. Slegers au ministre de la Justice sur 'l'enlèvement d'un enfant par des musulmans radicalisés' (*C.R.I.*, Chambre, 2019-2020, 3 juin 2020, COM 193, p. 46, Q. nºs 6674, 6716 et 6729)

Masques de protection: débat d'actualité et questions jointes de P. Prévot, J. Bertels, P. Buysrogge, K. Verduyckt, S. Creyelman, J. Crombez, Y. Van Camp, N. Moscufo, H. Bayet, J. Chanson, G. Dallemagne, W. De Vriendt, K. Depoorter et M. Freilich au ministre de Affaires sociales sur 'la commande de 15 millions de masques à la société luxembourgeoise Avrox' (*C.R.I.*, Chambre, 2019-2020, 3 juin 2020, COM 195, p. 1, Q. nºs 6195, 6290, 6340, 6354, 6359, 6389, 6393, 6403, 6435, 6461, 6486, 6610, 6618, 6627, 6684, 6690 et 6724)

Question de K. Jadin au ministre de l'lntérieur sur 'la mise en garde contre l'extrême droite' (*Q.R.*, Chambre, 2019-2020, 9 juin 2020, nº 20, p. 204, Q. nº 516)

Question de K. Jadin au ministre de l'lntérieur sur 'l'extrême gauche' (*Q.R.*, Chambre, 2019-2020, 9 juin 2020, nº 20, p. 207, Q. n° 517)

Question de S. Mahdi au ministre des Affaires étrangères sur 'la gestion de la menace représentée par les drones' (*C.R.I.*, Chambre, 2019-2020, 17 juin 2020, COM 210, p. 33, Q. nº 6187)

Question de Ph. Pivin au ministre de la Justice sur 'la récidive chez les terroristes belges condamnés ' (*C.R.I.*, Chambre, 2019-2020, 17 juin 2020, COM 216, p. 1, Q. n° 6818)

Question de L. Dierick au ministre de la Justice sur le 'SPF Justice — délais de paiement' (*Q.R.*, Chambre, 2019-2020, 18 juin 2020, n° 21, p. 96, Q. n° 306)

Question de J. Soors au ministre de la Justice sur 'l'évaluation finale de la Note-cadre de Sécurité intégrale' (*Q.R.*, Chambre, 2019-2020, 18 juin 2020, n° 21, p. 101, Q. n° 364)

Question de S. Van Hecke au ministre de la Justice sur les 'arriérés de paiement des pouvoirs publics – introduction de FEDCOM auprès du SPF Justice' (*Q.R.*, Chambre, 2019-2020, 18 juin 2020, n° 21, p. 103, Q. n° 373)

Question de M. Freilich au ministre des Affaires étrangères sur '5G et F-35' (*Q.R.*, Chambre, 2019-2020, 18 juin 2020, n° 21, p. 378, Q. n° 374)

Questions jointes de S. De Wit et K. Bury au ministre de la Justice sur 'les suites de l'enlèvement d'un mineur d'âge par des extrémistes musulmans' (*C.R.I.*, Chambre, 2019-2020, 24 juin 2020, COM 219, p. 4, Q. nos 7238 et 7256)

Question de G. Colebunders au ministre de la Justice sur 'la préoccupation des services de renseignement concernant la montée de l'extrême droite' (*C.R.I.*, Chambre, 2019-2020, 24 juin 2020, COM 219, p. 14, Q. n° 7388)

Question de J. Soors au ministre de la Justice sur 'la menace de l'extrême droite' (*C.R.I.*, Chambre, 2019-2020, 25 juin 2020, PLEN 047, p. 19, Q. n° 863)

Questions jointes de K. Verhelst et M. Freilich au ministre des Télécommunications sur 'les décisions du CNS ayant une incidence sur le choix des fournisseurs pour la 5G' (*C.R.I.*, Chambre, 2019-2020, 25 juin 2020, PLEN 047, p. 28, Q. nos 852 et 870)

Débat d'actualité sur le COVID-19 et questions jointes de P. De Spiegeleer, M. Kitir, M. Bihet, C. Thibaut, O. Depoortere, T. Vandenput, F. Demon, J. Donné, C. Thibaut, B. Segers, K. Metsu, D. Senesael, L. Zanchetta et J. Chanson au ministre de l'Intérieur sur 'les interventions dans les trains et les gares dans le cadre des manifestations BLM' (*C.R.I.*, Chambre, 2019-2020, 30 juin 2020, COM 223, p. 1, Q. nos 6955, 6957, 7027, 7032, 7223, 7248, 7363, 7373, 7399, 7463, 7514, 7431, 7503, 7525 et 7527)

