ACTIVITEITENVERSLAG 2014
RAPPORT D'ACTIVITÉS 2014

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 5, 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.

ACTIVITEITENVERSLAG 2014

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

Vast Comité van Toezicht op de inlichtingen-
en veiligheidsdiensten

intersentia
Antwerpen – Cambridge

Voorliggend *Activiteitenverslag 2014* werd door het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten goedgekeurd op de vergadering van 29 juni 2015.

(*getekend*)
Guy Rapaille, voorzitter
Gérald Vande Walle, raadsheer
Pieter-Alexander De Brock, raadsheer
Wouter De Ridder, griffier

Activiteitenverslag 2014
Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

ISBN 978-94-000-0614-0
D/2015/7849/123
NUR 823

INHOUD

LIJST MET AFKORTINGEN

ADCC	Algemene Directie Crisiscentrum
ADIV	Algemene Dienst inlichting en veiligheid van de Krijgsmacht
BIA	*Belgian Intelligence Academy*
BICS	*Belgacom International Carrier Services*
BIM	Bijzondere inlichtingenmethoden
BIM-Commissie	Bestuurlijke Commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door inlichtingen- en veiligheidsdiensten
BIM-Wet	Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten
BISC	*Belgian Intelligence Studies Centre*
BS	Belgisch Staatsblad
BSS	*British Security Service (MI5)*
CBPL	Commissie voor de bescherming van de persoonlijke levenssfeer
CCB	Centrum voor Cybersecurity België
CERT	*Computer Emergency Respons Team*
CIA	*Central Intelligence Agency*
CRIV	Compte Rendu Intégral – Integraal Verslag
CTIVD	Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (Nederland)
DCSG	Dienst Controle Strategische Goederen
DVZ	Dienst Vreemdelingenzaken
D&A	Administratie der Douane en Accijnzen
EU	Europese Unie
EVRM	Europees Verdrag voor de Rechten van de Mens
FOD	Federale overheidsdienst
GCHQ	*Government Communications Headquarters*
Parl.St.	Parlementaire Stukken van Kamer en Senaat
Hand.	Handelingen
HUMINT	*Human intelligence*
ICT	*Information and Communication Technologies*
IMINT	*Image intelligence*
INT-regeling	Interceptiebevoegdheid op basis van art. 259*bis* § 5 Strafwetboek en art. 44*bis* W.I&V

ISTAR	*Intellligence, Surveillance, Target Acquisition and Reconnaissance*
JIB	*Joint information box*
K.B.	Koninklijk besluit
KB C&VM	Koninklijk besluit van 24 maart 2000 tot uitvoering van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen
KB OCAD	Koninklijk besluit van 28 november 2006 tot uitvoering van de Wet van 10 juli 2006 betreffende de analyse van de dreiging
M.B.	Ministerieel besluit
MCIV	Ministerieel Comité voor inlichting en veiligheid
NSA	*National Security Agency*
NVO	Nationale Veiligheidsoverheid
NVR	Nationale Veiligheidsraad
OCAD	Coördinatieorgaan voor de dreigingsanalyse
OSINT	*Open sources intelligence*
Parl. St.	Parlementaire Stukken
SIGINT	*Signals intelligence*
SIS	*Secret Intelligence Service (MI6)*
Sv.	Wetboek van Strafvordering
Sw.	Strafwetboek
UNO	*United Nations Organisation*
Vast Comité I	Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten
Vast Comité P	Vast Comité van Toezicht op de politiediensten
VPN	*Virtual Private Network*
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
WEP	Wetenschappelijk en economisch potentieel
W.OCAD	Wet van 10 juli 2006 betreffende de analyse van de dreiging
W.Toezicht	Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatie-orgaan voor de dreigingsanalyse

WOORD VOORAF

Begin januari 2015 vallen tijdens een schietpartij in het hoofdkantoor van het Franse satirische weekblad 'Charlie Hebdo' twaalf dodelijke slachtoffers. Nagenoeg gelijktijdig speelt er zich een gijzeling af in een Joodse supermarkt ten oosten van Parijs. Hierbij komen vijf mensen om het leven. Amper enkele dagen later vindt in België een grote gecoördineerde antiterrorisme-actie plaats en worden op verschillende plaatsen huiszoekingen gehouden. Daarbij worden in Verviers tijdens een vuurgevecht twee teruggekeerde Syriëstrijders gedood en raakt een derde gewond. De drie mannen werden reeds langer in het oog gehouden door de inlichtingendiensten.

De reacties bleven niet uit. Het kernkabinet stelde meteen een lijst op met twaalf maatregelen in de strijd tegen terrorisme en radicalisme. De inzet van het leger voor bewakingsopdrachten was daarbij wellicht de meest in het oog springende.

Een aantal van die maatregelen hebben een directe impact op de werking van de Belgische inlichtingen- en veiligheidsdiensten: de Omzendbrief 'foreign fighters' van september 2014 zal worden aangepast; het Actieplan Radicalisme – dat ondertussen dateert van 2005 – moet worden geactualiseerd; er wordt een Nationale Veiligheidsraad opgericht; en de bijzondere beschermingsopdrachten die worden uitgevoerd door de Veiligheid van de Staat zullen worden overgeheveld naar de Federale Politie.

Het Vast Comité I heeft de gebeurtenissen in Parijs en Verviers niet afgewacht. In 2014 voerde het reeds een aantal toezichtonderzoeken die relevant zijn in het kader van deze regeringsbeslissingen en die zeker van nut kunnen zijn bij de implementatie van de voorgestelde maatregelen.

Zo werd begin 2014 een toezichtonderzoek afgerond naar de wettelijke opdracht van persoonsbescherming van de Veiligheid van de Staat. De resultaten van dit onderzoek kunnen hun nut bewijzen bij de discussie inzake de overheveling van deze opdracht van de VSSE naar de Federale Politie.

Het lopende toezichtonderzoek naar de opvolging van extremistische elementen in het leger werd vorig jaar ook uitgebreid met informatie over de Syriëproblematiek. Tevens werd de laatste hand gelegd aan een onderzoek naar de wijze waarop het Coördinatieorgaan voor de dreigingsanalyse de informatie opgeslagen in de zogenaamde 'Joint information box' (JIB) beheert, analyseert en verspreidt, en dit overeenkomstig de bepalingen uit het Plan Radicalisme.

Nog in 2014 opende het Comité een onderzoek naar de samenwerking tussen de Veiligheid van de Staat en het gevangeniswezen. Meer bepaald wil het Comité nagaan of de betere informatie-uitwisseling waartoe in een protocol is beslist, ook effectief plaatsvindt.

En ten slotte kon de problematiek van de 'foreign fighters' en de Syriëgangers uiteraard niet ontbreken. Het Vast Comité I startte een onderzoek naar de informatiepositie van de Algemene Dienst inlichting en veiligheid en de Veiligheid van de Staat over de rekrutering, de zending, het verblijf en de terugkeer van jongeren die vertrekken of vertrokken zijn naar Syrië of Irak.

Het Vast Comité I is er van overtuigd dat deze onderzoeken zullen leiden tot onderbouwde aanbevelingen die nuttig zijn voor de verdere implementatie van de maatregelen die noodzakelijk zijn in de strijd tegen het radicalisme en het terrorisme, zonder daarbij evenwel de aandacht te verliezen voor de bescherming van de fundamentele rechten van de mens.

Wat betreft dat aspect van de bescherming van de mensenrechten, werd in 2014 door het Vast Comité I overigens nauw samengewerkt met de Commissie Burgerlijke Vrijheden, Justitie en Binnenlandse Zaken (LIBE) van het Europees Parlement, onder meer met het oog op het finaliseren van een Resolutie naar aanleiding van de Snowden-onthullingen.

Guy Rapaille,
Voorzitter van het Vast Comité van Toezicht
op de inlichtingen- en veiligheidsdiensten

1 juni 2015

HOOFDSTUK I
DE OPVOLGING VAN DE AANBEVELINGEN VAN HET VAST COMITÉ I

Het Vast Comité I formuleert ten behoeve van de wetgever en de uitvoerende macht jaarlijks aanbevelingen die in het bijzonder betrekking hebben op de rechtmatigheid, de coördinatie en de doelmatigheid van het optreden van de twee Belgische inlichtingendiensten, van het OCAD en – in beperkte mate – van zijn ondersteunende diensten.[1] De aanbevelingen die het Comité in 2014 formuleerde, zijn opgenomen in het laatste hoofdstuk van dit activiteitenverslag. In dit inleidende hoofdstuk worden de belangrijkste initiatieven[2] opgesomd die de diverse actoren namen in de lijn van voorgaande aanbevelingen van het Vast Comité I. Tevens wordt extra aandacht gevestigd op aanbevelingen die het Comité essentieel acht, maar die vooralsnog niet werden geïmplementeerd.

I.1. INITIATIEVEN EN REALISATIES IN DE LIJN VAN DE DIVERSE AANBEVELINGEN

I.1.1. HAALBARE PRIORITEITEN

Tot voor kort somde de VSSE in het operationele luik van haar jaarlijkse actieplannen om en bij de 150 thema's op die 'actief prioritair' of 'actief' dienden opgevolgd te worden. De VSSE besloot zelf dat het – rekening houdend met de personele middelen waarover ze beschikt – niet mogelijk was om voor elk van deze problematieken de nodige inlichtingenagenten in te zetten. Het Vast Comité I was de mening toegedaan dat het opstellen van actieplannen dient te gebeuren in functie van de beschikbare personele, budgettaire en technische middelen en dit in over-

1 Wat het OCAD en de ondersteunende diensten betreft, gebeuren de onderzoeken samen met het Vast Comité P (art. 53, 6° W.Toezicht). De bijzondere commissie belast met de begeleiding van het Vast Comité van toezicht op de politiediensten en het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten, stemde tijdens de bespreking van het Activiteitenverslag 2013 van het Vast Comité I in met de erin vervatte aanbevelingen (*Parl. St.* Kamer 2014-15, nr. 54K0720/001).

2 Deze opsomming is niet exhaustief.

eenstemming met de politieke beleidskeuzes.[3] Met andere woorden, indien er onvoldoende *resources* voorhanden zijn, dient er in de prioriteitenlijst te worden gesnoeid. Zoniet verwordt deze lijst tot een *a priori* onhaalbare opsomming.

De VSSE kwam tegemoet aan deze aanbeveling in haar Actieplan 2014.

I.1.2. DE OPRICHTING VAN EEN CENTRUM VOOR CYBERSECURITY

Eind november 2014 verscheen in het Belgisch Staatsblad het Koninklijk besluit tot oprichting van het Centrum voor Cybersecurity België (CCB).[4] Het CCB staat onder het gezag van de Eerste Minister en heeft diverse opdrachten: het opvolgen en coördineren van en toezien op de uitvoering van een Belgisch beleid inzake cybersecurity; vanuit een geïntegreerde en gecentraliseerde aanpak de verschillende projecten op het vlak van cyberveiligheid beheren; in samenwerking met het Crisiscentrum van de Regering het crisisbeheer bij cyberincidenten waarnemen… Het Centrum neemt eveneens van de FOD Informatie- en Communicatietechnologie het beheer over van het Computer Emergency Respons Team (CERT) dat onder meer instaat voor het opsporen, het observeren en analyseren van *online* veiligheidsproblemen.

Al in 2011 achtte het Vast Comité I '*de oprichting van een agentschap dat de activiteiten rond informatieveiligheid kan coördineren, onontbeerlijk*'.[5]

I.1.3. PERMANENTE VORMING EN REËLE KWALITEITSBEWAKING INZAKE COLLECTEVERSLAGEN

In het inlichtingenwerk is het niet steeds evident om op het moment van de collecte zelf uit te maken welke informatie ooit relevant zal blijken of niet. Dit neemt niet weg dat de eisen ter zake zoals die omschreven zijn in de W.I&V alsook in de Privacywet (doelbindingsprincipe, adequaatheid, correctheid…) moeten nageleefd worden. Dit betekent bijvoorbeeld dat het al dan niet opnemen van een bepaald feit in een collecteverslag en de wijze waarop dit gebeurt, een cruciaal gegeven vormt. Het Comité was van oordeel dat de wijze waarop die *input* dient

---

3 VAST COMITÉ I, *Activiteitenverslag 2012*, 94 (IX.2.2. Het vastleggen en formuleren van haalbare prioriteiten).

4 K.B. van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België, *BS* 21 november 2014. Voor 2015 zou een budget van 719.000 euro zijn uitgetrokken. De selectieprocedure tot aanstelling van een directeur en een adjunct-directeur zouden worden afgerond eind juni 2015.

5 VAST COMITÉ I, *Activiteitenverslag 2011*, 108 e.v. (IX.2.3. Aanbevelingen met betrekking tot informatieveiligheid). Zie hierover eveneens: Voorstel van resolutie over de aanscherping van de cyberveiligheid in België, *Parl. St.* Kamer 2013-14, 54K0257/001.

te gebeuren, het voorwerp moest uitmaken van permanente vorming en onderworpen worden aan een ernstige kwaliteitsbewaking.[6] In dit kader maakte de VSSE in 2014 werk van een interne opleiding inzake het opstellen van verslagen.

I.1.4. TOEZICHT OP DE ACTIVITEITEN VAN BUITENLANDSE INLICHTINGENDIENSTEN IN BELGIË

In 2012 herhaalde het Comité zijn steun voor de aanbeveling van de Senaat om in de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst een specifieke bevoegdheid op te nemen inzake toezicht door de VSSE en de ADIV op de (wettelijkheid van de) activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied.[7] Vanuit de Kamer van Volksvertegenwoordigers werd begin november 2014 een wetsvoorstel ingediend om de controle op buitenlandse inlichtingendiensten expliciet in de wet op te nemen door in de artikelen 7 en 11 W.I&V toe te voegen: '*het nagaan van de legaliteit van de activiteiten van de buitenlandse inlichtingendiensten op Belgisch grondgebied*'.[8]

I.1.5. GEDOCUMENTEERDE WERKAFSPRAKEN

Niet alleen tussen de diensten onderling en tussen de inlichtingen- en politiediensten dient accurater te worden samengewerkt. Het Vast Comité I drong ook aan op het realiseren van gedocumenteerde werkafspraken met andere overheden.[9] In die zin dient het 'Protocolakkoord tussen de VSSE en de Diensten van de Vlaamse Onderwijsadministratie' van 27 januari 2014 te worden toegejuicht. Het akkoord legt praktische afspraken vast voor de onderlinge uitwisseling van informatie en persoonsgegevens opdat zowel de Veiligheid van de Staat als de Vlaamse onderwijsadministratie hun wettelijke opdrachten beter en efficiënter kunnen vervullen.

---

6 VAST COMITÉ I, *Activiteitenverslag 2013*, 113.

7 VAST COMITÉ I, *Activiteitenverslag 2006*, 132, *Activiteitenverslag 2008*, 2 en *Activiteitenverslag 2012*, 91. In een reactie op deze aanbeveling toonde de minister van Landsverdediging zich ook voorstander van een wetgevend initiatief dat de controle op de wettelijkheid van de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied mogelijk zou maken.

8 Wetsvoorstel tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, aangaande het toezicht op de activiteiten van de buitenlandse inlichtingendiensten in België, *Parl. St.* Kamer 2014-15, 54K0553/001. Ook werd voorgesteld om art. 18/9 W.I&V uit te breiden met '*inmenging van een buitenlandse inlichtingendienst*'.

9 VAST COMITÉ I, 'Aanbevelingen van het Vast Comité I in aansluiting met het Regeerakkoord. Denkpistes voor de minister van Justitie', 11 december 2014.

I.1.6. RICHTLIJNEN AANGAANDE DE WERKING MET HUMINT

Het Vast Comité I moest in het verleden – onder meer in het kader van de zaak-Belliraj – vaststellen dat de richtlijnen met betrekking tot de informantenwerking verspreid lagen over diverse documenten die daarenboven slechts een fragmentarisch beeld gaven van de thematiek. Dit was des te meer problematisch nu de informantenwerking slechts een zeer summiere wettelijke basis heeft (art. 18 W.I&V). Alhoewel Comité meerdere malen gepleit heeft voor een nadere wettelijke regeling ter zake, werd geen dergelijk wetgevend initiatief genomen. Om die redenen beval het Comité aan dat de VSSE haar interne richtlijnen en *best practices* met betrekking tot de informantenwerking verder zou ontwikkelen en uitschrijven in duidelijke dienstnota's.[10] In 2011 werd hieraan reeds grotendeels tegemoet gekomen door de realisatie van de *'Instructies over het werken met menselijke bronnen'* en een dienstnota over *'de evaluatie van de informatie aangeleverd door menselijke bronnen'*.[11] Eind januari 2014 verspreidde de VSSE opnieuw een omstandige en gedetailleerde nota over het omgaan met menselijke bronnen. Het Comité herhaalt evenwel dat de verplichting om richtlijnen uit te vaardigen inzake de werking met menselijke bronnen sinds januari 2011 rust op het Ministerieel Comité voor inlichting en veiligheid (art. 18 W.I&V), nu Nationale Veiligheidsraad.

I.1.7. PROCES VAN OPERATIONELE ANALYSE

In het kader van de aanbevelingen die het Comité formuleerde na een uitgebreide audit bij de VSSE, werd voorgesteld om over te gaan tot de aanstelling van een procesbeheerder voor het beheer en de implementatie van de beheers-, kern- en ondersteunende processen. Het Comité beval tevens aan op korte termijn alle primaire processen en op middellange termijn de kern- en ondersteunende processen te beschrijven.[12] Het Strategisch plan van de VSSE stelde als project de ontwikkeling van een proces van Operationele Analyse voorop; een werkgroep Operationele Analyse beschreef in januari 2014 dit proces in een dienstnota.

---

10 VAST COMITÉ I, *Activiteitenverslag 2009*, 84 (VIII.2.2. Een duidelijke, allesomvattende richtlijn inzake de informantenwerking).

11 VAST COMITÉ I, *Activiteitenverslag 2011*, 3.

12 VAST COMITÉ I, *Activiteitenverslag 2009*, 84 (VIII.2.1.3. Aanbevelingen i.v.m. de werk-processen – Procesmanagement).

I.1.8. HET STATUUT VAN HET ADIV-PERSONEEL

In het kader van de audit bij de ADIV formuleerde het Vast Comité I talrijke aanbevelingen, onder meer aangaande het beheer en de leiding van het personeel van de dienst. Het Comité stelde dat er diende '*verholpen te worden aan de vele geldelijke en administratieve verschillen die bestaan tussen de diverse personeelsgroepen binnen de ADIV en tussen deze van de ADIV en andere diensten uit de inlichtingensector (VSSE en OCAD)*'.[13] Deze verschillen zijn immers nefast voor een degelijke personeelsbeheer. Halfweg juli 2014 verscheen een Koninklijk besluit dat de statuten vastlegt van de burgerlijke ambtenaren van het stafdepartement inlichting en veiligheid.[14] Het besluit beoogt de herwaardering van de functie van de betrokken ambtenaren door hun administratief en geldelijk statuut af te stemmen op dat van de ambtenaren van de Buitendiensten van de Veiligheid van de Staat, die taken van dezelfde aard vervullen. Hierdoor werden een aantal verschillen weggewerkt.

I.2. EEN HERNEMING VAN EERDERE AANBEVELINGEN

Artikel 35, 3° W.Toezicht geeft het Vast Comité I de opdracht verslag te doen aan het Parlement '*wanneer het vaststelt dat, bij het verstrijken van een termijn die het redelijk acht, geen gevolg werd gegeven aan zijn besluiten of dat de genomen maatregelen niet passend of ontoereikend zijn*'. In dit kader herneemt het Comité jaarlijks een of meerdere aanbevelingen die het essentieel acht vanuit zijn dubbele finaliteit: de efficiënte werking van de diensten en het waarborgen van fundamentele rechten.

Het Vast Comité I blijft in dit kader met klem herhalen dat er uitvoering moet worden gegeven aan de verplichtingen gesteld in de artikelen 19 en 20 W.I&V om de informatie-uitwisseling en de samenwerking van de Belgische inlichtingendiensten met andere (ook buitenlandse) overheden nader te regelen.[15] Het Comité vraagt aandacht voor deze delicate materie, vanwege de Nationale Veiligheidsraad.

Het Vast Comité I beval eerder[16] aan dat er tussen de inlichtingendiensten enerzijds en de (federale en lokale) politiediensten anderzijds, gestructureerd overleg zou plaatsvinden om via welbepaalde procedures gegevens uit te wisselen.

---

13 VAST COMITÉ I, *Activiteitenverslag 2011*, 104-107.

14 K.B. van 4 juli 2014 tot vaststelling van het statuut van bepaalde burgerlijke ambtenaren van het stafdepartement inlichtingen en veiligheid van de Krijgsmacht, *BS* 18 juli 2014.

15 VAST COMITÉ I, *Activiteitenverslag 2010*, 3-4 en *Activiteitenverslag 2011*, 5-6. Deze aanbeveling werd ook steeds onderschreven door de Begeleidingscommissies. Hierover uitvoerig: VAST COMITÉ I, *Activiteitenverslag 2013*, 4-5.

16 VAST COMITÉ I, *Activiteitenverslag 2011*, 112-113.

Het ontbreken van een samenwerkingsakkoord tussen deze diensten vormt zonder twijfel een tekortkoming in ons veiligheidssysteem. Het Vast Comité I heeft hier in het verleden al meermaals op gewezen en brengt dit, gezien het grote belang, opnieuw in herinnering.[17]

Het Comité merkte reeds in 2010 op dat de SIGINT-procesbeschrijvingen van de intercepties door de ADIV niet waren gefinaliseerd. Dit is nog steeds niet het geval. Het Vast Comité I benadrukt het belang van deze procesbeschrijvingen omdat ze onder meer zullen toelaten de wettelijke verificaties op een meer performante manier te laten verlopen. Het beveelt de ADIV daarom aan deze procesbeschrijvingen af te ronden.

17 VAST COMITÉ I, *Activiteitenverslag 2006*, 135; *Activiteitenverslag 2007*, 77 en *Activiteitenverslag 2009*, 86.

HOOFDSTUK II
DE TOEZICHTONDERZOEKEN

In 2014 werden, net als in 2013, negen onderzoeken afgesloten. Twee toezichtonderzoeken gebeurden op verzoek van de Begeleidingscommissie; vijf toezichtonderzoeken werden opgestart na een klacht of een aangifte en twee onderzoeken werden ambtshalve geïnitieerd. Eén onderzoek werd gevoerd samen met het Vast Comité van Toezicht op de politiediensten.[18] In wat volgt, worden de negen eindverslagen (II.1 tot II.9) verkort weergegeven.

Daarna volgt een opsomming en een korte situering van de nog lopende onderzoeken (II.10). Onder deze laatste rubriek staan ook de vijf in 2014 geopende toezichtonderzoeken vermeld. Van deze vijf nieuwe onderzoeken werden er drie opgestart naar aanleiding van een klacht en twee ambtshalve door het Comité.

In totaal ontving het Comité in 2014 31 klachten of aangiften. Na verificatie van een aantal objectieve gegevens wees het Comité 28 van deze klachten of aangiften af omdat ze kennelijk niet gegrond waren (art. 34 W.Toezicht) of omdat het Comité onbevoegd was om de opgeworpen vraag te behandelen. In die laatste gevallen werden de klagers zo mogelijk doorverwezen naar de bevoegde instantie. In enkele gevallen werden daarenboven de politionele of gerechtelijke overheden in kennis gesteld omwille van een potentieel risico. Zoals gezegd, gaven drie klachten uit 2014 aanleiding tot het openen van een toezichtonderzoek.

[18] Samenvattingen van gemeenschappelijke toezichtonderzoeken opgenomen in dit activiteitenverslag werden niet opgesteld door beide Comités, maar door het Vast Comité I alleen.

II.1. DE SNOWDEN-ONTHULLINGEN EN DE INFORMATIEPOSITIE VAN DE BELGISCHE INLICHTINGENDIENSTEN

II.1.1. INLEIDING

Op 6 juni 2013 publiceerden *The Guardian*[19] en *The Washington Post*[20] voor het eerst informatie uit de tienduizenden (geclassificeerde) documenten die door Edward Snowden, die verschillende functies heeft vervuld in of voor Amerikaanse inlichtingendiensten, waren gelekt. Sindsdien volgden nieuwe onthullingen elkaar op.

De berichten gaven een inkijk in geheime programma's van voornamelijk de Amerikaanse National Security Agency (NSA) en de Britse General Communications Headquarters (GCHQ). Ze onthulden onder meer het bestaan van het PRISM-programma waarbij de NSA (meta)data van telecommunicatie verkrijgt en brachten aan het licht dat Amerikaanse maar ook Britse diensten inlichtingenoperaties hebben opgezet ten aanzien van bepaalde internationale instellingen en samenwerkingsverbanden (VN, EU en G20) en waarbij ook zogenaamde 'bevriende landen' werden geviseerd.

Deze onthullingen waren het startschot voor vele parlementaire, gerechtelijke en inlichtingenonderzoeken over heel de wereld. Zo ook in België. Op 1 juli 2013 vroeg de Begeleidingscommissie van de Senaat aan het Vast Comité I '*[…] een update van de bestaande informatie over de praktijken op het vlak van datamining. […] In de tweede plaats wil de begeleidingscommissie dat het Comité I onderzoekt welke de gevolgen zijn voor de bescherming van het economisch en wetenschappelijk potentieel van ons land, en van de wettelijke opdrachten van onze inlichtingendiensten. Ten slotte wenst de begeleidingscommissie dat het Comité I onderzoekt hoe dergelijke praktijken worden getoetst aan de nationale en internationale rechtsregels die de privacy van burgers beschermen*.'

Het Vast Comité I heeft daarop drie toezichtonderzoeken[21] geopend die uiteraard nauw met elkaar verweven zijn. Dit geldt ook voor een vierde onderzoek[22]

---

19 G. GREENWALD en E. MACASKILL, *The Guardian*, 6 juni 2013 (NSA Taps in to Internet Giant's Systems to Mine User Data, Secret *files* Reveals).

20 B. GELLMAN en L. POITRAS, *The Washington Post*, 6 juni 2013 (US Intelligence Mining Data from Nine US Internet Companies in Broad Secret Program).

21 Naast voorliggend toezichtonderzoek werd ook een onderzoek geopend naar de in België geldende (inter)nationale rechtsregels ter bescherming van de privacy ten aanzien van massale data-captatie (zie Hoofdstuk II.2) en naar de mogelijke implicaties van datamining op de bescherming van het wetenschappelijk en economisch potentieel van het land (zie Hoofdstuk II.10.7).

22 Toezichtonderzoek ingevolge een klacht van een Stafhouder naar het gebruik van informatie afkomstig van massale buitenlandse data-captatie in Belgische strafzaken. Zie hierover Hoofdstuk II.3 'Het gebruik in strafzaken van informatie afkomstig van massale datacaptatie door buitenlandse diensten'.

dat werd geïnitieerd op klacht van de voorzitter van de Nederlandse Orde van advocaten bij de Balie van Brussel.

Het eerste toezichtonderzoek, waarvan voorliggend verslag een samenvatting vormt, biedt een antwoord op volgende vragen:

- Over welke mogelijkheden beschikken grootmachten als de Verenigde Staten en Groot-Brittannië om op grote schaal gegevens van in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) te onderscheppen en te exploiteren en over welke gegevens gaat het (zowel kwantitatief als kwalitatief)?
- In welke mate waren de Belgische inlichtingendiensten op de hoogte van de mogelijkheden van deze grootmachten (of in welke mate dienden ze er – gegeven hun wettelijke opdrachten – van op de hoogte te zijn)? Werden hierover inlichtingen verzameld of werd dit niet wenselijk geacht? Bieden onze diensten voldoende bescherming ter zake?
- 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 onze eigen inlichtingendiensten?

In een eerste fase van het onderzoek wenste het Vast Comité I aan de hand van open bronnen een zo accuraat mogelijk beeld te krijgen van de massale data-captatie door bepaalde Staten en de wijze waarop deze landen aan politieke spionage doen bij zogenaamde 'bevriende Staten'.[23]

Tegelijkertijd werd de informatie die reeds beschikbaar was op het Comité, geanalyseerd en verwerkt. Ook werd de binnen- en buitenlandse berichtgeving zorgvuldig bijgehouden. Ten slotte werden parlementaire vragen en antwoorden, (buitenlandse) academische analyses, *online* discussie-platformen… geraadpleegd.

Ook vonden diverse interviews plaats. Zo bijvoorbeeld kwam halfweg oktober 2013 een contact tot stand tussen het Vast Comité I en Laura Poitras (één van de journalisten die documenten ontving van Edward Snowden) en Jacob Appelbaum (onderzoeksjournalist en softwareontwikkelaar). Dit gesprek leverde interessante inzichten op. Ook werd getracht een onderhoud te realiseren met de NSA-delegatie, op bezoek in België in het kader van de *ad hoc EU-US Working Group on Data Protection*. De delegatie liet weten niet over een mandaat te beschikken om het Vast Comité I te ontmoeten.

In een tweede fase werden de inlichtingendiensten verzocht te antwoorden op een aantal gerichte onderzoeksvragen en het Comité een aantal documenten met

---

[23] Dit deel van het toezichtonderzoek werd uitbesteed aan drs. Mathias Vermeulen, toen *Research Fellow* aan het European University Institute (EUI) in Firenze en het Centre for Law, Science and Technology Studies aan de VU Brussel, die als deskundige werd aangesteld. Zijn werk resulteerde in de studie '*De Snowden-revelaties, massale data-captatie en politieke spionage*'. Deze studie werd integraal hernomen als Bijlage D van het *Activiteitenverslag 2013* (pp. 132-184) van het Vast Comité I.

betrekking tot de behandelde thematiek toe te sturen. Nadien werden uitgebreide briefings[24] georganiseerd en bijkomende documenten opgevraagd. Ten slotte werd tijdens vergaderingen met respectievelijk de directie van de VSSE en de staf van de ADIV gepolst naar de (reeds genomen en toekomstige) beleidsopties.

Het feit dat beide diensten als expert werden aangesteld in het kader van het gerechtelijk onderzoek naar de *hacking* van het Belgacom/BICS-netwerk, vormde in dit toezichtonderzoek geen obstakel: de diensten konden alle voor het onderzoek nuttig en noodzakelijk geachte informatie met het Comité delen.[25]

II.1.2. DE SNOWDEN-REVELATIES GEKADERD

Sinds de eerste gelekte NSA-*slides* kwamen onophoudelijk nieuwe (uitermate gevoelige) gegevens aan het licht die wezen op massale data-captatie én politieke en economische spionage van en bij bevriende landen. Reeds snel bleek ook dat de problematiek zich niet beperkte tot PRISM, TEMPURA of de spionage van de G20 zoals aanvankelijk gedacht.[26]

Het Vast Comité I benadrukte dat het geen onderbouwde indicaties vond waaruit bleek dat de Snowden-*slides* niet authentiek zouden zijn. Integendeel, uit de verrichte onderzoeken meende het Comité te kunnen afleiden dat de onthullingen, zeker wat betreft de 'grote lijnen' het bestaan van massale data-captatie, economische en politieke spionage door bevriende diensten, waarheidsgetrouw waren.[27] Dat daarbij – mede gelet op het fragmentarische karakter van de onthullingen[28] – geen zekerheid bestond omtrent de interpretatie die aan de *slides* werd gegeven, deed geen afbreuk aan deze vaststelling. Dit neemt evenwel niet weg dat omzichtigheid geboden blijft bij de interpretatie. Zo bijvoorbeeld werd aanvankelijk aangenomen dat de NSA in Noorwegen en in Nederland miljoenen gesprekken zou hebben afgeluisterd. Uiteindelijk bleek het te gaan om interceptie van

---

24 Het Comité had niet minder dan vier briefings met de ADIV. Het kon daarbij rekenen op een grote openheid en professionaliteit van het ADIV-personeel.

25 Het toezichtonderzoek resulteerde in een lijvig verslag ten behoeve van de bevoegde ministers. Bepaalde onderdelen van het verslag dienden als 'ZEER GEHEIM Wet 11.12.1998' te worden geclassificeerd wat betreft de ADIV en als 'GEHEIM Wet 11.12.1998' wat betreft de VSSE. Het verslag werd ter advies voorgelegd aan de betrokken diensten. Hun opmerkingen werden bestudeerd en er werden wijzigingen aangebracht in de tekst. Op basis van het geclassificeerde verslag, werd een verslag 'Beperkte verspreiding' opgemaakt voor de opdrachtgever. Voorliggend publiek verslag bevat de belangrijkste elementen uit het rapport 'Beperkte verspreiding'.

26 Exemplarisch in dit verband is de 'Boundless Informant Head Map' van maart 2013, gepubliceerd in G. GREENWALD en E. MAC ASKILL, *The Guardian*, 11 juni 2013 (Boundless Informant: the NSA's secret tool to track global surveillance data).

27 Daarbij moet ook rekening worden gehouden met het gegeven dat de Amerikaanse noch de Britse overheden tot op heden de authenticiteit van de gelekte documenten betwijfeld hebben. Hooguit werd de interpretatie die er soms aan werd gegeven in open bronnen, betwist.

28 *The Guardian* zou slechts één procent van alle documenten die ze van Snowden kreeg, hebben gepubliceerd (X, *De Standaard*, 3 december 2013 (Amper 1 procent van informatie Snowden gepubliceerd)).

telecommunicatie die de Noorse en Nederlandse inlichtingendiensten zélf uitvoerden in het buitenland en dit naar aanleiding van militaire operaties. Wel bleken data zonder meer gedeeld met de NSA.

In wat volgt, worden de Snowden-onthullingen in een breder kader geplaatst.

II.1.2.1. Niet alleen de NSA en het GCHQ

Het toezichtonderzoek richtte zich uitsluitend op de massale data-captatie door het Amerikaanse National Security Agency (NSA) en het Britse Government Communications Headquarters (GCHQ). Mogelijks zijn er in deze landen nog andere diensten die aan massale data-captatie doen. En uiteraard zijn Amerika en Groot-Brittannië niet de enige grootmachten die op dergelijke wijze te werk gaan.

In de marge van de Snowden-onthullingen zijn bijvoorbeeld ook de activiteiten van de Franse, Duitse en Zweedse inlichtingendiensten aangekaart. En natuurlijk zijn er ook de mogelijkheden die ontplooid kunnen worden door bijvoorbeeld Rusland en China. Maar minstens even belangrijk in dit kader zijn de samenwerkingsverbanden inzake *Signals Intelligence* (SIGINT) die bestaan tussen bepaalde landen. Het meest gekend is de zogenaamde FIVE EYES dat naast Amerika en Groot-Brittannië ook Canada, Australië en Nieuw-Zeeland telt. Deze landen werken sinds decennia zeer nauw samen en gecapteerde data-communicatie zou *quasi* ongelimiteerd worden uitgewisseld. Daarnaast werd in de pers bijvoorbeeld ook gewag gemaakt van de NINE EYES en de FOURTEEN EYES, waartoe volgens open bronnen ook België behoorde.[29]

Ten slotte is massale data-captatie en -exploitatie geen exclusiviteit van de overheid. Grote private spelers beschikken soms over gelijkaardige mogelijkheden, al ligt de finaliteit van hun activiteiten meestal elders. Deze problematiek werd om evidente redenen niet bestudeerd door het Comité: ze ligt buiten zijn bevoegdheidssfeer.

II.1.2.2. Niet alleen PRISM en TEMPURA

De eerste onthullingen hadden vooral betrekking op – wat betreft de Amerikanen – PRISM en – wat betreft de Britten – TEMPURA. Deze twee inlichtingenprogramma's bleken een zeer belangrijke bron van informatie, maar ze waren zeker niet de enigen. Enigszins schematiserend onderscheidde het Comité vijf vormen of technieken van massale data-captatie of 'ongerichte interceptie' van (tele)communicatie (*infra*).

---

29 E. MACASKILL en J. BALL, *The Observer*, 2 november 2013 (Portrait of the NSA: no detail too small in quest for total surveillance).

II.1.2.2.1. Ongericht en massaal

Het toezichtonderzoek van het Comité beperkte zich daarbij tot inlichtingenprogramma's of -technieken waarbij in essentie 'ongericht' gecapteerd wordt (ook '*fishing expedition*' genoemd) en er, bij wijze van spreken, een gigantisch fijnmazig net wordt uitgegooid en pas nadien, manueel of aan de hand van geautomatiseerde processen, wordt bekeken wat mogelijks relevant en nuttig is.[30] Het betrof dus *niet* het afluisteren van het telefoonverkeer van één persoon of instantie (ook al kan het gaan om veel én gevoelige gegevens). Een zuivere vorm van 'ongericht' capteren is bijvoorbeeld het aftappen en bewaren van *alle* informatie die via een internationale internetkabel passeert om vervolgens op digitale wijze zoekingen te verrichten (*data-mining*). Een ander voorbeeld is het capteren van alle gsm-signalen in een bepaalde regio.

Maar niet alle door de Snowden-*files* beschreven technieken wijzen noodzakelijkerwijs op 'massale' captatie. Bij het capteren van bijvoorbeeld glasvezelkabels, wordt meestal met zogenaamde '*selectors*' gewerkt: een gsm-nummer, een IP-adres of een bepaald woord (bijv. 'aanslag'). Dit betekent dat alle data die door de kabel passeren weliswaar gescreend worden, maar dat alleen informatie die beantwoordt aan een of meerdere selectiecriteria effectief wordt weggeplukt en bewaard. In dit geval hangt de appreciatie van het feit of de captatie 'gericht' of 'ongericht' gebeurt grotendeels af van de hoeveelheid en van de omschrijving van de selectoren. Wanneer de 'selectoren' voornamelijk beperkt blijven tot welbepaalde gsm-nummers of IP-adressen, dan lijkt de inlichtingengaring eerder 'gericht' (in de veronderstelling uiteraard dat er niet massaal veel nummers en adressen worden ingegeven). Worden daarentegen zeer ruime selectiecriteria gehanteerd (zoals het gebruik van bepaalde woorden, een domeinnaam (bijv. '@comiteri.be'), het gebruik van bepaalde zoektermen op internetzoekmachines of het gebruik van bepaalde toepassingen (bijvoorbeeld VPN-technieken of TOR) dan kan men er niet omheen dat er op ongerichte wijze wordt gecollecteerd. Alhoewel hierover ten tijde van het onderzoek nog geen volledige duidelijkheid bestond, waren de aanwijzingen dat er zeker ook ongericht, massaal gecapteerd werd, overtuigend.

Het 'massale' karakter van de data-captatie kan, met andere woorden, vooreerst blijken uit het feit dat er 'ongericht' wordt gecapteerd. Maar in het kader van dit onderzoek werd de term 'massaal' evenzeer gebruikt in de betekenis dat er weliswaar 'gericht' wordt gecapteerd, maar wel op zoveel verschillende manieren en op zoveel verschillende punten dat de informatie die globaal gecapteerd wordt, 'massaal' is.

[30] Het Comité wees er op dat het capteren en opslaan van (meta)data steeds een inmenging is in de persoonlijke levenssfeer in de zin van artikel 8 EVRM, ook al worden die gegevens niet ingekeken of gebruikt.

II.1.2.2.2. Vijf technieken

Onderstaande vijf 'technieken' kunnen elkaar zowel aanvullen (bijvoorbeeld: omdat een e-mailbericht via een getapte kabel mogelijks niet volledig kan gelezen worden, kan het nuttig zijn het volledige bericht op te halen bij de *provider*) als overlappen (een gsm-gesprek kan rechtstreeks uit de ether zijn gehaald en ook van een kabel zijn geplukt):

1. *de upstream*-collectie of het 'aftappen' van internet of telefoonverkeer dat via (internationale) (glasvezel)kabels verloopt, bijvoorbeeld door apparatuur te plaatsen op cruciale punten die uitgebaat worden door grote telecom-operatoren of door de kabel zelf rechtstreeks te tappen en dit met of zonder medeweten van de operator/uitbater van de kabel[31];
2. *de downstream*-collectie waarbij data gecapteerd of – al dan niet onder dwang – opgevraagd wordt bij telecomoperatoren[32];
3. het onderscheppen van draadloze communicatie (klassieke radiosignalen of gsm-signalen die via zendmasten en satellieten verlopen)[33];
4. het *hacken* van IT-systemen van bijvoorbeeld operatoren om ongezien nuttige informatie weg te sluizen[34];
5. de samenwerking en uitwisseling van gegevens met partnerdiensten (al dan niet binnen het kader van een samenwerkingsverband zoals bijvoorbeeld de FIVE EYES).[35]

Het is uiteraard zinloos om massaal veel data te capteren wanneer die niet kan bewaard en geëxploiteerd worden. Gelet op de enorme hoeveelheden data die de diverse programma's samen genereren, is niet alleen gigantisch veel *hardware* nodig om gegevens te stockeren maar ook performante *software* die toelaat de spreekwoordelijke speld in de hooiberg te vinden. Het programma XKEYSCORE

---

31 TEMPURA is volgens de slides van Snowden de codenaam voor het Britse programma voor deze vorm van captatie.

32 Het meest bekende voorbeeld vormt het PRISM-programma waarbij negen grote Amerikaanse technologiebedrijven bereid werden gevonden en/of verplicht waren/zijn om op gestructureerde wijze gebruikersdata aan te leveren. Het betreft Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL en Apple.