Questions jointes de Ph. Pivin et S. Rohonyi au ministre de la Justice sur 'le rapatriement de combattants partis en Syrie' (*C.R.I.*, Chambre, 2019-2020, 1er juillet 2020, COM 226, p. 10, Q. nos 7449 et 7496)

Questions jointes de C. Taquin, Z. Khattabi et S. Van Hecke au ministre de la Justice sur 'le rapatriement de combattants partis en Syrie' (*C.R.I.*, Chambre, 2019-2020, 1er juillet 2020, COM 226, p. 22, Q. nos 7475, 7515 et 7574)

Questions jointes de K. Metsu et B. Pas au ministre de la Justice sur 'le rapatriement de combattants partis en Syrie' (*C.R.I.*, Chambre, 2019-2020, 1er juillet 2020, COM 226, p. 36, Q. nos 7544 et 7577)

Question de S. Cogolati au ministre de l'lntérieur sur 'l'activité sismique en Allemagne et les normes de sûreté nucléaire' (*C.R.I.*, Chambre, 2019-2020, 1er juillet 2020, COM 228, p. 23, Q. n° 7262)

Question de V. Matz au ministre de l'lntérieur sur 'le rapport de l'AIG de 2019 sur les contrôles d'intégrité à la police' (*C.R.I.*, Chambre, 2019-2020, 1er juillet 2020, COM 228, p. 21, Q. n° 6940)

Question d'O. Depoortere au ministre de l'lntérieur sur 'l'extrémisme de gauche en Belgique' (*C.R.I.*, Chambre, 2019-2020, 1er juillet 2020, COM 228, p. 31, Q. n° 7372)

Question de C. Taquin au ministre de l'lntérieur sur 'les mesures de contrôle et de lutte à l'encontre des organisations sectaires' (*C.R.I.*, Chambre, 2019-2020, 1er juillet 2020, COM 228, p. 33, Q. n° 7476)

Question de J. Soors au ministre de l'lntérieur sur 'les camps d'entraînement d'extrême droite en Russie' (*Q.R.*, Chambre, 2019-2020, 2 juli 2020, n° 22, p. 145, Q. n° 526)

Question de M. Freilich au ministre de l'lntérieur sur la 'mise en service de la DAB' (*Q.R.*, Chambre, 2019-2020, 2 juli 2020, nº 22, p. 224, Q. nº 299)
Question de M. Kitir au ministre des Affaires étrangères sur 'les habilitations de sécurité pour le personnel de Brussels Airport' (*Q.R.*, Chambre, 2019-2020, 2 juli 2020, nº 22, p. 390, Q. nº 301)
Question de T. Vandenput au ministre de l'lntérieur sur 'le maintien de l'habilitation de sécurité des travailleurs de Swissport chez Alyzia' (*C.R.I.*, Chambre, 2019-2020, 14 juillet 2020, COM 235, p. 35, Q. nº 7757)
Question de G. Dallemagne au ministre des Affaires étrangères sur 'la lettre de l'ambassade de Chine adressée à La Libre' (*C.R.I.*, Chambre, 2019-2020, 14 juillet 2020, COM 235, p. 39, Q. nº 7797)
Questions jointes de S. Cogolati et K. Metsu au ministre de la Justice sur 'le risque d'exécutions arbitraires de ressortissants belges en Irak' (*C.R.I.*, Chambre, 2019-2020, 14 juillet 2020, COM 236, p. 2, Q. nºs 7770 et 7851)
Question de S. Schlitz au ministre de l'lntérieur sur 'l'inquiétude d'Europol au sujet des «Incels», du terrorisme d'extrême droite et des antiféministes' (*C.R.I.*, Chambre, 2019-2020, 14 juillet 2020, COM 239, p. 1, Q. nº 7553)
Question de S. Creyelman au ministre de la Justice sur 'les dossiers politiques et la Sûreté de l'État' (*Q.R.*, Chambre, 2019-2020, 16 juillet 2020, nº 23, p. 73, Q. nº 351)
Question de J. Soors au ministre de la Justice sur les 'infox concernant le COVID-19 et la 5G' (*Q.R.*, Chambre, 2019-2020, 16 juillet 2020, nº 23, p. 78, Q. nº 424)
Question d'E. Burton au ministre de l'Intérieur sur 'le kidnapping de Genk' (*Q.R.*, Chambre, 2019-2020, 16 juillet 2020, nº 23, p. 141, Q. nº 618)
Question de Ph. Pivin au ministre de la Justice sur la 'Sûreté de l'État — espionnage économique en Belgique' (*Q.R.*, Chambre, 2019-2020, 5 août 2020, nº 24, p. 195, Q. nº 323)
Question de J. Soors au ministre de l'Intérieur sur 'l'extrémisme de droite en Belgique' (*Q.R.*, Chambre, 2019-2020, 5 août 2020, nº 24, p. 299, Q. nº 640)
Question de V. Scourneau au ministre des Affaires étrangères sur 'OSINT' (*Q.R.*, Chambre, 2019-2020, 5 août 2020, nº 24, p. 465, Q. nº 407)
Question de J. Soors au ministre de la Justice sur 'le rapport annuel de la Sûreté de l'État' (*Q.R.*, Chambre, 2019-2020, 27 août 2020, nº 25, p. 161, Q. nº 588)
Question de B. Friart au ministre de la Justice sur la 'Sûrêté de l'État' (*Q.R.*, Chambre, 2019-2020, 27 août 2020, nº 25, p. 164, Q. nº 590)
Question de G. Colebunders au ministre de l'Intérieur sur 'les inquiétudes des services de sécurité à propos de la menace d'extrême droite' (*Q.R.*, Chambre, 2019-2020, 27 août 2020, nº 25, p. 193, Q. nº 663)
Question de L. Dierick au ministre des Télécommunications sur la '5G Proximus' (*Q.R.*, Chambre, 2019-2020, 8 septembre 2020, nº 26, p. 303, Q. nº 252)
Question de S. Cogolati au ministre des Affaires étrangères sur 'le rôle du SGRS dans la surveillance de djihadistes belges' (*Q.R.*, Chambre, 2019-2020, 8 septembre 2020, nº 26, p. 373, Q. nº 460)
Questions jointes de K. Verduyckt, A. Ponthier, A. Vicaire et S. Mahdi au ministre de la Justice sur 'le manque de surveillance des sectes' (*C.R.I.*, Chambre, 2019-2020, 16 septembre 2020, COM 259, p. 19, Q. nºs 8364, 8386, 8493 et 8784)
Question de Z. Khattabi au ministre de la Justice sur les 'retards de paiements' (*Q.R.*, Chambre, 2019-2020, 22 septembre 2020, nº 27, p. 93, Q. nº 593)
Question d'E. Thiébaut au ministre de la Justice sur 'les modalités de visite des prisons belges pour les journalistes' (*Q.R.*, Chambre, 2019-2020, 22 septembre 2020, nº 27, p. 107, Q. nº 639)

Questions jointes de S. Van Hecke, S. De Wit, K. Gabriëls et N. Lanjri au ministre de la Justice sur 'le manque de surveillance des sectes' (*C.R.I.*, Chambre, 2019-2020, 23 septembre 2020, COM 268, p. 13, Q. nos 8511, 8512, 8649, 8757 et 8872)

Questions jointes de S. Van Hecke en Z. Khattabi au ministre de la Justice sur 'le manque de surveillance des sectes' (*C.R.I.*, Chambre, 2019-2020, 23 septembre 2020, COM 268, p. 21, Q. nos 8540 et 8725)

Questions jointes de S. Van Hecke au ministre de la Justice sur la 'personne de confiance et point de contact pour les atteintes à l'intégrité à la Sûreté de l'État' (*C.R.I.*, Chambre, 2019-2020, 23 septembre 2020, COM 268, p. 46, Q. nos 8894 et 8895)

Question de J. Soors au ministre de la Justice sur 'les camps d'entraînement à l'étranger' (*Q.R.*, Chambre, 2019-2020, 30 septembre 2020, no 28, p. 54, Q. n° 586)

Question de J. Chanson au ministre de l'Intérieur sur 'l'isolement des victimes d'organisations sectaires' (*Q.R.*, Chambre, 2019-2020, 30 septembre 2020, no 28, p. 107, Q. n° 707)

Question de J. Soors au ministre des Affaires étrangères sur 'l'avis de sécurité négatifs de l'Autorité Nationale de Sécurité' (*Q.R.*, Chambre, 2019-2020, 30 septembre 2020, no 28, p. 406, Q. n° 424)

Question d'A. Ponthier au ministre des Affaires étrangères sur 'le certificat de sécurité des militaires' (*Q.R.*, Chambre, 2019-2020, 30 septembre 2020, no 28, p. 433, Q. n° 466)