33 FORNSAT zou de codenaam zijn voor een van de programma's die zich richten op dergelijke captatie van communicatie die via satellieten verloopt. Maar ook de interceptie van communicatie vanuit tientallen Amerikaanse diplomatieke en consulaire posten verspreid over de hele wereld (de zogenaamde F6 SITES), zou onder deze noemer kunnen geplaatst worden.

34 Dit was het geval met BICS, een dochteronderneming van Belgacom, die instaat voor *roaming* van telecommunicatie in grote delen van de wereld. Via de Operatie SOCIALIST zouden de Britten er in geslaagd zijn om, met medewerking van de NSA, technisch zeer hoogstaande *malware* te installeren en zo naar alle waarschijnlijkheid een massa aan gegevens weg te sluizen.

35 Zoals open bronnen suggereren, bestaat hierbij de mogelijkheid dat dienst A doet wat dienst B niet mag volgens zijn nationale wetgeving en omgekeerd en waarbij men de gegevens uitwisselt zodat de wettelijke beperkingen *de facto* worden omzeild (X, *De Morgen*, 22 november 2013 (Britse burgers massaal bespioneerd).

stelde de NSA-analisten onder meer in staat om *upstream*-informatie te verwerken. Ongetwijfeld verloopt een deel van de analyse ook geautomatiseerd waarbij algoritmen speuren naar vooraf bepaalde 'patronen' en 'anomalieën' in de gegevens. Een andere mogelijkheid om de massa aan gegevens te verwerken, bestaat er in om ze voor analyse door te geven aan partnerlanden of -diensten.

II.1.2.3. Niet alleen meta-data en niet alleen terrorisme

De diverse programma's capteren niet alleen meta-data (zoals bijvoorbeeld het adres van afzender en bestemmeling, de connectie-identificatie, het tijdstip en duur, het gebruikte technische middel, de grootte van een bestand…) maar ook de inhoud van berichten, of deze nu verzonden zijn via gsm, telefoon, interne voip-mail, *chats*, *online* forumberichten, *clouding*, *e-mailattachments*, Skype…

Er is door de Amerikaanse overheid lang beweerd dat alleen berichten die gerelateerd zijn aan terrorisme, zware vormen van criminaliteit en proliferatie, werden onderschept. Maar ook hier hebben de open bronnen op overtuigende wijze aangetoond dat de interesse en de bevoegdheidssfeer van bijvoorbeeld de NSA, als toeleverancier van de gehele Amerikaanse inlichtingengemeenschap, vele malen ruimer is: ook economische en politieke informatie blijkt geviseerd.

II.1.2.4. Wat met gegevens van en over Belgen en België?

Het Vast Comité I was voornamelijk geïnteresseerd in de eventuele onderschepping van gegevens die betrekking hebben op of afkomstig zijn van in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België). Daarover is uiteindelijk relatief weinig verschenen. Het Comité benadrukte evenwel dat het naïef zou zijn hieruit te besluiten dat België buiten schot is gebleven, zeker gelet op de aanwezigheid van belangrijke internationale organisaties op Belgisch grondgebied. Bovendien zijn er in de onthullingen heel wat elementen aanwezig die aangeven dat ook 'Belgische data' op grote schaal kunnen worden onderschept, weze het rechtstreeks (bijvoorbeeld Belgacom/BICS) dan wel onrechtstreeks (Belgische onderdanen gebruiken Google, Hotmail, Facebook…).

II.1.2.5. Wat maakt de onthullingen belangrijk?

Dat bepaalde grootmachten al geruime tijd over verregaande middelen en programma's beschikten om aan massale data-captatie te doen, is algemeen geweten. Bij wijze van voorbeeld kan men hier verwijzen naar de onthullingen inzake het ECHELON-netwerk en de SWIFT-zaak.

Maar door de Snowden-onthullingen werd men geconfronteerd met drie nieuwe elementen.

Vooreerst is er het gegeven dat de elektronische spionage alomvattend en massaal plaatsgrijpt vanuit honderden SIGADS (dataverzamelingspunten) verspreid over de hele wereld en dit met de meest geavanceerde *soft-* en *hardware* en een ongekende inzet aan menselijke en financiële middelen. Weinige communicatiemiddelen of -berichten schijnen te kunnen ontsnappen aan een mogelijke onderschepping. Dat dit gebeurde vanuit een inlichtingencontext is niet eens zo verwonderlijk. Zo bijvoorbeeld biedt de internettechnologie, inclusief alle communicatievormen die zich via het internet voordoen, een gedroomde bron van gedetailleerde gegevens die voordien onbereikbaar waren. De exponentiële groei van de digitalisering van het dagelijkse leven, opende tegelijkertijd vele nieuwe dimensies voor de inlichtingenwereld.

Tweede nieuwe element is dat meer en meer duidelijk wordt dat grootmachten ook 'bevriende landen' economisch en politiek bespioneren en er aan massale data-captatie doen.

Laatste nieuwe element is dat er vandaag met *quasi* zekerheid – in de vorm van interne, officiële overheidsdocumenten (o.a. gelekte slides) – elementen voorhanden zijn die deze captaties en hun omvang aantonen.

II.1.3. JURIDISCHE ANALYSE VAN DE BEVOEGDHEID VAN DE VSSE, DE ADIV EN HET OCAD

II.1.3.1. De bevoegdheid van de VSSE om data-captatie en politieke en economische spionage door buitenlandse diensten op te volgen

In een eerste reactie stelde de VSSE dat haar bevoegdheid om de massale data-captatie door buitenlandse inlichtingendiensten op te volgen, blijkt uit de artikelen 7 en 8 W.I&V. Nadien stelde de dienst haar bevoegdheid ten aanzien van massale inbreuken op de privacy expliciet in vraag. In eerdere toezichtonderzoeken – zie bijvoorbeeld ECHELON[36] en SWIFT[37] – had het Comité reeds duidelijk gesteld dat het aan de VSSE toekomt dergelijke spionagepraktijken op te volgen. Het Comité herhaalde dan ook dat zowel *qua* 'op te volgen bedreigingen' (spionage[38]) als qua 'te verdedigen belangen' (het wetenschappelijk en economisch potentieel, de interne veiligheid onder de vorm van 'mensenrechten en fundamentele vrijheden'[39] en de externe veiligheid onder de vorm van de 'soevereiniteit

36 VAST COMITÉ I, *Activiteitenverslag 1999*, 24-51. Opmerkelijk is dat de VSSE destijds bij het Comité zelf had onderlijnd dat de opvolging van het ECHELON-systeem tot haar bevoegdheid behoorde.

37 VAST COMITÉ I, *Activiteitenverslag 2006*, 46-47.

38 'Spionage' heeft niet alleen betrekking op het heimelijk opzoeken van informatie van overheden; wie vertrouwelijke gegevens van particulieren of bedrijven tracht te achterhalen, valt ook onder deze definitie (VAST COMITÉ I, *Activiteitenverslag 2006*, 42-51 en VAST COMITÉ I, *Activiteitenverslag 2012*, 14-28).

39 Hierbij wordt in eerste instantie uiteraard de privacy geviseerd.

van de Staat'[40]), de Wet op de inlichtingen- en veiligheidsdiensten duidelijke aanknopingspunten biedt om de massale data-captatie door buitenlandse inlichtingendiensten op te volgen, ook al gaat die uit van een zogenaamd bevriend land of een bevriende dienst. Daarbij benadrukte het Comité dat het *in casu* niet ging om 'potentiële' dreigingen, maar wel om 'actuele' dreigingen.

In 2008 stelde de VSSE nog '*dat […] het Amerikaanse Echelon systeem […] al geruime tijd door haar diensten [wordt] opgevolgd. Mocht echter uit de toepassing van deze nieuwe Protect America Act een activiteit voortvloeien die een inbreuk zou veroorzaken op één van de wettelijk te beschermen belangen, zal de VSSE binnen haar wettelijk kader haar inlichtingen mede delen aan de betrokken overheden en bevoegde instanties overeenkomstig de doelstellingen van hun opdrachten*.'

Het Comité vestigde er ten slotte de aandacht op dat artikel 8 EVRM, dat bescherming biedt tegen onrechtmatige inbreuken op het privé-leven, een positieve verplichting met zich brengt voor de Lidstaten van de Raad van Europa. Eén van de manieren om die positieve verplichting vorm te geven, zou erin kunnen bestaan om de nationale inlichtingendiensten aan te zetten om massale inbreuken te detecteren en hierover te rapporteren. Het Comité verwees in dit verband ook naar de aanbeveling uit het ontwerprapport van de LIBE-commissie van het Europese Parlement: '*Roept de lidstaten onmiddellijk op te voldoen aan hun positieve verplichting uit hoofde van het Europees Verdrag voor de rechten van de mens om hun burgers te beschermen tegen door derde landen uitgeoefend toezicht dat in strijd is met de vereisten daarvan, ook wanneer het doel ervan de waarborging van de nationale veiligheid is, en te garanderen dat de rechtsstaat niet is verzwakt als gevolg van extraterritoriale toepassing van een wet van een derde land*.'[41] In die zin kunnen onder meer inlichtingendiensten gezien worden als een instrument in handen van de overheid om zijn positieve verplichting uit het Europese Verdrag waar te maken.

II.1.3.2. De bevoegdheid van de ADIV om data-captatie en politieke en economische spionage op te volgen

In 1999 stelde het Comité vast dat de ADIV '*geen actief onderzoek [voert] naar het systeem 'Echelon' en […] daarvoor enerzijds [steunt] op het feit dat een dergelijk onderzoek geen deel uitmaakt van zijn bevoegdheden die beschreven staan in de nieuwe wet van 30 november 1998 houdende regeling van de Inlichtingen- en Vei-*

---

40 Het ongelimiteerd en zonder toestemming afluisteren op het grondgebied van een vreemde Staat vormt een schending van de soevereiniteit, zelfs indien de afluisteroperaties conform zijn aan het recht van de Staat die ze uitvoert.

41 Deze aanbeveling werd *quasi* letterlijk overgenomen in het definitieve verslag (European Parliament, LIBE Committee Inquiry, *Electronic mass surveillance of EU citizens. Protecting fundamental rights in a digital age. Proceedings, Outcome and Background Documents*, 2013-2014, 29-30).

ligheidsdiensten […]'.[42] In 2006 werd dit standpunt herhaald naar aanleiding van de SWIFT-zaak.[43] Ook naar aanleiding van voorliggend toezichtonderzoek hield de ADIV voor niet bevoegd te zijn. Het Comité kon dit standpunt slechts gedeeltelijk onderschrijven. Vooreerst viel niet uit te sluiten dat de spionageactiviteiten van de NSA of andere bevriende diensten zich ook uitstrekten over de Belgische defensiepolitiek. Ingevolge artikel 11 W.I&V hoort de ADIV inlichtingenwerk te verrichten wanneer wordt getracht '*op ongeoorloofde wijze kennis te nemen*' van aspecten van de defensiepolitiek. Het Comité concludeerde dan ook dat de ADIV niet bevoegd is voor massale data-captatie als fenomeen *an sich* maar wel voor spionage op het vlak van de defensiepolitiek. Het Comité benadrukte wel dat er voor dit laatste aspect in de Snowden-onthullingen ten aanzien van België geen concrete aanwijzingen waren.

Daarenboven is de ADIV sinds 2010 bevoegd voor de bescherming van het WEP ten aanzien van bedrijven of instellingen die op een specifieke lijst zijn opgenomen. Eind 2012 werd een voorstel van lijst opgesteld door de ministers van Justitie en Landsverdediging. Hoewel de formele goedkeuring van deze lijst door het Ministerieel Comité ontbrak, achtte de ADIV zich sinds 2013 bevoegd voor de bescherming van het WEP van deze bedrijven. De dienst kon dan ook niet langer zondermeer stellen dat hij geen enkele bevoegdheid heeft inzake de opvolging van massale data-captatie aangezien de in de lijst opgenomen bedrijven ook bedreigd kunnen worden door dergelijke praktijken.

Nog in 2010 kreeg de ADIV als opdracht om '*in het kader van cyberaanvallen op militaire informatica- en verbindingssystemen of systemen die de minister van Landsverdediging beheert, de aanval [te] neutraliseren en er de daders van [te] identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het recht van de gewapende conflicten*' (art. 11 § 1, 2° W.I&V). Het Comité wees reeds op het beperkte toepassingsgebied van deze bepaling: indien aanvallen plaatsvinden op andere FOD's of nationale kritieke infrastructuur (zoals communicatienetwerken), kan hierop slechts defensief worden gereageerd, zonder dat het vijandelijke systeem mag worden geneutraliseerd.[44]

II.1.3.3. De bevoegdheid van het OCAD

Het Coördinatieorgaan voor de dreigingsanalyse heeft als kerntaak het – op vraag of ambtshalve – opstellen van punctuele of strategische dreigingsanalyses (art. 8 W.OCAD). Wel is de bevoegdheid van het OCAD in deze beperkt tot 'terrorisme en extremisme'. In het kader van voorliggende problematiek had het OCAD dan ook geen specifieke taak.

---

42 VAST COMITÉ I, *Activiteitenverslag 1999*, 45.
43 VAST COMITÉ I, *Activiteitenverslag 2006*, 47.
44 VAST COMITÉ I, *Activiteitenverslag 2011,* 21.

Bij Wet van 1 juli 2011 betreffende de beveiliging en de bescherming van kritieke infrastructuren heeft het OCAD een bijkomende taak toebedeeld gekregen: zij dient in bepaalde gevallen dreigingsanalyses uit te voeren op specifieke 'kritieke infrastructuren'. Dit concept omvat ook de 'openbare elektronische communicatie'. De wet is voornamelijk gericht op 'risico's op de verstoring van de werking of de vernietiging van zijn infrastructuur'. Het OCAD stelde dat het op eigen initiatief noch op verzoek dergelijke analyses verrichtte.

II.1.3.4. De bevoegdheid van de Belgische inlichtingendiensten om communicatie te capteren

Voor de Belgische inlichtingendiensten gelden wat betreft het onderscheppen van communicatie twee regelingen: de BIM-Wet die sinds 2010 de inzet van specifieke en uitzonderlijke inlichtingenmethoden toelaat aan zowel de VSSE als de ADIV en de INT-regeling (art. 259*bis* § 5 Strafwetboek in combinatie met art. 44*bis* W.I&V) die een specifieke interceptiebevoegdheid verleent aan de ADIV.

Geen van beide regelingen houden een principieel verbod in op de *up-* of *downstream*-collectie van gegevens, op het onderscheppen van draadloze communicatie of op het *hacken* van IT-systemen. Dit is onder meer zo omdat de Belgische regeling bij de inzet van methoden geen onderscheid maakt tussen kabelgebonden en niet-kabelgebonden communicatie zoals dat bijvoorbeeld wel het geval is in Nederland en Zweden. Specifiek voor de BIM-methoden bepaalt de wet bovendien dat bijvoorbeeld het inbreken in computersystemen op verschillende wijzen kan gebeuren '*al dan niet met behulp van technische middelen, valse signalen, valse sleutels of valse hoedanigheden*' (art. 18/16 W.I&V). Ook voor de andere methoden geldt dat de inlichtingendienst de gegevens op verschillende wijzen mag trachten te bekomen: rechtstreeks of via de operator. Bovendien is voor zowel de BIM-Wet als voor de INT-regeling het middel waarmee wordt gecommuniceerd (een vaste lijn, een gsm, een satelliettelefoon…), de aard van de communicatie (een geschreven bericht, een gesproken woord, klank én beeld), noch de nationaliteit van diegenen die communiceren van belang.

Alhoewel in beide regelingen geen expliciete verbodsbepalingen zijn opgenomen, moeten er toch een aantal grenzen voor ogen worden gehouden.

Vooreerst lijkt het verwerven van communicatiegegevens bij een in België gevestigde operator buiten diens medeweten (zoals is gebeurd bij de *hacking* van de Belgacom-dochter BICS) niet toegestaan. Artikel 18/17 § 3 W.I&V stelt immers dat '*[i]ndien er een ingreep nodig is op een elektronisch communicatienetwerk, […] de operator van het netwerk of de verstrekker van een elektronische communicatiedienst met een schriftelijke vraag van het diensthoofd [wordt] gevorderd en is hij, als gevolg van deze aanvraag ertoe gehouden zijn technische medewerking te verlenen*'.

Verder is er het feit dat de communicaties die ingevolge de INT-regeling kunnen worden geïntercepteerd, beperkt lijken tot wat traditioneel onder een 'com-

municatie of mededeling tussen personen' (weze het verbaal of schriftelijk, gecodeerd of niet) moet begrepen worden zodat bijvoorbeeld een controle van het surfgedrag van een persoon niet mag worden opgevolgd.

Belangrijker is het feit dat de BIM-Wet en de INT-regeling een beperking inhouden *qua* territoriale toepassing van de interceptiemogelijkheden. Deze beperking kan als volgt worden samengevat[45]:

- een BIM-methode mag niet worden ingezet vanuit het buitenland;
- een BIM-methode mag niet worden ingezet wanneer de communicatie zich in het buitenland bevindt[46];
- een BIM-methode mag worden ingezet vanop Belgisch grondgebied voor dat gedeelte van de communicatie dat zich in België afspeelt;
- op basis van de INT-regeling mag geen communicatie worden afgeluisterd die vertrekt vanuit België[47];
- op basis van de INT-regeling mag vanuit België communicatie worden afgeluisterd wanneer deze vertrekt vanuit het buitenland;
- op basis van de INT-regeling mag naar Belgisch recht in het buitenland communicatie worden afgeluisterd wanneer deze vertrekt vanuit het buitenland en dit '*zowel in het kader van gewapende conflicten als tijdens humanitaire opdrachten. In laatstgenoemd geval staat het aan België aan te tonen dat die apparatuur legitiem is, gelet op de opdrachten die aan haar militaire troepen zijn toevertrouwd krachtens het internationale mandaat op basis waarvan ze zich op het grondgebied van een buitenlandse staat begeven.*'[48]

---

45 In beide wettelijke regelingen werd het territoriaal toepassingsgebied slechts zeer summier omschreven.
Bij de BIM-Wet heeft de betreffende bepaling (m.n. '*op het grondgebied van het Rijk*' – art. 18/1 W.I&V) betrekking op *de plaats vanwaar* of *waar* (dit is onduidelijk) de methode kan worden toegepast. Het Comité is van oordeel dat deze regeling voorzichtigheidshalve in die zin wordt geïnterpreteerd dat de BIM-methode alleen mag ingezet worden op het ogenblik dat het signaal van de te capteren communicatie zich op Belgisch grondgebied bevindt. De ADIV interpreteerde de BIM-regeling in die zin dat ze BIM-methoden in het buitenland mag inzetten, als dit gebeurt in het kader van een opdracht die wordt uitgeoefend in België. Het Comité kon deze redenering niet onderschrijven.
Bij de INT-regeling is het criterium *de plaats vanwaar de communicatie wordt uitgezonden*, en dit ongeacht waar ze toekomt of (van)waar ze geïntercepteerd wordt. Het vertrekpunt van een communicatie bepaalt dus de bevoegdheid van de ADIV (*Parl. St.* Kamer, 2002-03, 50K2059/001, 9 e.v.).

46 Dit betekent bijvoorbeeld dat de communicatie van een persoon die vanuit het buitenland naar België belt, kan onderschept worden op het ogenblik dat het signaal zich in België bevindt.

47 Door de wereldwijde *roaming* en de technologische evolutie is het technisch gezien niet evident voor de ADIV om hieraan tegemoet te komen. Dit is bijvoorbeeld het geval met een telefoongesprek dat vertrekt vanuit België, maar onderschept wordt in het buitenland. Veelal is het niet mogelijk voor de ADIV om dit vetrekpunt te bepalen.

48 Deze uitleg werd gegeven door de gemachtigde ambtenaar die het regeringsontwerp inzake intercepties destijds toelichtte voor de Raad van State (*Parl. St.* Kamer, 2002-03, 50K2059/001, 9 e.v.). Het Vast Comité I merkte dat niet elke interventie kadert binnen een internationaal mandaat noch dat elke interceptie kadert in een beslissing om troepen in te zetten.

Een laatste beperking zit hem in het feit dat in principe alleen 'gerichte' captaties toegelaten zijn.

Zo is de inzet van een BIM-methode in hoofdzaak 'gericht' op een persoon of een groepering. Daarenboven moet aangetoond worden dat er een reëel verband is met één van de in de wet opgesomde dreigingen. Ook de praktijk laat zien dat de BIM-methoden niet ongericht worden ingezet: in 2012 bijvoorbeeld werden voor de VSSE en de ADIV samen slechts een 700-tal toelatingen verleend om communicatie- of lokalisatiegegevens te verwerven. Uiteraard kan één methode vrij veel data opleveren (zoals bijvoorbeeld alle in- en uitgaande telefoonverkeer gedurende een aantal maanden) maar, zoals gezegd, zit de beperking hem voornamelijk in het feit dat de methode gericht is op een persoon of een groepering.

Wat betreft de mogelijkheid van de ADIV om in het buitenland uitgezonden communicaties te onderscheppen, had de wetgever ook niet voor ogen dat er 'verkennend' zou geïntercepteerd worden. Uit de voorbereidende werken die aanleiding hebben gegeven tot de wetswijziging van 2003, komen op duidelijke wijze limieten naar voor zoals '*het verbod op het verkennende of het algemene afluisteren*', het feit dat er '*ernstige indicaties* [moeten voorhanden zijn] *die verband houden met de bedreiging gedefinieerd in artikel 11, § 2, van de wet van 30 november 1998 of in de hypothesen die artikel 44 beoogt*'[49], het feit dat '*de mogelijkheid tot afluisteren enkel een bijkomstig karakter*' heeft en '*goed [moet] gemotiveerd zijn om ertoe over te gaan en er […] een evenwicht [moet] worden gevonden tussen de bescherming van persoonlijke levenssfeer en de belangrijke risico's voor de veiligheid en mogelijke aantasting van de werking van de democratische instellingen.*'[50] Daarenboven vereist artikel 44*bis* W.I&V dat het zogenaamde Afluisterplan van de ADIV de organisaties of instellingen vermeldt die het voorwerp zullen uitmaken van interceptie van hun communicaties tijdens het komende jaar. Deze lijst moet daarenboven voor iedere interceptie de voorziene duur weergeven en uit de motieven moet blijken dat de interceptie aansluiting vindt bij een van de legitieme redenen opgesomd in artikel 44*bis* W.I&V.

De INT-regeling werd in 2010 gewijzigd. Gevolg gevend aan een aanbeveling van het Vast Comité I, werd naast '*het onderscheppen, het afluisteren, het kennisnemen of het opnemen*' van telecommunicatie ook '*het zoeken*' mogelijk gemaakt. De bedoeling was een bestaande, onwettelijke maar operationeel noodzakelijke situatie te legitimeren: vooraleer de ADIV weet op welke frequenties een in het Afluisterplan opgenomen *target* uitzendt, moet de bandbreedte worden afgegaan. Er moet dus worden 'gezocht'. Zoeken naar frequenties of signalen waarop vooraf in het Afluisterplan opgenomen *targets* uitzenden, is met andere woorden legitiem. Maar zonder enig voorafgaand concreet aanknopingspunt zoeken naar nieuwe potentiële dreigingen die niet in het Afluisterplan voorkomen door alle frequenties of signalen op te vangen, is wettelijk niet toegelaten.

---

49 *Parl. St.* Kamer, DOC 50, 2059/001, 6.

50 *Parl. St.* Kamer 2002-03, nr. 50K2059/003, 7 – Verhoor van toenmalig voorzitter Vast Comité I.

II.1.3.5. De bevoegdheid van de Belgische inlichtingendiensten om gegevens te verkrijgen van partnerdiensten

Artikel 20 W.I&V bepaalt dat de Belgische inlichtingendiensten moeten zorgen voor een samenwerking met hun buitenlandse homologen. Dit betekent uiteraard in de eerste plaats dat ze informatie en inlichtingen moeten kunnen ontvangen van buitenlandse partners. Maar betekent dit ook dat dergelijke gegevens verder mogen gebruikt worden indien men weet of vermoedt dat ze illegaal of onrechtmatig werden verkregen? Of wat indien een buitenlandse dienst bijvoorbeeld gegevens over een Belg op een voor hem legale manier verkrijgt en doorgeeft aan zijn Belgische partner die die gegevens niet (zonder machtiging) had kunnen bekomen?

In het kader van het onderzoek was de vraag concreet of gegevens die met een schending van de privacy werden verkregen, verder mogen gebruikt worden in een inlichtingencontext. In de Wet van 30 november 1998 is alleen voorzien in een vernietiging van gegevens wanneer die werden verkregen met miskenning van de BIM-voorschriften. Ook het Ministerieel Comité voor inlichting en veiligheid[51], dat volgens de wet nadere uitvoering dient te geven aan de samenwerking met buitenlandse diensten, heeft hieromtrent niets geregeld. In dit kader wees het Vast Comité I naar een aanbeveling opgenomen in een Resolutie van het Europese Parlement: '*Dringt er bij de lidstaten op aan gegevens van derde landen die op onrechtmatige wijze zijn verzameld niet te aanvaarden en observatieactiviteiten op hun grondgebied door overheden of bureaus van derde landen die volgens nationaal recht onrechtmatig zijn of niet voldoen aan de juridische waarborgen die in internationale of EU-instrumenten zijn vastgelegd, waaronder de bescherming van de mensenrechten in het kader van het VEU, het EVRM en het Handvest van de grondrechten van de EU, te weigeren*'.[52] Deze aanbeveling ligt in de lijn van het standpunt dat de VSSE naar aanleiding van de zaak-ECHELON had ingenomen: '*De Veiligheid van de Staat is formeel in haar verklaring, dat zijn geen dergelijke onwettig verkregen inlichtingen heeft ontvangen. Indien deze hen zouden worden aangeboden, zouden zij ze weigeren.*'[53] Dit veronderstelt natuurlijk dat de ontvangende dienst minimale inspanningen zou leveren om te achterhalen op welke wijze de betrokken inlichtingen werden verkregen. De praktijk leert echter dat 'aanleverende inlichtingendiensten' in regel hun bronnen (en dus de oorsprong van een inlichting) geheim houden en dat de 'ontvangende diensten' dit ook aan-

---

51 Het Ministerieel Comité werd vervangen door de Nationale Veiligheidsraad, zie K.B. van 28 januari 2015 tot oprichting van de Nationale Veiligheidsraad, *BS* 30 januari 2015.

52 Resolutie van het Europees Parlement van 12 maart 2014 over het surveillanceprogramma van de NSA in de VS, toezichthoudende instanties in verschillende lidstaten en gevolgen voor de grondrechten en voor de trans-Atlantische samenwerking op het gebied van justitie en binnenlandse zaken (2013/2188 (INI)). De voorzitter van het Vast Comité I, Guy Rapaille, werd samen met Senator en lid van de toenmalige Senatoriële Begeleidingscommissie, Armand De Decker, gehoord door de LIBE-commissie die deze resolutie voorbereidde.

53 *Hand.* Kamer 1997-98, 16 februari 1998, CRIV49KC0504, 15, Vr. nr. 740.

vaarden. Deze vorm van verstandhouding maakt deel uit van de internationale inlichtingencultuur, net zoals de regel van de derde dienst, het 'voor-wat-hoort-wat'-principe en de eisen van geheimhouding. Deze vaststelling betekent evenwel niet dat het Comité deze principes ongenuanceerd onderschrijft. Zij kunnen echter niet bruusk en unilateraal worden doorbroken.

II.1.3.6. De bevoegdheid van de Belgische inlichtingendiensten om aan politieke of economische inlichtingengaring te doen in het buitenland

De VSSE heeft als opdracht dreigingen te counteren, niet door zelf op te treden maar door een goede informatiepositie uit te bouwen en de bevoegde overheden tijdig in kennis te stellen van nakende of actuele dreigingen. Uiteraard is de VSSE daarbij geïnteresseerd in 'politieke' informatie van private of publieke personen of instanties die een bedreiging (kunnen) vormen voor de belangen die tot de bevoegdheidssfeer van de dienst behoren, ook indien het buitenlandse personen of instanties betreffen. De dienst is daarbij evident niet uitsluitend op zoek naar publiek toegankelijke informatie. Hij heeft hiertoe een wettelijk mandaat. Anders dan de meeste buitenlandse diensten, treedt de VSSE hiervoor uitsluitend op vanop Belgisch grondgebied. Wettelijk gezien is er naar Belgisch recht echter geen verbod om effectief in het buitenland informatie te verzamelen. Op deze regel bestaat evenwel een belangrijke uitzondering: BIM-methoden mogen alleen in België worden ingezet (zie II.1.3.4). Een ander verschil met bepaalde buitenlandse diensten, is dat de VSSE ook niet zelf op actieve wijze op zoek zal gaan naar bijvoorbeeld economische informatie van buitenlandse bedrijven om hiermee Belgische bedrijven te bevoordelen. Dit behoort niet tot haar wettelijke opdracht. De VSSE moet informatie verzamelen om het economisch potentieel van het land te beschermen tegen bijvoorbeeld spionage of inmenging door derden; het moet niet zelf spioneren om op zoek te gaan naar interessante informatie voor Belgische bedrijven.

Ook de ADIV heeft niet de bevoegdheid om aan economische inlichtingengaring te doen. Wat betreft de 'politieke spionage' verschilt de analyse in dit opzicht van die van de VSSE dat de militaire inlichtingendienst wél actief is in het buitenland en dit voornamelijk ter ondersteuning van militaire operaties. Het is evident dat naar aanleiding van dergelijke operaties politieke informatie kan worden verzameld.

II.1.3.7. De samenwerking met buitenlandse diensten

Hoger werd reeds gewezen op artikel 20 W.I&V dat bepaalt dat de Belgische inlichtingendiensten moeten zorgen voor een samenwerking met hun buitenlandse homologen. De derde paragraaf van diezelfde bepaling draagt het Ministerieel Comité voor inlichting en veiligheid op om '*de voorwaarden van de in § 1 van dit artikel bedoelde samenwerking*' te bepalen. Het Ministerieel Comité heeft echter nog geen dergelijke richtlijn uitgevaardigd. Wel stelde de VSSE een gede-

tailleerde (geclassificeerde) instructie op over de bilaterale samenwerking met correspondenten. Het Vast Comité I heeft reeds gesteld dat ze deze richtlijn als waardevol beschouwt, maar wees er tevens op dat bepaalde door de VSSE genomen opties, gedragen dienen te worden door de politieke verantwoordelijken, met name de leden van het Ministerieel Comité.[54] Tevens werd een van de belangrijkste aspecten van die samenwerking – welke inlichtingen mogen meegedeeld worden aan buitenlandse diensten? – slechts summier aangeraakt.

De ADIV werkte ten tijde van het toezichtonderzoek nog steeds aan een soortgelijke nota met 'aftoetsbare criteria' met het oog op de samenwerking met buitenlandse inlichtingendiensten (in ruime zin). Deze zou in de loop van 2014 gefinaliseerd worden. In het kader van voorliggend onderzoek, benadrukte het Comité het belang van dergelijke richtlijn voor de ADIV omdat het – na goedkeuring door het Ministerieel Comité – een democratisch gelegitimeerd kader kan bieden voor samenwerkingsverbanden die de militaire inlichtingendienst vandaag reeds aangaat.

II.1.4. DE VSSE, MASSALE DATA-CAPTATIE EN POLITIEKE EN ECONOMISCHE SPIONAGE

II.1.4.1. Verleende de VSSE medewerking aan de NSA-programma's?

De VSSE was of is op geen enkele wijze betrokken bij de massale data-captatie door de NSA en het GCHQ. Meer specifiek had de VSSE bijvoorbeeld geen toegang tot het PRISM- of XKEYSCORE-programma van de NSA, noch was zij betrokken bij de spionage van Belgacom/BICS. Het is overigens zo dat de VSSE slechts uitzonderlijk rechtstreekse contacten heeft met de NSA. Het Vast Comité I noteerde de afgelopen jaren slechts één ontmoeting en dit in het kader van een concrete problematiek. Dat de VSSE zo weinig contacten heeft met de NSA, is te verklaren door het feit dat de burgerlijke inlichtingendienst wat betreft de Verenigde Staten voornamelijk met de FBI en de CIA correspondeert.

II.1.4.2. Was er sprake van massale data-captatie door de VSSE?

Er blijkt uit geen enkel element dat de VSSE zelf of in samenwerking met andere partners aan massale data-captatie zou doen. De BIM-Wet laat overigens geen massale data-captatie toe; daarenboven kunnen BIM-methoden niet in het buitenland worden ingezet. Ten slotte moet opgemerkt worden dat de VSSE – in tegenstelling tot de ADIV – geen interceptiebevoegdheid heeft in het buitenland.

---

[54] Het Vast Comité I heeft de VSSE aanbevolen haar richtlijn ter goedkeuring over te zenden naar het Ministerieel Comité (VAST COMITÉ I, *Activiteitenverslag 2012*, 95 en *Activiteitenverslag 2013*, 4 en 111). Tot op heden is dit niet gebeurd.

II.1.4.3. Politieke en economische inlichtingengaring door de VSSE?

Zoals eerder reeds werd toegelicht (zie II.1.3.1), verzamelt de VSSE informatie van '*politieke, ideologische, confessionele of filosofische aard*' over Belgische of buitenlandse personen en groeperingen die een bedreiging (kunnen) vormen voor de interne en externe veiligheid van het land. Het Comité heeft binnen het kader van dit onderzoek niet kunnen vaststellen dat de dienst daarbij niet zou opereren binnen het wettelijke kader. Ook heeft het Comité geen enkele aanwijzing dat de VSSE actief op zoek zou zijn naar economische informatie van buitenlandse bedrijven bijvoorbeeld om die met Belgische ondernemingen te delen.

II.1.4.4. De informatiepositie van de VSSE voor en na de Snowden-onthullingen

Was, kon of hoorde de VSSE – gelet op haar bevoegdheid ter zake – vóór de Snowden-onthullingen op de hoogte (te zijn) van de wijze waarop de NSA en het GCHQ opereerden? En wat heeft de VSSE gedaan na de onthullingen: werd de problematiek opgevolgd, welke analyses werden opgesteld, welke overheden werden betrokken…? Uit het antwoord op deze vragen moest het Comité opmaken dat de VSSE een zeer passieve houding heeft aangenomen tegenover de onthullingen.

II.1.4.4.1. De houding van de VSSE voor de onthullingen

Wanneer in 1998 de ECHELON-zaak uitbarst, blijkt de VSSE niet op de hoogte van het bestaan van dit programma uitgaande van de Verenigde Staten waarbij onder meer Europees telefoon-, fax- en e-mailverkeer werd onderschept. De VSSE wijdde dit aan een gebrek aan personele en materiële middelen en aan het feit dat de bescherming van het WEP haar pas recent als opdracht was toegewezen.

Een jaar na zijn eerste ECHELON-verslag wenste het Comité na te gaan of de VSSE getracht had zich verder te informeren over het wereldwijde afluisternetwerk. Het antwoord was negatief. Er werd onder meer gewezen op het feit dat het Ministerieel Comité voor inlichting en veiligheid nog geen definitie had opgesteld van 'het wetenschappelijk en economisch potentieel van het land'.

Ook in 2006 was de VSSE vóór de berichtgeving in de pers niet op de hoogte van het feit dat Amerikaanse diensten op massale wijze gegevens van financiële transacties die via SWIFT werden uitgewisseld, konden inkijken. De dienst haalde hiervoor dezelfde argumenten aan. Het Vast Comité I kon zich hierin niet vinden.[55] Overigens gaf de VSSE ook na het bekendraken van de affaire niet echt blijk van zin voor initiatief.[56]

[55] VAST COMITÉ I, *Activiteitenverslag 2006*, 50.
[56] VAST COMITÉ I, *Activiteitenverslag 2006*, 51.

In augustus 2007 bevroeg het Comité de VSSE in verband met de mogelijke gevolgen van de *Protect America Act* waardoor de Amerikaanse inlichtingendiensten uitgebreide bevoegdheden kregen om communicaties allerhande te intercepteren. De dienst antwoordde dat ECHELON al geruime tijd werd opgevolgd en dat ze, mocht er uit de toepassing van die *Protect America Act* activiteiten voortvloeien die een inbreuk zouden uitmaken tegen één van de te beschermen belangen, haar inlichtingen zou meedelen aan de bevoegde overheden (zie ook II.1.3.1).

Eind 2008 meldde de VSSE aan het Comité dat ze nog geen rapporten over ECHELON had opgesteld. Wel zou het naar eigen zeggen het ECHELON-systeem of eender welk mogelijk onderscheppend communicatiesysteem opvolgen. Maar er werd nog geen bedreiging vastgesteld voor de interne en externe veiligheid of het WEP. De VSSE stelde wel dat de opvolging van dergelijke systemen geen prioriteit vormde.

Ook in 2008 waarschuwde de VSSE de leden van de Regering voor het gebruik van BlackBerry's omdat de communicatie via dit (toen zeer populaire) middel niet veilig verliep. Het gehele Europese BlackBerry-dataverkeer transiteerde immers via Groot-Brittannië dat op basis van de RIPA-wetgeving de encryptiesleutels kon opvragen om de nationale veiligheid of de economische welvaart van het land te verdedigen. De VSSE voegde er aan toe dat gelijkaardige wetgeving in de Verenigde Staten de toegang tot de SWIFT-database door de Amerikaanse autoriteiten had mogelijk gemaakt. De redenering die aan de basis lag van deze waarschuwing, bleek op te gaan voor vele vormen van data-captatie die door Snowden werden onthuld: Belgische of Europese communicaties verlopen veelal via het buitenland waar lokale overheden personen of bedrijven kunnen verplichten deze gegevens kenbaar te maken. Het Comité beschouwde de waarschuwing als een goed voorbeeld van actieve belangstelling, maar stelde vast dat de dienst daar op dat ogenblik geen algemene waarschuwing uit distilleerde naar andere vormen van telecommunicatie.

Het Comité moest besluiten dat de VSSE vóór de onthullingen in 2013 weliswaar op de hoogte was van het feit dat bepaalde – ook bevriende – grootmachten over enorme interceptiecapaciteiten beschikten, maar dat ze geen idee had dat die ook wereldwijd op dergelijk massale wijze werden ingezet en dat daarbij ook politiek en economisch Europa als *target* werd beschouwd. Het Comité stelde vast dat de VSSE weinig zicht had op de aard en grootte van de acties van bevriende grootmachten, en dit ondanks alle voorgaande casussen maar ook gelet op de informatie die beschikbaar was in open bronnen. Het Comité noteerde dat de VSSE voorafgaand aan de onthullingen ten behoeve van de overheid geen globale analyse had gemaakt, noch een nota had opgesteld met betrekking tot massale data-captatie. Wel werden de burgers en ondernemingen via studiedagen, een brochure en de media gewezen op mogelijke of reële dreigingen van vooral economische spionage, ook door bevriende landen.

Sinds de zaak-ECHELON is er vanuit de hiërarchie ook op geen enkel ogenblik de opdracht gegeven om dergelijke fenomenen op te volgen. In de jaarlijkse actieplannen van de VSSE was dan ook geen spoor terug te vinden over 'massale data-captatie' of 'economische en politieke spionage door bevriende diensten'. Ook in een informeel overlegplatform van Westerse inlichtingendiensten, is het thema voor de onthullingen nooit ter sprake gebracht wat betreft de Verenigde Staten en Groot-Brittannië.

II.1.4.4.2. De houding van de VSSE na de onthullingen

Na de onthullingen nam de VSSE drie initiatieven. Vooreerst werden de vertegenwoordigers van de Amerikaanse correspondenten van de VSSE, de CIA en de FBI, geconfronteerd met de persberichten. De VSSE heeft echter nooit een officieel bericht gekregen en heeft hierop niet verder aangedrongen. Ten tweede werden – net zoals in de zaak-ECHELON – algemene antwoorden geformuleerd op een aantal ministeriële en parlementaire vragen. Ten slotte is de VSSE opgetreden naar aanleiding van de *hacking* van Belgacom/BICS en dit zowel als expert in het kader van het gerechtelijk onderzoek als binnen haar inlichtingenopdracht.

Het Comité moest niettemin vaststellen dat de VSSE ook na de onthullingen weinig actie ondernomen heeft. Er gebeurde geen actieve zoeking in de open bronnen, er werd geen analyse opgesteld en er gebeurde geen rapportering. Vanuit de directie werd geen signaal gegeven om deze zaak op te volgen en bijvoorbeeld uit te maken of en in welke mate de Belgische belangen bedreigd zouden kunnen zijn. Ook binnen het hogergenoemde overlegplatform werd de problematiek door België niet op de agenda geplaatst. Verder is er ook geen officiële vraag gericht aan de ADIV terwijl deze dienst, als natuurlijke gesprekspartner van de NSA, mogelijk over meer informatie zou kunnen beschikken. Het Comité besloot hieruit dat de dienst de problematiek niet aanvoelde en onvoldoende de link zag met zijn wettelijke opdrachten.

II.1.4.4.3. Analyse van de werking en de houding van de VSSE voor en na de onthullingen

Zoals vermeld, haalde de VSSE zowel na de ECHELON- als de SWIFT-zaak een aantal elementen aan die mee moesten verklaren waarom de dienst niet op de hoogte was of kon zijn van de spionagepraktijken. Het Comité merkte op dat op elk van die vlakken grote vooruitgang was gemaakt: de bescherming van het WEP en de fundamentele vrijheden werden in de wet opgenomen, het Ministerieel Comité vaardigde een richtlijn uit over het WEP, het personeelskader was het afgelopen decennium gegroeid en de dienst kreeg de mogelijkheid om bijzondere inlichtingenmethoden in te zetten. Toch volgde de VSSE het fenomeen van massale data-captatie nauwelijks op en stelde zich opnieuw de vraag hoe de dienst dergelijke operaties van buitenlandse inlichtingendiensten zou kunnen opsporen

en of dit wel mogelijk was binnen het huidige wettelijk kader en gegeven de beschikbare middelen.

Het Comité was van oordeel dat het voor de VSSE mogelijk was geweest de massale data-captatie, ook door bevriende landen, op een algemeen niveau en niet noodzakelijk in detail op te volgen en overheden op regelmatige tijdstippen te briefen en sensibiliseren over nieuwe praktijken, technische mogelijkheden en potentiële gevaren. De informatiepositie die dergelijke sensibilisering toelaat, kon opgebouwd worden op basis van open bronnen, van informatie afkomstig van de ADIV en van andere buitenlandse partners en dit binnen het kader van de actueel beschikbare middelen en wettelijk toegelaten methoden.

Het Comité was bovendien van oordeel dat de opvolging van massale data-captatie niet alleen noodzakelijk was om de overheden hiervan in te lichten en desgevallend tegenmaatregelen te kunnen nemen, maar ook om zijn eigen collecte-technieken te moderniseren.

Het Vast Comité I meende een aantal andere verklaringen te moeten aanhalen waarom de VSSE voor noch na de onthullingen van Snowden actie had ondernomen.

Vooreerst vormen de Verenigde Staten en Groot-Brittannië zogenaamde 'bevriende landen'. De dienst zag dan ook geen reden om zijn prioriteiten op het vlak van contraspionage te veranderen. Het Comité stelde dan ook vast dat de notie 'bevriende Staat' een verregaande invloed had op de houding van de VSSE. Wel leek de VSSE steeds meer gewonnen voor het concept 'strategische partners' in plaats van 'bevriende diensten'.

De VSSE ondernam geen initiatief om deze problematiek te laten opnemen in het door de bevoegde minister goed te keuren Actieplan. Het Vast Comité I meende dat in deze eveneens een rol is weggelegd voor de bevoegde politieke overheden (te weten de minister van Justitie en/of het Ministerieel Comité voor inlichting en veiligheid) op het ogenblik dat de VSSE zijn jaarlijkse prioriteiten voorstelt. In het *Actieplan 2014* werd wat betreft spionage opnieuw uitgegaan van een klassiek 'dreigingsbeeld'.

Samenhangend hiermee is er uiteraard het feit dat de Amerikaanse en Britse diensten volgens de VSSE veel nuttige informatie aanleveren en de dienst deze informatiestromen niet in gevaar wil brengen.

Verder is de kennis over *signals intelligence* en zijn technische mogelijkheden in het algemeen minder aanwezig bij de VSSE.

Ten slotte zag de VSSE de mogelijks massale schending van de privacy van Belgische burgers en ondernemingen niet als een dreiging die door haar diende te worden opgevolgd.

II.1.5. DE ADIV, MASSALE DATA-CAPTATIE EN POLITIEKE EN ECONOMISCHE SPIONAGE

II.1.5.1. Verleende de ADIV medewerking aan de NSA-programma's?

Net zoals voor de VSSE, kon het Vast Comité I vaststellen dat de ADIV geen medewerking had verleend aan de *upstream*-collectie, de *downstream*-collectie en het *hacken* van IT-systemen. Met andere woorden, de ADIV nam niet deel aan programma's zoals PRISM, XKEYSCORE of TEMPURA en de dienst verleende geen medewerking aan de *hacking* van het netwerk van Belgacom/BICS.[57] Personeelsleden van de ADIV hebben ook nooit directe toegang gehad tot of opleiding gekregen over deze programma's of operaties.

Wat betreft de twee andere 'data-captatietechnieken' die in dit toezichtonderzoek worden onderscheiden (het onderscheppen van draadloze communicatie en de samenwerking met homologe diensten), is het antwoord genuanceerder. Er is immers een vorm van medewerking door de ADIV aan internationale programma's waaraan ook de NSA deelneemt, weze het dat die medewerking in het licht van de Snowden-*files* zeer bescheiden is. De medewerking beperkt zich tot het in zeer specifieke en uitzonderlijke gevallen participeren aan intercepties en tot het doorgeven van geïntercepteerde SIGINT-informatie aan de NSA als partnerdienst in bi- of multilateraal verband. De samenwerking kadert binnen de verplichting *ex* artikel 20 W.I&V (samenwerken met buitenlandse diensten – *supra*) en viseert in essentie de strijd tegen het terrorisme en de bescherming van Belgische en geallieerde troepen.

De internationale samenwerking op het vlak van SIGINT vindt algemeen gesproken plaats binnen diverse fora die een zekere formalisering kennen (bijvoorbeeld via een *Memorandum of Understanding* (MOU), afgesloten op het niveau van diverse SIGINT-diensten veelal zonder expliciete en formele politieke dekking). Het Vast Comité I onderzocht nader twee multilaterale SIGINT-samenwerkingsverbanden waarvan de ADIV lid is: één dat reeds diverse decennia bestaat en aanvankelijk was gericht op de dreiging in de context van de Koude Oorlog en een tweede dat werd opgericht naar aanleiding van een specifieke internationale militaire operatie en met het oog op een verdeling van de SIGINT-taken aldaar. Wat betreft deze twee samenwerkingsverbanden kwam het Comité onder meer tot volgende bevindingen:

– De doelstellingen van een samenwerkingsverband zijn soms ruim omschreven en laten dan ook in theorie activiteiten toe die zich, wat België betreft, buiten de wettelijke bevoegdheidssfeer van de ADIV zouden kunnen bevinden.
– De toetreding tot bepaalde verbanden is onderworpen aan het *do ut des*-principe in die zin dat van de partner bepaalde inspanningen/investeringen/

[57] De dienst bevestigde dit ook expliciet ten aanzien van de Eerste Minister.

inlichtingen worden verwacht. Het is evident dat er in een samenwerkingsverband tussen een kleine en een grote dienst nooit sprake kan zijn van een evenwicht tussen 'geven en nemen'. Maar de meerwaarde van de aanwezigheid van een kleinere dienst binnen een samenwerkingsverband situeert zich niet (uitsluitend) bij de informatie die zij kan aanleveren of wanneer zij een deel van het analysewerk of van de kosten voor haar rekening neemt. Het is daarenboven plausibel te denken dat het voor bepaalde landen ook interessant is om via een netwerk een breder internationaal draagvlak te creëren voor hun werkzaamheden.

- In de loop der jaren is er – en dit is volkomen begrijpelijk – tussen de landen die inzake SIGINT nauw samenwerken, een groot vertrouwen gegroeid met als gevolg een grote loyauteit en verbondenheid. Misschien kon dit verklaren waarom de NSA onmiddellijk werd bijgetreden toen die publiekelijk verklaarde dat er in België op basis van zijn informatie drie aanslagen waren voorkomen.[58] Nadien bleek dat het om informatie ging die nuttig had bijgedragen tot een betere informatiepositie in één concreet Belgisch terrorismedossier.
- Binnen samenwerkingsverbanden geldt als principe het niet-bespioneren van partnerlanden. De NSA en het GCHQ blijken zich niet aan deze laatste gedragsregel te hebben gehouden.
- Internationale samenwerking is kwantitatief zeer belangrijk voor de Belgische SIGINT-afdeling. Een grote meerderheid van de informatie die deze afdeling onder de vorm van rapporten doorzendt naar in- of externe klanten, is afkomstig van buitenlandse partners.
- Ondanks het feit dat deze vorm van samenwerking als zeer belangrijk wordt omschreven, bleek er geen formele evaluatie voorhanden van de globale waarde van de informatie die vanuit de samenwerkingsverbanden wordt aangeleverd.
- In het kader van een van beide samenwerkingen zond de ADIV in 2013 slechts een gering aantal rapporten door, waarvan de helft informatie over Belgen bevatte. Het merendeel van die informatie was terro-gelieerd. Anders is het evenwel gesteld in het kader van het tweede netwerk omdat het interceptiedispositief van de ADIV de meta-data van alle uitgezonden communicaties doorzendt zodat ze kunnen geraadpleegd worden door alle partners.
- De door de ADIV uitgevoerde intercepties in het kader van de internationale militaire operatie waren legaal: ze waren opgenomen in het Afluisterplan, ze kaderden in de opdracht van de ADIV om de Belgische en geallieerde troepen te beschermen die actief zijn binnen een internationaal mandaat en ze waren – door het gebruik van een beperkt aantal criteria – 'gericht'. Tevens was de ontplooiing van het SIGINT-personeel door de Regering goedgekeurd in het

58 K. CLERIX, *MO Magazine*, 6 augustus 2013 (Militaire inlichtingendienst getroffen door ernstig cyberincident).

bredere kader van de beslissing om troepen te zenden. Wel bestonden er geen richtlijnen van het Ministerieel Comité voor inlichting en veiligheid, noch wat betreft de samenwerking, noch wat betreft het doorzenden van inlichtingen aan derde diensten.[59]

- In een welbepaald kader werden de meta-data van *alle* communicatie van een bepaalde regio opgeslagen en gedeeld tussen de partnerlanden. De ADIV had geen idee van het volume van de aldus opgeslagen gegevens. Alle partnerlanden hadden toegang tot deze gegevens en konden er zoekingen in verrichten. De ADIV maakte ook gebruik van deze mogelijkheid. Op wettelijk vlak was het gebruik hiervan minder eenduidig. Afhankelijk van de wijze van zoeking (bijvoorbeeld *datamining* om nieuwe dreigingen te detecteren), opereerde de ADIV mogelijks in een wettelijk vacuüm. Het Comité is van oordeel dat de interceptieregels *in casu* verduidelijkt dienen te worden.
- Het Comité benadrukte dat het geen enkele aanduiding had dat de ADIV samenwerkingsverbanden zou gebruiken om informatie te bekomen die het wettelijk gezien zelf niet mag collecteren. Wel was het zo dat de ADIV geen enkele controle uitoefende op de eventuele rechtmatigheid (naar Belgisch of buitenlands recht) van de wijze waarop gegevens zijn verkregen door buitenlandse partners. De voornaamste reden hiervoor was dat dit *quasi* onmogelijk is. Daarbij komt dat de personen die de ruwe informatie te zien krijgen (en dit is *de facto* de enige informatie die een aanwijzing zou kunnen geven over de rechtmatigheid van de verkrijging) niet juridisch onderlegd zijn.
- Binnen de samenwerkingsverbanden geldt een absolute geheimhouding, waarover streng gewaakt wordt. Deze geheimhouding speelt niet alleen intern de ADIV (door een sterk doorgedreven compartimentering) maar ook daarbuiten. Het belang van dit aspect, wordt hieronder verder toegelicht.

De geheimhouding die rust op de SIGINT-samenwerkingsverbanden is zeer groot. Op formeel vlak wordt alle informatie die betrekking heeft op SIGINT afgeschermd door de vereiste om over een specifieke machtiging te beschikken, en dit bovenop de normale Belgische veiligheidsmachtiging van het niveau 'ZEER GEHEIM'. Het betreft géén vereiste die zijn grondslag vindt in Belgische regelgeving; de verplichting vindt zijn oorsprong in NATO-reglementen. Het verkrijgen van deze machtiging is niet onderworpen aan een bijkomend onderzoek; de kandidaten – die reeds houder moeten zijn van een veiligheidsmachtiging van het niveau 'ZEER GEHEIM' – krijgen een briefing waarin vooral de gevoeligheid van het werken met en rond SIGINT wordt benadrukt. De ADIV waakt er ook over dat het aantal personen dat deze machtiging krijgt, tot een minimum beperkt blijft.

[59] Dat dergelijke richtlijnen essentieel zijn, blijkt bijvoorbeeld uit het feit dat doorgezonden gegevens door partnerlanden zouden kunnen gebruikt worden voor andere doelstellingen dan waarvoor ze werden gecollecteerd.

Alhoewel het Comité begrijpt dat *signals intelligence* een zeer gevoelige materie is waar de *need to know* strikt moet worden toegepast en waar een zekere compartimentering is aangewezen, ziet het geen fundamentele verschillen met bepaalde andere domeinen van het inlichtingenwerk die even gevoelig zijn. Hierbij kan worden gedacht aan *image intelligence* (IMINT) of de inzet van BIM-methoden. Hoe dan ook, dergelijke geheimhouding mag niet doorgetrokken worden op het politieke niveau (bedoeld wordt de minister van Defensie en/of het Ministerieel Comité voor inlichting en veiligheid). Alleen de minister van Defensie beschikte ten tijde van het onderzoek over de specifieke SIGINT-machtiging. Het Vast Comité I stelde zich de vraag of de voorgaande en huidige ministers van Defensie wel 'afdoende' – met andere woorden, in de mogelijkheid zijnde om zijn politieke verantwoordelijkheid ten aanzien van het Parlement op te nemen – in kennis werden gesteld van politiek relevante elementen inzake de SIGINT-samenwerking van de ADIV en dus of de sfeer van strikte geheimhouding die SIGINT kenmerkt, niet geleid heeft tot onvoldoende transparantie. Uiteraard is de vraag of een bepaald element 'politiek relevant' is, een evolutief gegeven (cf. veranderende politieke gevoeligheid, wijzigende geopolitieke toestand en nieuwe technologische ontwikkelingen…).[60]

Wel benadrukte het Comité dat de geheimhouding niet was ingegeven door een of andere vorm van moedwillige retentie.

Tijdens andere gelegenheden stelde de ADIV dat zijn taak om de autoriteiten in te lichten voldoende (of zelfs volledig) vervuld wordt door het Vast Comité I over SIGINT-details in kennis te stellen. Echter, het is evident dat het toezichtorgaan niet kan zorgen voor een politieke dekking.

Het Comité wees in deze ook op het ontbreken van een richtlijn van het Ministerieel Comité in uitvoering van artikel 20 W.I&V. Dergelijke richtlijn zou minstens de krijtlijnen van de samenwerking van de ADIV op SIGINT-vlak moeten weergeven alsmede regels voor de uitwisseling van SIGINT-informatie met diverse partners. Hierop wordt uitgebreider teruggekomen in de aanbevelingen.

II.1.5.2. Is er sprake van massale data-captatie door de ADIV?

Het Vast Comité I kwam tot de bevinding dat de data-captatie die door de ADIV zelf werd uitgevoerd, op het ogenblik van het onderzoek niet als 'massaal' kon worden omschreven, en dit als gevolg van wettelijke, technische en personele beperkingen. Wel plaatste het Comité hierbij een aantal kanttekeningen.

Zoals reeds gesteld, vormde het interceptiedispositief dat in de bedoelde militaire operatie werd gebruikt, hierop in zekere zin een uitzondering.

Ten tweede was het 'Afluisterplan 2014' dermate ruim geformuleerd, dat er in theorie weinig beperkingen werden gesteld aan de afluistermogelijkheden van de

60 Wel zou enige vorm van controle mogelijk zijn via de goedkeuring van de budgetten die nodig zijn om bepaalde aankopen te doen.

ADIV. Mede gelet op de groeiende technologische mogelijkheden en de aanwezigheid van de ADIV in bepaalde SIGINT-samenwerkingsverbanden, heeft het Comité, in uitvoering van zijn bevoegdheid opgenomen in artikel 44*bis* W.I&V, zijn opmerkingen hieromtrent geformuleerd. Bij de eventuele inzet door de ADIV van nieuwe technologische mogelijkheden, moet de ADIV rekening houden met de beperkingen gesteld door de INT-regeling (zie II.1.3.2).

II.1.5.3. Politieke en economische inlichtingengaring door de ADIV?

De ADIV verzamelt met betrekking tot het buitenland enkel informatie in de politieke of economische sfeer in de mate waarin dit relevant is in het kader van zijn opdrachten zoals bijvoorbeeld de bescherming van Belgische en geallieerde troepen.

II.1.5.4. De informatiepositie van de ADIV voor en na de Snowden-onthullingen

Zoals gezegd, is de ADIV onder meer bevoegd voor spionage op het vlak van defensiepolitiek. Hiervoor werden er in de Snowden-onthullingen ten aanzien van België geen concrete aanwijzingen gevonden. Daarnaast was de dienst sinds 2013 bevoegd om massale data-captatie op te volgen, en wel in de mate waarin dit een bedreiging kan betekenen voor het WEP van een aantal bij naam genoemde bedrijven en instellingen. Daarenboven is het Comité van oordeel dat het de taak is van een inlichtingendienst om de mogelijkheden en de werkwijzen van andere diensten te kennen, niet alleen om de bevoegde overheden te informeren en tegenmaatregelen te kunnen nemen maar ook om zijn eigen collecte-technieken te moderniseren. Dit staat los van de vraag of het daarbij om al dan niet bevriende diensten gaat.

Het Comité was dan ook van oordeel dat ook voor de ADIV de vraag moest gesteld worden of de dienst vóór de onthullingen op de hoogte was of kon zijn van de wijze waarop de NSA en het GCHQ opereerden. Tevens werd onderzocht welke acties de ADIV na de onthullingen had ondernomen.

II.1.5.4.1. De houding van de ADIV voor de onthullingen

De ADIV was voor het uitbreken van de ECHELON-zaak in 1998 op de hoogte van de samenwerking die bestond tussen de zogenaamde FIVE EYES. Maar omdat deze landen geen bedreiging vormden op het militaire vlak oordeelde de ADIV – op dat ogenblik volgens het Comité terecht – dat zij in deze geen bijzondere inlichtingeninspanningen moest verrichten.

Een jaar na zijn eerste ECHELON-verslag wenste het Comité na te gaan of ook de ADIV sindsdien verdere stappen had ondernomen. De dienst wees toentertijd

op het feit dat de toenemende digitalisering van de maatschappij enorme bedreigingen met zich brengt op het vlak van de veiligheid van communicaties.

In 2006 bleek de ADIV niet op de hoogte van het feit dat Amerikaanse diensten toegang hadden tot de gegevens van SWIFT. Het Vast Comité I besloot echter dat dit normaal was, gelet op bevoegdheid van de ADIV.[61]

Naar aanleiding van de ondertekening van de *Protect America Act* in 2007 die de Amerikaanse inlichtingendiensten uitgebreide bevoegdheden gaf om communicaties allerhande te intercepteren, bevroeg het Comité ook de ADIV. Een divisie stelde onder meer dat het niet onredelijk was te denken dat de NSA intercepties uitvoerde op Belgisch grondgebied en dit ten aanzien van binnen- of buitenlandse overheden en privé-instellingen. Daarenboven wees ze op mogelijke consequenties van de door de *Protect America Act* gegeven bijkomende interceptiemogelijkheden. Opmerkelijk was echter dat een andere divisie de zaken anders zag. Deze ontwaarde geen dreiging aangezien ze in goede verstandhouding werkte met de Amerikaanse diensten en ze rekende op de onderlinge loyauteit.

Wat betreft de informatiepositie van de ADIV voorafgaand aan de Snowden-onthullingen, maakte het Comité een onderscheid tussen het inzicht van de dienst in de theoretische en werkelijk toegepaste SIGINT-capaciteiten van de NSA en de GCHQ enerzijds en haar inzicht in de schaal en de SIGINT-targetstrategie van deze diensten anderzijds.

De technologische capaciteiten waarover de NSA in theorie beschikt, vormden geen verrassing voor de SIGINT-afdeling van de ADIV, die goed op de hoogte was en is van de technologische ontwikkelingen. Deze afdeling had bovendien ook een zicht op het soort informatie en de oorsprong ervan die via dergelijke methoden effectief kan worden opgespoord. Wel had de SIGINT-afdeling geen kennis van concrete programma's en hun codenamen. De SIGINT-afdeling heeft hierover echter geen specifieke studies uitgevoerd of rapporten opgesteld. Naast de hogervermelde geheimhouding heeft hier ongetwijfeld het feit een rol gespeeld dat deze mogelijkheden voor technologisch geschoolde personen in de SIGINT-sector niet bijzonder verrassend zijn en dus geen aanleiding gaven tot een specifiek initiatief.

Wat betreft de schaal waarop de data-captatie gebeurde, de targetstrategie alsook de integratie van de talrijke technische mogelijkheden, kon het Comité vaststellen dat de ADIV hierover niet veel vaststaande gegevens had om op voort te bouwen.

Ten slotte moet vermeld worden dat inzake de aard van de gevolgde personen, de ADIV uit de door de NSA verstrekte SIGINT-inlichtingen globaal slechts kon afleiden dat het ging om personen die verdacht werden van (banden met het) internationaal terrorisme. Er waren geen indicaties dat gewone burgers, beleidsmensen of ondernemingen de aandacht van de NSA genoten.

61 VAST COMITÉ I, *Activiteitenverslag 2006,* 47.

II.1.5.4.2. De houding van de ADIV na de onthullingen

Vooreerst had de ADIV verschillende contacten met vertegenwoordigers van diverse inlichtingendiensten, waaronder ook de NSA en het GCHQ, waarbij de dienst het Belgisch ongenoegen liet blijken. Ook werd tijdens een *meeting* met Europese homologe diensten een initiatief genomen om het onderlinge vertrouwen te verstreken waarbij de aanwezigen zich vrijwillig konden engageren om geen clandestiene SIGINT-operaties uit te voeren ten opzichte van andere EU-landen. Ten slotte wees de ADIV binnen een van zijn netwerken op de mogelijke operationele en politieke gevolgen van de feiten die aan de basis lagen van de Snowden-onthullingen.[62]

Daarnaast heeft de ADIV briefings over de zaak georganiseerd ten behoeve van diverse overheden. Tevens werden antwoorden voorbereid op de vele parlementaire vragen.

Verder heeft de ADIV zijn technische medewerking verleend aan het gerechtelijk onderzoek naar aanleiding van de *hacking* van het BICS-netwerk. De ADIV was ook betrokken bij de analyse van de *malware*.

Ten slotte stelde de ADIV een dubbele reactie/houding in het vooruitzicht: één op nationaal niveau en één op internationaal niveau.

Op nationaal niveau zou nog meer aandacht moeten worden besteed aan *cybersecurity*, intern de ADIV maar ook daarbuiten, én aan *cyberintelligence*. De Snowden-onthullingen hebben gewezen op zwaktes in het beveiligingssysteem. Hiertegen moet gereageerd worden via technische maatregelen, briefings, *screening*… Er dient met andere woorden een volwaardig risicomanagement te worden uitgebouwd ten aanzien van mogelijke lekken.

Op internationaal vlak moet het vertrouwen met de betrokken inlichtingendiensten worden herbevestigd. De ADIV wees er op dat het verkeerd zou zijn als reactie 'zich terug te plooien'. De internationale samenwerking moet behouden blijven. Wel dient men er zich bewust van te zijn dat, waar vroeger duidelijk was wie de bevriende diensten waren, dat beeld vandaag diffuser is. Daarnaast dient in navolging van de VSSE een richtlijn te worden opgesteld inzake de samenwerking met buitenlandse diensten.

Het Comité heeft wel moeten vaststellen dat de ADIV, buiten het opstellen van een dossier ter voorbereiding van een internationale *meeting*, geen gestructureerde zoeking in de open bronnen heeft verricht, geen *all sources*-analyse heeft opgesteld en zijn eigen informatie onvoldoende heeft geëxploiteerd.

Over de onthullingen is er éénmaal een bespreking gevoerd met de VSSE.

---

62 Met politieke gevolgen wordt onder meer verwezen naar een scherper toezicht op de inlichtingendiensten zoals in Nederland en Duitsland.

II.1.5.5. Analyse van de werking en de houding van de ADIV voor en na de onthullingen

Dat de ADIV zowel voor als na de onthullingen aanvankelijk weinig initiatieven heeft ondernomen op inlichtingenvlak, is vooral te verklaren door het feit dat de achterliggende dreigingen zoals die ten tijde van het onderzoek bleken uit de berichtgeving, niet tot zijn bevoegdheid behoorden. Daartegenover staat dat het Comité van oordeel is dat elke inlichtingendienst een gedocumenteerd zicht moet hebben op de mogelijkheden van homologe diensten, ofwel om zijn eigen collecte te ondersteunen ofwel om tegenmaatregelen te kunnen treffen indien nodig (bijvoorbeeld indien mocht blijken dat ook de Belgische defensiepolitiek het voorwerp is van spionage). In die optiek was een zekere opvolging van de thematiek wel aangewezen.

De houding van de ADIV was uiteraard ook te verklaren door het feit dat het om bevriende naties ging. In het kader van het toezichtonderzoek naar de bescherming van communicatiesystemen tegen mogelijke buitenlandse intercepties en cyberaanvallen bijvoorbeeld kon het Comité vaststellen dat de acties van de Amerikaanse inlichtingendiensten niet voorkwamen in het Inlichtingenstuurplan.[63] De ADIV rekende immers op de loyaliteit van de partnerdiensten binnen de NAVO aangezien de toepassing van de *Patriot Act* gericht is tegen de vijanden van de Verenigde Staten.[64, 65] Het Comité kon wel vaststellen dat vandaag steeds meer actoren stellen dat er op vlak van inlichtingenwerk wel veel partners bestaan, maar geen vrienden.

Een derde element dat mee kan verklaren waarom de ADIV weinig actie heeft ondernomen, is ongetwijfeld het feit dat de Amerikaanse inlichtingendienst voor hem een belangrijke bron van informatie vormt. Dit kan ertoe leiden dat bepaalde inlichtingenactiviteiten niet of minder geproblematiseerd worden.

Wel benadrukte het Comité dat de ADIV sinds het einde van 2013 inspanningen heeft geleverd om binnen internationale SIGINT-fora de thematiek bespreekbaar te maken.

II.2. PRIVACYBESCHERMING EN MASSALE DATA-CAPTATIE

In de nasleep van de Snowden-onthullingen vroeg de toenmalige Begeleidingscommissie van de Senaat aan het Comité om een overzicht te bieden van de in

63 Zie VAST COMITÉ I, *Activiteitenverslag 2011*, 19.

64 Die houding is ook waargenomen bij bijvoorbeeld de Duitse inlichtingendiensten.

65 In eerder onderzoek moest het Comité zelfs noteren dat een eventuele spionage door bevriende diensten niet als een onmiddellijke dreiging werd gezien die een prioritaire aandacht zou moeten genieten (Zie VAST COMITÉ I, *Activiteitenverslag 2000*, 57).

België geldende regels ter bescherming van de privacy ten aanzien van middelen die toelaten om op grote schaal gegevens van in België verblijvende personen, organisaties, ondernemingen of instanties te onderscheppen en te exploiteren. Ook diende het onderzoek een inzicht te verschaffen in het juridische instrumentarium waarover Staten, burgers of bedrijven beschikken om actie te ondernemen tegen (mogelijke) inbreuken op (grond)rechten.

Voor dit onderzoek deed het Comité een beroep op de expertise van Prof. Annemie Schaus (ULB). Uit het uitgebreide advies, dat integraal werd weergegeven in zijn vorige jaarverslag[66], onthield het Comité onder meer het volgende[67]:

- De massale en willekeurige aard van de onderschepping, de *monitoring*, het gebruik en de opslag van persoonsgegevens zijn op alle vlakken in strijd met het EVRM.
- De eerbiediging van het privéleven is ook een taak van de *providers* van sociale-netwerkdiensten die onder het territoriaal toepassingsgebied van het EVRM vallen.
- Het Verdrag nr. 108 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens, dat bindend is voor alle Lidstaten van de Raad van Europa, is een van de beste juridische instrumenten om individuen te beschermen tegen de risico's die gepaard gaan met elektronische *monitoring*.
- Richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, is *rationae loci* van toepassing op *providers* van sociale-netwerkdiensten, ook indien hun hoofdkantoor buiten de Europese Economische Ruimte (EER) is gevestigd.[68] Deze richtlijn verbiedt de doorgifte van persoonsgegevens aan Staten die geen lid zijn van de EER indien deze niet minstens dezelfde graad van bescherming kunnen garanderen.
- Het EU-VS 'Veilige haven-akkoord' inzake databescherming (*Safe Harbor*) werd duidelijk geschonden, en dit aangezien bedrijven met een veilige havencertificering het gebruik van persoonsgegevens hebben toegelaten in het kader van de grootschalige datacollecte door de National Security Agency (NSA).

---

66 A. SCHAUS, 'Advies over de in België geldende regels ter bescherming van de privacy ten aanzien van middelen die toelaten op grote schaal gegevens van in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) te onderscheppen en te exploiteren', VAST COMITÉ I, *Activiteitenverslag 2013*, 185-210.

67 Sommige van deze conclusies werden door het Comité reeds geformuleerd naar aanleiding van zijn onderzoek naar het ECHELON-netwerk (VAST COMITÉ I, *Activiteitenverslag 2000*, 27-60) en de zaak-SWIFT (VAST COMITÉ I, *Activiteitenverslag 2006*, 42-51). Ook het Belgische parlement kwam ten tijde van de ECHOLON-zaak tot de conclusie dat het systeem een schending inhield van artikel 8 EVRM omdat het niet beantwoordde aan de eisen van legaliteit, legitimiteit en noodzakelijkheid (*Parl. St.* Senaat 2001-02, nr. 2-754/1 en *Parl. St.* Kamer 2001-02, nr. 50 1660/001).

68 Zie hierover: Groep 29, WP 163 'Advies 5/2009 over online sociale netwerken' van 12 juni 2009.

- Persoonsgegevens die worden verwerkt in het kader van de politionele en justitiële samenwerking in strafzaken vallen niet onder de toepassing van Richtlijn 95/46/EG of de Veilige haven-beginselen. De uitwisseling van dergelijke gegevens tussen de Europese Unie en de Verenigde Staten wordt geregeld door *ad hoc*-akkoorden, zoals bijvoorbeeld de overeenkomst inzake wederzijdse rechtshulp, de overeenkomst inzake het gebruik en de doorgifte van persoonsgegevens van passagiers (PNR) en de overeenkomst inzake de verwerking en doorgifte van gegevens betreffende het financiële berichtenverkeer ten behoeve van het programma voor het traceren van terrorismefinanciering (TFTP).
- De grootschalige controle van elektronische communicatie zonder instemming van de Staat op wiens grondgebied de controle plaats heeft, schendt de soevereiniteit van die Staat, zelfs indien de interceptie gebeurt vanaf een installatie op het grondgebied van een derde Staat. Dat die afluisteroperaties conform zijn aan het recht van de Staat die ze uitvoert, verandert daar niets aan. Hetzelfde geldt voor clandestiene afluisteroperaties vanuit ambassades van derde Staten op het grondgebied van het gastland.
- De Staat, burgers en bedrijven beschikken over diverse actiemiddelen voor het Internationaal Gerechtshof, het Europees Hof voor de Rechten van de Mens, de Belgische rechtbanken… om inbreuken op grondrechten te bestrijden.
- De inzet van bepaalde methoden (bijvoorbeeld het afluisteren van telefoongesprekken of *hacking*) door een buitenlandse inlichtingendienst op Belgisch grondgebied vormt een strafbaar feit.

Op aangeven van zijn Commissie Burgerlijke vrijheden, Justitie en Binnenlandse Zaken (LIBE-Committee) formuleerde het Europese Parlement verschillende gelijkluidende conclusies in zijn Resolutie over '*het surveillanceprogramma van de NSA in de VS, toezichthoudende instanties in verschillende lidstaten en gevolgen voor de grondrechten van EU-burgers en voor de trans-Atlantische samenwerking op het gebied van justitie en binnenlandse zaken*'[69]:

- Het onthulde toezichtprogramma PRISM vormt een ernstige inbreuk op de grondrechten van de burgers.[70] Er wordt onderstreept dat de bescherming van de persoonlijke levenssfeer geen luxerecht is, maar het fundament vormt van een vrije en democratische samenleving.
- De Lidstaten mogen de gegevens van derde landen die op onrechtmatige wijze zijn verzameld, niet aanvaarden en moeten observatieactiviteiten op hun grondgebied door overheden van derde landen die volgens nationaal recht onrechtmatig zijn of niet voldoen aan de juridische waarborgen die in internationale of EU-instrumenten zijn vastgelegd, weigeren.

69 Resolutie 2013/2188 (INI) van het Europees Parlement (12 maart 2014), P7_TA(2014)0230.

70 Ook het Europees Hof voor de rechten van de mens zal zich dienen uit te spreken over de massale datacaptatie. In oktober 2013 werd het gevat door verschillende verenigingen, die de onthulde praktijken aankloegen. Tot op heden is er geen uitspraak in deze zaak.

– De Lidstaten worden opgeroepen om onmiddellijk te voldoen aan hun positieve verplichting uit hoofde van het EVRM om hun burgers te beschermen tegen observatieactiviteiten van derde landen die in strijd zijn met de bepalingen van het Verdrag, ook wanneer die activiteiten tot doel hebben de nationale veiligheid te waarborgen, en te garanderen dat de rechtsstaat niet wordt verzwakt door de extraterritoriale toepassing van een wet van een derde land.
– De Lidstaten moeten een doelmatig toezicht instellen op inlichtingenactiviteiten en dit door parlementsleden of door expertorganen met wettelijke onderzoeksbevoegdheden.

II.3. HET GEBRUIK IN STRAFZAKEN VAN INFORMATIE AFKOMSTIG VAN MASSALE DATA-CAPTATIE DOOR BUITENLANDSE DIENSTEN

In juli 2013 diende de Stafhouder van de Nederlandse Orde van Advocaten te Brussel een klacht in met betrekking tot een '*statelijk georganiseerde internetspionage zonder grenzen waarvan massaal gedurende jaren werd gebruik gemaakt*'. De Stafhouder verwees daarmee naar de door Edward Snowden aan het licht gebrachte activiteiten inzake datacaptatie door de Amerikaanse en Britse inlichtingendiensten via *Signals intelligence* (SIGINT). Hij stelde dat deze activiteiten, in zoverre zij ook Belgen kunnen treffen, strijdig zijn met onder meer het artikel 8 EVRM, met de bepalingen uit het Verdrag nr. 108 inzake informationele privacy[71] en met de artikelen 7 en 8 van het Handvest van de Grondrechten van de Europese Unie. De Stafhouder stelde ook dat de VSSE[72] niet zou voldaan hebben aan de positieve rechtsplicht die op de overheid rust om de fundamentele rechten en vrijheden van de burgers te verdedigen[73] en dat het gebruik voor de rechter van via massale datacaptatie verkregen gegevens '*op gespannen voet [staat] met de verplichting de rechten en fundamentele vrijheden te beschermen.*'[74]

---

71 Raad van Europa, Verdrag van 28 januari 1981 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens, door België geratificeerd bij wet van 17 juni 1991.

72 Alhoewel de klager alleen de VSSE viseerde, heeft het Vast Comité I geoordeeld dat ook de ADIV in het onderzoek moest betrokken worden.

73 Zie hierover EHRM, nr. 38478/05 van 5 maart 2009, Jankovic *v.* Kroatië, en EHRM, nr. 32881/04 van 28 april 2009, KH *v.* Slovakije.

74 Het is van belang te onderlijnen dat de Stafhouder, die op een mogelijke 'doorsijpeling' van informatie afkomstig van de spionageactiviteiten naar Belgische strafrechtelijke dossiers had gewezen, geen concrete dossiers kon aanbrengen waarin dit het geval kon zijn geweest. Ook een rondvraag binnen zijn Balie leverde geen specifieke dossiers op die door het Comité nuttig hadden kunnen worden onderzocht.

Het onderzoek van het Vast Comité I spitste zich voornamelijk toe op deze laatste problematiek aangezien de andere aspecten van de klacht reeds waren behandeld in twee voorgaande onderzoeken.[75]

II.3.1. WETTELIJK KADER INZAKE INFORMATIE-OVERDRACHT NAAR GERECHTELIJKE AUTORITEITEN

Er zijn meerdere bepalingen die de informatieoverdracht vanuit de inlichtingendiensten naar het gerecht regelen:

- Artikel 29 Sv. bepaalt dat een ambtenaar – en dus ook een lid van de VSSE of de ADIV – die in het kader van de uitoefening van zijn functie van een wanbedrijf of misdaad kennis krijgt, dit aan de gerechtelijke overheden moet melden;
- Wanneer dergelijke gegevens verkregen zijn via specifieke of uitzonderlijke methoden, geldt de regeling uit artikel 19/1 W.I&V die inhoudt dat de transfer plaatsvindt aan de hand van een niet-geclassificeerd proces-verbaal dat wordt opgesteld door de BIM-commissie;
- Artikel 19 W.I&V stelt dat de VSSE en de ADIV de inlichtingen die zij ter beschikking hebben (slechts) kunnen meedelen aan onder meer de gerechtelijke overheden wanneer deze relevant zijn in het kader van hun opdrachten;
- Ten slotte beroepen de inlichtingendiensten en de gerechtelijke overheden zich doorgaans op artikel 20 § 2 W.I&V (dat voorziet in een technische bijstand door de VSSE en de ADIV) als basis voor de onderlinge informatiedoorstroming. Het Vast Comité I heeft echter reeds meermaals onderlijnd dat deze bepaling restrictief moet geïnterpreteerd worden en aldus niet de basis vormt voor het doorgeven van inlichtingen.[76]

Deze regels werden nader uitgewerkt in de omzendbrieven COL 9/2005 en COL 9/2012 van het College van Procureurs-generaal.

II.3.2. WETTELIJK KADER INZAKE HET GEBRUIK VAN INLICHTINGEN IN STRAFZAKEN

Zoals COL 9/2012 stelt, is de bewijsvoering in strafzaken vrij zodat alle nuttige stukken bij het onderzoekdossier kunnen gevoegd worden mits ze niet geclassifi-

---

75 Zie Hoofdstuk II.1. 'De Snowden-onthullingen en de informatiepositie van de Belgische inlichtingendiensten' en Hoofdstuk II.2. 'Privacybescherming en massale data-captatie'.

76 Zie VAST COMITÉ I, *Activiteitenverslag 2004*, 137 en VAST COMITÉ I, *Activiteitenverslag 2006*, 58-59.

ceerd zijn. De inlichtingen van de VSSE of de ADIV hebben wel geen bijzondere bewijswaarde.

Cruciaal voor dit toezichtonderzoek was echter volgende vraag: wat indien de inlichtingen die de Belgische inlichtingendiensten aan de gerechtelijke overheden overmaken, zouden verkregen zijn door een volgens de Belgische wetgeving onwettig systeem van gegevensverzameling? Het Comité verwees in dit verband naar het advies dat zijn expert[77] in een eerder toezichtonderzoek had geformuleerd:

'Het Belgisch strafprocesrecht voorziet […] in een regel die onwettig verkregen bewijselementen uitsluit. Deze uitsluiting is echter niet absoluut. De wet van 24 oktober 2013 heeft in het Wetboek van Strafvordering immers een nieuw artikel 32 ingevoegd, dat als volgt luidt:

'Art. 32. Tot nietigheid van onregelmatig verkregen bewijselement wordt enkel besloten indien:

- *de naleving van de betrokken vormvoorwaarden wordt voorgeschreven op straffe van nietigheid, of;*
- *de begane onregelmatigheid de betrouwbaarheid van het bewijs heeft aangetast, of;*
- *het gebruik van het bewijs in strijd is met het recht op een eerlijk proces.'*

Deze wet geeft gevolg aan de zogenaamde arrest-'Antigoon' van 14 oktober 2003 van het Hof van Cassatie. Deze rechtspraak had al aanleiding gegeven tot de wet van 9 december 2004 betreffende de wederzijdse internationale rechtshulp in strafzaken en tot wijziging van artikel 90ter van het Wetboek van strafvordering, die in artikel 13 bepaalt:

'Art. 13. In het kader van een in België gevoerde strafrechtspleging mag geen gebruik worden gemaakt van bewijsmateriaal:

1° dat in het buitenland op onregelmatige wijze is verzameld indien de onregelmatigheid:

- *volgens het recht van de Staat waarin het bewijsmateriaal is verzameld volgt uit de overtreding van een op straffe van nietigheid voorgeschreven vormvereiste;*
- *de betrouwbaarheid van het bewijsmateriaal aantast;*

2° waarvan de aanwending een schending inhoudt van het recht op een eerlijk proces.'