Question de S. Cogolati au ministre des Affaires étrangères sur 'l'accord de coopération entre le SGRS et le NISS' (*Q.R.*, Chambre, 2019-2020, 30 septembre 2020, no 28, p. 451, Q. n° 495)

Externalisation : débat d'actualité et questions jointes d'A.Ponthier, K. Jadin, J. Pillen, R. D'Amico en J. Chanson à la ministre de la Défense sur 'la collaboration entre la Défense et Katoen Natie en matière d'externalisation' (*C.R.I.*, Chambre, 2019-2020, 14 octobre 2020, COM 278, p. 1, Q. Q. nos 9181, 9382, 9637, 9660 et 9672)

Question d'A. Van Bossuyt au ministre de la Justice sur 'la lutte contre les activités d'espionnage de la Chine et leur suivi par la Sûreté de l'État' (*C.R.I.*, Chambre, 2019-2020, 14 octobre 2020, COM 281, p. 19, Q. no 9255)

Question de G. Dallemagne et J. Soors au ministre de la Justice sur 'l'ASBL Smals et la Sûreté de l'État' (*C.R.I.*, Chambre, 2019-2020, 14 octobre 2020, COM 281, p. 26, Q. nos 9357, 9361 et 9457)

Question de G. Dallemagne au ministre de la Justice sur 'le conflit au sein de la VSSE' (*C.R.I.*, Chambre, 2019-2020, 14 octobre 2020, COM 281, p. 30, Q. no 9358)

Question de K. Metsu au premier ministre sur 'la lutte contre le terrorisme à la suite des initiatives du président français' (*C.R.I.*, Chambre, 2019-2020, 22 octobre 2020, COM 265, p. 36, Q. no 1051)

Questions jointes d'O. Depoortere et Ph. Pivin au ministre de l'Intérieur sur 'la lutte contre les associations islamistes suite aux actes terroristes en Allemagne et en France' (*C.R.I.*, Chambre, 2019-2020, 22 octobre 2020, PLEN 265, p. 39, Q. nos 1046 et 1052)

Question d'A. Van Bossuyt au premier ministre sur 'les cyberattaques de la Chine ciblant la Belgique' (*C.R.I.*, Chambre, 2020-2021, 28 octobre 2020, COM 291, p. 12, Q. no 9252)

Question de K. Metsu au ministre de la Justice sur 'la formation d'imam' (*C.R.I.*, Chambre, 2020-2021, 28 octobre 2020, COM 295, p. 28, Q. no 10116)

Questions jointes de S. Cogolati, B. Segers, Koen Metsu et K. Bury au ministre de la Justice sur 'la présence de criminels de guerre syriens en Belgique' (*C.R.I.*, Chambre, 2020-2021, 28 octobre 2020, COM 295, p. 46, Q. nos 10264, 10298, 10350 et 10405)

Question de K. Metsu au ministre de la Justice sur 'les organisations islamistes belges incitant à la haine, à la violence et à la discrimination' (*C.R.I.*, Chambre, 2020-2021, 28 octobre 2020, COM 295, p. 63, Q. no 10349)

Questions jointes de K. Metsu et M. Dillen au premier ministre sur 'l'attentat de Nice' (*C.R.I.*, Chambre, 2020-2021, 29 octobre 2020, PLEN 066, p. 19, Q. n^{os} 1072 et 1076)

Question d'Y. Van Camp au ministre de la Migration sur 'les musulmans radicalisés' (*C.R.I.*, Chambre, 2020-2021, 30 octobre 2020, COM 296, p. 20, Q. n^{o} 10086)

Question de D. Ducarme au ministre de l'Intérieur sur 'la collaboration entre la police et la Défense dans la lutte contre le terrorisme' (*C.R.I.*, Chambre, 2019-2020, 12 novembre 2020, PLEN 70, p. 30, Q. n^{o} 1104)

Débat d'actualité et questions jointes de M. De Maegd, K. Metsu, O. Depoortere, Ph. Pivin, T. Vandenput, F. Demon, E. Thiébaut, D. Ducarme, G. Dallemagne, F. De Smet, sur 'la menace terroriste' (*C.R.I.*, Chambre, 2020-2021, 16 novembre 2020, COM 303, p. 1, Q. n^{os} 10001, 10412, 10424, 10516, 10522, 10525, 10524, 10526, 10565, 10679, 10690, 10692, 10724, 10812, 10813, 10814, 10816 et 10817)