Deze reglementering van het bewijs impliceert dus dat eender welke onwettigheid of onregelmatigheid er niet automatisch toe leidt dat dit bewijselement terzijde wordt geschoven.'

---

77 Zie 'Advies over de in België geldende regels ter bescherming van de privacy ten aanzien van middelen die toelaten op grote schaal gegevens van in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) te onderscheppen en te exploiteren', in VAST COMITÉ I, *Activiteitenverslag 2013*, 209-210.

Hieruit volgt dat inlichtingen die – per hypothese – in het land van oorsprong wettig zijn verzameld en geen aantasting vormen van het recht op een eerlijk proces, wel degelijk in Belgische strafprocedures mogen worden gebruikt zelfs indien ze volgens Belgisch recht niet hadden mogen verzameld worden.

II.3.3. DE BEHANDELING EN DOORZENDING VAN BUITENLANDSE SIGINT-INLICHTINGEN DOOR DE VSSE EN DE ADIV

II.3.3.1. Algemeen

De VSSE onderhoudt geen reguliere contacten met de buitenlandse diensten die luidens de Snowden-onthullingen de programma's van massale datacaptatie via *Signals intelligence* (SIGINT) op touw hebben gezet. De internationale partners van de VSSE zijn de ('civiele') Amerikaanse FBI en CIA en de *British Security Service* (MI5) en de *Secret Intelligence Service* (MI6), die zelf geen SIGINT-agentschappen zijn (in tegenstelling tot de NSA en het GCHQ). Wanneer via deze partners bepaalde inlichtingen de VSSE bereiken en de VSSE deze eventueel aan de parketten doorspeelt, dan is de oorspronkelijke SIGINT-bron (bijvoorbeeld vanuit de NSA of het GCHQ) reeds meerdere stappen verwijderd. Ook is het zo dat de VSSE de ontvangen buitenlandse gegevens niet zonder meer doorzendt naar andere Belgische diensten. De informatie wordt in principe geëvalueerd en eventueel aangevuld of genuanceerd.

Wat de ADIV betreft – die wél rechtstreekse contacten met de *National Security Agency* (NSA) en het *Government Communications Headquarters* (GCHQ) heeft – toonde eerder onderzoek aan dat de gegevens die deze buitenlandse diensten mogelijks op massale wijze verzamelen, niet op evenredige wijze met de ADIV worden gedeeld. De uitwisseling van informatie tussen de diensten is heel beperkt, wat echter niet uitsluit dat de mogelijkheid bestaat dat sommige van deze gegevens uit de gewraakte programma's afkomstig zouden kunnen zijn. Wel is het zo dat ADIV geen controle uitoefent op de eventuele rechtmatigheid naar Belgisch of buitenlands recht van de wijze waarop gegevens werden verkregen door buitenlandse partners. Nu is dit ook *quasi* onmogelijk aangezien zelden wordt meegedeeld op welke wijze informatie is gecollecteerd. Toch stelde het Comité – net zoals in het eerste thematische onderzoek naar 'De Snowden-onthullingen en de informatiepositie van de Belgische inlichtingendiensten' (zie II.1) – dat de ontvangende dienst minimale inspanningen zou leveren om te achterhalen op welke wijze de betrokken inlichtingen werden verkregen. De praktijk leert echter dat 'aanleverende inlichtingendiensten' in regel hun bronnen (en dus de oorsprong van een inlichting) geheim houden en dat de 'ontvangende diensten' dit ook aanvaarden. Deze vorm van verstandhouding maakt deel uit van de internationale inlichtingencultuur, net zoals de regel van de derde dienst, het do ut des-principe

en de eisen van geheimhouding. Deze vaststelling betekent evenwel niet dat het Comité deze principes ongenuanceerd onderschrijft. Het Comité herhaalde wel dat deze principes niet bruusk en uinilateraal kunnen worden doorbroken.

Het Comité wees in dit kader ook op een uitspraak van een Nederlandse rechter die zich moest buigen over de vraag of en in hoeverre een (Nederlandse) inlichtingendienst van buitenlandse partners gegevens mag aanvaarden en gebruiken indien het niet zeker is op welke manier deze gegevens zijn verzameld, waarbij de hypothese bestaat (of minstens niet weerlegd is) dat ze eventueel verzameld zijn via methoden die de eigen dienst niet kan toepassen of niet mag toepassen.[78] De rechter stelde onder meer het volgende: '*Gegeven het uitgangspunt van artikel 59 lid 1 Wiv 2002 en de ruime beoordelingsvrijheid van de lidstaten bij de toetsing aan artikel 8 EVRM, betoogt de Staat op toereikende gronden dat van hem niet kan worden gevergd dat hij de dringend noodzakelijke samenwerking met buitenlandse diensten, zoals die van de VS, op het spel zet louter op grond van onbekendheid met hun werkwijze en de kans dat de Nederlandse diensten informatie ontvangen die is vergaard op een in Nederland niet toegelaten wijze. Het zwaarwegende belang van de nationale veiligheid geeft hier de doorslag'.*

II.3.3.2. Concreet

Zoals gezegd, bracht de consultatie door de Stafhouder van de leden van zijn Balie geen specifieke dossiers naar boven die konden wijzen op informaties opgenomen in strafdossiers en afkomstig van (buitenlandse) programma's van massale datacaptatie. Ook het onderzoek van het Vast Comité I – dat in principe betrekking had op de periode 2011-2013 – leverde weinig concrete gegevens op.

II.3.3.2.1. Wat de VSSE betreft

De gegevens afkomstig van de VSSE betroffen slechts de periode vanaf november 2012 (weliswaar tot juni 2014) aangezien de database van deze dienst pas vanaf dat ogenblik een verband kon leggen tussen de uitgaande nota's en de inkomende berichten die er aan de basis van liggen.

In die periode ontving de VSSE ongeveer 4.000 inlichtingenrapporten van de FBI, CIA, BSS en SIS. Maar van de ongeveer 550 nota's die de VSSE in dezelfde periode aan de parketten zond, kon in slechts 14 gevallen een rechtstreeks verband worden gelegd tussen de originele buitenlandse inlichtingen en de aan de parketten verzonden nota's. Daarenboven was slechts in twee nota's (die op eenzelfde casus betrekking hadden) informatie opgenomen die van SIGINT-oorsprong was. Maar de aanleverende dienst was geen inlichtingendienst. Overigens was het voor de VSSE onmogelijk uit te maken welke SIGINT-middelen precies

78 Rechtbank Den Haag van 23 juli 2014, rolnummer C/09/455237 / HA ZA 13.1325. Tegen dit vonnis is beroep aangetekend.

waren ingezet, alhoewel niets er op wees dat er in deze sprake was van massale (ongerichte) captatie. De SIGINT-informatie werd in de nota's aan het parket zeer summier weergegeven en zonder vermelding van de oorspronkelijke bron. Daarenboven bevatte de nota's nog andere inlichtingen die uit de eigen productie van de VSSE afkomstig waren. In deze nota's was er geen sprake van informatie over de relaties tussen een cliënt en zijn advocaat.

In het algemeen gaf dit onderzoek aan dat de VSSE slechts in uiterst beperkte mate SIGINT-gegevens vanuit Amerikaanse en Britse bronnen aan de gerechtelijke autoriteiten meedeelde.

II.3.3.2.2. Wat de ADIV betreft

Ook de ADIV gaf slechts in twee gevallen aan het parket gegevens door die afkomstig waren van SIGINT-operaties van de Amerikaanse of Britse diensten. In beide gevallen stuurde de ADIV een geclassificeerd én een niet-geclassificeerd verslag.

In een van de twee gevallen bleken de inlichtingen afkomstig van SIGINT-operaties van één van de geviseerde buitenlandse inlichtingendiensten. Het betrof in deze geen 'ongerichte' operatie, maar een gerichte actie op één welbepaalde target. In het andere geval was de informatie afkomstig van het internet.

II.3.4. CONCLUSIE

Het volume aan uit het buitenland afkomstige inlichtingen en informatie dat de Belgische inlichtingendiensten in de onderzochte periode aan de gerechtelijke autoriteiten doorspeelde, was zeer beperkt.

Bovendien vond het Vast Comité I geen aanwijzingen dat het inlichtingen betrof die hun oorsprong vonden in (Amerikaanse of Britse) programma's van massale (SIGINT-)datacaptatie. Evenmin betrof het informatie die betrekking had op de relatie tussen advocaten en hun cliënten.

Het Vast Comité I vond in het kader van voorliggend toezichtonderzoek dan ook geen enkel element waaruit kon afgeleid worden dat informatie van buitenlandse oorsprong de rechten van Belgische rechtsonderhorigen op die wijze in het gedrang had gebracht.

II.4. DE VSSE EN HAAR WETTELIJKE OPDRACHT VAN PERSOONSBESCHERMING

II.4.1. TIJDSKADER

In de marge van een eerder toezichtonderzoek[79] vernam het Vast Comité I dat er zich mogelijks problemen voordeden inzake de beschikbaarheid van 'protectieagenten' bij de VSSE voor het uitvoeren van opdrachten tot bescherming van personen. Een aantal opdrachten zou niet worden uitgevoerd. Daarop besloot het Comité een onderzoek te openen. Volgende vragen stonden daarbij centraal: voert de VSSE alle aan haar toevertrouwde opdrachten inzake personenbescherming uit, met welke problemen wordt zij hierbij geconfronteerd en welke zijn de oorzaken van deze problemen.

Midden juli 2013 – het onderzoek liep toen volop – besliste de federale Regering om deze opdracht van de Veiligheid van de Staat over te hevelen naar de Federale Politie.[80] Deze beslissing kwam niet geheel onverwacht: eind maart 2013 legde de VSSE aan de minister van Justitie een (ontwerp van) 'Strategisch plan 2013-2016' voor waarin het afstoten van de opdracht personenbescherming vermeld werd. Dit paste in de strategische richting van de VSSE waarbij de inlichtingenopdracht prioritair is: door herintegratie van de inspecteurs die thans in de Dienst Persoonsbescherming werkzaam zijn, kon ruimte gecreëerd worden voor de versterking van de inlichtingenopdracht.

De besprekingen over de overheveling werden weliswaar aangevat, maar de toenmalige Ministerraad besliste uiteindelijk in februari 2014 om zich tijdens de lopende legislatuur niet meer uit te spreken over het dossier.

Dat deed de nieuwe meerderheid wel in het federaal Regeerakkoord van oktober 2014: *'De regering zal de nodige initiatieven nemen zodat de federale politie de opdrachten van persoonsbescherming (met inbegrip van de personeelsleden en bijhorende middelen) integraal kan overnemen van de Veiligheid van de Staat. Dit initiatief zal budgettair neutraal zijn'*.[81]

Eens de overheveling zal gerealiseerd zijn, zullen een aantal vaststellingen uit dit onderzoek ongetwijfeld minder relevant worden. Dit geldt echter niet voor alle door het Comité geformuleerde conclusies. Immers, een aantal problemen blijven

---

79 VAST COMITÉ I, *Activiteitenverslag 2012*, 35 e.v. (II.5. Gemeenschappelijk onderzoek naar de dreigingsevaluaties van het OCAD inzake buitenlandse VIP's op bezoek in België). De personenbeschermingsopdracht van de VSSE weerhield al eerder de aandacht van het Vast Comité I. Zie hierover onder meer VAST COMITÉ I, *Activiteitenverslag 1996*, 70-86 en 231; *Activiteitenverslag 2003*, 164-168 en *Activiteitenverslag 2011*, 42 e.v.

80 Volgens berichten in de pers van 7 oktober 2013 (*Belga, De Morgen, het Nieuwsblad*) verklaarde de woordvoerder van de minister van Binnenlandse Zaken dat de overdracht zou plaatsvinden op 1 april 2014.

81 Bij het afsluiten van de redactie van dit activiteitenverslag was de overheveling nog geen feit.

wellicht onverminderd bestaan, zelfs indien het niet langer de VSSE maar wel de Federale Politie is die met de opdracht belast wordt.

II.4.2. JURIDISCH KADER

Het beschermen van personen is een taak van (administratieve) politie, en wordt sinds lang uitgevoerd door de VSSE, die hiertoe in 1998 uitdrukkelijk de opdracht kreeg. Artikel 7, 3° W.I&V bepaalt dat '*het uitvoeren van de opdrachten tot bescherming van personen die haar worden toevertrouwd door de Minister van Binnenlandse Zaken*' een taak is voor de Veiligheid van de Staat.

Artikel 5 W.I&V bepaalt verder: '*Voor de uitvoering van haar opdrachten staat de Veiligheid van de Staat onder het gezag van de Minister van Justitie. De Minister van Binnenlandse Zaken kan echter de Veiligheid van de Staat vorderen in verband met de uitvoering van de opdrachten bepaald bij artikel 7, wanneer ze betrekking hebben […] op de bescherming van personen. In dat geval preciseert de Minister van Binnenlandse Zaken, zonder zich te mengen in de organisatie van de dienst, het voorwerp van de vordering en kan hij aanbevelingen doen en precieze aanwijzingen geven omtrent de in het werk te stellen middelen en aan te wenden geldmiddelen. Wanneer het niet mogelijk is gevolg te geven aan deze aanbevelingen en aanwijzingen omdat hun uitvoering de uitvoering van andere opdrachten in het gedrang zou brengen, wordt de Minister van Binnenlandse Zaken hierover zo spoedig mogelijk ingelicht. Die ontheft de Veiligheid van de Staat niet van de verplichting om de vorderingen uit te voeren.*'

De opdracht wordt nader gepreciseerd in artikel 8, 5° W.I&V "*personen beschermen': de bescherming van het leven en de fysieke integriteit verzekeren van de volgende personen, aangewezen door de Minister van Binnenlandse Zaken: a) de buitenlandse staatshoofden; b) de buitenlandse regeringshoofden; c) de familieleden van de buitenlandse staats- en regeringshoofden; d) de Belgische en buitenlandse regeringsleden; e) sommige belangrijke personen die het voorwerp zijn van bedreigingen voortvloeiende uit activiteiten bepaald in artikel 8, 1°*'.

De beschermingsofficieren '*zijn de enige agenten van de Buitendiensten van de VSSE die bevoegd zijn de opdrachten met betrekking tot de bescherming van personen uit te voeren, met uitsluiting van elke andere opdracht*' (art. 22 W.I&V). Ze beschikken daartoe over de algemene bevoegdheden waarover alle agenten van de VSSE beschikken[82] en kunnen bijgevolg *quasi* alle gewone inlichtingenmethoden inzetten. Bijkomend kregen de beschermingsofficieren zuiver politionele bevoegdheden (bijvoorbeeld het recht om verlaten gebouwen te betreden, de veiligheidsfouillering, de identiteitscontrole…).

82 Cf. art. 24 W.I&V, met verwijzing naar de artt. 12 tot 14 en 16 tot 18 W.I&V.

Naast de bepalingen uit de W.I&V, zijn nog een aantal andere regels van belang. Zo werd op 8 februari 2000 een protocolakkoord inzake '*Politiemaatregelen in het kader van bezoeken van bepaalde buitenlandse personaliteiten*' gesloten tussen de ministers van Binnenlandse Zaken, Buitenlandse Zaken en Justitie, waarin beschermingsmaatregelen werden vastgelegd die '*altijd worden verleend*' in een aantal vooraf bepaalde gevallen. De persoonsbeschermingsopdracht binnen dit protocolakkoord is (enkel) van toepassing op staatshoofden, regeringsleiders en ministers van Buitenlandse Zaken. Het akkoord voorziet voor de betrokken personaliteiten in een c*lose protection* door de beschermingsofficieren van de VSSE. In september 2003 werd dit protocol geëvalueerd en werd de capaciteit van de VSSE inzake de diverse beschermingsopdrachten vastgesteld.

Begin maart 2004 werd de Omzendbrief nr. 6/2004 van het College van Procureurs-generaal inzake de bescherming van bedreigde personaliteiten, overheidsfunctionarissen en privé-personen uitgevaardigd.[83] Deze omzendbrief werkt onder meer de bepalingen van artikel 23 W.I&V verder uit. De bepaling regelt de informatie-uitwisseling met de gerechtelijke overheden in het kader van de persoonsbescherming.

Tevens kan nog verwezen worden naar de Regeringsonderrichting MO 100.A van 10 juni 1974. Alhoewel deze onderrichting is achterhaald, blijft de geest ervan nog van belang, meer bepaald daar waar het gaat om de samenwerking en de rolverdeling tussen de diensten.

Ten slotte stelde de VSSE een aantal interne richtlijnen op, waarvan de meest recente van februari 2013 dateert.

II.4.3. PROCESMATIGE BESCHRIJVING VAN DE BESCHERMINGSOPDRACHTEN

De beschermingsopdrachten worden onderverdeeld in 'permanente' en 'punctuele' (of ook 'officiële') opdrachten. De permanente opdrachten hebben betrekking op de bescherming van buitenlandse diplomaten die in België geaccrediteerd zijn en er gedurende hun verblijf in ons land (en dus in principe permanent) bescherming krijgen. De punctuele opdrachten betreffen de bescherming van VIP's tijdens hun officieel bezoek aan België.

In het kader van de punctuele opdrachten vormt de VSSE de laatste schakel in een proces waarbij de behoefte aan bescherming van een bezoekende VIP wordt geëvalueerd en daarna uitgevoerd.

---

83 De Omzendbrief COL 1/2001 '*betreffende de bepaling van de modaliteiten die dienen in acht genomen bij de mededeling van informatie betreffende de persoonsbescherming – Uitvoering van artikel 23 van de wet van 30 november 1998*' van 5 februari 2001 werd daarmee opgeheven.

Vooreerst wordt de FOD Buitenlandse Zaken, via de diplomatieke kanalen, op de hoogte gebracht van het bezoek van een te beschermen persoon. Een vraag tot bescherming wordt opgemaakt. Het Crisiscentrum van de Regering opent vervolgens een dossier ten einde na te gaan of de betrokken persoon bescherming nodig heeft, en zo ja, welke.[84] Daartoe vraagt het aan het OCAD en aan de Federale Politie, elk voor wat hun bevoegdheid betreft, om te onderzoeken welke dreigingen naar de betrokken persoon uitgaan. Tevens wordt informatie aangeleverd door onder meer de gerechtelijke autoriteiten.[85, 86] Het OCAD[87] (en de Federale Politie wanneer er concrete elementen van een criminele dreiging zijn) deelt zijn bevindingen mee aan het Crisiscentrum, dat op zijn beurt beslist welke maatregelen zich opdringen.[88] Desgevallend wordt een opdracht tot tussenkomst gericht aan de VSSE. De VSSE voert vervolgens de opdracht uit. Ook de Lokale Politie of andere instanties (bijvoorbeeld de Luchthavenpolitie) kunnen bepaalde taken toegewezen krijgen.

II.4.4. DE DIENST PERSOONSBESCHERMING VAN DE VSSE

De Dienst Persoonsbescherming maakt deel uit van de Buitendiensten van de VSSE en valt onder de bevoegdheid van de Directeur Operaties.

De dienst wordt – in principe – geleid door een sectiechef, bijgestaan door één of meer adjuncten. Sinds oktober 2011 was de leiding *de facto* in handen van één adjunct-sectiechef (commissaris), die sedert september 2012 werd bijgestaan door een afdelingsinspecteur. Het secretariaat van de dienst werd waargenomen door een groep van zes beschermingsassistenten (m.a.w. geen administratief personeel en ook niet voor deze taak aangeworven), die beurtelings het secretariaat bemanden.

---

84 Aan het Crisiscentrum is een verbindingsofficier van de VSSE verbonden.

85 Cf. Omzendbrief nr. COL 6/2004 van 1 maart 2004 van het College van Procureurs-generaal betreffende de bescherming van bedreigde personaliteiten, overheidsfunctionarissen en privépersonen.

86 Indien nodig – bijvoorbeeld wanneer er bepaalde elementen onduidelijk zijn – organiseert het Crisiscentrum een coördinatievergadering met de bij het dossier betrokken instanties.

87 De evaluatie van de dreiging tijdens een bezoek van een buitenlandse VIP in België behoort tot de wettelijke opdrachten van het OCAD. Immers, een van zijn taken is '*op punctuele basis een gemeenschappelijke evaluatie uit te voeren die moet toelaten te oordelen of dreigingen, bedoeld in artikel 3, zich voordoen en welke maatregelen in voorkomend geval noodzakelijk zijn*' (art. 8, 2° W.OCAD). Zie hierover uitvoerig: VAST COMITÉ I, *Activiteitenverslag 2012*, 35-38 (II.5. Gemeenschappelijk onderzoek naar de dreigingsevaluaties van het OCAD inzake buitenlandse VIP's op bezoek in België).

88 De beschermingsopdrachten zijn ingedeeld in categorieën en dit al naargelang het 'dreigingsniveau' zoals omschreven in de Wet van 10 juli 2006 betreffende de analyse van de dreiging (W.OCAD) en het K.B. van 28 november 2006 tot uitvoering van deze wet (KB OCAD). In art. 11 KB OCAD worden vier dreigingsniveaus omschreven: niveau 1 of 'laag', niveau 2 of 'gemiddeld', niveau 3 of 'ernstig' en niveau 4 of 'zeer ernstig'.

De eigenlijke bescherming is de taak van beschermingsofficieren en –assistenten. De beschermingsofficieren hebben de graad van inspecteur (niveau B). Hun taak bestaat er in de leiding op zich nemen van elk type van beschermingsopdracht of de functie van *key-man*[89] te bekleden. De beschermingsassistenten zijn personeelsleden van het niveau C.[90]

Het statuut van de personeelsleden die opdrachten van persoonsbescherming uitvoeren, wordt geregeld door het K.B. van 13 december 2006 houdende het statuut van de ambtenaren van de buitendiensten van de VSSE.

Het personeelsbestand van de Dienst Persoonsbescherming kende over de jaren heen een sterke evolutie: sinds 2000 is er *quasi* een verdriedubbeling. De grootste wijziging inzake samenstelling van het personeelsbestand deed zich in 2009 voor: het effectief steeg sterk door de aanwerving van beschermingsassistenten.[91] In 2010 – het jaar van het Belgisch Europees Voorzitterschap – was het personeelsbestand het grootst. Sindsdien werden stelselmatig inspecteurs (ongeveer één derde van het personeelseffectief) weggetrokken uit de dienst om de inlichtingensecties van de VSSE te versterken.

II.4.5. VASTSTELLINGEN

II.4.5.1. Al dan niet uitvoering van de opdrachten

Zoals vermeld, voert de Veiligheid van de Staat twee vormen van beschermingsopdrachten uit: de 'permanente' en de 'punctuele' of 'officiële'.

Het aantal punctuele opdrachten fluctueerde in de loop der jaren. Het Comité stelde vast dat een aantal van deze opdrachten niet werd uitgevoerd. Naar luid van de VSSE gold dat in de periode 2010-2012 voor zowat één op vier opdrachten. Dit aantal verminderde: in 2012 bedroeg het aantal 'weigeringen' al naargelang de bron nog tussen 4% (VSSE) of 11% (Crisiscentrum).[92] Een belangrijke vaststelling was echter dat deze opdrachten in feite een eerder beperkt deel van de werklast van de Dienst Persoonsbescherming uitmaakte: slechts één vijfde van het aantal gepresteerde uren werd aan 'officiële opdrachten' gespendeerd.

---

89 De *key-man* is de persoon die vooraan op de passagierszetel plaatsneemt in het voertuig van de VIP.

90 Het vereiste diploma voor niveau C is hoger secundair onderwijs, dat van niveau B hoger onderwijs van het korte type. Mits het slagen in een vergelijkende selectie voor de overgang tot het hogere niveau, kan een beschermingsassistent opklimmen naar het niveau B.

91 Voordien bestond deze functie, die in 2012 ongeveer twee derden van het personeel uitmaakte, niet.

92 Het verschil tussen beiden heeft te maken met de referentiepunten die worden gebruikt en de wijze waarop de artt. 7 en 8 W.I&V door beide instellingen worden geïnterpreteerd.

De permanente opdrachten werden wel steeds uitgevoerd.[93] De impact op de werking van de dienst van deze permanente opdrachten, was groot. Het Vast Comité I beveelde aan om prioritair deze permanente opdrachten te herbekijken en te onderzoeken of ze op een andere manier kunnen worden ingevuld zodanig dat ze minder middelen zouden vergen (*infra*).

II.4.5.2. Beschermingsassistenten versus inspecteurs

Het personeelsbestand van de dienst wordt uitgemaakt door beschermingsassistenten (niveau C) en beschermingsofficieren met de graad van inspecteur (niveau B). De beschermingsassistenten vormen meer dan twee derden van het bestand. De afbakening van de taken tussen de assistenten en de officieren bleek evenwel minder stringent dan de functiebeschrijvingen formeel doen vermoeden (bijvoorbeeld inzake het al dan niet opnemen van verantwoordelijkheid). Het Comité benadrukte dat er dient over te worden gewaakt dat deze tweedeling niet tot spanningen leidt.

II.4.5.3. De overurenproblematiek

Een precair probleem vormde het 'inhaalverlof' – verlof toegekend wanneer de prestaties gerekend over een periode van vier maanden de gemiddelde normale duur van een werkweek overstijgen – en de 'inhaalrust' – bijvoorbeeld toegekend na het overschrijden van het maximale aantal arbeidsuren per dag. Het aantal nog niet opgenomen uren inhaalverlof en -rust is opmerkelijk hoog. Het Comité kon vaststellen dat dit tussen januari 2010 en eind december 2012 met meer dan 44.000 uren toenam. Sindsdien is er een afname, maar slechts in geringe mate: tijdens de eerste drie maanden van 2013 werden ongeveer 3.300 uren ingelopen, maar het resterende totaal bleef hoe dan ook bijzonder hoog.

Vooral de beslissing om inspecteurs uit de Dienst Persoonsbescherming weg te trekken (*infra*), had een negatieve impact op het aantal overuren. De aangroei van het personeel, en meer bepaald het in dienst nemen van de beschermingsassistenten, had klaarblijkelijk geen effect op de overurenproblematiek. De weerslag van maatregelen als een doorgedreven rationalisering van de teams en een uitbesteding aan derden om deze overurenproblematiek onder controle te brengen, bleek (zeer) beperkt. Andere maatregelen zoals het uitbetalen van overuren en het herdefiniëren of het afstoten van – vooral permanente – opdrachten, werden overwogen doch nooit geconcretiseerd.

[93] Wel blijken de te beschermen personen zelf niet steeds 'risicobewust'; daardoor zorgt de uitvoering van deze opdrachten soms voor problemen.

II.4.5.4. De protocollaire begeleidingsopdrachten

'Protocollaire begeleiding' – dit wil zeggen begeleiding waarvan de VSSE meent dat er geen dreiging mee verbonden is, maar waar de status van de VIP toch vereist dat er in een officiële begeleiding wordt voorzien – werd ten tijde van het onderzoek uitgevoerd door een beperkt dispositief, gelinkt aan een private chauffeur en limousine. Het Vast Comité I kon niet vaststellen dat de inzet van privé-chauffeurs en -limousines budgettair gunstiger was, eerder integendeel. Het Comité was anderzijds wel van mening dat er op functioneel vlak een kwaliteitsverlies optrad en dat het in plaats gezette dispositief risico's opleverde, zowel voor de te beschermen personen als voor de leden van de VSSE zelf. Het Vast Comité I was dan ook van mening dat zich een grondige evaluatie van deze manier van werken opdrong.

II.4.5.5. Inspecteurs 'weghalen' van hun inlichtingenopdracht

In het verleden werden inspecteurs uit de Dienst Persoonsbescherming gehaald om de inlichtingensecties te versterken. Maar ook het omgekeerde gebeurde: bij een teveel aan werk bij de Dienst Persoonsbescherming werden leden van de inlichtingensecties (Buitendiensten) van de VSSE ingeschakeld.[94] Het Comité kon vaststellen dat dit mettertijd sterk werd afgebouwd: in 2012 kwam het nog slechts éénmaal voor. Sinds 2013 deed de Dienst Persoonsbescherming geen beroep meer op leden van de inlichtingensecties.

II.4.5.6. Definiëring van de dreigingsniveaus

Het behoorde niet tot de *scope* van het toezichtonderzoek om zich uit te spreken over de manier waarop de dreigingsniveaus door de diverse actoren (de VSSE, het OCAD, het Crisiscentrum) worden bepaald of geïnterpreteerd.[95] Wel kon worden vastgesteld dat de concrete toepassing van de dreigingsniveaus op het terrein geen consistent beeld opleverde. De op het terrein in stelling gebrachte dispositieven vertoonden immers een zeer losse band met de formele dreigingsniveaus die door het OCAD werden bepaald.

II.4.5.7. De desinvestering in materiaal

Ten slotte stelde het Vast Comité I nog een aantal andere – hoofdzakelijk materiële – problemen vast bij de uitvoering van de opdracht van persoons-

94 Deze praktijk had veel nadelen: de uitvoering van de inlichtingenopdrachten van de VSSE werden op die manier verzwakt en leden van de inlichtingensecties die normaliter in alle discretie moeten optreden (contact met bronnen, filature…) werden voor het voetlicht geplaatst.

95 Hierover: VAST COMITÉ I, *Activiteitenverslag 2012*, 35-38 (II.5. Gemeenschappelijk onderzoek naar de dreigingsevaluaties van het OCAD inzake buitenlandse VIP's op bezoek in België).

bescherming. Het Vast Comité I beval aan om deze punten stelselmatig te verhelpen en daarbij personen te betrekken die de juiste terreinkennis hebben en dus praktische oplossingen kunnen aanbrengen.

II.5. EEN KLACHT VAN DE SCIENTOLOGYKERK TEGEN DE VEILIGHEID VAN DE STAAT

In maart 2013 diende de vzw Scientologykerk van België een klacht in bij het Vast Comité I.[96] De klager verwees daarbij naar krantenberichten uit *La Dernière Heure*, *Het Laatste Nieuws* en *De Morgen* die gebaseerd waren op twee uitgelekte nota's van de VSSE. Eén nota handelde over de '*Scientologykerk – infiltratie van de Congolese of van oorsprong Congolese gemeenschap van België, inplanting in de Democratische Republiek Congo*'; de andere betrof een '*Fenomeenanalyse van niet-staats-gestuurde inmengingsactiviteiten*'.[97] Uit de berichtgeving bleek dat de VSSE van oordeel was dat de Scientologykerk voet aan de grond wou krijgen in de Democratische Republiek Congo en daartoe op zoek ging naar tussenpersonen in de Belgisch-Congolese gemeenschap. Maar de religieuze beweging zou ook steun hebben willen bieden aan de Oost-Congolese rebellengroep 'Beweging van 23 maart', kortweg M23. De Scientologykerk stelde het Comité drie precieze vragen:

- *'enquêter sur la réalité du fondement de ces informations et sur la manière avec laquelle ces informations ont été diffusées au public;*
- *opérer un contrôle sur la manière avec laquelle ce rapport a été rédigé et sur la manière avec laquelle ce rapport a été diffusé;*
- *dire si ces dénigrements portent atteinte aux droits fondamentaux conférés par la Constitution à l'association plaignante, notamment à la présomption d'innocence.'*[98]

Sommige van die vragen kregen reeds een antwoord in het toezichtonderzoek '*Geheime nota's over de Scientologykerk in de pers*'. Daarin rapporteerde het Comité uitgebreid over de totstandkoming en de verspreiding van de bedoelde

96 Het onderzoek, dat op 14 april 2013 werd geopend en waarvan het eindverslag op 21 mei 2014 werd goedgekeurd, werd gedurende lange periode geschorst omdat er op verzoek van de Senaat een gelijkaardig onderzoek lopende was.

97 Zie meer in detail over deze twee nota's: VAST COMITÉ I, *Activiteitenverslag 2013*, 25-31 (II.2. Geheime nota's over de Scientologykerk in de pers).

98 – *'een onderzoek voeren naar de realiteit van de grond van deze informatie en naar de manier waarop die informatie ter kennis van het publiek is gebracht;*
– *een controle voeren naar de manier waarop dit verslag is opgesteld en naar de manier waarop dit verslag werd verspreid;*
– b*epalen of die laster afbreuk doet aan de fundamentele rechten die de Grondwet verleent aan de vereniging die klacht indient, meer bepaald het vermoeden van onschuld'*. (vrije vertaling)

geclassificeerde nota's. In voorliggend verslag worden die elementen dan ook slechts summier hernomen.

II.5.1. HET OPVOLGEN VAN DE SCIENTOLOGYKERK DOOR DE VSSE

Het Vast Comité I is zich ervan bewust dat het toezicht door een inlichtingendienst op een religieuze beweging aanleiding kan geven tot een zekere vrees met betrekking tot de vrijheid van godsdienst en van vereniging.

Het Vast Comité I stelde dat wanneer de VSSE toezicht uitoefent op de activiteiten van de Scientologykerk in België, de dienst handelt in het kader van haar wettelijke bevoegdheden zoals vastgelegd in de artikelen 7 en 8 van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst. Tot de activiteiten die de fundamentele belangen van de Staat (zouden kunnen) bedreigen, behoren volgens artikel 8 W.I&V meer bepaald inmenging, schadelijke sektarische organisaties en criminele organisaties. Ook '*de veiligheid en de fysieke en morele vrijwaring van personen*' en '*de veiligheid en de vrijwaring van goederen*' zijn belangen die artikel 8 W.I&V opneemt in de begrippen '*inwendige veiligheid van de Staat'* en '*voortbestaan van de democratische en grondwettelijke orde*', en hetzelfde geldt voor de veiligheid en de vrijwaring van de Staat, de rechtsstaat en de democratische instellingen.

In een eerder toezichtonderzoek betreffende de opvolging van schadelijke sektarische organisaties door de VSSE[99] was het Vast Comité I tot het besluit gekomen dat:

- de criteria inzake schadelijkheid die worden gebruikt om de handelingen van een religieuze beweging te analyseren en die beweging te kwalificeren als 'sektarisch' en 'schadelijk' relevant waren en verwezen naar de fundamentele beginselen zoals beschreven in de Grondwet, de wetten en internationale verdragen betreffende de bescherming van de mensenrechten;
- de prioriteiten ook waren aangepast aan de ernst van sommige in België vastgestelde bedreigingen;
- de geïdentificeerde bedreigingen niet alleen betrekking hadden op de uitoefening van de vrijheid van de persoon, de gezondheid en de fysieke integriteit van de personen, maar dat er ook sprake was van inmenging in de werking van de overheid en de economie.

Specifiek met betrekking tot de Scientologykerk vestigde de VSSE de aandacht op het streven naar verovering en totalitaire transformatie van de wereld waarvan

[99] Een samenvatting van dit onderzoek werd opgenomen in het activiteitenverslag van 2010 (VAST COMITÉ I, *Activiteitenverslag 2010*, 13 e.v.).

deze sekte blijk geeft. De dienst besloot dan ook dat dit doel strijdig is met de democratische beginselen van onze samenleving.

Tot in 2007 was de grootste bedreiging van de Scientologykerk volgens de VSSE dat ze een gevaar vormde voor de fysieke en/of psychologische integriteit van de personen, waarbij zelfs hun leven uiteindelijk gevaar kon lopen. In 2008 heeft de VSSE haar werk in verband met de Scientologykerk bijgestuurd, omdat ze van mening was dat de prioriteit voortaan moest uitgaan naar de inmenging door deze sekte ten aanzien van de overheid.

Het Vast Comité I nam akte van de globale analyse door de VSSE van de vele vormen van inmenging die de Scientologykerk beoefent ten aanzien van de overheden. Het Comité stelde echter vast dat de eigen waarnemingen van de VSSE nooit middelen aan het licht hebben gebracht die eigenlijk '*ongeoorloofd*' zijn en waarvan de Scientologykerk gebruik maakt om politieke beleidsmakers te benaderen. De VSSE beschikte echter over tal van aanwijzingen die deden vermoeden dat er daartoe gebruik wordt gemaakt van '*bedrieglijke en clandestiene middelen*'.

Het Vast Comité I kwam dan ook tot het besluit dat de VSSE de activiteiten van de vzw Scientologykerk van België op wettige wijze volgt, zonder inbreuk op de rechten die de Grondwet en de wet aan de klagende partij verlenen.

II.5.2. DE INFORMATIE DIE AAN DE BASIS LAG VAN DE GELEKTE NOTA'S

De informatie uit de twee nota's was verzameld op basis van uiteenlopende inlichtingenmethoden (waaronder ook een analyse van open bronnen en van getuigenissen van gewezen volgelingen) en dit door verschillende afdelingen binnen de VSSE. Het Vast Comité I heeft hierbij geen onregelmatigheden vastgesteld.

De informatie die aan de overheden werd bezorgd, werd geëvalueerd en geanalyseerd overeenkomstig de regels van de kunst.

De verslagen die het Comité heeft bestudeerd, waren beknopt en bevatten voornamelijk feiten. Ze maakten het nodige voorbehoud wanneer bepaalde gegevens niet konden worden bevestigd.

De analyses hadden voornamelijk betrekking op de ideologie, de praktische organisatie, de activiteiten en de inplanting van de Scientologykerk.

II.5.3. DE VERSPREIDING VAN DE TWEE NOTA'S EN HET VERMOEDEN VAN ONSCHULD

De klager was van oordeel dat de lekken in de pers niet toevallig samenvielen met het moment waarop het strafdossier tegen de Scientologykerk voor de raadkamer

zou behandeld worden. Het zou de bedoeling zijn geweest om deze kerk schade toe te brengen of minstens in een negatief daglicht te stellen. Voorts wees de klager op het feit dat de VSSE in de strafzaak was aangesteld als technisch deskundige.

Met betrekking tot dit aspect van de klacht hernam het Comité zijn vaststellingen uit het eerdere toezichtonderzoek.[100] Het besloot dan ook dat zijn onderzoek naar de verspreiding van de bewuste documenten en het lekken ervan, geen enkel doorslaggevend element aan het licht had gebracht op grond waarvan de VSSE hiervoor aansprakelijk kon worden gesteld.

II.6. DE INFORMATIEPOSITIE VAN DE INLICHTINGENDIENSTEN EN VAN HET OCAD MET BETREKKING TOT EEN LEERLING-PILOOT

In een toezichtonderzoek van het Vast Comité P naar '*informatiestromen op de luchthavens*'[101] werd onder meer verwezen naar een persoon die een pilotenopleiding kon volgen op een Belgische luchthaven, alhoewel hij een verleden had dat mogelijks wees op radicalisering. Aangezien dit voorbeeld kon wijzen op een gebrekkige informatie-uitwisseling tussen de betrokken overheidsdiensten, werd in juni 2013 besloten om een gemeenschappelijk toezichtonderzoek te openen '*betreffende de informatiepositie en de opvolging door de ondersteunende diensten van het OCAD – alsook naar de evaluatie van de dreiging door het OCAD – betreffende een particulier die toelating verkreeg om een cursus als vliegtuigpiloot te volgen in België*'.[102, 103]

De betrokken leerling-piloot – van buitenlandse origine en in België aangekomen begin jaren '90 – kwam ten tijde van zijn naturalisatieaanvraag eind jaren '90 voor het eerst in het vizier van de VSSE.[104] De dienst was in het bezit van informatie waaruit zou blijken dat hij deel uitmaakte van een welbepaalde organisatie en

100 VAST COMITÉ I, *Activiteitenverslag 2013*, 25-31.

101 www.comitep.be/AdditionalReports/2012-06-12_NL_informatiestromen_luchthavens.pdf ('Operationele informatiestromen op luchthavens').

102 De onderzoeksresultaten met betrekking tot het luik 'politie' worden in voorliggend verslag slechts summier weergegeven. Voor een meer volledige rapportage verwijst het Vast Comité I naar de publicaties van het Vast Comité P.

103 Naar aanleiding van de bespreking van voorliggend toezichtonderzoek in de Begeleidingscommissie van de Kamer werd in 2015 besloten een aspect verder uit te diepen in een nieuw toezichtonderzoek '*naar het bepalen – door het OCAD – van het niveau van de dreiging die uitgaat van en naar een individu, en naar de gevolgen dat dergelijk dreigingsniveau heeft op het vlak van taakverdeling, maatregelen, informatiestroom, praktische gevolgen voor een burger en opvolging*'.

104 De VSSE bewaarde geen afschrift van het advies dat ze in 1998 uitbracht in het kader van de naturalisatieprocedure. Zie hierover ook: VAST COMITÉ I, *Activiteitenverslag 2012,* 5-14 (II.1. De rol van de VSSE in het kader van procedures tot het verkrijgen van de Belgische nationaliteit).

een opleiding luchtvaartkunde had gekregen. In een gesprek met agenten van de VSSE bevestigde de man deze informatie. Hij verklaarde daarin ook dat zijn weigering om deel te nemen aan bepaalde 'acties' van die organisatie die gericht waren tegen een andere Staat, ertoe hadden geleid dat hij zijn toevlucht zocht in België. Zijn lidmaatschap bij de organisatie was naar eigen zeggen de enige mogelijkheid om te kunnen studeren. De VSSE beoordeelde deze verklaringen als aannemelijk.

In datzelfde jaar solliciteerde de betrokkene voor de job van onderhoudstechnicus op de Luchthaven van Zaventem. In dat verband werd de veiligheidspost van de VSSE die werkzaam is op de luchthaven om bijkomend onderzoek verzocht. Dat onderzoek leverde evenwel niets bijzonder op.

Pas in maart 2006 trok de man opnieuw de aandacht van de veiligheidsdiensten: volgens de Luchtvaartpolitie Brussel-Nationaal zou hij zich – onder invloed van een radicale imam – agressief hebben gedragen en mogelijks zelf radicaliseren. De VSSE wordt hiervan in kennis gesteld; zij ontmoet de man voor de tweede maal, maar ook nu levert dit niets op. Wel blijkt de betrokkene een door de VSSE gekende moskee te bezoeken.

In november 2007 ontvangt de VSSE opnieuw informatie, nu van de Luchtvaartpolitie Oostende-Wevelgem: de betrokkene volgt vlieglessen met het oog op het behalen van een brevet van privépiloot. Hij blijkt bijzonder gehaast te zijn en betaalt zijn lessen contant, hetgeen gelet op de politionele informatie uit maart 2006 problematisch zou kunnen zijn. De VSSE beschikte echter ook nu niet over concrete elementen die zouden wijzen op een neiging tot radicalisering.[105]

Toch wisselen de verschillende veiligheidsdiensten (politie, VSSE, ADIV en OCAD) vanaf nu regelmatig informatie uit. Het is overigens voor het eerst dat de ADIV informatie krijgt over de betrokkene. De dienst voerde echter geen onderzoek naar hem, dit ondanks dat de ADIV stelde na de aanslagen van 11 september 2001 bijzondere aandacht te besteden aan leerling-piloten.

Op vraag van de Luchtvaartpolitie Oostende-Wevelgem wordt in december 2007 een coördinatievergadering gehouden over de betrokkene. Daarop zijn diverse politiediensten en de twee inlichtingendiensten aanwezig. De VSSE en de ADIV kunnen geen nieuwe informatie bijbrengen.

Na de vergadering is de Federale Politie DJP/Terro van oordeel dat er geen reden is om de veiligheidsbadge van betrokkene, die hem toegang verleent tot de luchthaven van Wevelgem, te weigeren. Wel wordt beslist de betrokkene te seinen op basis van de Schengenovereenkomst én een dreigingsevaluatie te vragen aan het OCAD.

---

105 De VSSE voerde geen onderzoek naar de gelden waarmee de vlieglessen werden gefinancierd. Bij gebrek aan elementen die wezen op radicalisering werd een dergelijk onderzoek als zijnde niet-proportioneel beoordeeld.

Midden december 2007 is de analyse van het OCAD klaar[106]: ze bepaalt de dreiging op niveau '2'.[107, 108] Desgevraagd verduidelijkte het OCAD ten aanzien van de Comités dat het nooit precieze informatie kreeg die liet vermoeden dat de betrokkene een terreuractie zou uitvoeren. De enige verontrustende elementen waren zijn verleden bij een welbepaalde organisatie, zijn vlieglessen en een (tijdelijke) gedragswijziging. Dreigingsniveau 3, wat staat voor '*een mogelijke en waarschijnlijke dreiging*', was in deze dan ook niet gerechtvaardigd. Niettemin raadde het OCAD alle diensten aan om waakzaam te blijven en de situatie van de betrokkene permanent op te volgen en aandacht te besteden aan eventuele evoluties in zijn gedrag die konden wijzen op een radicalisering. In geval van een 'niveau 2', volgt het OCAD het dossier zelf niet actief op maar laat dit over aan de bevoegde diensten, zonder daartoe specifiek een 'pilootdienst' aan te duiden. Pas vanaf een evaluatie van 'niveau 3' zal het OCAD zelf een actieve opvolging verzorgen. De Comités moesten echter vaststellen dat het voor de verschillende betrokken ondersteunende diensten niet duidelijk was, wie moest instaan voor de coördinatie noch waaruit de gevraagde opvolging juist moest bestaan. Ook was het voor een ondersteunende dienst die niet van bij aanvang betrokken was bij de evaluatie, niet altijd mogelijk om te weten of er al dan niet een permanente opvolging werd gevraagd door het OCAD.

Begin 2008 volgden diverse bijkomende vergaderingen met de veiligheidsdiensten en wordt er regelmatig informatie uitgewisseld. In april 2008 stelt de VSSE zelfs een interne synthesenota op over de dreiging die van de betrokkene zou kunnen uitgaan. De dienst besluit opnieuw over geen negatieve informatie te beschikken.

Half november 2008 blijkt uit nieuwe politionele informatie dat de betrokkene zich op de luchthaven vreemd zou gedragen hebben bij zijn terugkeer uit vakantie. Er wordt opnieuw een coördinatievergadering belegd. Kort nadien beslist de VSSE de man voor een derde maal te spreken. Ook zijn werkgever wordt ditmaal bevraagd. En opnieuw blijken er geen elementen voorhanden die zouden kunnen wijzen op een radicalisering.

Tussen 2009 en 2011 ontving de VSSE nog enkele nota's van de politie. De VSSE maakt in juni 2010 nog een rapport waarin wordt meegedeeld dat betrokkene zijn diploma (*Private Pilot License*) haalde en een opleiding tot commercieel

---

106 Zowel de Dienst Vreemdelingenzaken (DVZ) als de FOD Mobiliteit, zijnde twee steundiensten van het OCAD, werden verzocht om bijkomende informatie. Het OCAD kreeg van deze diensten echter geen aanvullende informatie die zou kunnen wijzen op een verhoogde kans tot gevaar.

107 *'Het niveau 2 of GEMIDDELD' wordt toegekend indien blijkt dat de dreiging tegen de persoon, de groepering of de gebeurtenis die het voorwerp uitmaakt van de analyse weinig waarschijnlijk is'* (art. 11, § 6, 2° KB OCAD).

108 Het OCAD merkte op dat er geen elementen waren die er op wezen dat de betrokkene een radicaliserend effect zou hebben op anderen. In die zin viel hij niet onder het Plan Radicalisme.

piloot wil volgen.[109] Hij werd evenwel niet meer systematisch opgevolgd door de VSSE.

II.7. TOEZICHTONDERZOEK NAAR DE ELEMENTEN DIE DE VSSE VERSCHAFTE IN HET KADER VAN EEN NATURALISATIEDOSSIER

Een procureur des Konings verzette zich tegen de verlening van de Belgische nationaliteit van een particulier, daarbij verwijzend naar de door de VSSE bijgebrachte '*gewichtige feiten eigen aan de persoon*'. De betrokkene was echter van oordeel dat er sprake was van een misverstand. Eind juli 2013 diende de man klacht in bij het Vast Comité I.[110] Het Comité opende daarop een toezichtonderzoek dat in februari 2014 werd gefinaliseerd.

II.7.1. DE KLACHT

De klager was van mening het slachtoffer te zijn van een inbreuk op zijn individuele rechten door de VSSE. Immers, uit het advies van de procureur des Konings bleek dat de betrokkene bij de VSSE bekend stond wegens zijn actieve betrokkenheid bij een beweging die voorkomt op de Europese lijst van terroristische organisaties, alsook wegens zijn '*implication présumée*'[111] bij activiteiten van afpersing, omkoping van ambtenaren, witwassen van geld en financiering van terrorisme met vals geld.

Voormelde redenen waren volgens de klager volkomen uit de lucht gegrepen. Hij omschreef deze als '*zeer kwetsend, vernederend en beledigend*'. Geen van de feiten die de VSSE ter kennis van de procureur des Koning had gebracht, zouden volgens hem door een concreet element worden gestaafd. Bovendien verwees de klager naar zijn blanco strafblad.

---

109 Vanaf mei 2012 beschikte betrokkene niet meer over een geldige machtiging. Hij mag bijgevolg geen vliegtuig meer besturen.

110 De klager wendde zich in mei 2013 ook tot de Commissie voor de bescherming van de persoonlijke levenssfeer om toegang te krijgen tot de door de VSSE verwerkte persoonsgegevens. Conform art. 13, derde lid van de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (de Privacywet) deelde de Commissie aan de klager mee dat de noodzakelijke verificaties werden verricht. Ook vroeg de betrokkene om de zaak aanhangig te maken bij de rechtbank van eerste aanleg. Dit had tot gevolg dat zijn dossier als naturalisatieverzoek aan de Kamer van Volksvertegenwoordigers werd bezorgd.

111 'vermoedelijke betrokkenheid' (vrije vertaling).

II.7.2. VASTSTELLINGEN

Na onderzoek kwam het Comité tot de conclusie dat er in voorliggend geval effectief sprake was van een probleem in de beoordeling, de verwerking en de mededeling van informatie door de Veiligheid van de Staat aan de gerechtelijke overheden.

De klager komt voor het eerst bij de VSSE in beeld in 2009. Op dat ogenblik ontvangt de VSSE informatie die aangeeft dat de persoon in kwestie een militant is van een bepaalde terroristische organisatie. De informatie maakt tevens gewag van zijn betrokkenheid bij gemeenrechtelijke misdrijven. De beschikbare informatie was evenwel afkomstig uit één enkele bron. Er werd dan ook bijkomend onderzoek verricht.

Bij toepassing van artikel 29 Sv. bracht de VSSE begin 2010 de procureur des Konings en de federaal procureur van alle eerder vage en niet-bevestigde informatie op de hoogte. Omdat de VSSE met geen expertise-opdracht werd belast, leidde de dienst daaruit af dat er als gevolg van deze melding geen gerechtelijk onderzoek was geopend.

Als de klager in december 2012 zijn aanvraag indient om de Belgische nationaliteit te verkrijgen, bezorgt de VSSE dezelfde (niet-geactualiseerde) informatie zonder voorbehoud aan het parket. Op grond daarvan brengt de bevoegde procureur des Konings een negatief advies uit over de nationaliteitsaanvraag.

Door na te laten de informatie over de klager te actualiseren, is de VSSE lichtzinnig te werk gegaan. De dienst heeft zodoende de mogelijkheden van de klager om de Belgische nationaliteit te verkrijgen, in het gedrang gebracht.

Als gevolg van de klacht die de benadeelde had ingediend bij het Vast Comité I, stuurde de VSSE haar positie bij en werd de informatie vooralsnog geactualiseerd. Rekening houdende met deze nieuw verzamelde informatie, meende de VSSE dat de klager moet worden beschouwd als zijnde '*niet ongunstig gekend door de VSSE*'. De VSSE verbond zich ertoe de bevoegde procureur des Konings daarvan op de hoogte te brengen.

II.8. KLACHT OVER DE WIJZE WAAROP DE VSSE EEN ZAAKVOERDER VAN EEN BELGISCH EXPORTBEDRIJF OPVOLGT

Midden 2013 beklaagt een zaakvoerder van een firma zich bij het Comité.[112] Bepaalde leden van de VSSE zouden sinds 2010 geregeld bij hem langskomen met tal van vragen over klanten en leveranciers en hun bankgegevens. Het bedrijf is

[112] Op 3 oktober 2013 werd het toezichtonderzoek geopend. Het eindverslag werd aan de Begeleidingscommissie toegestuurd op 12 september 2014.

een '*broker*': het fungeert als bemiddelaar of tussenpersoon bij de verkoop of export van producten.[113] *In casu* betrof het zogenaamde '*producten voor tweeërlei gebruik'* of met andere woorden *'producten, met inbegrip van programmatuur en technologie, die zowel een civiele als militaire bestemming kunnen hebben, met inbegrip van alle goederen die voor niet-explosieve doeleinden gebruikt kunnen worden en op enige manier bijdragen in de vervaardiging van nucleaire wapens of andere nucleaire explosiemiddelen.*'[114]

De contacten tussen de klager en de VSSE zouden mettertijd steeds stroever zijn gaan verlopen; de klager voelde zich zelfs geïntimideerd en bedreigd. Hij vreesde ook dat de informatie die hij moest geven bij derden zou terecht komen en vroeg zich af of er wel een verplichting bestond om mee te werken met de inlichtingendienst.

II.8.1. HET FEITENRELAAS

Wanneer de Administratie der Douane en Accijnzen (D&A) in 2010 een routinecontrole uitvoert, stuit zij bij de betrokken firma op een poging tot uitvoer van goederen die onder een embargo vallen. Er wordt een substantiële som als minnelijke schikking betaald en de firma ontsnapt zo aan gerechtelijke vervolging.

De VSSE wordt echter van de zaak op de hoogte gebracht door de Dienst Controle Strategische Goederen (DCSG), die in Vlaanderen toeziet op de activiteiten van dergelijke firma's en die reguliere contacten onderhoudt met de inlichtingendienst. Daarop opent de VSSE een dossier. Uit de navolgende contacten met de twee betrokken overheden (D&A en DCSG) blijken er zich in het verleden nog andere 'incidenten'[115] te hebben voorgedaan. Mogelijks neemt de firma het niet nauw met de geldende regels. Ook buitenlandse correspondenten maken melding van verdachte gedragingen en contacten tussen de firma en buitenlandse zakenpartners.

De VSSE nam ook rechtstreeks contact op met de betrokken firma. In totaal ging de VSSE tussen 2010 en eind 2013 twaalf maal ter plaatse om gegevens op te vragen.

---

113 Een *broker* kan diverse rollen op zich nemen, wat het moeilijk maakt om een eenduidig zicht te krijgen op zijn functioneren. Bovendien komt het voor dat een *broker* bemiddelt tussen twee (rechts)personen die in het buitenland gevestigd zijn zodat de verhandelde producten nooit via ons land worden getransporteerd.

114 Verordening (EG) nr. 1334/2000 van de Raad van 22 juni 2000 tot instelling van een communautaire regeling voor controle op de uitvoer van producten en technologie voor tweeërlei gebruik.

115 Beide administraties hadden veelvuldige contacten met de firma die schijnbaar problemen had met het beheer van documenten en met de regelgeving. Zo werden er met de DCSG meerdere overlegmomenten georganiseerd om de firma wegwijs te maken in de wetgeving, de sancties, de noodzaak tot het aanleveren van technische informatie… De D&A op zijn beurt had onder meer afspraken gemaakt met de firma om een volledige douanecontrole te laten uitvoeren, maar deze werden door de firma niet gehonoreerd.

II.8.2. DE VASTSTELLINGEN

II.8.2.1. Bevoegdheid van de VSSE

De activiteiten van de betrokken firma konden gerelateerd worden aan proliferatie, zijnde één van de kernopdrachten van de VSSE (art. 8 W.I&V). Bovendien verdiende deze dreiging volgens het toenmalige actieplan een 'actieve prioritaire opvolging'.[116] Gelet op de aanwijzingen die vanuit derde diensten waren aangebracht, zou de VSSE ernstig tekortgeschoten zijn, mocht ze niet zijn opgetreden.

De klacht die de firma formuleerde – met name dat de VSSE haar ten onrechte opvolgde – miste dus grond: het optreden van de VSSE was niet willekeurig maar gebaseerd op belangrijke aanwijzingen en de dienst bleef daarbij binnen zijn wettelijke bevoegdheden. Bovendien bleek de VSSE bij de beoordeling van de zaak niet overhaast of op ongenuanceerde wijze te werk te zijn gegaan.

II.8.2.2. De rechtstreekse contacten met de klager

De VSSE heeft er vrij snel voor geopteerd om rechtstreeks contact op te nemen met de betrokken firma. Men ging er van uit dat de vastgestelde onregelmatigheden niet bedoeld waren om doelbewust de exportbeperkingen te overtreden, maar dat het eerder ging om handelingen van een klein bedrijf dat financieel trachtte te overleven en zich wellicht niet volledig bewust was van de reikwijdte van haar acties. De VSSE koos derhalve terecht voor een gewone methode van gegevensverzameling, met name het rechtstreeks benaderen van de betrokkene.

De vragen die de VSSE met betrekking tot de klanten- en bankgegevens stelde, waren terecht en pasten binnen de bevoegdheid van de VSSE. Gelet op de omstandigheden van de zaak vormde dit een toereikende en proportionele inlichtingenmethode.[117] Dergelijke informatie mag ingewonnen worden bij elke privépersoon of -organisatie (art. 16 W.I&V). De betrokkene blijft echter zelf gebonden door het beroepsgeheim waaraan hij desgevallend is onderworpen of aan de eisen van de wetgeving inzake de bescherming van de persoonlijke levenssfeer. Beide regelingen leggen beperkingen op inzake het mededelen van gegevens aan derden.

De klacht aangaande de intimiderende houding van een lid van de VSSE kon niet aan de hand van VSSE-documenten op zijn waarheid worden getoetst en

---

116 Uit rapporten van de Verenigde Naties blijkt overigens dat proliferatie van NRBC-wapens als één van de belangrijkste bedreigingen moet beschouwd worden. De strijd tegen proliferatie is fundamenteel in de (inter)nationale veiligheidsproblematiek. Hierin is een belangrijke opdracht weggelegd voor de VSSE. Het Vast Comité I heeft zich in het verleden reeds over de proliferatie-gerelateerde activiteit van de VSSE gebogen: VAST COMITÉ I, *Activiteitenverslag 2008,* 42-43, *Activiteitenverslag 2011*, 37-40 en *Activiteitenverslag 2013*, 47-50.

117 In theorie zou de inzet van uitzonderlijke BIM-methoden om bankgegevens of communicatie met klanten te bekomen ook mogelijk zijn geweest aangezien het dossier betrekking had op de strijd tegen proliferatie; *in casu* was de inzet van uitzonderlijke methoden echter niet noodzakelijk.

daaromtrent uitdrukkelijk ondervraagd, ontkenden de leden van de VSSE dat ze zich intimiderend hadden gedragen. Het Comité oordeelde dat het niet meer mogelijk was om *a posteriori* de ware toedracht te achterhalen, maar het benadrukte dat intimidatie vanzelfsprekend niet duldbaar is.

Het Comité benadrukte ten slotte ook dat de burger het recht heeft om niet mee te werken aan een inlichtingenonderzoek.

II.8.2.3. De complexiteit van de strijd tegen proliferatie

Het Vast Comité I stelde in de marge van het onderzoek vast dat de problematiek rond proliferatie heel complex en weinig doorzichtig is, zowel voor de ondernemingen die er mee te maken hebben, als voor de diensten die in dit kader een rol te vervullen hebben.

Bovendien blijkt een adequate controle- en sanctieregeling nog steeds te ontbreken. Alhoewel de VSSE vanzelfsprekend controlerend noch sanctionerend moet optreden, betekent dit wel dat de bevoegdheidsproblemen die op dit vlak tussen de federale Staat en de Gewesten bestaan[118], niet bevorderlijk zijn voor de werkzaamheden van de betrokken diensten, en dus ook niet voor de VSSE die van deze diensten nuttige informatie zou moeten kunnen krijgen.

In de conclusies van het toezichtonderzoek '*De rol van de inlichtingendiensten in het kader van de strijd tegen proliferatie van niet-conventionele en zeer geavanceerde wapens*' van 2008 wees het Vast Comité I er reeds op dat de detectie van transacties betreffende proliferatie en de *catch all*-clausule[119] moeilijk is om diverse redenen. Zo is er de veelheid van transacties naar 'proliferatielanden', is er de problematiek van de *dual use*-goederen, het gebrek aan betrouwbare en transparante gegevens die verstrekt worden door de firma's, en de complexiteit van de codering van goederen door de douanediensten.[120]

Het voorliggend onderzoek toonde aan dat voornoemde problemen nog niet opgelost zijn, wat het optreden van de VSSE in deze materie bemoeilijkt.

---

118 Uit een parlementaire vraag gericht aan de minister-president van de Vlaamse regering over een structurele samenwerking tussen de DCSG, de VSSE en de D&A blijkt dat deze nog niet op punt staat. Immers, in 2007 werd een samenwerkingsakkoord gesloten door de federale Staat en de drie Gewesten betreffende de in-, uit-, en doorvoer evenals producten en technologie van tweeërlei gebruik en de toekenning van vergunningen in verband daarmee. Maar dit akkoord sloeg enkel op de FOD Buitenlandse Zaken en de Gewesten, en niet op de FOD Economie, de VSSE en de D&A (*Hand.* Vlaams Parlement 2013-14, 1 april 2014, nr. C172-BUI7, 15, Vr. nr. 1159).

119 Welke goederen militair zijn, en dus gecontroleerd moeten worden, werd op internationaal niveau bepaald en vastgelegd in productielijsten. Verschillende landen hebben echter ook een clausule in de wetgeving die toelaat om producten die niet op de lijst staan om veiligheidsredenen, toch onder vergunning te plaatsen, bijvoorbeeld omdat ze militair ingezet worden. Dit is de '*catch all*'.

120 VAST COMITÉ I, *Activiteitenverslag 2008,* 42-57, in het bijzonder p. 56.

II.9. EEN PARTICULIER GEVOLGD DOOR DE INLICHTINGENDIENSTEN?

Eind november 2013 wordt een klacht ingediend bij het Vast Comité I. De klager, sinds 1994 gedomicilieerd in België en in het bezit van de Belgische nationaliteit, was er van overtuigd dat hij het voorwerp uitmaakte van fysieke observatie en schaduwing door 'de inlichtingendiensten'. Hij zag hiervoor meerdere mogelijke aanleidingen. Zo maakt hij bijvoorbeeld deel uit van een bepaalde religieuze, islamitische beweging. De klager had de indruk dat zijn telefoongesprekken en mailverkeer werden onderschept. De feiten zouden zich zowel in België als in zijn land van herkomst voordoen.

Daarop opende het Comité begin februari 2014 een toezichtonderzoek: was betrokkene effectief bekend bij de Veiligheid van de Staat en de ADIV? Zoja, sinds wanneer en in welk kader? Werden daarbij bijzondere inlichtingenmethoden ingezet? Welke inlichtingen werden over hem ingewonnen?… Het Comité was uiteraard niet bevoegd om de eventuele rol van buitenlandse inlichtingendiensten te onderzoeken.

Het toezichtonderzoek werd midden mei 2014 afgerond. Hieruit bleek dat de Belgische inlichtingendiensten geen enkele onwettige handeling hadden uitgevoerd met betrekking tot de klager.

II.10. TOEZICHTONDERZOEKEN WAAR IN DE LOOP VAN 2014 ONDERZOEKSDADEN WERDEN GESTELD EN ONDERZOEKEN DIE IN 2014 WERDEN OPGESTART

Dit onderdeel bevat een opsomming en een korte situering van alle in 2014 opgestarte onderzoeken alsook van die onderzoeken waaraan tijdens het werkingsjaar 2014 werd verder gewerkt maar die nog niet konden worden afgerond.

II.10.1. DE OPVOLGING VAN EXTREMISTISCHE ELEMENTEN IN HET LEGER

Naar aanleiding van briefings gegeven door de ADIV, nam het Vast Comité I kennis van de problematiek van militairen die zich binnen extremistische kringen bewegen en militairen die lid of sympathisant zijn van motorbendes. In diezelfde periode maakte de media gewag van de (tijdelijke) aanwezigheid van een militant-djihadist bij het Bataljon Ardense Jagers, die met de opgedane ervaring gevechtshandboeken zou hebben opgesteld.

Het Comité besloot een toezichtonderzoek te openen naar '*de opsporing en de opvolging door de ADIV van extremistische elementen bij het personeel van Defensie en de Krijgsmacht*'. Het onderzoek wil nagaan of de ADIV deze problematiek op een efficiënte wijze aanpakt en of de dienst hierbij de rechten van de burgers respecteert.

In de loop van het onderzoek werd de regelgeving met betrekking tot de verificatie of zogenaamde *screening* van kandidaat-leden van Defensie gewijzigd. Er werd beslist het onderzoek uit te breiden tot die materie zodat de aandacht van het onderzoek komt te liggen op twee processen: het screeningsproces gedurende de rekruteringsfase en het detectieproces en de opvolging van radicale of extremistische elementen die reeds eerder werden gerekruteerd.

In de loop van 2014 werd onder andere aanvullende informatie opgevraagd bij het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten of –adviezen en werden andere bijkomende onderzoeksdaden verricht. Ook werd beslist om de voorlopige resultaten van het onderzoek aan te vullen met informatie over de Syriëproblematiek.[121]

II.10.2. DE WIJZE VAN BEHEER, BESTEDING EN CONTROLE VAN DE SPECIALE FONDSEN

In 2011-2012 werden door de gerechtelijke overheden twee strafonderzoeken opgestart naar het eventuele misbruik van gelden bestemd voor de vergoeding van informanten. De Dienst Enquêtes I werd vanuit zijn gerechtelijke opdracht ingeschakeld in beide onderzoeken.[122] Gezien de elementen waarover het Vast Comité I kon beschikken op mogelijke structurele problemen wezen, werd begin september 2012 beslist een thematisch onderzoek te openen naar '*de wijze van beheer, besteding en controle van de fondsen bestemd voor de vergoeding van informanten van de VSSE en de ADIV*'.

Gelet op de lopende strafonderzoeken, werd het toezichtonderzoek echter meteen opgeschort. Eind maart 2014 werd besloten dat het toezichtonderzoek kon worden heropgestart. Het rapport zal worden gefinaliseerd in 2015.

121 In maart 2015 maakte de minister van Defensie in de Commissie voor Landsverdediging bekend dat twee geradicaliseerde Belgische ex-militairen in Syrië zouden strijden.

122 VAST COMITÉ I, *Activiteitenverslag 2013*, 97-98 (Hoofdstuk VI. De opsporings- en gerechtelijke onderzoeken).

II.10.3. TOEZICHTONDERZOEK NAAR DE *JOINT INFORMATION BOX*

De oprichting van een zogenaamde *Joint Information Box* (JIB) – goedgekeurd door het Ministerieel Comité voor inlichting en veiligheid – vormde volgens de initiatiefnemers het speerpunt van het 'Actieplan Radicalisme'. Het betreft een werkbestand dat werd ondergebracht bij het OCAD, en dat onder meer de structurele verzameling van informatie over entiteiten die in het kader van het Actieplan Radicalisme worden opgevolgd, tot doel heeft.

In een gezamenlijke vergadering van de Vaste Comités P en I van midden november 2012 werd beslist een toezichtonderzoek te openen '*over de wijze waarop het OCAD de informatie, opgeslagen in de Joint Information Box (JIB) beheert, analyseert en verspreidt, overeenkomstig de uitvoering van het Plan Radicalisme*'.

In 2014 werden door de Enquêtediensten P en I diverse onderzoekverrichtingen gesteld. Het toezichtrapport werd gefinaliseerd in april 2015 en naar de voorzitter van de Begeleidingscommissie en naar de ministers van Justitie en Binnenlandse Zaken gestuurd.

II.10.4. INLICHTINGENAGENTEN EN SOCIALE MEDIA

Eind 2012 berichtte de media over profielen van medewerkers van de inlichtingendiensten op sociale netwerksites als *Facebook* en *LinkedIn*. Daarop verzocht de toenmalige Senatoriële Begeleidingscommissie het Vast Comité I een toezichtonderzoek te openen naar '*wat de omvang is van het fenomeen dat medewerkers van de Veiligheid van de Staat, maar eventueel ook van de ADIV en OCAD, zich hun hoedanigheid van agent van die instellingen bekend maken op Internet via sociale media*'. Tevens diende het Comité na te gaan welke risico's dergelijke bekendmaking met zich kan brengen en in welke mate hiertegen maatregelen kunnen en mogen genomen worden.

Het Vast Comité I nam in december 2012 een aanvang met zijn toezichtonderzoek met betrekking tot de medewerkers van de ADIV en de VSSE. Diverse onderzoekdaden werden verricht. Het eindrapport werd in de eerste helft van 2015 gefinaliseerd.

II.10.5. PERSONEELSLEDEN VAN HET OCAD EN SOCIALE MEDIA

Wat betreft het luik met betrekking tot de medewerkers van het OCAD en hun aanwezigheid op sociale netwerksites, werd begin 2013 ook een gemeenschappelijk toezichtonderzoek opgestart met het Vast Comité P. Immers, ingevolge arti-

kel 56, 6° W.Toezicht wordt de externe controle op de werking van het OCAD waargenomen door beide Comités gezamenlijk.

Het eindrapport werd in maart 2015 goedgekeurd op de gemeenschappelijke vergadering van de Vaste Comités I en P en naar de Begeleidingscommissie van de Kamer verzonden.

II.10.6. DE INTERNATIONALE CONTACTEN VAN HET OCAD

Een van de opdrachten van het Coördinatieorgaan voor de dreigingsanalyse bestaat er in contacten te onderhouden met 'gelijkaardige buitenlandse of internationale diensten' (art. 8, 3° W. OCAD). In zijn gezamenlijke vergadering van begin mei 2013 besloten de Vaste Comités I en P een onderzoek te voeren naar de wijze waarop het OCAD die opdracht invult.[123] In 2013 en 2014 werden diverse onderzoeksdaden uitgevoerd. Het onderzoek werd afgesloten in juni 2015.

II.10.7. DE BESCHERMING VAN HET WETENSCHAPPELIJK EN ECONOMISCH POTENTIEEL EN DE SNOWDEN-ONTHULLINGEN

De onthullingen van Edward Snowden gaven een inkijk in uitermate geheime programma's van voornamelijk de Amerikaanse *National Security Agency* (NSA). Ze waren het startschot voor vele (parlementaire, gerechtelijke en inlichtingen) onderzoeken over heel de wereld. Zo ook in België. Het Vast Comité I opende vier toezichtonderzoeken die uiteraard nauw met elkaar verweven zijn.

Drie van de vier onderzoeken werden in 2014 afgerond (zie II.1, II.2 en II.3). Een laatste toezichtonderzoek[124] – dat nog niet werd gefinaliseerd – behandelt de mogelijke implicaties van deze buitenlandse programma's op de bescherming van het wetenschappelijk en economisch potentieel van het land. Het wil nagaan of de Belgische inlichtingendiensten:

- aandacht hebben besteed aan dit fenomeen;
- een reële of mogelijke bedreiging hebben gedetecteerd voor het Belgische wetenschappelijk en economisch potentieel;

---

123 'Gemeenschappelijk toezichtonderzoek over de wijze waarop het OCAD internationale relaties onderhoudt met gelijkaardige buitenlandse of internationale diensten in toepassing van artikel 8, 3° van de W.OCAD van 10 juli 2006'.

124 Toezichtonderzoek 'over de aandacht die de Belgische inlichtingendiensten (al dan niet) besteden aan de mogelijke dreigingen voor het Belgisch wetenschappelijk en economisch potentieel uitgaande van op grote schaal door buitenlandse grootmachten en/of inlichtingendiensten gehanteerde elektronische bewakingsprogramma's op communicatie- en informatiesystemen'.

– er de bevoegde overheden van in kennis hebben gesteld en beschermingsmaatregelen hebben voorgesteld; en
– over voldoende en adequate middelen beschikken om deze problematiek op te volgen.

De Senaat verzocht destijds ook om de gevolgen te onderzoeken van de massale data-captatie op het wetenschappelijk en economisch potentieel van ons land. Het Vast Comité I heeft echter de wettelijke bevoegdheid noch de technische en personele middelen om in eigen naam een evaluatie te maken van de eventuele massale data-captatie door buitenlandse inlichtingendiensten tegen Belgische ondernemingen en/of onderzoekscentra. Echter, vanuit de bekommernis om alsnog een antwoord te bieden op het verzoek van de Senaat, heeft het Comité zich niet beperkt tot een bevraging van de VSSE en de ADIV. In de loop van 2014 richtte het zich tot een panel van personen die representatief zijn voor het wetenschappelijk en economisch milieu in België. Het Comité heeft op deze wijze getracht eventuele gevallen aan de oppervlakte te brengen waarin Belgische ondernemingen en/of onderzoekscentra slachtoffer zouden geweest zijn van dergelijke praktijken of dit vermoedden. Het Comité heeft zijn informatie ook aangevuld via consultatie van de vele Belgische en buitenlandse open bronnen (persartikels, officiële rapporten, parlementaire documenten…) waarin het op zoek ging naar cijfermateriaal, aanwijzingen en/of getuigenissen die toelieten om de implicaties van massale data-captatiesystemen op het wetenschappelijk en economisch potentieel van het land te begrijpen. Indien dergelijke indicaties zouden ontbreken, nam het Comité zich voor om een poging te ondernemen om enkele theoretische denkpistes over het fenomeen uit te werken.

Het rapport zal in de loop van 2015 worden afgerond.

II.10.8. ONTERECHT OPGEVOLGD DOOR DE INLICHTINGENDIENSTEN?

Eind februari 2014 wordt door een persoon van Noord-Afrikaanse afkomst klacht ingediend bij het Vast Comité I. De betrokkene, die sinds mei 2012 met zijn familie in België verblijft, beklaagde zich over het feit dat hij op 'beklemmende wijze' in het oog wordt gehouden door de inlichtingendiensten. De klager beweerde geen enkel idee te hebben waarom hij de aandacht zou trekken; hij heeft nooit problemen gehad in zijn land van herkomst noch in het Aziatisch land waar hij meerdere jaren heeft gewerkt. Hij zou geen gerechtelijke antecedenten hebben of banden met terrorisme of radicalisme. Hij verklaarde bovendien het voorwerp te zijn geweest van toezichtoperaties, een gevoel dat nog werd versterkt door de bijzondere behandeling die hem tweemaal te beurt viel op de luchthaven van Zaventem.

In juli 2014 besliste het Comité een toezichtonderzoek te openen. Daarmee wou het Comité zich ervan gewissen of de klager effectief onder de aandacht was gekomen van de Veiligheid van de Staat of de ADIV, en zoja, waarom en met welke resultaten.

Diverse onderzoeksdaden werden gesteld en in februari 2015 werd het eindrapport verzonden naar de voorzitter van de Begeleidingscommissie, alsook naar de ministers van Justitie en Defensie.

II.10.9. DE VSSE EN DE TOEPASSING VAN HET ARBEIDSREGLEMENT

Het Comité besliste midden 2014 een toezichtonderzoek te openen *'naar de wijze waarop de VSSE het arbeidsreglement en meer in het bijzonder de regels inzake ziekteverlof interpreteert en er uitvoering aan geeft'*. Aanleiding was een klacht van een beschermingsassistent bij de Dienst Persoonsbescherming van de VSSE. Betrokkene, die in non-activiteit werd geplaatst en daardoor naar eigen zeggen financiële (afwezigheid zonder wedde) en administratieve (vertraging in de loopbaan) schade leed, kaartte ook andere problemen aan: het beheer van overuren, het vage wettelijk kader met betrekking tot de arbeidsreglementering, de reglementering betreffende de ziekteverloven en de preventieve geneeskunde…

In februari 2015 werd het eindrapport van het Comité verzonden naar de minister van Justitie en de voorzitter van de Begeleidingscommissie.

II.10.10. DE PROBLEMATIEK VAN DE 'FOREIGN FIGHTERS' EN DE SYRIËGANGERS

Sinds 2013 oefent het Syrische strijdtoneel een grote aantrekkingskracht uit op de zogenaamde '*foreign fighters*' vanuit de hele wereld. Feit is dat daarbij – verhoudingsgewijs – veel strijders uit België komen.

Vandaar dat het Vast Comité I in oktober 2014 besloot een toezichtonderzoek te openen naar '*de informatiepositie van de twee inlichtingendiensten (ADIV en VSSE) over de rekrutering, de zending, het verblijf en de terugkeer in België van jongeren (van Belgische en andere nationaliteiten die in België verblijven) die vertrekken of vertrokken zijn naar Syrië of Irak en aangaande de uitwisseling van inlichtingen met diverse overheden.*' Daarbij zijn verschillende thema's aan de orde: welke opdracht hebben de Belgische inlichtingendiensten in dit kader en op welke wijze werden/worden zij aangestuurd? Hebben de inlichtingendiensten een kijk op de rekruterings- en vertrekfase? Kunnen zij zich een beeld vormen van de Syriëstrijders? Zijn ze op de hoogte van de activiteiten die deze strijders ter plaatste ontwikkelen? Wordt de evolutie in het buitenland vertaald naar mogelijke binnenlandse dreigingen, en zo ja, welke? En wat met de opvolging en aan-

pak bij hun terugkeer naar België? Op welke wijze wordt er in deze samengewerkt (ADIV, VSSE, OCAD maar ook politie)? Op welke wijze en aan wie wordt gerapporteerd?…

Begin maart 2015 was een eerste, tussentijds rapport het voorwerp van bespreking in de Kamercommissie belast met de begeleiding van het Vast Comité P en I. Een tweede rapport zal worden afgeleverd na het zomerreces 2015.

II.10.11. DE VSSE EN HET SAMENWERKINGSPROTOCOL MET DE STRAFINRICHTINGEN

Op 1 oktober 2014 wordt een toezichtonderzoek opgestart naar de wijze waarop de VSSE het '*protocolakkoord tot regeling van de samenwerking tussen de Veiligheid van de Staat en het Directoraat-generaal Uitvoerig van Straffen en Maatregelen*' uitvoert. Rechtstreekse aanleiding van het onderzoek vormden twee eerder afgesloten toezichtonderzoeken.[125] Het doel ligt erin te bestuderen of het akkoord efficiënt wordt toegepast, of de VSSE er voor de uitvoering van zijn opdrachten nuttige informatie uit kan putten en, zij het in de marge, na te kijken of de uitwisseling van gegevens van gedetineerden conform de bescherming van de rechten die de Grondwet en de wet aan de personen waarborgen verloopt.

Het onderzoek zal worden afgerond in 2015.

II.10.12. ONTERECHT DOORSTUREN VAN INFORMATIE DOOR DE ADIV?

Begin oktober 2014 wordt bij het Vast Comité I klacht neergelegd door een particulier. De klager werd naar eigen zeggen omwille van dringende reden ontslagen en dit op basis van informatie die zijn werkgever eerder had verkregen van een medewerker van de ADIV. Het Comité besliste eind oktober 2014 een toezichtonderzoek te openen.

Het onderzoek moest duidelijk maken op welke wijze het dossier werd behandeld door de ADIV, of de dienst zich daarbij heeft gehouden aan de vigerende regelgeving en of er inderdaad informatie werd doorgegeven aan een derde.

Het onderzoek werd afgerond in juni 2015.

---

125 VAST COMITÉ I, *Activiteitenverslag 2011*, 22-25 (II.3. De informatiepositie en acties van de inlichtingendiensten met betrekking tot Lors Doukaev) en *Activiteitenverslag 2012*, 28-33 (II.3. De eventuele opvolging van een particulier tijdens en na zijn opsluiting in België).

HOOFDSTUK III
CONTROLE OP DE BIJZONDERE INLICHTINGENMETHODEN

Artikel 35 § 1, 1° W.Toezicht bepaalt dat het Comité in zijn jaarlijks activiteitenverslag '*specifiek aandacht [moet besteden] aan de specifieke en de uitzonderlijke methoden voor het verzamelen van gegevens, zoals bedoeld in artikel 18/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten [en] aan de toepassing van hoofdstuk IV/2 van dezelfde wet*'.[126] Dit hoofdstuk behandelt dan ook de inzet van bijzondere inlichtingenmethoden door de beide inlichtingendiensten en de wijze waarop het Vast Comité I zijn jurisdictionele rol in deze waarneemt. Het vormt de verkorte weergave van de twee zesmaandelijkse verslagen die het Comité ten behoeve van zijn Begeleidingscommissie moet opstellen.[127]

III.1. VOORAFGAAND: DE 'WERKGROEP BIM'

In april 2014 werd door de beide inlichtingendiensten, de BIM-Commissie en de Dienst Enquêtes van het Vast Comité I de zogenaamde 'werkgroep BIM' opgericht. In 2014 kwam deze werkgroep viermaal samen rond volgende thema's: een bespreking van de meest recente jurisprudentie van zowel de Commissie als het Comité; de toelichting van juridische en operationele *ad hoc* vragen (bijvoorbeeld de modaliteiten van de hoogdringendheidsprocedure); de voorstelling van en toelichting bij een concrete casus; en ten slotte de concrete uitwerking van een bepaald BIM-gerelateerd onderwerp (bijvoorbeeld *best practices* inzake de motivering van een verlenging van een ingezette methode). Deze vergaderingen dragen bij tot de goede verstandhouding en stimuleert de onderlinge communicatie tussen de betrokken partners. Dit informele overleg doet uiteraard geen afbreuk aan de onafhankelijkheid van de beoordeling van de wettigheid van de methoden door het Vast Comité I.