Question de K. Metsu au ministre de la Justice sur 'la récidive chez les terroristes condamnés' (*Q.R.*, Chambre, 2019-2020, 2 décembre 2020, n^{o} 29, p. 184, Q. n° 6)

Question de J. Soors au ministre de la Justice sur 'la liste nationale des terroristes' (*Q.R.*, Chambre, 2019-2020, 2 décembre 2020, n^{o} 29, p. 188, Q. n° 11)

Question de M. Dillen au ministre de la Justice sur la 'libération de terroristes condamnés' (*Q.R.*, Chambre, 2019-2020, 2 décembre 2020, n^{o} 29, p. 222, Q. n° 95)

Question de K. Metsu au ministre de l'Intérieur sur 'la poursuite judicieuse de projets de la Suédoise en matière de sécurité' (*Q.R.*, Chambre, 2019-2020, 2 décembre 2020, n^{o} 29, p. 260, Q. n° 82)

Question de M. Vindevoghel au ministre de la Fonction publique sur 'le rôle de bpost et Proximus dans le cadre de la vaccination contre le coronavirus' (*C.R.I.*, Chambre, 2020-2021, 8 décembre 2020, COM 313, p. 53, Q. n^{o} 11472)

Question de K. Verduyckt au ministre de l'Intérieur sur 'l'accès aux informations cryptées et aux chats dans le cadre de la lutte contre le terrorisme' (*C.R.I.*, Chambre, 2020-2021, 9 décembre 2020, COM 315, p. 43, Q. n^{o} 11428)

Question de S. Verherstraeten au ministre de la Justice sur 'le procès pénal faisant suite à la tentative d'attentat à la bombe par un couple belgo-iranien' (*C.R.I.*, Chambre, 2020-2021, 9 décembre 2020, COM 316, p. 18, Q. n^{o} 11196)

Question de C. Thibaut au ministre de la Justice sur 'la présence d'adeptes de la théorie QAnon sur notre territoire' (*C.R.I.*, Chambre, 2020-2021, 9 décembre 2020, COM 316, p. 27, Q. n^{o} 11299)

Question de C. Thibaut au ministre de la Justice sur 'les activités éventuelles de personnes proches des Loups gris en Belgique' (*C.R.I.*, Chambre, 2020-2021, 9 décembre 2020, COM 316, p. 29, Q. n^{o} 11300)

Questions jointes de C. Thibaut au ministre de la Justice sur 'le rôle et la lenteur du fédéral quant à la reconnaissance de la Grande Mosquée à Bruxelles' (*C.R.I.*, Chambre, 2020-2021, 9 décembre 2020, COM 316, p. 30, Q. n^{os} 11301 et 11386)

Question de M. Freilich au ministre de la Justice sur 'TikTok' (*Q.R.*, Chambre, 2020-2021, 9 décembre 2020, n^{o} 29, p. 257, Q. n° 49)

Question de K. Jadin au ministre de l'Intérieur sur 'les avis de sécurité négatifs à l'encontre de douaniers' (*Q.R.*, Chambre, 2020-2021, 9 décembre 2020, n^{o} 30, p. 352, Q. n° 12)

Question de K. Bury au ministre de la Justice sur 'les imams, mosquées et associations prêchant le radicalisme islamique' (*Q.R.*, Chambre, 2020-2021, 16 décembre 2020, n^{o} 31, p. 315, Q. n° 58)

Question de T. Van Grieken au ministre de la Justice sur 'l'agrément des mosquées' (*Q.R.*, Chambre, 2020-2021, 16 décembre 2020, n^{o} 31, p. 318, Q. n° 63)

Question de T. Van Grieken au ministre de la Justice sur le 'screening des candidats à l'asile' (*Q.R.*, Chambre, 2020-2021, 16 décembre 2020, n^{o} 31, p. 339, Q. n° 115)

Question de S. Van Hecke au ministre de la Justice sur la 'VSSE — bien-être — personne de confiance et intégrité' (*Q.R.*, Chambre, 2020-2021, 16 décembre 2020, n° 32, p. 383, Q. n° 57)

Question de K. Gabriëls au ministre de la Justice sur la 'VSSE — réformes récentes' (*Q.R.*, Chambre, 2020-2021, 16 décembre 2020, n° 32, p. 385, Q. n° 67)

Question de Ph. Pivin au ministre de la Justice sur le 'screening visiteurs prisons' (*Q.R.*, Chambre, 2020-2021, 16 décembre 2020, n° 33, p. 238, Q. n° 181)