---

126 Zie voor een bespreking van de bijzondere inlichtingenmethoden en de controle hierop: VAST COMITÉ I, *Activiteitenverslag 2010*, 51-63 en W. VAN LAETHEM, D. VAN DAELE en B. VANGEEBERGEN (eds.), *De Wet op de bijzondere inlichtingenmethoden*, Antwerpen, Intersentia, 2010, 299 p.

127 Art. 35 § 2 en 66*bis* § 2, derde lid, W.Toezicht.

III.2. CIJFERS MET BETREKKING TOT SPECIFIEKE EN UITZONDERLIJKE METHODEN

Tussen 1 januari en 31 december 2014 werden door de twee inlichtingendiensten samen 1282 toelatingen verleend tot het aanwenden van bijzondere inlichtingenmethoden: 1132 door de VSSE (waarvan 976 specifieke en 156 uitzonderlijke) en 150 door de ADIV (waarvan 114 specifieke en 36 uitzonderlijke).

Onderstaande tabel maakt een vergelijking met de cijfers van de afgelopen jaren. Daarbij moet opgemerkt worden dat het Comité sinds januari 2013 een andere telling hanteert voor één welbepaalde bijzondere methode. Voorheen werden het aantal 'Kennisnames van identificatiegegevens van elektronisch communicatieverkeer' niet als dusdanig meegeteld in de totalen. Hiervoor werd geopteerd omdat (de meeste) 'Kennisnames van identificatiegegevens' door de diensthoofden van de inlichtingendiensten werden toegelaten in eenzelfde document waar ook bijvoorbeeld een 'Kennisname van de oproepgegevens' of een 'Kennisname van lokalisatiegegevens' werd toegelaten. Omdat het strikt genomen om andere methoden gaat, heeft het Vast Comité I geoordeeld dat het apart meetellen van dergelijke 'Kennisnames van identificatiegegevens' een juister beeld oplevert van het effectief aantal ingezette specifieke methoden. Met andere woorden: wanneer het vermelde aantal bijzondere methoden sinds 2013 hoger ligt dan de jaren voordien, is dit grotendeels te wijten aan een andere telwijze en dus niet aan het feit dat er zoveel meer methoden werden aangewend.

	ADIV		VSSE		TOTAAL
	Specifieke methode	**Uitzonderlijke methode**	**Specifieke methode**	**Uitzonderlijke methode**	
2012	67	24	655	102	848
2013	131	23	1102	122	1378
2014	114	36	976	156	1282

Waar in 2013 nog een stijging van ongeveer 13% werd genoteerd (en dit rekening houdend met de nieuwe telwijze), is het totaal aantal bijzondere inlichtingenmethoden in 2014 gedaald met 7%. Deze daling situeert zich voor beide diensten bij de specifieke methoden; de uitzonderlijke methoden kenden daarentegen een stijging.

In wat volgt, worden per dienst drie grote rubrieken onderscheiden: cijfers over de specifieke methoden, cijfers over de uitzonderlijke methoden en cijfers inzake de dreigingen en te verdedigen belangen die door de methoden geviseerd worden.

III.2.1. TOELATINGEN MET BETREKKING TOT DE ADIV

III.2.1.1. De specifieke methoden

AARD SPECIFIEKE METHODE	AANTAL 2012	AANTAL 2013	AANTAL 2014
Betreden van en observeren op of in publiek toegankelijke plaatsen met een technisch middel	8	14	7
Betreden en doorzoeken van publiek toegankelijke plaatsen met een technisch middel	0	0	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator	0	0	0
Kennisnemen van identificatiegegevens van elektronisch communicatieverkeer; het vorderen van de medewerking van een operator; of de rechtstreekse toegang tot gegevensbestanden	25 dossiers	66 methoden[128]	67 methoden
Kennisnemen van oproepgegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	30	15	12
Kennisnemen van lokalisatiegegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	4	36	28
TOTAAL	**67**[129]	**131**[130]	**114**

Daar waar er voor de ADIV vorig jaar nog een stijging te noteren viel van het aantal observaties en lokalisaties, werden deze methoden in 2014 minder frequent toegepast.

128 In vergelijking met vorige jaren is er een daling te noteren: de 66 toelatingen hebben immers betrekking op 16 dossiers.

129 In één geval had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

130 In één geval had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

III.2.1.2. Uitzonderlijke methoden

AARD UITZONDERLIJKE METHODE	AANTAL 2012	AANTAL 2013	AANTAL 2014
Betreden van en observeren in niet publiek toegankelijke plaatsen met of zonder een technisch middel	1	1	1
Betreden en doorzoeken van niet publiek toegankelijke plaatsen met of zonder een technisch middel	0	0	1
Oprichten en gebruiken van een fictieve rechtspersoon	0	0	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post	0	0	0
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen	7	5	5
Binnendringen in een informaticasysteem	2	0	3
Afluisteren, kennisnemen en opnemen van communicaties	14	17	26
TOTAAL	**24**[131]	**23**[132]	**36**

Wat betreft de uitzonderlijke methoden valt één cijfer onmiddellijk op: het aantal tapmaatregelen is gestegen van 17 naar 26.

III.2.1.3. De belangen en dreigingen die de inzet van de bijzondere methoden rechtvaardigen[133]

De ADIV mag de specifieke en de uitzonderlijke methoden aanwenden in het kader van drie van zijn opdrachten die elk op zich specifieke te vrijwaren belangen behelzen:

– de inlichtingenopdracht die gericht is op dreigingen tegen onder meer de onschendbaarheid van het nationaal grondgebied, de militaire defensieplannen en het wetenschappelijk en economisch potentieel op vlak van defensie (art. 11, 1° W.I&V);
– de opdracht inzake de militaire veiligheid die bijvoorbeeld gericht is op het behoud van de militaire veiligheid van het defensiepersoneel, van de militaire

131 In één geval had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

132 In één geval had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

133 Per toelating kunnen meerdere belangen en dreigingen aan de orde zijn.

installaties en de militaire informatica- en verbindingssystemen (art. 11, 2° W.I&V);
– de bescherming van militaire geheimen (art. 11, 3° W.I&V).

AARD VAN DE OPDRACHT	AANTAL 2012	AANTAL 2013	AANTAL 2014
Inlichtingenopdracht	63	111	109
Militaire veiligheid	7	15	5
Bescherming geheimen	21	28	36

AARD DREIGING	AANTAL 2012	AANTAL 2013	AANTAL 2014
Spionage	78	94	123
Terrorisme (en radicaliseringsproces)	3	6	7
Extremisme	3	24	15
Inmenging	2	1	0
Criminele organisatie	1	16	2
Andere	5	13	0

Wat betreft de ADIV eist de dreiging 'spionage' nog steeds de meeste BIM-methoden op. Opvallend is de eerder beperkte inzet van BIM-methoden in het kader van de dreigingen 'terrorisme' en 'extremisme' (in 2013 nog goed voor 53, in 2014 gedaald naar 22).

III.2.2. TOELATINGEN MET BETREKKING TOT DE VSSE

III.2.2.1. De specifieke methoden

AARD SPECIFIEKE METHODE	AANTAL 2012	AANTAL 2013	AANTAL 2014
Betreden van en observeren op of in publiek toegankelijke plaatsen met een technisch middel	75	109	86
Betreden en doorzoeken van publiek toegankelijke plaatsen met een technisch middel	1	0	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator	2	0	0

AARD SPECIFIEKE METHODE	AANTAL 2012	AANTAL 2013	AANTAL 2014
Kennisnemen van identificatiegegevens van elektronisch communicatie-verkeer; het vorderen van de medewerking van een operator; of de rechtstreekse toegang tot gegevensbestanden	254 dossiers	613[134] methoden	554 methoden
Kennisnemen van oproepgegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	147	136	88
Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator	176	244	248
TOTAAL	**655**[135]	**1102**[136]	**976**

De lichte terugval van het aantal specifieke methoden die door de VSSE werden ingezet, is veroorzaakt door het feit dat er minder specifieke 'observaties' werden verricht (86 in plaats van 109), minder 'Kennisnames van identificatiegegevens' (554 in plaats van 613) en minder 'Kennisnames van oproepgegevens' (88 in plaats van 136). Alleen het aantal uitgevoerde 'Lokalisaties' bleef stabiel.

III.2.2.2. De uitzonderlijke methoden

AARD UITZONDERLIJKE METHODE	AANTAL 2012	AANTAL 2013	AANTAL 2014
Betreden van en observeren in niet publiek toegankelijke plaatsen met of zonder een technisch middel	8	6	9
Betreden en doorzoeken van niet publiek toegankelijke plaatsen met of zonder een technisch middel	6	6	21
Oprichten en gebruiken van een fictieve rechtspersoon	0	0	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post	12	6	18

134 In vergelijking met vorige jaren is er een daling te noteren: de 613 toelatingen hebben immers betrekking op 243 dossiers.

135 In zeventien gevallen had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist. Vorig jaar betroffen het negen gevallen.

136 In negen gevallen had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist. Ook vorig jaar betrof het negen gevallen.

AARD UITZONDERLIJKE METHODE	AANTAL 2012	AANTAL 2013	AANTAL 2014
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen	16	11	8
Binnendringen in een informaticasysteem	10	12	18
Afluisteren, kennisnemen en opnemen van communicaties	50	81	86
TOTAAL	**102**[137]	**122**[138]	**156**

De stijging van het aantal uitzonderlijke methoden is dit jaar niet uitsluitend toe te schrijven aan de 'afluistermaatregelen' (van 81 naar 86), maar – voornamelijk – aan de 'doorzoekingen' (van 6 naar 21) en het 'openen van post' (van 6 naar 18).

Tevens valt er te noteren dat er in 19 gevallen (vorig jaar 11) gebruik werd gemaakt van de hoogdringendheidsprocedure waarbij alleen de voorzitter van de BIM-Commissie om advies wordt gevraagd.

III.2.2.3. De belangen en dreigingen die de inzet van de 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). Uitzonderlijke methoden mogen niet ingezet worden in het kader van het extremisme en de inmenging. Zij zijn wel toegelaten in het kader van het aan het terrorisme voorafgaande radicaliseringsproces (art. 3, 15° 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;

137 In vijf gevallen had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

138 In één geval had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

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.

AARD DREIGING	AANTAL 2012	AANTAL 2013	AANTAL 2014
Spionage	243	359	319
Terrorisme (en radicaliseringsproces)	288	580	499
Extremisme	177	216	267
Proliferatie	28	15	33
Schadelijke sektarische organisaties	7	9	0
Inmenging	10	8	10
Criminele organisaties	5	9	8

Bovenstaande cijfers vertonen geen opvallende wijzigingen tegenover 2013: 'terrorisme' en 'extremisme' samen blijven vanuit de BIM-methoden gezien, de prioriteit voor de VSSE. Wel werd, ondanks de Syriëproblematiek, een lichte daling van het aantal methoden voor deze dreigingen opgetekend (van 826 in 2013 naar 766 in 2014). Dit valt deels te verklaren doordat de VSSE zich in het kader van 'terrorisme' en 'extremisme' voornamelijk focuste op de Syriëstrijders en minder op de andere vormen van extremisme.

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:

- 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
- 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;
- de vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel.

In acht genomen dat per toelating verschillende belangen aan de orde kunnen zijn, komen we tot volgende cijfers voor 2014:

AARD BELANG	AANTAL 2012	AANTAL 2013	AANTAL 2014
De inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde	704	1177	1100
De uitwendige veiligheid van de Staat en de internationale betrekkingen	693	1160	1075
De vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel	15	11	10

III.3. DE ACTIVITEITEN VAN HET VAST COMITÉ I ALS JURDISCTIONEEL ORGAAN EN ALS PREJUDICIEEL ADVIESVERLENER

III.3.1. 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. 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.

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

- op eigen initiatief;
- op verzoek van de Commissie voor de bescherming van de persoonlijke levenssfeer;
- op klacht van een burger;
- van rechtswege als de BIM-Commissie een specifieke of een uitzonderlijke methode wegens onwettigheid heeft geschorst en de exploitatie van de gegevens heeft verboden;
- van rechtswege als de bevoegde minister een toelating heeft verleend op basis van artikel 18/10 § 3 W.I&V.

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

WIJZE VAN VATTING	AANTAL 2012	AANTAL 2013	AANTAL 2014
1. Op eigen initiatief	19	16	13[139]
2. Privacycommissie	0	0	0
3. Klacht	0	0	0
4. Schorsing door BIM-Commissie	17	5	5
5. Toelating minister	2	2	1
6. Prejudicieel adviesverlener	0	0	0
TOTAAL	**38**	**23**	**19**

[139] In twee gevallen viel de beslissing van het Comité pas in januari 2015.

Eens gevat, kan het Comité verschillende soorten (tussen)beslissingen nemen. In twee gevallen (1. en 2. hieronder) wordt evenwel een beslissing genomen vóór de eigenlijke vatting.

1. Nietigheid van de klacht wegens vormgebrek of afwezigheid van een persoonlijk en rechtmatig belang (art. 43/4, eerste lid, W.I&V);
2. Beslissing om geen gevolg te geven aan een klacht die kennelijk niet gegrond is (art. 43/4, eerste lid, W.I&V);
3. Schorsing van de betwiste methode in afwachting van een definitieve beslissing (art. 43/4, laatste lid, W.I&V);
4. Vordering tot bijkomende informatie ten aanzien van de BIM-Commissie (43/5 § 1, eerste tot derde lid, W.I&V);
5. Vordering tot bijkomende informatie ten aanzien van de betrokken inlichtingendienst (43/5 § 1, derde lid, W.I&V);
6. Onderzoeksopdracht voor de Dienst Enquêtes I (art. 43/5 § 2 W.I&V). In deze rubriek wordt zowel verwezen naar de veelvuldige bijkomende informatie die door de Dienst Enquêtes I op eerder informele wijze wordt ingewonnen vóór de eigenlijke vatting als naar informatie die op verzoek van het Comité wordt ingewonnen na de vatting;
7. Horen van de BIM-Commissieleden (art. 43/5 § 4, eerste lid, W.I&V);
8. Horen van het diensthoofd of de leden van de betrokken inlichtingendienst (art. 43/5 § 4, eerste lid, W.I&V);
9. Beslissing over geheimen die betrekking hebben op een lopend opsporings- of gerechtelijk onderzoek waarvan de leden van de inlichtingendiensten drager zijn, na overleg met de bevoegde magistraat (art. 43/5 § 4, tweede lid, W.I&V);
10. Uitspraak door de voorzitter van het Vast Comité I, na het diensthoofd te hebben gehoord, indien het lid van de inlichtingendienst meent het geheim waarvan hij drager is te moeten bewaren omdat de onthulling ervan nadelig is voor de bescherming van de bronnen, de bescherming van de persoonlijke levenssfeer van derden of de vervulling van de opdrachten van de inlichtingendienst (art. 43/5 § 4, derde lid, W.I&V);
11. Stopzetting van een methode indien ze nog steeds in uitvoering is of indien zij werd geschorst door de BIM-Commissie en bevel dat de gegevens die met deze methode werden verkregen niet mogen worden geëxploiteerd en dienen te worden vernietigd (art. 43/6 § 1, eerste lid, W.I&V);
12. Gedeeltelijke stopzetting van een toegelaten methode. Hier wordt de situatie bedoeld waarbij bijvoorbeeld één methode in tijd wordt beperkt, niet de situatie waarbij in één toelating van een diensthoofd meerdere methoden worden gemachtigd en het Comité slechts één ervan stopzet;
13. Gehele of gedeeltelijke opheffing van de schorsing en het verbod die door de BIM-Commissie was uitgesproken (art. 43/6 § 1, eerste lid, W.I&V). Dit houdt in dat de door het diensthoofd toegelaten methode door het Comité wel (gedeeltelijk) wettelijk, proportioneel en subsidiair werd bevonden;

14. Onbevoegdheid van het Vast Comité I;
15. Ongegrondheid van de aanhangige zaak en geen stopzetting van de methode;
16. Advies als prejudicieel adviesverlener (artt. 131*bis*, 189*quater* en 279*bis* Sv.).

Het Vast Comité I moet binnen een termijn van een maand volgend op de dag waarop het werd gevat een definitieve uitspraak doen (art. 43/4 W.I&V). In alle dossiers werd die termijn gerespecteerd.

AARD VAN DE BESLISSING	**2012**	**EIND-BESLISSING 2012**	**2013**	**EIND-BESLISSING 2013**	**2014**	**EIND-BESLISSING 2014**
1. Nietige klacht	0		0		0	
2. Kennelijk ongegronde klacht	0		0		0	
3. Schorsing methode	1		0		3	
4. Bijkomende informatie van BIM-Commissie	0		0		0	
5. Bijkomende informatie van inlichtingendienst	6		0		1	
6. Onderzoeksopdracht Dienst Enquêtes	11		50		54	
7. Horen BIM-Commissieleden	0		0		0	
8. Horen leden inlichtingendiensten	0		0		0	
9. Beslissing m.b.t. geheim van onderzoek	0		0		0	
10. Gevoelige informatie tijdens verhoor	0		0		0	
11. Stopzetting methode	4		9		3	
12. Gedeeltelijke stopzetting methode	18		5		10	
13. (Gedeeltelijke) opheffing verbod van BIM-Commissie	13	**38**	2[140]	**23**	0	**17**
14. Onbevoegd	0		0		0	
15. Wettige toelating / Geen stopzetting methode / Ongegrond	3		7		4	
16. Prejudicieel advies	0		0		0	

[140] Eigenlijk besliste het Comité dat de schorsing van de BIM-Commissie zonder voorwerp was (zie dossier 2013/1728).

Het Vast Comité I heeft in 2014 17 beslissingen genomen. In 2013 waren dat er 23 en in 2012 en 2011 nog respectievelijk 39 en 38. Eén van de redenen voor deze daling is de vaststelling dat de BIM-Commissie minder methoden schorst (in 2011 en 2012 nog respectievelijk 15 en 17). Daarnaast is er ongetwijfeld het feit dat heel wat juridische discussiepunten definitief zijn uitgeklaard in de rechtspraak zoals die zich in de afgelopen jaren heeft ontwikkeld en zoals die nadien werd geïmplementeerd door de diensten.

III.3.2. DE RECHTSPRAAK

Hieronder wordt de essentie weergegeven van de 17 eindbeslissingen die het Vast Comité I in 2014 nam. De samenvattingen zijn ontdaan van operationele gegevens. Alleen die elementen die van belang zijn voor het juridische vraagstuk worden opgenomen. In enkele gevallen was het Comité echter genoodzaakt in dit activiteitenverslag bepaalde elementen van het juridische vraagstuk niet expliciet op te nemen ter vrijwaring van de verplichte geheimhouding.

De beslissingen werden gegroepeerd onder vijf rubrieken:

- Wettelijke (vorm)vereisten voorafgaandelijk aan de uitvoering van een methode;
- Motivering van de toelating;
- De proportionaliteits- en de subsidiariteitseis;
- Wettelijkheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van dreiging;
- De gevolgen van een onwettig(e) (uitgevoerde) methode.

Indien relevant werden sommige beslissingen onder meerdere rubrieken opgenomen.

III.3.2.1. Wettelijke (vorm)vereisten voorafgaandelijk aan de uitvoering van een methode

III.3.2.1.1. Voorafgaande kennisgeving BIM-Commissie

Een specifieke methode kan pas effectief worden aangewend na kennisgeving van de toelating aan de BIM-Commissie. In dossier 2014/3291 was de Commissie in kennis gesteld van een toelating, terwijl de methode volgens die beslissing reeds de dag voordien zou opgestart worden. De Commissie schorste dan ook de methode voor het gedeelte vóór de kennisgeving. Het Comité bevestigde die beslissing.

III.3.2.1.2. Verplichte vermeldingen in de toelating

De inlichtingendienst wou overgaan tot de doorzoeking van een hotelkamer die gehuurd werd door een *target* (dossier 2014/2898). De machtiging zelf bevatte echter nog geen naam van het hotel en uiteraard ook geen kamernummer. Die informatie deelde de inlichtingendienst in de loop van dezelfde dag mee aan de BIM-Commissie. De dienst voegde er aan toe dat indien het *target* nog van hotel zou veranderen, de Commissie hiervan onmiddellijk zou verwittigd worden. Het Comité oordeelde dat deze werkwijze wettig was. Vooreerst eist de wet niet '*que la décision précise le nom de l'hôtel (et sa localisation) ni même le numéro de la chambre qui doit être inspectée […]; Attendu cependant que l'indication qu'il s'agit d'une chambre d'hôtel et non un immeuble servant de domicile ou de résidence d'une personne est indispensable pour apprécier le respect des principes de proportionnalité et de subsidiarité*'.[141] Daarenboven stelde het Comité vast dat de voorzitter van de BIM-Commissie onmiddellijk op de hoogte was gebracht van de exacte locatie.

III.3.2.1.3. Methode ten aanzien van een mogelijke journalist

De inlichtingendienst wenste een specifieke methode in te zetten ten aanzien van een persoon waarvan het '*ne serait pas exclu*'[142] dat hij een journalist was (dossier 2014/2723). Het Comité besliste dat '*l'absence de précision sur l'identité de cette personne n'a pas permis de vérifier si la procédure prévue par l'article 18/2 § 3 devait ou non être mise en œuvre*'.[143] De methode was dan ook onwettig.

III.3.2.2. Motivering van de toelating

III.3.2.2.1. Onvoldoende accurate motivering

In bovenstaand dossier wou de inlichtingendienst vier methoden inzetten om een bepaalde persoon te identificeren (dossier 2014/2723). Deze werd er namelijk van verdacht geheime informatie te willen verkopen aan een derde die in contact staat met een buitenlandse inlichtingendienst. Maar zelfs na het inwinnen van bijkomende inlichtingen was er bijzonder weinig geweten over de koper en de verkoper, over de aard van de informatie en over de intenties van de betrokken perso-

141 '*dat de beslissing de naam (en de locatie) van een hotel, noch het nummer van de te inspecteren kamer zou preciseren […]; Overwegende echter dat de aanduiding dat het een hotelkamer betreft en geen gebouw dat dienst doet als woning of als verblijfplaats van een persoon onontbeerlijk is om het respect voor de principes van proportionaliteit en subsidiariteit te beoordelen.*' (vrije vertaling).

142 '*niet uitgesloten zou zijn*' (vrije vertaling).

143 '*de afwezigheid van preciseringen omtrent de identiteit van deze persoon heeft niet toegelaten te verifiëren of de door artikel 18/2 § 3 voorziene procedure al dan niet moest toegepast worden*' (vrije vertaling).

nen of diensten. Dit maakte het '*difficile d'apprécier in concreto la nature de la menace réelle ou potentielle contre l'intérêt à protéger si ce n'est sur base d'une affirmation que cette menace existe bien; que le texte et l'esprit de la loi exigent des indications plus précises que celles développées dans la décision*'.[144]

III.3.2.2.2. Versterkte motivering in geval van tweede verlenging

Een ontwerp van machtiging tot het inzetten van een uitzonderlijke methode moet aan het advies van de BIM-Commissie worden onderworpen, die hiervoor over een termijn van vier dagen beschikt. Aangezien de Commissie zich in de onmogelijkheid bevond om binnen die termijn een advies te verlenen, werd de machtiging door de bevoegde minister verleend op basis van artikel 18/10 § 3, derde lid W.I&V. Het Comité stelde vast dat het om een tweede verlenging ging van een uitzonderlijke methode. Aangezien '*les circonstances particulières nécessitant de prolonger une deuxième fois la méthode exceptionnelle à l'égard de la cible sont indiquées à suffisance dans l'autorisation donnée par le ministre; Que ces motifs font suffisamment apparaître la menace représentée par la cible ainsi que la subsidiarité et la proportionnalité de la méthode mise en œuvre à son égard.*'[145]

III.3.2.3. De proportionaliteits- en de subsidiariteitseis

III.3.2.3.1. Afwachten resultaten eerste methode

In 2014 kwam het Vast Comité I vijfmaal tussen in dossiers waarin de inlichtingendienst methoden had toegelaten zonder eerst de resultaten van een eerdere methode af te wachten. De problematiek was voor het eerst aan de orde in dossier 2014/2744. Een inlichtingendienst wenste aan de hand van elektronische communicatiedata na te gaan welke contacten een *target* onderhield in België. Het was de bedoeling om eerst op te lijsten wie hij belde en door wie hij gebeld werd. Maar de methode had ook als finaliteit om onmiddellijk over te gaan tot de lokalisatie van alle contacten van de *target*. Het Comité oordeelde echter dat het op het ogenblik van zijn beslissing '*onmogelijk is vast te stellen welke telefoonnummers het voorwerp zullen uitmaken van een daarop volgende lokalisatie*' waardoor het in de onmogelijkheid was om de subsidiariteit en de proportionaliteit van de lokalisatie van de nog niet-geïdentificeerde telefoonnummers na te gaan.

144 '*behoudens de bevestiging dat de dreiging werkelijk bestond, moeilijk om in concreto de aard van de reële of potentiële dreiging tegen het te beschermen belang te beoordelen; dat de tekst en de geest van de wet meer precieze aanwijzingen vereisen dan deze uiteengezet in de beslissing.*' (vrije vertaling).

145 '*de bijzondere omstandigheden die noodzaken om voor een tweede maal de uitzonderlijke methode ten aanzien van de target te verlengen, voldoende werden uiteengezet in de door de minister verleende toelating; Dat deze motieven voldoende blijk geven van de dreiging die van de target uitgaat evenals van de subsidiariteit en de proportionaliteit van de ingezette methode.*' (vrije vertaling).

In de dossiers 2014/2774 en 2014/2778 diende zich een zelfde problematiek aan. De inlichtingendienst wou vooreerst overgaan tot de kennisname van de in- en uitgaande nummers van de gsm van een *target*. Vervolgens zou worden overgegaan tot de identificatie van alle nummers, *'pour autant que cela soit nécessaire à l'enquête.'*[146] Tot daar stelde zich geen probleem. Maar de dienst wou ook een lokalisatie van alle geïdentificeerde nummers '*afin de nous donner des indices sur l'identité de celles-ci'*.[147] Het Comité herhaalde dat het '*[est] impossible de préciser actuellement quels numéros feront l'objet d'une telle localisation. Qu'il est dès lors impossible au Comité R de statuer actuellement sur la subsidiarité et la proportionnalité de la méthode de localisation visant les numéros non-encore identifiés*'.[148]

In het vierde dossier (2014/3253) wou een inlichtingendienst ten aanzien van een persoon terzelfdertijd vier methoden toelaten: de identificatie van zijn elektronische communicatiemiddelen, de 'observatie' van die toestellen, de lokalisatie van alle aldus bekomen gegevens en de identificatie van alle betrokkenen. Het Comité oordeelde dat de dienst eerst de eerste methode diende in te zetten aangezien '*qu'en l'absence d'informations obtenues par la méthode sollicitée, il n'est pas permis de juger du respect des principes de proportionnalité, de subsidiarité donc de la légalité des trois autres méthodes sollicitées et qui sont la poursuite de la première méthode*'.[149]

In dossier 2014/3493 ten slotte herhaalde het Comité dat er in onderscheiden stappen dient gewerkt te worden wanneer men enerzijds wil weten welk communicatiemiddel een *target* gebruikt (art. 18/7, 2° W. I&V[150]) en anderzijds met wie hij op een bepaald ogenblik een telefoongesprek heeft gevoerd (art. 18/8, 1° – het opsporen van oproepgegevens van elektronische communicatiemiddelen van of waarnaar oproepen worden of werden gericht – gekoppeld aan art. 18/7, 1° – de identificatie van een abonnee of gebruiker van een elektronische communicatiedienst of -middel). Het Comité oordeelde dat '*het tweede gedeelte van de methode, gesteund op art. 18/8, 1°, vooralsnog niet beantwoordt aan de vereiste van proportionaliteit en subsidiariteit.*'

146 '*in zoverre dit nodig zou zijn voor het onderzoek*' (vrije vertaling).

147 '*teneinde ons aanwijzingen te geven over de hun identiteit'* (vrije vertaling).

148 '*onmogelijk is om op dit ogenblik te preciseren welke nummers het voorwerp zullen uitmaken van een dergelijke lokalisatie. Dat het dan ook onmogelijk is voor het Comité om nu reeds de subsidiariteit en de proportionaliteit te beoordelen van de lokalisatiemethode van die nog niet geïdentificeerde nummers*' (vrije vertaling).

149 '*bij gebrek aan informatie verkregen door de aangevraagde methode, is het onmogelijk om te oordelen of de principes van proportionaliteit en subsidiariteit werden gerespecteerd of met andere woorden de wettelijkheid van de drie andere aangevraagde methoden die voortvloeien uit de eerste methode*'. (vrije vertaling)

150 De betrokken dienst had zich in de toelating verkeerdelijk op art. 18/7, 1° W. I&V gebaseerd.

III.3.2.3.2. Niet aangetoonde noodzaak

De problematiek van de proportionaliteit was nog aan de orde in een andere casus. De inlichtingendienst wenste bij uiterste hoogdringendheid een uitzonderlijke methode aan te wenden op een welbepaald telefoonnummer (dossier 2014/3424). De dag nadat de machtiging op basis van het mondelinge eensluidend advies effectief is verleend, stelt de inlichtingendienst echter vast dat het nummer bij vergissing niet in de machtiging was opgenomen. Het concrete telefoonnummer wordt nog de dag zelf naar de Commissie gezonden. Een typfout maakt echter dat een verkeerd nummer wordt opgegeven. De BIM-Commissie ging hierop over tot de schorsing. Het Comité bevestigde die beslissing, maar op andere gronden. Uit de ingewonnen informatie bleek immers dat de noodzaak om een uitzonderlijke methode toe te passen op het nummer niet was aangetoond. Het Comité oordeelde dan ook dat de methode niet beantwoordde aan de vereiste van proportionaliteit.

III.3.2.3.3. Subsidiariteit

In dossier 2014/2908 was alleen de subsidiariteit aan de orde. De BIM-Commissie had de toelating om een observatie met camera uit te voeren op een persoon geschorst, omdat de inlichtingendienst naliet concreet toe te lichten welke informatie, die afkomstig was van een buitenlandse dienst, haar daartoe had aangezet. Ook het Comité beoordeelde de initiële beslissing als onvoldoende gemotiveerd. Het vroeg bijkomende informatie en kreeg als antwoord '*dat er geen noodzaak was om een specifieke methode aan te wenden bij de observatie van de betrokken persoon; dat er immers geen technisch middel bij de beoogde observatie vereist was*' zodat een gewone methode volstond voor de observatie. Met andere woorden, de beslissing om een specifieke methode aan te wenden beantwoordde niet aan de vereiste van subsidiariteit zodat het Comité de stopzetting van de methode beval.

III.3.2.4. Wettelijkheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van dreiging

III.3.2.4.1. Medewerking van buitenlandse diensten

Het Comité oordeelde reeds eerder dat de Belgische inlichtingendiensten ook in het kader van de bijzondere methoden mogen samenwerken met buitenlandse zusterdiensten, weze het onder de voorwaarde dat de Belgische dienst de daadwerkelijke controle behoudt over de ingezette methode.[151] In dossier 2014/2723

[151] Zie bijvoorbeeld VAST COMITÉ I, *Activiteitenverslag 2013*, 83 (III.3.2.4.1. De controle over de uitvoering van de BIM-methode).

wees het Comité in verband hiermee op de noodzaak van nadere richtlijnen van het Ministerieel Comité voor inlichting en veiligheid[152]: '*[…] l'absence de directives du Comité ministériel du Renseignement et de la Sécurité quant aux conditions de la coopération avec les services de renseignement étranger oblige la VSSE à agir par elle-même et au cas par cas*'.[153] Dit neemt echter niet weg '*les nécessités d'assurer une coopération entre les services de renseignement belges […] et les services de renseignement étrangers, notamment lorsque des actions sont entreprises sur le territoire belge*.'[154]

III.3.2.4.2. De BIM-Wet en het Verdrag van Wenen inzake diplomatiek verkeer van 18 april 1961

In de referteperiode nam het Comité vier beslissingen (dossiers 2014/2758, 2014/3148, 2014/3306 en 2014/3488) waarin onder meer het Verdrag van Wenen van 1961 ter sprake kwam. Het Comité kan in dit activiteitenverslag niet ingaan op de inhoud van deze beslissingen aangezien ze als 'geheim' dienden te worden geclassificeerd. Wel benadrukt het Comité dat het Verdrag van Wenen ook van toepassing is op de werking van de inlichtingendiensten die daarom bepaalde grenzen in acht moeten nemen, maar ook dat er nood is aan klare richtlijnen van de Nationale Veiligheidsraad, mede gelet op de politieke verantwoordelijkheid die het gevolg kan zijn van bepaalde activiteiten van inlichtingendiensten.

III.3.2.5. De gevolgen van een onwettig(e) (uitgevoerde) methode

De BIM-Commissie had een methode gedeeltelijk geschorst (dossier 2014/2724). Uit de toelating van het diensthoofd bleek dat de betrokken inlichtingendienst wou overgaan tot de identificatie van de elektronische communicatie van twee personen die op dat ogenblik nog niet identificeerbaar waren. Maar dit berustte blijkbaar op een vergissing. De betrokken dienst had niet de intentie om de methode aan te wenden en het Comité bevestigde dan ook de beslissing van de BIM-Commissie.

---

152 Het K.B. van 21 juni 1996 houdende oprichting van een Ministerieel Comité voor inlichting en veiligheid werd opgeheven door het K.B. van 28 januari 2015 tot oprichting van een Nationale Veiligheidsraad, *BS* 30 januari 2015.

153 '*de afwezigheid van richtlijnen van het Ministerieel Comité voor inlichting en veiligheid met betrekking tot de voorwaarden tot samenwerking met buitenlandse inlichtingendiensten verplicht de VSSE zelfstandig en geval per geval te handelen*'. (vrije vertaling)

154 '*de noodwendigheden om een samenwerking te garanderen tussen de Belgische en de buitenlandse inlichtingendiensten, meer in het bijzonder wanneer acties worden ondernomen op Belgisch grondgebied*.' (vrije vertaling)

III.4. CONCLUSIES

Op basis van de cijfers uit het werkingsjaar 2014 formuleerde het Vast Comité I volgende algemene conclusies:

- Waar in 2013 nog een stijging van ongeveer 13% werd genoteerd, is het aantal bijzondere inlichtingenmethoden in 2014 gedaald met 7%. Deze daling situeert zich voor beide diensten bij de specifieke methoden; de uitzonderlijke methoden kenden wel nog een lichte stijging.
- Wat betreft de ADIV, is de stijging van de uitzonderlijke methoden te wijten aan het toenemend aantal tapmaatregelen (gestegen van 17 naar 26), al blijft dit in absolute cijfers, een beperkt aantal.
- Wat betreft de VSSE, is de stijging van het aantal uitzonderlijke methoden in 2014 niet uitsluitend toe te schrijven aan de afluistermaatregelen (van 81 naar 86), maar – voornamelijk – aan de doorzoekingen (van 6 naar 21) en het openen van post (van 6 naar 18).
- Wat betreft de ADIV eist de dreiging 'spionage' nog steeds de meeste BIM-methoden op terwijl de BIM-werking bij de VSSE vooral gericht is op de strijd tegen 'terrorisme/extremisme'.
- Tevens valt er te noteren dat er in 19 gevallen (vorig jaar 11) gebruik werd gemaakt van de hoogdringendheidsprocedure waarbij alleen de voorzitter van de BIM-Commissie om advies wordt gevraagd voor de inzet van een uitzonderlijke methode.
- Het Vast Comité I heeft in 2014 17 beslissingen genomen. In 2013 waren er dat er 23 en in 2012 en 2011 nog respectievelijk 39 en 38. Eén van de redenen voor deze daling is de vaststelling dat de BIM-Commissie minder methoden schorst (in 2011 en 2012 nog respectievelijk 15 en 17; in 2013 en 2014 telkens 5). Ook zijn ondertussen heel wat juridische discussiepunten uitgeklaard in de rechtspraak van het Vast Comité I en de beslissingen van de BIM-Commissie.

HOOFDSTUK IV
HET TOEZICHT OP DE INTERCEPTIE VAN COMMUNICATIE UITGEZONDEN IN HET BUITENLAND

Sinds begin 2011 kunnen zowel de VSSE als de ADIV onder zeer strikte voorwaarden communicaties afluisteren, er kennis van nemen en ze registreren (art. 18/17 § 1 W.I&V).

Deze zogenaamde 'BIM-intercepties' moeten evenwel duidelijk worden onderscheiden van '*het zoeken, het onderscheppen, het afluisteren, het kennisnemen of het opnemen door de Algemene Dienst inlichting en veiligheid van de Krijgsmacht van elke vorm van communicatie uitgezonden in het buitenland*.' Deze tweede vorm van afluisteren was al langer mogelijk en kan worden ingezet om redenen van militaire aard in het kader van de opdrachten gedefinieerd in artikel 11 § 2, 1° en 2°, W.I&V als om redenen van veiligheid en bescherming van Belgische en van geallieerde troepen tijdens opdrachten in het buitenland alsook van onze onderdanen die in het buitenland gevestigd zijn (art. 11 § 2, 3° en 4° W.I&V). Ook dit worden klassiek 'veiligheidsintercepties' genoemd, maar zij kennen een volkomen ander controlekader. Het externe toezicht erop is namelijk uitsluitend opgedragen aan het Vast Comité I, en dit zowel voor, tijdens als na de intercepties (art. 44*bis* W.I&V). Het Comité heeft hierbij de bevoegdheid om lopende intercepties te doen stopzetten wanneer blijkt dat de voorwaarden waarin ze uitgevoerd worden, de wettelijke bepalingen en/of de ministeriële toelating niet respecteren (art. 44*ter* W.I&V). Elk jaar, begin december, dient de ADIV immers aan de minister van Landsverdediging zijn gemotiveerde lijst voor te leggen met organisaties of instellingen, van wie de communicatie het komende jaar mag onderschept worden. Dit gebeurt met het oog op de ministeriële toelating van deze intercepties. De minister dient zijn beslissing te nemen binnen tien werkdagen en moet ze vervolgens meedelen aan de ADIV. Nadien moeten zowel de lijst als de ministeriële toelating door de ADIV worden overgezonden aan het Vast Comité I.

In 2014 verrichte het Vast Comité I de vereiste verificaties.

Daarnaast ontving het Comité van de ADIV een antwoord op zijn vragen in verband met de keuzes en de omschrijving van de voorgenomen intercepties van 'organisaties of instellingen' en de motivering ervan.[155] Het Comité bestudeerde

155 Zie VAST COMITÉ I, *Activiteitenverslag 2013*, 89-90.

het antwoord en vroeg om bijkomende toelichting, onder meer over de SIGINT-cyclus en over het gebruikte materiaal. Op een briefing in oktober 2014 verschafte de ADIV nadere toelichtingen. Het Vast Comité I besloot om de aangehaalde kwesties het komende jaar nader op te volgen bij het uitvoeren van zijn verificaties.

HOOFDSTUK V
ADVIEZEN, STUDIES EN ANDERE ACTIVITEITEN

V.1. TWINTIG JAAR DEMOCRATISCH TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN: BEZOEK VAN DE KONING

In 2013 vierde het Vast Comité I zijn twintigjarig bestaan.[156] Ter gelegenheid van die verjaardag, vereerde Zijne Majesteit de Koning op 25 april 2014 het Comité met een werkbezoek. Ook de diensthoofden van de VSSE, de ADIV en het OCAD werden uitgenodigd. De Koning werd geïnformeerd over de organisatie en de opdrachten van het Comité en kreeg aansluitend toelichting over de lopende toezichtonderzoeken, de controle op de bijzondere inlichtingenmethoden en het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen.

V.2. ADVIES AAN DE MINISTER VAN JUSTITIE

De afgelopen jaren formuleerde het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten tientallen aanbevelingen die gericht waren op een efficiënte werking van de inlichtingendiensten en op een betere bescherming van de rechten en vrijheden van de burgers. Ze kenden echter niet allemaal een gepast gevolg. Het Vast Comité I kon vaststellen dat heel wat van de aanbevelingen rechtstreeks of onrechtstreeks terug te vinden waren in het federaal Regeerakkoord van 9 oktober 2014. Op verzoek van de minister van Justitie heeft het Comité een document[157] gezonden waarin enkele van zijn belangrijkste aanbevelingen in herinnering werden gebracht.

156 W. VAN LAETHEM en J. VANDERBORGHT (eds.), *Inzicht in toezicht. Twintig jaar democratische controle op de inlichtingendiensten*, Intersentia, Antwerpen, 2013, 565 p.

157 VAST COMITÉ I, 'Belangrijke aanbevelingen van het Vast Comité I in aansluiting met het Regeerakkoord Michel I. Denkpistes voor de minister van Justitie', 11 december 2014.

V.3. INFORMATIEDOSSIERS

Naast toezichtonderzoeken (zie hierover uitvoerig Hoofdstuk II), opent het Vast Comité I ook zogenaamde 'informatiedossiers'. Deze moeten toelaten om een gestructureerde respons te bieden op vragen met betrekking tot de werking van de inlichtingendiensten en het OCAD.[158] 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 naderhand overgaan tot het initiëren van een formeel toezichtonderzoek.

Een informatiedossier dat uitmondde in een toezichtonderzoek betrof de problematiek van de 'foreign fighters' en het Syrische strijdtoneel.

Ook in 2014 werd de gedachtenwisseling omtrent de mogelijke inlichtingenactiviteiten van het binnen de Krijgsmacht opgerichte ISTAR-bataljon verder gezet. Eerder werd de Begeleidingscommissie in kennis gesteld van het juridisch standpunt van het Comité. Hieruit mocht blijken dat het Comité de uitgesproken en toegenomen behoefte van Defensie aan een performant georganiseerde *battlefield intelligence*-capaciteit onderschreef, doch dat dit niet zonder ernstige juridische complicaties bleek. De toenmalige minister van Defensie verduidelijkte de visie de Krijgsmacht. Het Comité kon zich in beginsel vinden in de voorgestelde oplossingen, maar verzocht om een bespreking over de praktische uitvoeringsmodaliteiten. Uiteindelijk komt het aan het Parlement toe te oordelen of de vooropgestelde regeling zijn goedkeuring kan wegdragen.

V.4. EXPERT OP DIVERSE FORA

Leden van het Vast Comité I en van zijn personeel werden in 2014 diverse malen als expert geconsulteerd door binnen- en buitenlandse publieke en private instellingen.

De voorzitter van het Vast Comité I oefent sinds 2011 het voorzitterschap uit van het *Belgian Intelligence Studies Centre (BISC)*. Dit centrum voor inlichtingenstudies stelt zich tot doel de inlichtingen- en veiligheidsdiensten en de wetenschappelijke wereld dichter bij elkaar brengen en een bijdrage te leveren aan de reflectie over inlichtingenvraagstukken.[159] In 2014 organiseerde het BISC twee studiedagen: een eerste deel van een drieluik over de Atlantikwall georganiseerd

158 De aanleiding voor het opstarten van informatiedossiers is zeer divers: er wordt een klacht neergelegd en het Vast Comité I wil via een snelle verificatie de manifeste ongegrondheid zo snel als mogelijk uitsluiten; 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…

159 www.intelligencestudies.be. Het BISC publiceerde in 2014 zijn vierde *Cahiers Inlichtingenstudies*.

in samenwerking met de Provincie West-Vlaanderen ('D-Day minus x – Inlichtingenactiviteiten bij en over de Atlantikwall', mei 2014) alsook een studiedag over cyberintelligence ('Building Belgium's Cyber Intelligence Knowledge Capacity', december 2014).

De frequentie van de werkzaamheden van de zogenaamde 'Werkgroep Analyse', waarin vertegenwoordigers van de twee inlichtingendiensten én het Vast Comité zetelen, werd in 2014 afgebouwd. De werkgroep begeleidde de verdere ontwikkeling van de *Belgian Intelligence Academy* (BIA)[160], een academie die opleidingen voor analisten uit zowel de burgerlijke als de militaire inlichtingendienst organiseert. Afgelopen jaar werden huishoudelijke reglementen uitgewerkt voor de diverse beheersorganen (het Directiecomité, het Uitvoerend Comité en het Wetenschappelijk Comité) en werd een ontwerp van algemene beleidsnota opgesteld. Ook ging de eerste opleiding 'Intelligence and Analysis Course (IAC)' van start die plaatsvond in juni/juli en september/oktober 2014, telkenmale gedurende veertien dagen. Het officiële protocolakkoord tot oprichting van het BIA werd, uiteindelijk, ondertekend begin 2015.

Ten slotte werd het Vast Comité I in 2014 ook vanuit de academische wereld geconsulteerd. Een vertegenwoordiger van het Vast Comité I nam deel aan een debat over de rol van de Amerikaanse FBI en de (nood aan) scheiding tussen klassieke politietaken en *(counter)intelligence*.[161] Ook werd het hoofd van de *Sector of Information Society, Privacy and Data Protection Freedoms and Justice Department* van het *European Union Agency for Fundamental Rights*[162] te woord gestaan. Deze is, in opdracht van het Europees Parlement en naar aanleiding van de Resolutie van 12 maart 2014, belast met een vergelijkende studie over democratisch toezicht op de inlichtingendiensten in de Europese lidstaten. De voorzitter van het Vast Comité I en een commissaris-auditor van zijn Dienst Enquêtes namen eveneens deel aan de voorbereidende vergaderingen van de *Community of Interest on the Practice and Organization of Intelligence (COI POI)*.[163] Ook blijft het Comité deelnemen aan de vergaderingen van de *Groupe européen de recherche sur l'éthique du renseignement* (GERER). Een werkgroep, samengesteld uit vertegenwoordigers vanuit het academische milieu en practici (vertegenwoordigers vanuit de (militaire) Franse, Belgische en Luxemburgse inlichtingendiensten, het Vast Comité I…) reflecteert er over de relatie 'ethiek – inlichtingendiensten.[164] In oktober 2014 nam het Comité, op uitnodiging van het Centrum voor Migraties en

---

160 De missie van de academie luidt als volgt: *'La Belgian Intelligence Academy vise à être le moteur et la référence en matière de formation professionnelle dans le renseignement civil et militaire, et à être reconnue pour son expertise et ses compétences. Elle a pour mission de dispenser des formations communes et structurées, de qualité, au personnel des services de renseignement'.*

161 'Zonde(n) van het FBI: Politiediensten als inlichtingendiensten, politiediensten en inlichtingendiensten', Metaforum Leuven, KU Leuven, Hollands College, 4 december 2014.

162 http://fra.europa.eu.

163 Hierover VAST COMITÉ I, *Activiteitenverslag 2008*, 88-89.

164 De werkzaamheden resulteerden in een eerste publicatie: P. KLAOUSEN en T. PICHEVIN, *Renseignement et éthique. Le moindre mal nécessaire*, Groupe européen de recherche sur

Interculturele Studies (CEMIS) van de Universiteit Antwerpen, deel aan een brainstormsessie 'over onderzoek naar radicalisering en mogelijke oplossingen'. Onderzoekers van meerdere universiteiten (UAntwerpen, UGent, KULeuven en VUBrussel) werkten er aan een onderzoeksvoorstel dat kadert binnen het financieringskanaal Strategisch Basisonderzoek van het Agentschap voor Innovatie door Wetenschap en Technologie van de Vlaamse overheid. Eerder maakte een vertegenwoordiger van het Vast Comité I deel uit van de begeleidingscommissie van het onderzoeksproject 'Radicalisering en sociale media: een test van een geïntegreerd model (RADIMED)'.[165] In dezelfde zin werd het Comité verzocht zijn medewerking te verlenen aan IMPACT Europe, een grootschalig Europees onderzoek gefinancierd door de Europese Commissie naar het effectief voorkomen en tegengaan van radicalisering.[166] Ten slotte nam een raadsheer van het Comité het woord op de studiedag 'Les méthodes particulières de recherches face aux nouvelles formes de cybercriminalité', georganiseerd door het *Belgian Cybercrime Center of Excellence* (B-CCENTRE) en het *Centre de Recherche Information, Droit et Société* van de *Université de Namur* (CRIDS).

V.5. SAMENWERKINGSPROTOCOL MENSENRECHTEN

Reeds lang wordt er vanuit diverse hoeken aangedrongen om, net als in de buurlanden, ook in ons land een onafhankelijk, nationaal mensenrechteninstituut (NMRI) op te richten.[167] In België bestond tot voor kort immers geen publieke instantie die nagaat of de huidige en toekomstige wetgeving conform is met de arresten van het Europees Hof voor de Rechten van de Mens en met internationale mensenrechtenverdragen.

Het ontbreken van een publieke mensenrechteninstantie werd beschouwd als een aanzienlijke leemte.[168] De oprichting ervan haalde de Regeerakkoorden van Verhofdstadt II (2003) en Di Rupo (2011), maar bleef dode letter.

---

l'éthique du renseignement (GERER), Lavauzelle, Panazol, 2014, 332 met een voorwoord van de voorzitter van het Vast Comité I.

165 De onderzoeksequipe (UGent, Hogeschool Gent en UCL) finaliseerde in 2014 zijn wetenschappelijk onderzoek: L. PAUWELS, F. BRION, B. DE RUYVER et al, *Verklaren en begrijpen van de rol van blootstelling aan nieuwe sociale media en gewelddadig extremisme. Een geïntegreerde kwalitatieve en kwantitatieve benadering (RADIMED)*, Brussel, Federaal Wetenschapsbeleid, 2014 (SP2587).

166 IMPACT Europe staat voor *Innovative Method and Procedure to Assess Counter-violent-radicalisation Techniques in Europe*. Hierover: www.impacteurope.eu.

167 Zie bijvoorbeeld *Parl. St.* Kamer 2012-13, 53K2946/001 (Wetsvoorstel houdende oprichting van een Mensenrechteninstituut) en www.mensenrechten.be.

168 Ook de Mensenrechtenraad van de Verenigde Naties stelde dit vast in 2011 tijdens zijn zogenaamd 'Universeel Periodiek Onderzoek (UPO)'. In 2016 wordt België opnieuw aan dit onderzoek onderworpen.

Daar kwam in 2014 verandering in. Het Comité nam, samen met andere instellingen met een mandaat op gebied van mensenrechten[169], deel aan diverse voorbereidende vergaderingen. Dit resulteerde op 13 januari 2015 in een samenwerkingsprotocol[170] waarin alle deelnemende instanties overeen kwamen om hun praktijken en methodes uit te wisselen, om gemeenschappelijke kwesties te onderzoeken en om de onderlinge samenwerking te bevorderen.

V.6. CONTACTEN MET BUITENLANDSE TOEZICHTHOUDERS

Begin februari 2014 werd de voorzitter van het Vast Comité I uitgenodigd door de Luxemburgse *Commission de Contrôle parlementaire du Service de Renseignement de l'Etat*. De voorzitter werd gevraagd om het Belgische model van parlementaire controle op de inlichtingen- en veiligheidsdienten toe te lichten.

Begin mei werd de voorzitter van het Vast Comité I uitgenodigd door de Franse *Assemblée Nationale* om het Belgische toezichtmodel toe te lichten.

Eind mei 2014 werd een werkbezoek georganiseerd in Brussel tussen een vertegenwoordiging van het Vast Comité I en de Nederlandse Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD). Daarbij waren onder meer de afgelopen en lopende toezichtonderzoeken aan de orde, de recente ontwikkelingen in het parlementair toezicht, de wijze van rapportering aan de opdrachtgevers en werd gedebatteerd over het thema van de 'bindende beslissingen'.

In het verlengde hiervan organiseerde de CTIVD halverwege november 2014 een overlegmoment. De vergadering werd uitgebreid met vertegenwoordigers van de Zwitserse *Strategic Intelligence Service Supervision*, dat deel uitmaakt van het *Departement fédéral de la défense, de la protection de la population et des sports*. Er werd van gedachten gewisseld over werkmethoden en -processen (Hoe prioriteiten stellen? Op welke wijze kan toezicht meer efficiënt worden gemaakt? Hoe verhoudt transparantie zich tot classificatie?…) en uitdagingen voor de toekomst (Hoe de onafhankelijkheid bewaren? Wat met *blind spots*?…).

Nog in november 2014 vond een ontmoeting plaats tussen vertegenwoordigers van het Vast Comité I en de vice-voorzitter van het Italiaanse parlementaire toezichtorgaan (*Comitato Parlementare per la Sicurezza della Republica Italiana*, COPASIR). De organisatie van de democratische controle op de inlichtingendiensten en een kennismaking met het Belgische model stonden hier centraal.

---

169 Zoals het Interfederaal Gelijkekansencentrum, het Federaal Migratiecentrum, het Instituut voor de gelijkheid van vrouwen en mannen, de Privacycommissie, de federale Ombudsman, de Hoge Raad voor Justitie, de Vaste Comités P en I.

170 'Samenwerkingsprotocol tussen de instellingen met een volledig of gedeeltelijk mandaat belast met de eerbiediging van de rechten van de mens'.

V.7. LID VAN EEN SELECTIECOMITÉ

De voorzitter van het Vast Comité I werd, samen met de procureurs-generaal van Gent en Luik, een academicus van de Universiteit Gent, de administrateur-generaal van de RVA en een gedelegeerd bestuurder van SELOR, aangesteld als lid van het selectiecomité belast met het geven van een omstandig advies aan de minister van Justitie omtrent de kandidaturen voor de posten van administrateur-generaal en van adjunct-administrateur-generaal bij de Veiligheid van de Staat.[171]

De voorzitter van het Vast Comité I werd op verzoek van het selectiebureau van de federale overheid SELOR eveneens betrokken bij de selectie van de kandidaturen voor de functie van administrateur-generaal van de Administratie der Douane en Accijnzen van de FOD Financiën.

V.8. CONTROLE OP DE SPECIALE FONDSEN

Namens de Kamer van Volksvertegenwoordigers houdt het Rekenhof toezicht op het gebruik van de financiële middelen door overheidsdiensten. Het Rekenhof controleert de wettigheid en de rechtmatigheid van alle uitgaven. Dat geldt in principe ook voor alle uitgaven van de inlichtingendiensten. Echter, omwille van de gevoeligheid van de materie wordt een deel van het budget van de VSSE en de ADIV (met name de 'speciale fondsen' met uitgaven voor bijvoorbeeld operaties en informanten) niet onderzocht door het Rekenhof. Voor de VSSE wordt de controle van deze uitgaven verricht door de Kabinetschef van de minister van Justitie. Sinds 2006 wordt de controle van de speciale fondsen van de ADIV echter alleen uitgevoerd door het hoofd van de Krijgsmacht en dit vier maal per jaar. Op suggestie van het Rekenhof gebeurt dit sinds 2010 in aanwezigheid van de voorzitter van het Vast Comité I.[172]

171 M.B. van 5 februari 2014 tot wijziging van het ministerieel besluit van 4 april 2006 houdende aanwijzing van een sectiecomité belast met de evaluatie van de kandidaturen voor de post van administrateur-generaal van de Veiligheid van de Staat, *BS* 7 februari 2014. In maart 2014 besliste de Minsterraad om Jaak Raes als administrateur-generaal en Pascal Petry als adjunct-administrateur-generaal van de VSSE te benoemen.

172 Enkele strafonderzoeken wezen evenwel op het mogelijks misbruik van gelden bestemd voor de betaling van informanten. Het Comité werd door zijn Dienst Enquêtes op de hoogte gebracht van mogelijke structurele problemen, en besliste een onderzoek te openen naar 'de wijze van beheer, besteding en controle van de fondsen bestemd voor de vergoeding van informanten van de VSSE en de ADIV' (cf. II.10.2).

V.9. AANWEZIGHEID IN DE MEDIA

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

Datum	Onderwerp/titel	Forum
7 februari 2014	Persbericht over het EU Intelligence Analysis Centre (EU INTCEN)	via Belga
17 maart 2014	Qui surveille les espions?	France Culture
28 maart 2014	Waakhond geheime diensten is tevreden over inlichtingenwerk in Afghanistan'	MO*
3 april 2014	'Waarom onze staatsveiligheid faalde in opsporen NSA-spionage'	De Morgen
15 april 2014	'Les mails du comité R ouverts à tout vent' en 'Aucune intrusion constatée dans le système externe, indique le Comité R'	La Libre
15 april 2014	'Comité I eist rechtzetting over hacking van intern systeem'	Belga
25 april 2014	'Le Comité R qui contrôle les services de renseignements fête ses 20 ans'	RTBF Info
28 april 2014	Espionnage à Bruxelles	RTBF (Matchpoint)
16 juli 2014	'Renseignements: les élus ne font pas leur travail. Parlement et gouvernement mis en cause'	Le Soir
26 november 2014	Staatsveiligheid luistert steeds meer communicatie af'	MO*
26 november 2014	'Belgische spionnen opereren in buitenland zonder wettelijk kader'	De Standaard

HOOFDSTUK VI
DE OPSPORINGS- EN GERECHTELIJKE ONDERZOEKEN

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

Wanneer zij een opdracht van gerechtelijke politie vervullen, staan de leden en de directeur van de Dienst Enquêtes I onder het toezicht van de procureur-generaal bij het hof van beroep of van de federaal procureur (art. 39 W.Toezicht) en heeft het Vast Comité I geen zeggenschap over hen. De voorzitter van het Vast Comité I moet er echter zorg voor dragen dat de uitvoering van de opdrachten van gerechtelijke politie de uitvoering van de toezichtonderzoeken niet hindert. De reden daarvoor ligt voor de hand: het controleorgaan staat in de eerste plaats ter beschikking van het parlement. Die opdracht zou 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). Van deze mogelijkheid werd nog nooit gebruik gemaakt.

In de gevallen waarin de Dienst Enquêtes I strafonderzoeken voert, moet de directeur na het afronden van dit onderzoek verslag uitbrengen bij het Vast Comité I. In dat geval '*beperkt het verslag zich evenwel tot de informatie die nuttig is voor de uitoefening door het Vast Comité I van zijn opdrachten*' (art. 43, derde lid, W.Toezicht).

In 2014 voerde de Dienst Enquêtes I een aanzienlijk aantal onderzoeksdaden uit in het kader van meerdere belangrijke onderzoeken. Zo werden bijvoorbeeld 36 processen-verbaal opgesteld.

Een eerste dossier betrof een onderzoek in opdracht van het parket van Marche-en-Famenne en vervolgens van het arbeidsauditoraat van Luik. Het had betrekking op feiten van vermeende morele intimidatie die zouden uitgemond zijn in de zelfmoord van een personeelslid van de VSSE. Het arbeidsauditoraat klasseerde dit dossier begin 2015 evenwel zonder gevolg wegens onvoldoende bewijzen. Na het afronden van het onderzoek bracht de Dienst Enquêtes – conform artikel 43 derde lid W.Toezicht – het Comité op de hoogte van zijn vaststellingen.

Een tweede dossier werd uitgevoerd in opdracht van parket van Charleroi en betrof een geval van vermeende geldverduistering door een lid van de Buitendiensten van de VSSE tijdens de uitvoering van zijn opdrachten. Na diverse gerechtelijke opdrachten, werd ook dit dossier zonder gevolg geklasseerd.

De andere in 2014 opgestarte dossiers zijn nog lopende.

HOOFDSTUK VII

DE GRIFFIE VAN HET BEROEPSORGAAN INZAKE VEILIGHEIDSMACHTIGINGEN, -ATTESTEN EN -ADVIEZEN

De voorzitter van het Vast Comité I neemt ook het voorzitterschap van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen waar. De griffiefunctie wordt uitgeoefend door de griffier en door de administratie van het Vast Comité I.

Het Beroepsorgaan is bevoegd voor geschillen die betrekking hebben op beslissingen in vier domeinen: de veiligheidsmachtigingen, de veiligheidsattesten die toegang moeten verlenen tot plaatsen waar zich geclassificeerde documenten bevinden, de veiligheidsattesten die toegang moeten verlenen tot welbepaalde plaatsen waar zich een dreiging voordoet en, ten slotte, de veiligheidsadviezen. Daarnaast kan het Beroepsorgaan ook optreden als 'annulatierechter' tegen beslissingen van publieke of administratieve overheden om in een bepaalde sector of voor een bepaalde plaats of evenement veiligheidsattesten of -adviezen aan te vragen.[173]

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

In dit hoofdstuk worden de aard van de bestreden beslissingen, de hoedanigheid van de bevoegde overheden en van 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 afgelopen twee jaar eveneens opgenomen.

In 2014 daalde het aantal beroepen en beslissingen lichtjes in vergelijking met 2013: 171 beroepen tegenover 189 en 163 beslissingen tegenover 187. Deze lichte

173 Zie hierover uitgebreid het *Activiteitenverslag 2006* van het Vast Comité I (91-119).

daling is quasi volledig te wijten aan het mindere aantal beroepen tegen weigeringen of intrekkingen van veiligheidmachtigingen.

Tabel 1. Betrokken veiligheidsoverheid

	2012	2013	2014
Nationale Veiligheidsoverheid	40	98	99
Veiligheid van de Staat	0	1	0
Algemene Dienst inlichting en veiligheid	27	78[174]	60
Federaal Agentschap voor Nucleaire Controle	11	9	8
Federale politie	1	1	3
Lokale politie	2	2	1
Lokale luchthavencommissie	10	–[175]	–
TOTAAL	**91**	**189**	**171**

Tabel 2. Aard van de bestreden beslissing

	2012	2013	2014
Veiligheidsmachtigingen			
Vertrouwelijk	7	5	5
Geheim	29	56	43
Zeer geheim	9	5	4
Totaal veiligheidsmachtigingen	45	66	52
Weigering	33	41	25
Intrekking	12	5	9
Weigering en intrekking	–	4	–
Machtiging voor beperkte duur	0	1	2

174 De sterke stijging van het aantal dossiers komende van de ADIV was te wijten aan het systeem waarbij kandidaat-militairen kunnen onderworpen worden aan een veiligheidsverificatie.

175 Sinds 2013 worden de adviezen in het kader van de veiligheidsbadges voor de toegang tot de beveiligde zones van luchthavens niet meer verleend door de lokale luchthavencommissies maar door de Nationale Veiligheidsoverheid. Vandaar ook de stijging van het aantal dossiers komende van de NVO in vergelijking met vorige jaren.

	2012	2013	2014
Machtiging voor lager niveau	1	0	1
Geen beslissing binnen termijn	1	15	15
Geen beslissing binnen verlengde termijn	0	0	0
Totaal veiligheidsmachtigingen	45	66	52
SUBTOTAAL VEILIGHEIDSMACHTIGINGEN	**45**	**66**	**52**
Veiligheidsattesten geclassificeerde documenten			
Weigering	23	0	4
Intrekking	0	0	0
Geen beslissing binnen termijn	0	0	0
Veiligheidsattesten plaats of gebeurtenis			
Weigering	0	15	16
Intrekking	0	0	0
Geen beslissing binnen termijn	0	0	0
Veiligheidsadviezen			
Negatief advies	23	106	99
Geen advies	0	2	0
'Herroeping' van een positief advies	0	0	0
Normatieve rechtshandelingen	0	0	0
Beslissing van publieke overheid om attesten te eisen	0	0	0
Weigering NVO om verificaties voor attesten te verrichten	0	0	0
Beslissing van administratieve overheid om adviezen te eisen	0	0	0
Weigering NVO om verificaties voor adviezen te verrichten	0	0	0
SUBTOTAAL ATTESTEN EN ADVIEZEN	**46**	**123**	**119**
TOTAAL BESTREDEN BESLISSINGEN	**91**	**189**	**171**

Tabel 3. Hoedanigheid van de verzoeker

	2012	2013	2014
Ambtenaar	5	4	0
Militair	26	26	17
Particulier	54	159	145
Rechtspersoon	6	0	6

Tabel 4. Taal van de verzoeker

	2012	2013	2014
Franstalig	51	92	92
Nederlandstalig	40	97	76
Duitstalig	0	0	0
Anderstalig	0	0	0

Tabel 5. Aard van de door het Beroepsorgaan genomen voorbereidende beslissingen[176]

	2012	2013	2014
Volledig dossier opvragen (1)	90	187	168
Aanvullende informatie opvragen (2)	5	12	16
Horen lid overheid (3)	10	3	11
Beslissing voorzitter (4)	0	0	0
Informatie uit dossier halen door Beroepsorgaan (5)	44	68	78
Informatie uit dossier halen door inlichtingendienst (6)	0	0	0

(1) Het Beroepsorgaan beschikt over de mogelijkheid het gehele onderzoeksdossier bij de veiligheidsoverheden op te vragen. Aangezien dit dossier meer gegevens bevat dan het onderzoeksverslag alleen, wordt dit verzoek systematisch gedaan.

176 Het 'aantal genomen voorbereidende beslissingen' (tabel 5), de 'wijze waarop de verzoeker zijn rechten van verdediging gebruikt' (tabel 6) of nog, de 'aard van de beslissingen van het beroepsorgaan' (tabel 7) is niet noodzakelijkerwijs gelijklopend met het aantal ingediende verzoeken uit de tabellen 1 tot en met 4. Immers, sommige dossiers werden bijvoorbeeld al opgestart in 2014, terwijl de beslissing pas viel in 2015.

(2) Het Beroepsorgaan heeft de mogelijkheid om tijdens de procedure aanvullende informatie die het nuttig acht, op te vragen.
(3) Het Beroepsorgaan kan beslissen om de leden van de inlichtingen- en politiediensten of van de veiligheidsoverheden die aan het veiligheidsonderzoek of de -verificatie hebben meegewerkt, te horen.
(4) De voorzitter van het Beroepsorgaan kan beslissen dat het lid van de inlichtingendienst bepaalde gegevens geheim houdt tijdens zijn verhoor.
(5) Indien de betrokken inlichtingendienst hierom verzoekt, kan het Beroepsorgaan beslissen dat bepaalde informatie uit het dossier dat aan de verzoeker ter inzage zal worden voorgelegd, wordt gehaald.
(6) Indien het informatie betreft die afkomstig is van een buitenlandse inlichtingendienst, beslist de Belgische inlichtingendienst zelf of de informatie ter inzage is. Dit is een aspect van de toepassing van de zogenaamde 'derdenregel'.

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

	2012	2013	2014
Dossierinzage door klager / advocaat	54	103	84
Horen van de klager / advocaat[177]	65	138	115

Tabel 7. Aard van de beslissingen van het beroepsorgaan

	2012	2013	2014
Veiligheidsmachtigingen			
Beroep onontvankelijk	0	2	0
Beroep zonder voorwerp	1	3	3
Beroep ongegrond	19	20	12
Beroep gegrond (volledige of gedeeltelijke toekenning)	23	35	14
Bijkomende onderzoeksdaden door overheid	1	0	0
Bijkomende termijn voor overheid	0	14	12[178]
Veiligheidsattesten geclassificeerde documenten			
Beroep onontvankelijk	0	0	0

177 In bepaalde dossiers wordt de klager/advocaat meermaals gehoord.
178 Net als in 2013 hadden deze dossiers in hoofdzaak betrekking op de toekenning van veiligheidsmachtigingen voor personeelsleden van de SHAPE. Aangezien de Belgische veiligheidsoverheid hierbij soms tevergeefs wachtte op informatie vanuit Frankrijk, werden de wettelijke termijnen regelmatig overschreden. Het Beroepsorgaan besloot in 12 gevallen de NVO een bijkomende termijn te verlenen om alsnog een beslissing te nemen.

	2012	2013	2014
Beroep zonder voorwerp	0	0	0
Beroep ongegrond	0	0	2
Beroep gegrond (toekenning)	0	0	0
Veiligheidsattesten plaats of gebeurtenis			
Beroep onontvankelijk	3	1	0
Beroep zonder voorwerp	1	0	0
Beroep ongegrond	8	6	6
Beroep gegrond (toekenning)	6	11	8
Veiligheidsadviezen			
Beroep onbevoegd	5	0	4
Beroep onontvankelijk	1	4	4
Beroep zonder voorwerp	0	1	4
Bevestiging negatief advies	9	25	53
Omvorming in positief advies	4	65	41
Beroep tegen normatieve rechtshandelingen	0	0	0
TOTAAL	**81**	**187**	**163**

HOOFDSTUK VIII
DE INTERNE WERKING VAN HET VAST COMITÉ I

VIII.1. SAMENSTELLING VAN HET VAST COMITÉ I

De samenstelling van het Comité bleef in 2014 ongewijzigd: voorzitter Guy Rapaille (F), advocaat-generaal bij het hof van beroep te Luik en raadsheren Gérald Vande Walle (F) en Pieter-Alexander De Brock (N).[179]

Ook bij de Dienst Enquêtes I vielen er geen verschuivingen te noteren. De dienst bestaat uit vijf commissaris-auditoren en wordt geleid door Frank Franceus (N).

De administratieve staf van het Vast Comité I, onder leiding van griffier Wouter De Ridder, kende evenmin wijzigingen en bleef op een totaal van 16 personeelsleden.

VIII.2. VERGADERINGEN MET DE BEGELEIDINGSCOMMISSIE(S)

In de loop van 2014 vonden nog twee vergaderingen plaats met de toenmalige Senatoriële Begeleidingscommissie aan wie het Vast Comité I rapporteerde. Tijdens deze vergaderingen werden – achter gesloten deuren – diverse toezichtonderzoeken besproken.

Met de herschikking van de bevoegdheden van de Senaat door de zesde staatshervorming en ingevolge de Wet van 6 januari 2014[180], verhuisde de controle op de inlichtingendiensten in 2014 naar de ééngemaakte 'Commissie belast met de begeleiding van het Vast Comité P en het Vast Comité I' in de Kamer van Volksvertegenwoordigers, die zowel de politie- als de inlichtingendiensten zal controleren.[181] De vorige meerderheid had voor de verkiezingen van mei 2014 nog beslist dat die nieuwe parlementaire commissie zou bestaan uit de fractieleiders. Begin

179 Wel werd in 2014 een tweede Nederlandstalig plaatsvervangend lid benoemd (*Hand.* Senaat 213-14, 13 maart 2014, nr. 5-144, 47).

180 *BS* 31 januari 2014.

181 Hierover uitvoerig: W. VAN LAETHEM, *Juristenkrant*, 28 mei 2014 (Nieuwe Kamercommissie ziet toe op geheime diensten) en W. VAN LAETHEM, *Juristenkrant*, 8 april 2015 (Dan toch geen geheime informatie voor het parlement).

oktober 2014 vond dan ook, in deze vernieuwde samenstelling en onder het voorzitterschap van Kamervoorzitter *ad interim* Patrick Dewael, een gedachtenwisseling plaats met de Vaste Comités P en I.

De nieuwe meerderheid opteerde echter voor een meer evenredige vertegenwoordiging, waarbij werd afgestapt van de idee dat de fractieleiders van rechtswege deel zouden uitmaken van de Commissie. Daartoe werd artikel 149 van het Reglement van de Kamer van Volksvertegenwoordigers gewijzigd.[182] Voortaan telt de Commissie dertien stemgerechtigde leden, die als volgt werden aangewezen: Koenraad Degroote (N-VA), Peter Buysrogge (N-VA), Hendrik Vuye (N-VA), Laurette Onkelinx (PS), André Frédéric (PS), Denis Ducarme (MR), Philippe Pivin (MR), Servais Verherstraeten (CD&V), Franky Demon (CD&V), Patrick Dewael (Open Vld), Karin Temmerman (sp.a), Stefaan Van Hecke (Ecolo-Groen) en Christian Brotcorne (cdH).[183] De commissie vergadert onder het voorzitterschap van Kamervoorzitter Siegfried Bracke (N-VA).

Eind november 2014 werd voor het eerst in deze samenstelling vergaderd en stonden de besprekingen van het *Activiteitenverslag 2013* alsook drie toezichtonderzoeken op de agenda.[184]

VIII.3. GEMEENSCHAPPELIJKE VERGADERINGEN MET HET VAST COMITÉ P

De artikelen 52 tot 55 W.Toezicht bepalen de gevallen waarin en de wijze waarop het Vast Comité I en het Vast Comité P gemeenschappelijke vergaderingen dienen te organiseren. Het doel van deze vergaderingen is tweeërlei: het uitwisselen van informatie en het bespreken van lopende gemeenschappelijke toezichtonderzoeken, zoals *in casu* de onderzoeken naar de *Joint information box* (II.10.3), naar de personeelsleden van het OCAD en sociale media (II.10.5) en naar de internationale contacten van het OCAD (II.10.6).

In 2014 vonden vier gemeenschappelijke vergaderingen plaats.

---

182 Reglement van de Kamer van Volksvertegenwoordigers – Wijziging (1), *BS* 31 oktober 2014: *'De Kamer wijst bij het begin van iedere zittingsperiode, overeenkomstig de artikelen 157 en 158, uit haar midden de vaste leden aan van de commissie belast met de begeleiding van het Vast Comité P en het Vast Comité I, bedoeld in artikel 66bis van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, waarbij zoveel leden worden benoemd als nodig is opdat elke politieke fractie ten minste een commissielid telt. Artikel 22 is niet van toepassing.'*

183 *Hand.* Kamer CRIV54PLEN015, 13 november 2014, 32.

184 *Parl. St.* Kamer 2014-15, nr. 54K0720/001.

VIII.4. FINANCIËLE MIDDELEN EN BEHEERSACTIVITEITEN

In de globale saneringscontext van de overheidsfinanciën heeft het Comité aan zijn toezichthoudende overheid voor het activiteitenjaar 2014 een dotatie van 3,75 miljoen euro voorgesteld.[185] Dit in vergelijking tot de gevraagde 3,86 miljoen euro in 2013, ofte een vermindering van 2,82% van zijn totale werkingsbudget. Rationeel beheer van de ter beschikking gestelde fondsen voor 2013 leverde bovendien een budgettaire bonus op van 1,13 miljoen euro, dewelke werd toegevoegd aan de financiering van de dotatie van 2014. Dit liet toe om de door de Staat toegekende middelen voor de financiering van de dotatie in hoofde van artikel 57 W.Toezicht met 14,6% te verminderen. Het Vast Comité I heeft er de Commissie van comptabiliteit op gewezen dat op termijn de gecumuleerde effecten van een verminderde begroting ten laste van de Rijksbegroting en de afname van de boni, een financieringsprobleem kunnen stellen.

Sinds zijn vestiging in de FORUM-gebouwen, eigendom van de Kamer van Volksvertegenwoordigers, worden voortdurend synergieën gezocht en ontwikkeld met de Kamer en andere overheidsinstellingen met het oog op een optimalisering en/of inperking van de werkingskosten.

VIII.5. VORMING

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

DATUM	TITEL	ORGANISATIE	PLAATS
2014-2015	Hogere Studies Veiligheid en Defensie	KHID	Brussel
4 en 11 februari 2014	Sociale media op de politionele werkvloer	Belgian Cybercrime Centre of Excellence for Training, Research and Education	Gent en Leuven
6 februari 2014	Bewapende drones. Technische, juridische en ethische overwegingen	KHID	Brussel

185 Wet van 19 december 2013 houdende de algemene uitgavenbegroting voor het begrotingsjaar 2014, *BS* 27 december 2013 en *Parl. St.* Kamer 2013-2014, nr. 53K3237/001.

DATUM	TITEL	ORGANISATIE	PLAATS
7 maart 2014	Social media intelligence (SocMint): Intelligent? No borders? The egg of Colombus? Raising Expectations?	Netherlands Intelligence Studies Association	Amsterdam
13 mei 2014	De toekomst van de nucleaire afschrikking in Europa	KHID	Brussel
19 mei 2014	Les enjeux géopolitiques du golfe arabo-persique	Métis	Parijs
23 mei 2014	D-day minus x – Inlichtingenactiviteiten bij en over de Atlantikwall	BISC	Raversijde
10 juni 2014	Le danger des sectes en Belgique – Illusion ou réalité?	AVCB	Brussel
17 juni 2014	Open school Cyber security, challenges for Belgian defence	ADIV	Brussel
26 juni 2014	The public regulated service of the European Galileo navigation satellite system	KMS/NVO	Brussel
4 juli 2014	Ethique et renseignement	GERER	Parijs
7-10 juli 2014	International Intelligence Review Agencies Conference	IIRAC	Londen
15 september 2014	Intelligence économique et renseignement. Quelles différences et quelles intéractions?	Métis	Parijs
18-19 september 2014	Telling truth to power. The past, present and futur of military intelligence	NISA/DISS	Amsterdam
25 september 2014	Ethische competentie: het belang van selectie en socialisatie	KUL/LINC	Leuven
24 oktober 2014	La sécurité privée, la défense et les études de renseignement	Universiteit Gent en Universiteit Lille	Lille
6 november 2014	'Blowback' – een analyse van de dreiging van buitenlandse strijders uit Europa	KHID	Brussel
14 november 2014	Les méthodes particulières de recherches face aux nouvelles formes de cybercriminalité	B-CCENTRE / CRIDS / Universiteit Namen	Brussel
20 november 2014	La sécurité privée, la défense et les études de renseignement	Universiteit Gent en Universiteit Lille	Lille
2 december 2014	Building Belgium's cyber intelligence knowledge capacity	BISC	Brussel
4 december 2014	Ethique et renseignement	GERER	Parijs

HOOFDSTUK IX
AANBEVELINGEN

Op basis van de in 2014 afgesloten toezichtonderzoeken en de behandelde BIM-dossiers, formuleert het Vast Comité I onderstaande aanbevelingen. Zij hebben in het bijzonder betrekking op de bescherming van de rechten die de Grondwet en de wet aan de personen verlenen (IX.1), op de coördinatie en de efficiëntie van de inlichtingendiensten, het OCAD en de ondersteunende diensten (IX.2) en – ten slotte – op de optimalisatie van de toezichtmogelijkheden van het Vast Comité I (IX.3).

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

IX.1.1. AANDACHT VOOR MASSALE DATA-CAPTATIE EN POLITIEKE EN ECONOMISCHE SPIONAGE[186]

Beide inlichtingendiensten moeten aandacht hebben voor de risico's die nieuwe technologische mogelijkheden met zich kunnen brengen op vlak van massale data-captatie en economische en politieke spionage, ook al gaan die uit van 'bevriende landen'. Hierover zouden risicoanalyses moeten worden opgesteld, waarbinnen ook aandacht is voor de aanwezigheid van internationale instellingen op Belgisch grondgebied.

De aandacht voor deze fenomenen is wat betreft de VSSE en de ADIV noodzakelijk om een goede informatiepositie op te bouwen om de mogelijkheden en de werkwijzen van andere diensten te kennen, niet alleen om desgevallend de overheden in te kunnen lichten of tegenmaatregelen te treffen, maar ook om zijn eigen collecte-technieken te evalueren.

Wat betreft de VSSE is de aandacht voor massale data-captatie evident noodzakelijk omdat dit fenomeen een reële bedreiging vormt voor minstens twee wet-

[186] Deze aanbeveling komt voort uit het eerste toezichtonderzoek naar de onthullingen van Edward Snowden (II.1. De Snowden-onthullingen en de informatiepositie van de Belgische inlichtingendiensten).

telijk te beschermen belangen, te weten de fundamentele rechten en vrijheden en de soevereiniteit van de Staat. Veel informatie is bijvoorbeeld reeds terug te vinden in open bronnen of opvraagbaar bij de militaire inlichtingendienst. Op basis van die elementen kan reeds een globaal beeld gevormd worden van het fenomeen en van de risico's. Dit zou zijn neerslag kunnen vinden in een fenomeenanalyse[187] die op regelmatige tijdstippen naar de betrokken overheden wordt gezonden. Maar ook de burgers en de ondernemingen zouden, meer nog dan nu, moeten gesensibiliseerd worden voor de problematiek.

IX.1.2. RICHTLIJNEN INZAKE DE SAMENWERKING MET BUITENLANDSE DIENSTEN[188]

De VSSE stelde in 2012 een gedetailleerde 'Instructie voor de bilaterale samenwerking met de correspondenten' op. Het Vast Comité I beschouwde deze richtlijn als bijzonder waardevol. Wel wees het er op dat bepaalde door de VSSE genomen opties, gedragen moeten worden door de politieke verantwoordelijken, te weten de leden van het (toenmalige) Ministerieel Comité voor inlichting en veiligheid. Tevens werd één van de belangrijkste aspecten van die samenwerking – welke inlichtingen mogen meegedeeld worden aan buitenlandse diensten? – in de instructie slechts summier aangeraakt. Het Vast Comité I herhaalt[189] dan ook zijn aanbeveling aan de VSSE om haar richtlijn – aangevuld met meer precieze regels over informatie-uitwisseling – onverwijld toe te zenden naar de Nationale Veiligheidsraad als opvolger van het Ministerieel Comité voor inlichting en veiligheid.

Eenzelfde aanbeveling geldt voor de ADIV, zeker nu het Vast Comité I heeft kunnen vaststellen dat er nauw wordt samengewerkt met buitenlandse SIGINT-afdelingen (zoals bijvoorbeeld de NSA). De ADIV bereidt in navolging van de VSSE een soortgelijke nota voor met 'aftoetsbare criteria' in het kader van de samenwerking met buitenlandse inlichtingendiensten (in ruime zin). Deze nota zou in de loop van 2014 gefinaliseerd worden. Het Comité benadrukt het belang

---

187 Het Vast Comité I wees reeds eerder op de meerwaarde van wat de VSSE een 'fenomeenanalyse' noemt: *'L'analyse du phénomène expose un thème actuel qui relève des sphères d'intérêt et des missions dévolues à un service de renseignement et qui représente un défi politique et social majeur, tant aujourd'hui que pour les années à venir. Elle s'attache à décrire ce problème tant au niveau de ses origines historiques, qu'au plan de l'idéologie, de l'organisation, de la structure et des activités y relatives. Elle contextualise les défis et les risques, établit une "évaluation du risque" à destination de nos responsables politiques, des autorités administratives concernées et des autorités judiciaires qui sont également confrontées à cette problématique'*, aldus de VSSE in haar eerste fenomeenanalyse. Mede omdat dergelijke analyses bedoeld zijn om een ruimere verspreiding te krijgen, lenen ze zich goed voor de problematiek van data-captatie.

188 Deze aanbeveling komt voort uit de twee volgende toezichtonderzoeken: 'II.1. De Snowden-onthullingen en de informatiepositie van de Belgische inlichtingendiensten' en 'II.3. Het gebruik in strafzaken van informatie afkomstig van massale datacaptatie door buitenlandse diensten'.

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

van dergelijke richtlijn voor de ADIV omdat ze – eveneens na goedkeuring door de Nationale Veiligheidsraad – een gelegitimeerd kader kan bieden voor samenwerkingsverbanden die de militaire inlichtingendienst vandaag reeds aangaat.

Het Comité beveelt daarenboven aan dat de richtlijnen voor zowel de ADIV als de VSSE, in de mate van het mogelijke, gelijklopend zouden zijn. De ADIV kan zich volgens het Comité dan ook inspireren op volgende elementen die door de VSSE werden aangebracht in haar hierboven vermelde instructie:

- er dient rekening te worden gehouden met factoren die de samenwerking kunnen bezwaren (zoals problemen van inmenging, tegenstrijdige belangen, het respect voor fundamentele rechten…);
- de eigen wettelijke missie dient steeds gevrijwaard te blijven, zeker in materies als terrorisme en extremisme waaraan al snel een gerechtelijke dimensie is verbonden;
- de samenwerking met buitenlandse diensten moet volledig transparant en traceerbaar zijn (waardoor onder meer een controle door het Vast Comité I mogelijk wordt);
- er dient een periodieke evaluatie van de samenwerking plaats te vinden.

Tevens beveelt het Comité aan dat de evaluatie van de samenwerking aan de hand van de vooropgestelde criteria ook effectief én op geregelde tijdstippen plaatvindt. De Snowden-onthullingen tonen de noodzaak hiervan aan.

Wel wil het Vast Comité I er geen misverstand over laten bestaan dat het overtuigd is van het feit dat de Belgische inlichtingendiensten blijvend moeten investeren in een goede samenwerking met buitenlandse diensten en dit zowel op bi- als op multilateraal vlak.

IX.1.3. DE NOOD AAN EEN POLITIEKE DEKKING VOOR SAMENWERKINGSVERBANDEN[190]

Het Comité is 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.

190 Deze aanbeveling komt voort uit het eerste toezichtonderzoek naar de onthullingen van Edward Snowden (II.1. De Snowden-onthullingen en de informatiepositie van de Belgische inlichtingendiensten).

IX.1.4. DE NOOD AAN POLITIEKE STURING DOOR DE NATIONALE VEILIGHEIDSRAAD[191]

Het toenmalige Ministerieel Comité voor inlichting en veiligheid (nu: Nationale Veiligheidsraad) werd opgericht als politiek sturend orgaan van het inlichtingenwerk. Het heeft als taak bij wijze van richtlijnen de algemene politiek inzake inlichtingen te bepalen, de prioriteiten van beide inlichtingendiensten vast te leggen, te zorgen voor een coördinatie tussen de diensten en regels te bepalen inzake internationale samenwerking en gegevensuitwisseling. Het Ministerieel Comité is destijds na de Snowden-onthullingen echter niet samengekomen.

Het Comité acht het wenselijk dat de nieuwe Nationale Veiligheidsraad en bij uitbreiding het Strategisch Comité en het Coördinatiecomité voor inlichting en veiligheid – mede op aangeven van de twee inlichtingendiensten – hun sturende rol zouden opnemen ten aanzien van de fenomenen van massale data-captatie en politieke en economische spionage. Het Comité is van oordeel dat België daardoor minstens ten dele zou tegemoetkomen aan zijn positieve verplichting uit artikel 8 EVRM om de privacy van haar burgers te beschermen.

Daarnaast wijst het Comité op het ontbreken van de (wettelijk vereiste) formele goedkeuring door het Ministerieel Comité/Nationale Veiligheidsraad van de eind 2012 opgestelde lijst met bedrijven waarvan de ADIV het WEP moet beschermen.

IX.1.5. KRITISCHE EVALUATIE VAN REGELS VAN DE INTERNATIONALE INLICHTINGENCULTUUR[192]

In het eerste toezichtonderzoek naar aanleiding van de onthullingen door Edward Snowden, wees het Vast Comité I naar een aanbeveling opgenomen in het ontwerprapport van de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken van het Europese Parlement: '*Dringt er bij de lidstaten op aan gegevens van derde landen die op onrechtmatige wijze zijn verzameld niet te aanvaarden en toezichtsactiviteiten op hun grondgebied door overheden of bureaus van derde landen die volgens nationaal recht onrechtmatig zijn of niet voldoen aan de juridische waarborgen die in internationale of EU-instrumenten zijn vastgelegd, waaronder de bescherming van de mensenrechten in het kader van het VEU, het EVRM en het Handvest van de grondrechten van de EU, te weigeren.*' Het Vast Comité I merkt op dat de praktijk echter leert dat 'aanleverende inlichtingendiensten' in regel hun bronnen (en dus de oorsprong van een inlichting) afschermen en dat de 'ontvangende diensten' dit ook aanvaarden. Deze vorm van verstandhouding maakt deel

191 *Idem.*

192 Deze aanbeveling komt voort uit het toezichtonderzoek 'II.3. Het gebruik in strafzaken van informatie afkomstig van massale datacaptatie door buitenlandse diensten'.

uit van de internationale inlichtingencultuur, net zoals de regel van de derde dienst, het *do ut des*-principe en de eisen van geheimhouding.

Het Comité herhaalde dat deze vaststelling niet betekent dat het deze principes ongenuanceerd onderschrijft. Maar zij kunnen niet bruusk en unilateraal worden doorbroken.

Het Vast Comité I beveelt aan dat de Nationale Veiligheidsraad binnen een redelijke termijn zou onderzoeken welke maatregelen kunnen worden genomen om hieraan tegemoet te komen.

IX.1.6. BEPERKINGEN INZAKE INFORMATIEGARING BIJ (RECHTS)PERSONEN[193]

De VSSE mag bij elke persoon of organisatie die behoort tot de privésector informatie inwinnen over de dreigingen die ze opvolgt (art. 16 W.I&V). Daarbij blijft de betrokkene weliswaar gebonden door het beroepsgeheim waaraan hij desgevallend is gehouden en door de eisen van de Wet Verwerking Persoonsgegevens. Deze regelingen leggen beperkingen op inzake het meedelen van gegevens aan derden (zoals de VSSE). Daarnaast heeft de burger het recht om niet mee te werken aan een inlichtingenonderzoek. Daarom beveelt het Vast Comité I aan dat de leden van de VSSE in hun contacten met particulieren aandacht zouden schenken aan de wijze waarop hun optreden door personen die niet gewoon zijn om met de dienst contact te hebben, wordt gepercipieerd. Ook dient in de opleiding aandacht te worden besteed aan de correcte bejegening van de burgers waarmee de leden van de VSSE in contact treden.

IX.1.7. ACTUALISEREN VAN BESCHIKBARE INFORMATIE IN HET KADER VAN NATURALISATIES[194]

Het Comité beveelt aan dat informatie die door de VSSE wordt aangeleverd in het kader van de verkrijging van de Belgische nationaliteit systematisch wordt geactualiseerd indien die informatie betrekking heeft op '*gewichtige feiten eigen aan de persoon*' en die dus een tegenindicatie kunnen vormen in de toekenning van de Belgische nationaliteit.

---

193 Deze aanbeveling komt voort uit het toezichtonderzoek 'II.8. Klacht over de wijze waarop de VSSE de zaakvoerder van een bedrijf opvolgt'.

194 Aanbeveling afkomstig uit het 'II.7. Toezichtonderzoek naar de elementen die de VSSE verschafte in het kader van een naturalisatiedossier'.

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

IX.2.1. OMGAAN MET DE NOTIE 'BEVRIENDE DIENSTEN'[195]

Zowel de VSSE als de ADIV blijken 'omzichtiger' om te springen met bevriende diensten of diensten van bevriende landen. Alhoewel het Comité hier tot op zekere hoogte begrip voor kan opbrengen, beveelt het de Belgische inlichtingendiensten aan *elke* dreiging ernstig te nemen, ook indien ze uitgaat van bevriende diensten of diensten van bevriende landen. Het Vast Comité I onderschrijft de VSSE waar het stelt dat het aangewezen is te spreken over 'strategische partners' in plaats van 'bevriende diensten'.

IX.2.2. NAUWERE SAMENWERKING TUSSEN BEIDE INLICHTINGENDIENSTEN[196]

Het Comité moest vaststellen dat de VSSE en de ADIV in de periode vóór de Snowden-onthullingen nooit en nadien slechts beperkt onderling informatie hebben uitgewisseld over de bedreigingen gevormd door massale data-captatie en politieke en economische spionage. Het Comité stelt deze vaststelling vooreerst tegenover de wettelijke verplichting die berust bij de diensten om informatie uit te wisselen (art. 19 W.I&V). Daarenboven wijst het Comité op het bestaan van een onderling samenwerkingsakkoord (Protocolakkoord van 12 november 2004) dat er net op gericht is om spontaan informatie door te geven die tot de bevoegdheidssfeer van de andere dienst behoort. Minstens na de onthullingen hadden de mechanismen beschreven in dit Protocolakkoord gebruikt moeten worden om beider informatiepositie te verstevigen. Het Comité wijst in het bijzonder op de in het Protocol opgenomen mogelijkheid om een zogenaamd '*ad hoc* samenwerkingsplatform' op te richten waarbinnen gezamenlijke analyses kunnen worden opgesteld. Binnen een dergelijk platform zou de in het betrokken dossier aan het licht gekomen tegenstelling (met name het feit dat bij de ADIV relatief veel kennis aanwezig is, maar de dienst vóór de onthullingen niet bevoegd was voor de opvolging van massale data-captatie *versus* de VSSE die weliswaar bevoegd was maar weinig specifieke kennis had over het fenomeen) kunnen opgeheven worden.

---

195 Deze aanbeveling komt voor uit het eerste toezichtonderzoek naar de onthullingen van Edward Snowden (II.1. De Snowden-onthullingen en de informatiepositie van de Belgische inlichtingendiensten).

196 *Idem.*

IX.2.3. INTERDEPARTEMENTALE SAMENWERKING INZAKE *CYBERSECURITY*, *ICT-SECURITY* EN *CYBERINTELLIGENCE*[197]

Bepaalde aspecten van de Snowden-onthullingen wezen op zwaktes in de beveiligingssystemen van IT-netwerken van zowel private actoren als publieke instellingen. Het Comité herhaalt dan ook met klem dat er meer aandacht moet uitgaan naar *cyber-* en *ICT-Security* (INFOSEC) en dat deze problematieken – die niet alleen tot het takenpakket van de inlichtingendiensten behoren – een interdepartementale samenwerking vereisen. Zo bijvoorbeeld is in deze een cruciale rol weggelegd voor de Nationale Veiligheidsraad.

Het Comité verwijst in dit verband eveneens naar de goedkeuring destijds van een ontwerpbesluit door de Ministerraad op 19 december 2013 dat moest leiden tot de oprichting van een Centrum voor Cybersecurity België bij de Kanselarij van de Eerste minister. Bij K.B. van 10 oktober 2014 werd dit centrum officieel opgericht.

Ook werden destijds bijkomende middelen toegewezen om de *cybersecurity*-strategie zoals die eind 2012 was goedgekeurd, uit te voeren. Een deel van deze middelen zou bestemd zijn voor de ADIV wat deze dienst moet toelaten zijn capaciteit te verhogen en meer aandacht te besteden aan *cyberintelligence*. Het Vast Comité I is echter overtuigd dat *cybersecurity* en *-intelligence* de komende decennia blijvende investeringen zullen vereisen.

IX.2.4. DE NEGATIEVE GEVOLGEN VAN COMPARTIMENTERING EN GEHEIMHOUDING BINNEN DE ADIV[198]

Het feit dat binnen de ADIV slechts een zeer beperkt aantal personen rechtstreeks toegang heeft tot SIGINT-informatie én de strikte geheimhouding rond dit thema, kan de totstandkoming van een overkoepelend beeld met betrekking tot SIGINT-capaciteiten en -strategieën van buitenlandse grootmachten, bemoeilijkt hebben. Het Comité is dan ook van oordeel dat de ADIV zich zou moeten beraden over de vraag hoe in deze het principe van de *need to know* beter kan worden verzoend met de *need to share*.

197 *Idem.*
198 *Idem.*

IX.2.5. HET TERRITORIAAL TOEPASSINGSGEBIED VAN DE BIM-WET[199]

Ingevolge technologische evoluties dient het territoriale toepassingsgebied van de BIM-Wet verduidelijkt te worden. In afwachting van een eventueel wetgevend initiatief, interpreteert het Comité de huidige regeling voorzichtigheidshalve in die zin dat de BIM-methode alleen mag ingezet worden op communicaties op het ogenblik dat het signaal van een te capteren communicatie zich op Belgisch grondgebied bevindt.

IX.2.6. EEN VERDUIDELIJKING VAN DE INT-REGELING[200]

De Belgische INT-regeling, die de ADIV toelaat buitenlandse communicaties te intercepteren, is tot stand gekomen toen in essentie radiosignalen werden onderschept. Sindsdien is er op technologisch vlak dermate veel veranderd dat deze regeling opnieuw zou moeten onderzocht worden door de wetgever. De onthullingen van Edward Snowden hebben die vaststelling alleen maar bevestigd. Elementen die bij een dergelijke herziening alleszins moeten bestudeerd worden, zijn de mate waarin intercepties al dan niet gericht moeten gebeuren, de juiste draagwijdte van de mogelijkheid om signalen te 'zoeken', de mate van precisering van het jaarlijkse Afluisterplan, de mogelijkheid om aan data-*mining* te doen in bulkinformatie, en de vraag of buitenlandse SIGINT-operaties moeten kaderen binnen breder een 'internationaal mandaat'.

IX.2.7. AANBEVELINGEN IN HET KADER VAN DE PERSOONSBESCHERMING

In het kader van zijn toezichtonderzoek naar 'De VSSE en haar wettelijke opdracht van persoonsbescherming'[201] wees het Vast Comité I op enkele problemen en formuleerde het een aantal concrete aanbevelingen, waaronder:

- de verhouding tussen het aantal leidinggevenden van de Dienst Persoonsbescherming en het aantal uitvoerende personeelsleden (*span-of-control*) is zeer groot. Dit vormt geen werkbare situatie.
- Het Comité kon vaststellen dat sommige te beschermen personen niet steeds 'risicobewust' zijn. Niettemin is de VSSE, en dus finaal de Belgische Staat, in geval van een incident verantwoording verschuldigd. In dit verband moeten

199 *Idem*. In dezelfde zin, VAST COMITÉ I, *Activiteitenverslag 2013*, 114.
200 *Idem*. Zie tevens Hoofdstuk IV. Het toezicht op de interceptie van communicatie uitgezonden in het buitenland.
201 Zie Hoofdstuk II.4.

er dan ook dringend duidelijke afspraken worden gemaakt met de buitenlandse diplomaten. Het tot stand brengen van een degelijk canvas is niet alleen en wellicht zelfs niet in de eerste plaats een verantwoordelijkheid van de VSSE. Het Vast Comité I is van mening dat ook voor de politieke beleidsverantwoordelijken (Binnenlandse Zaken, Buitenlandse Zaken, Justitie) op korte termijn ter zake een belangrijke taak tot (her)evaluatie (en vandaaruit heroriëntering) is weggelegd.

– Het Vast Comité I beveelt aan om prioritair de permanente beschermingsopdrachten te herbekijken en te onderzoeken of ze op een andere manier kunnen worden ingevuld zodanig dat ze minder middelen zouden vergen.
– Het Vast Comité I beveelt aan blijvend aandacht te besteden aan het wegwerken van de overuren.
– Het onderzoek toonde aan dat de concrete toepassing van de dreigingsniveaus op het terrein geen consistent beeld opleverde. De op het terrein in stelling gebrachte dispositieven vertoonden immers een zeer losse band met het door het OCAD toegekende dreigingsniveau. Het Vast Comité I beveelt dan ook aan dat de betrokken diensten het over een in de praktijk werkbaar model of typologie eens worden en dit vervolgens consequent toepassen. De typologie die louter en alleen op 'dreiging' is gebaseerd, laat naar de mening van het Vast Comité I niet toe om voldoende nuances in te bouwen. Het Vast Comité I onderschrijft dan ook de door het Crisiscentrum van de regering geformuleerde suggestie om in een dergelijke typologie de concepten van 'beschermingsmaatregelen' versus 'voorzichtigheidsmaatregelen' op te nemen aangezien er niet in alle gevallen sprake zal zijn van een reële dreiging. Zo blijken niet alle VIP's rechtstreeks bedreigd, maar moeten er toch voorzorgsmaatregelen worden genomen om de reputatie van het gastland België hoog te houden. Ook de houding van de te beschermen VIP zou als een relevante factor of variabele een plaats in het model moeten krijgen.

IX.2.8. BETERE ONDERBOUWING VAN DE INMENGING DOOR DE SCIENTOLOGYKERK[202]

Het Vast Comité I nam akte van de globale analyse door de VSSE van de vele vormen van inmenging die de vzw Scientologykerk van België beoefent ten aanzien van de overheden. Het Comité stelt echter vast dat de eigen waarnemingen van de VSSE nooit middelen aan het licht hebben gebracht die eigenlijk 'ongeoorloofd' zijn en waarvan de beweging gebruik maakt om politieke beleidsmakers te benaderen. De VSSE beschikt echter over tal van aanwijzingen die doen vermoeden dat er daartoe gebruik wordt gemaakt van '*bedrieglijke of clandestiene mid-*

[202] Deze aanbeveling stamt uit het onderzoek 'II.5. Een klacht van de Scientologykerk tegen Veiligheid van de Staat'.

delen'. Het Comité formuleerde dan ook de aanbeveling dat de VSSE de inmenging door deze kerk beter zou aantonen door structuur te geven aan haar analyse betreffende de ongeoorloofde, bedrieglijke en clandestiene middelen waarvan gebruik gemaakt wordt om de overheden en politieke beleidsmakers in ons land te benaderen.

IX.2.9. SAMENWERKINGSVERBANDEN TEGEN PROLIFERATIE[203]

Ten einde de proliferatie op een effectieve manier aan te pakken, beveelt het Vast Comité I aan dat de diverse overheden formele samenwerkingsverbanden afsluiten. Dit is noodzakelijk gezien de complexe aard van het fenomeen, zowel qua techniciteit als qua regelgeving en bevoegdheid. Deze samenwerkingsverbanden dienen enerzijds te worden afgesloten tussen het federale en het gewestelijke niveau wat betreft het afstemmen van de regelgeving en het bepalen van sancties, en anderzijds tussen alle diensten die enige verantwoordelijkheid hebben op het terrein wat betreft controle en toezicht.

IX.3. AANBEVELING IN VERBAND MET DE DOELTREFFENDHEID VAN HET TOEZICHT: STRIKTE TOEPASSING VAN ARTIKEL 33 § 2 W.TOEZICHT[204]

Met het oog op zijn toezichtrol wees het Vast Comité I opnieuw[205] op de verplichting *ex* artikel 33 W.Toezicht om '*uit eigen beweging aan het Vast Comité I de interne reglementen en richtlijnen over, alsook alle documenten die de handelwijze van de leden van die diensten regelen*' over te zenden. Deze verplichting geldt ook voor afspraken, Memorandums of Understanding (MOU's) of akkoorden gesloten op internationaal vlak, weze het bi- of multilateraal.

---

203 Aanbeveling geput uit het onderzoek 'II.8. Klacht over de wijze waarop de VSSE de zaakvoerder van een bedrijf opvolgt'.

204 Deze aanbeveling komt voor uit het eerste toezichtonderzoek naar de onthullingen van Edward Snowden (II.1. De Snowden-onthullingen en de informatiepositie van de Belgische inlichtingendiensten).

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

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 2014 TOT 31 DECEMBER 2014)

Reglement van de Kamer van volksvertegenwoordigers – Wijzigingen, *BS* 21 mei 2014
Reglement van de Kamer van volksvertegenwoordigers – Wijziging, *BS* 31 oktober 2014

Wet 13 januari 2014 tot wijziging van de wet van 10 april 1990 tot regeling van de private en bijzondere veiligheid, *BS* 23 januari 2014
Wet 6 januari 2014 tot wijziging van diverse wetten ten gevolge van de hervorming van de Senaat, *BS* 31 januari 2014
Wet 19 november 2013 tot wijziging van de wet van 5 februari 2007 betreffende de maritieme beveiliging, *BS* 4 maart 2014
Wet 18 maart 2014 betreffende het politionele informatiebeheer en tot wijziging van de wet van 5 augustus 1992 op het politieambt, de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en het Wetboek van strafvordering, *BS* 28 maart 2014
Wet 27 maart 2014 houdende diverse bepalingen inzake elektronische communicatie, *BS* 28 april 2014
Wet 24 maart 2014 tot wijziging van de wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstintegrator, *BS* 2 mei 2014
Wet 25 april 2014 houdende diverse bepalingen, *BS* 7 mei 2014
Wet 5 mei 2014 ter verbetering van verschillende wetten inzake justitie, *BS* 8 juli 2014
Wet 15 mei 2014 tot wijziging van de wet van 9 december 2004 betreffende de wederzijdse internationale rechtshulp in strafzaken en tot wijziging van artikel 90*ter* van het Wetboek van strafvordering en tot wijziging van de wet van 5 augustus 1992 op het politieambt, *BS* 7 augustus 2014

K.B. 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, *BS* 19 december 2013
K.B. 29 januari 2014 tot wijziging van het koninklijk besluit van 14 januari 1994 houdende het statuut van de administrateur-generaal en de adjunct-administrateur-generaal van de Veiligheid van de Staat, *BS* 4 februari 2014

K.B. 26 januari 2014 tot wijziging van het koninklijk besluit van 3 juni 2007 betreffende de bewapening van de geïntegreerde politie, gestructureerd op twee niveaus, alsook de bewapening van de leden van de Diensten Enquêtes bij de Vaste Comités P en I en van het personeel van de Algemene Inspectie van de federale politie en van de lokale politie, *BS* 7 februari 2014

K.B. 16 februari 2014 betreffende het in aanmerking nemen voor het pensioen van de waarderingstoelagen toegekend aan sommige ambtenaren van de buitendiensten van de Veiligheid van de Staat, *BS* 11 maart 2014

K.B. 10 april 2014 tot wijziging van het koninklijk besluit van 28 september 1984 tot uitvoering van de wet van 19 december 1974 tot regeling van de betrekkingen tussen de overheid en de vakbonden van haar personeel, *BS* 30 april 2014

K.B. 24 april 2014 tot opheffing van het koninklijk besluit van 3 augustus 1950 tot oprichting van een ministerieel comité voor verdediging, *BS* 13 mei 2014

K.B. 25 april 2014 tot uitvoering voor de buitendiensten van de Veiligheid van de Staat, van artikel 15*septies* van de wet van 8 april 1965 tot instelling van de arbeidsreglementen, *BS* 30 juni 2014

K.B. 8 mei 2014 tot wijziging van het koninklijk besluit van 5 december 2006 betreffende het algemeen bestuur en de ondersteuningscel van de Veiligheid van de Staat, *BS* 22 mei 2014

K.B. 4 juli 2014 tot vaststelling van het statuut van bepaalde burgerlijke ambtenaren van het stafdepartement inlichtingen en veiligheid van de Krijgsmacht, *BS* 18 juli 2014

K.B. 25 juli 2014 tot wijziging van het koninklijk besluit van 21 december 2011 houdende aanwijzing van de leden van het Ministerieel Comité voor inlichting en veiligheid, *BS* 6 augustus 2014

K.B. 29 juni 2014 tot bepaling van de beroepen of activiteiten die niet beschouwd worden als activiteiten zoals bedoeld in artikel 1 van de wet van 10 april 1990 tot regeling van de bijzondere en private veiligheid, *BS* 27 augustus 2014

K.B. 21 juli 2014 tot wijziging van het koninklijk besluit van 16 mei 2004 betreffende de bestrijding van de mensensmokkel en mensenhandel, *BS* 1 september 2014

K.B. 23 augustus 2014 houdende organisatie van de 'Belgian Task Force for International Criminal Justice (BTF ICJ)', *BS* 5 september 2014

K.B. 4 september 2014 tot wijziging van het koninklijk besluit van 5 december 2006 betreffende het algemeen bestuur en de ondersteuningscel van de Veiligheid van de Staat, *BS* 12 september 2014

K.B. 25 september 2014 tot wijziging van het koninklijk besluit van 21 december 2011 houdende aanwijzing van de leden van het Ministerieel Comité voor inlichting en veiligheid, *BS* 2 oktober 2014

K.B. 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België, *BS* 21 november 2014

K.B. 10 oktober 2014 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* 3 december 2014

K.B. 26 november 2014 houdende gedeeltelijke verdeling van het provisioneel krediet ingeschreven op het programma 14-53-5 van de algemene uitgaven begroting voor het begrotingsjaar 2014 en bestemd voor de looncompensatie en de terugbetaling van vergoedingen en van kosten verbonden aan de ontplooiing en het functioneren van leden

van de Federale politie, van vertegenwoordigers van de Magistratuur en van personeelsleden van Justitie, van BuZa, van BiZa, van Financiën, van het OCAD, van Defensie en andere overheidsdiensten belast met zendingen in het buitenland, *BS* 5 december 2014

M.B. 5 februari 2014 tot wijziging van het ministerieel besluit van 4 april 2006 houdende aanwijzing van een selectiecomité belast met de evaluatie van de kandidaturen voor de post van administrateur-generaal van de Veiligheid van de Staat, *BS* 7 februari 2014

M.B. 10 maart 2014 tot bepaling van de wapens en de munitie die behoren tot de voorgeschreven uitrusting van de personeelsleden van de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht en tot vaststelling van de bijzondere bepalingen betreffende het voorhanden hebben, het bewaren, het dragen, het vervoeren en het gebruiken van de bewapening, *BS* 30 april 2014

M.B. 8 mei 2014 houdende overdracht van bevoegdheid door de Minister van Landsverdediging inzake het plaatsen en uitvoeren van overheidsopdrachten voor aanneming van werken, leveringen en diensten, inzake vervreemding en diverse uitgaven, *BS* 27 mei 2014

M.B. 7 oktober 2014 houdende aanwijzing van een selectiecomité belast met de evaluatie van de kandidaturen voor de post van stafdirecteur van de Veiligheid van de Staat, *BS* 17 oktober 2014

Besluit van de Brusselse Hoofdstedelijke Regering 3 april 2014 tot uitvoering van de Ordonnantie van 20 juni 2013 betreffende de in-, uit-, doorvoer en overbrenging van defensiegerelateerde producten, ander voor militair gebruik dienstig materiaal, ordehandhavingsmateriaal, civiele vuurwapens, onderdelen, toebehoren en munitie ervan, *BS* 17 juli 2014

Omzendbrief GPI 78L betreffende de informatieverwerking ten voordele van een geïntegreerde aanpak van terrorisme en gewelddadige radicalisering door de politie, *BS* 17 februari 2014

Ordonnantie 8 mei 2014 betreffende de oprichting en organisatie van een gewestelijke dienstintegrator, *BS* 6 juni 2014

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten – Benoeming van een tweede Nederlandstalig plaatsvervangend lid – Oproep aan de kandidaten, *BS* 13 januari 2014

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Directeur van de Dienst Enquêtes – Benoeming, *BS* 30 januari 2014

Vacante betrekking van administrateur-generaal en adjunct-administrateur-generaal van de Veiligheid van de Staat, Oproep tot kandidaten, *BS* 4 februari 2014

Personeel – Aanstelling van een titularis van een managementfunctie, *BS* 10 april 2014

Personeel – Aanstelling van een titularis van een managementfunctie, *BS* 28 april 2014

Vergelijkende selectie van Nederlandstalige analisten (m/v) (niveau A) voor de Veiligheid van de Staat (ANG14274), *BS* 5 september 2014

Vergelijkende selectie van Franstalige analisten (m/v) (niveau A) voor de Veiligheid van de Staat (AFG14260), *BS* 5 september 2014

Vacante betrekking van stafdirecteur van de Veiligheid van de Staat – Oproep tot kandidaten, *BS* 7 oktober 2014

Vergelijkende selectie van Nederlandstalige netwerkbeheerders (m/v) (niveau B) voor de Veiligheid van de Staat (ANG14343), *BS* 5 november 2014

Vergelijkende selectie van Nederlandstalige analisten-programmeurs (m/v) (niveau B) voor de FOD Justitie (ANG14354), *BS* 13 november 2014

Vergelijkende selectie van Franstalige analisten (AFG14295), *BS* 13 november 2014

Vacante betrekking van stafdirecteur van de Veiligheid van de Staat – Oproep tot kandidaten – Erratum, *BS* 23 december 2014

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 2014 TOT 31 DECEMBER 2014)

Senaat

Wetsvoorstel ter verbetering van verschillende wetten inzake justitie, *Parl. St.* Senaat 2013-14, nrs. 5-2326/1 en 5-2326/2

Wetsontwerp betreffende het politionele informatiebeheer en tot wijziging van de wet van 5 augustus 1992 op het politieambt, de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en het Wetboek van strafvordering, *Parl. St.* Senaat 2013-14, nr. 5-2366/3 en *Hand.* Senaat 2013-14, 6 februari 2014, nr. 5-139, 49

Voorstel tot oprichting van een parlementaire onderzoekscommissie belast met het onderzoek naar de rol van inlichtingendiensten in cyberspionage, *Parl. St.* Senaat 2013-14, nr. 5-2475/1

Wetsontwerp tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, *Parl. St.* Senaat 2013-14, nrs. 5-2746/1 tot 5-2746/3, *Hand.* Senaat 2013-14, 20 maart 2014, nr. 5-145, 61 en *Hand.* Senaat 2013-14, 3 avril 2014, nr. 5-148, 44

Voorstel van resolutie betreffende de samenwerking met buitenlandse veiligheids- en inlichtingendiensten, *Parl. St.* Senaat 2013-14, nr. 5-2849/1

Activiteitenverslag 2012 van het Vast Comité I, *Parl. St.* Senaat 2013-14, nr. 5-2426/1

Benoeming van een tweede Nederlandstalig plaatsvervangend lid van het Vast Comité van toezicht op de inlichtingendiensten (Comité I), *Parl. St.* Senaat 2013-14, nr. 5-2495/1 en *Hand.* Senaat 2013-14, 20 februari 2014, nr. 5-141, 41 en *Hand.* Senaat 2013-14, 13 maart 2014, nr. 5-144, 47

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, jaarverslag voor 2013 – ter Griffie gedeponeerd, *Hand.* Senaat 2014-15, 5 december 2014, nr. 6-7, 42

Kamer van Volksvertegenwoordigers

Wetsvoorstel tot wijziging van de wet 29 juli 1934 waarbij de private milities verboden worden, wat het verbod van ondemocratische groepering betreft, *Parl. St.* Kamer 2013-14, nr. 53K0809/014

Wetsontwerp houdende diverse bepalingen inzake elektronische communicatie, wetsontwerp tot wijziging van de wet van 6 juli 2005 betreffende sommige juridische bepalingen inzake elektronische communicatie, alsook de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, *Parl. St.* Kamer 2013-14, nrs. 53K3318/001 en 53K3318/004

Voorstel tot oprichting van een parlementaire onderzoekscommissie belast met het onderzoek naar de rol van inlichtingendiensten in cyberspionage, *Parl. St.* Kamer 2013-14, nr. 53K3341/001 en *Hand.* Kamer 2013-14, 6 februari 2014, CRIV53PLEN183, 42

Wetsontwerp tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse, *Parl. St.* Kamer 2013-14, nrs. 53K3376/001 en 53K3376/002 en *Hand.* Kamer 2013-14, 13 maart 2014, CRIV53PLEN189, 118

Wetsontwerp houdende eerste aanpassing van de Algemene uitgavenbegroting voor het begrotingsjaar 2014, *Parl. St.* Kamer 2013-14, nr. 53K3388/004

Wetsontwerp houdende diverse bepalingen, *Parl. St.* Kamer 2013-14, nr. 53K3413/007

Voorstel van technische wijzigingen van het Reglement van de Kamer van volksvertegenwoordigers ten gevolge van de zesde staatshervorming, *Parl. St.* Kamer 2013-14, nr. 53K33463/001

Voorstel tot wijziging van de artikelen 39 en 149 van het Reglement van de Kamer van volksvertegenwoordigers, *Parl. St.* Kamer 2013-14, nr. 53K3465/001

Wetsontwerp ter verbetering van verschillende wetten inzake justitie, *Parl. St.* Kamer 2013-14, nr. 53K3531/001

Lijst van verslagen, balansen en rekeningen die krachtens wetgevende bepalingen aan de Kamer werden overgezonden, *Parl. St.* Kamer 2014-15, nr. 54K0012/001

Beleidsverklaring, *Parl. St.* Kamer 2014, nrs. 54K0020/015, 54K0020/018, 54K0020/032, 54K0020/041 en 54K0020/056

Wetsvoorstel tot wijziging van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, *Parl. St.* Kamer 2014, nr. 54K0164/001

Voorstel van resolutie betreffende de hulp aan de natie, voor een burgergericht leger, *Parl. St.* Kamer 2014, nr. 54K0226/001

Voorstel van resolutie over de aanscherping van de cyberveiligheid in België, *Parl. St.* Kamer 2014, nr. 54K0257/001

Voorstel tot wijziging van artikel 149 van het Reglement van de Kamer van volksvertegenwoordigers betreffende de samenstelling van de commissie belast met de begeleiding van het Vast Comité P en het Vast Comité I, *Parl. St.* Kamer 2014-15, nrs. 54K0393/001 tot 54K0393/006

Herziening van de Grondwet – Herziening van artikel 10, tweede lid, tweede zinsdeel, van de Grondwet, *Parl. St.* Kamer 2014, nr. 54K0417/001

Ontwerp van Algemene Uitgavenbegroting voor het begrotingsjaar 2015, *Parl. St.* Kamer 2014-15, nrs. 54K0496/001, 54K0496/004, 54K0496/014, 54K0496/035 en 54K0496/036

Verantwoording van de Algemene Uitgavenbegroting voor het begrotingsjaar 2015, *Parl. St.* Kamer 2014-15, nrs. 54K0497/002, 54K0497/003, 54K0497/007, 54K0497/008, 54K0497/010 en 54K0497/013

Voorstel tot oprichting van een parlementaire onderzoekscommissie belast met het onderzoek naar de rol van inlichtingendiensten in cyberspionage, *Parl. St.* Kamer 2014-15, nr. 54K0552/001

Wetsvoorstel tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, aangaande het toezicht op de activiteiten van de buitenlandse inlichtingendiensten in België, *Parl. St.* Kamer 2014-15, nr. 54K0553/001

Algemene beleidsnota, *Parl. St.* Kamer 2014-15, nrs. 54K0588/001, 54K0588/018, 54K0588/22 en 54K0588/029

Wetsontwerp houdende de middelenbegroting voor het begrotingsjaar 2015 (495/1-6) – Ontwerp van algemene uitgavenbegroting voor het begrotingsjaar 2015 (496/1-43) – Begrotingen van ontvangsten en uitgaven voor het begrotingsjaar 2015. Algemene toelichting (494/1) – Verantwoording van de algemene uitgavenbegroting voor het begrotingsjaar 2015 (497/1-23) – Beleidsnota's (588/1-36), *Hand.* Kamer 2014-15, 17 december 2014, CRIV54PLEN022, 1

Activiteitenverslag 2012 van het Vast Comité I, *Parl. St.* Kamer 2013-14, nr. 53K3496/001

Benoeming van de bijzondere commissies, *Hand.* Kamer 2014, 17 juli 2014, CRIV-54PLEN003, 11

Gedachtewisseling met de staatssecretaris voor Leefmilieu en de minister van Binnenlandse Zaken over de problematiek van de elektriciteitsbevoorrading, *Hand.* Kamer 2014, 22 augustus 2014, CRIV54COM003, 5

Hoorzittingen over de problematiek van de elektriciteitsbevoorrading en het afschakelplan, *Hand.* Kamer 2014, 23 september 2014, CRIV54COM007, 1

Gedachtewisseling over de toestand in Irak en de eventuele deelneming van België aan de internationale coalitie, *Parl. St.* Kamer 2014, nr. 54K0305/001 en *Hand.* Kamer 2014, 26 september 2014, CRIV54PLEN005, 2

Gedachtewisseling over de debriefing over de te Parijs op 15 september 2014 gehouden internationale conferentie over Irak en de eventuele deelneming van België aan de internationale coalitie, *Parl. St.* Kamer 2014, nr. 54K0344/001

Inoverwegingneming van voorstellen, *Hand.* Kamer 2014, 7 oktober 2014, CRIV-54PLEN006, 3

Hervatting van de bespreking van de verklaring van de regering, *Hand.* Kamer 2014-15, 16 oktober 2014, CRIV54PLEN011, 1

Commissie belast met de begeleiding van het Vast Comité P en het Vast Comité I, *Hand.* Kamer 2014-15, 13 november 2014, CRIV54PLEN015, 48

Rekeningen van het begrotingsjaar 2013 van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten (680/1), *Hand.* Kamer 2014-15, 18 december 2014, CRIV-54PLEN024, 99

Rekeningen van het begrotingsjaar 2013 van de BIM-Commissie (680/1), *Hand.* Kamer 2014-15, 18 december 2014, CRIV54PLEN024, 100

Aanpassing van de begroting van het begrotingsjaar 2014 van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten (680/1), *Hand.* Kamer 2014-15, 18 december 2014, CRIV54PLEN024, 101

Begrotingsvoorstellen voor het begrotingsjaar 2015 van het Vast Comité van toezicht op de politiediensten (680/1), *Hand.* Kamer 2014-15, 18 december 2014, CRIV54PLEN024, 103

Begrotingsvoorstellen voor het begrotingsjaar 2015 van de BIM-Commissie (680/1), *Hand.* Kamer 2014-15, 18 december 2014, CRIV54PLEN024, 104

Activiteitenverslag 2013 van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten, *Parl. St.* Kamer 2014-15, nr. 54K0720/001

BIJLAGE C
OVERZICHT VAN INTERPELLATIES, VRAGEN OM UITLEG EN MONDELINGE EN SCHRIFTELIJKE VRAGEN MET BETREKKING TOT DE WERKING, DE BEVOEGDHEDEN EN HET TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN EN HET OCAD (1 JANUARI 2014 TOT 31 DECEMBER 2014)

Senaat

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over 'handel in illegale diamanten – witwaspraktijken – onderzoeken' (Senaat 2011-12, 28 december 2011, Vr. nr. 5-4620)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over 'mensenhandel en -smokkel – strafrechtelijke veroordelingen – daling – redenen' (Senaat 2011-12, 28 december 2011, Vr. nr. 5-4662)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over 'spionage in België' (Senaat 2011-12, 6 februari 2012, Vr. nr. 5-5495)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over 'externe servers – Cloud computing – Amerikaanse opsporingsdiensten – Patriot Act – privacywetten – beleid' (Senaat 2012-13, 23 oktober 2012, Vr. nr. 5-7189)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over 'Veiligheid van de Staat – jaarverslag – buitenlandse veiligheids- en spionagediensten – bevriende naties' (Senaat 2012-13, 23 november 2012, Vr. nr. 5-7364)

Schriftelijke vraag van N. Lijnen aan de eerste minister over 'overheidsdiensten – cyberaanvallen – computerbeveiliging – beveiligingssoftware – opleiding personeel' (Senaat 2012-13, 13 december 2012, Vr. nr. 5-7566)

Schriftelijke vraag van N. Lijnen aan de minister van Buitenlandse Zaken over 'overheidsdiensten – cyberaanvallen – computerbeveiliging – beveiligingssoftware – opleiding personeel' (Senaat 2012-13, 13 december 2012, Vr. nr. 5-7568)

Schriftelijke vraag van N. Lijnen aan de minister van Binnenlandse Zaken over 'overheidsdiensten – cyberaanvallen – computerbeveiliging – beveiligingssoftware – opleiding personeel' (Senaat 2012-13, 13 december 2012, Vr. nr. 5-7571)

Schriftelijke vraag van Y. Vastersavendts de minister van Justitie over 'aanslagen jegens Israëlische burgers – Bulgarije – toename van de dreiging – maatregelen' (Senaat 2012-13, 18 januari 2013, Vr. nr. 5-7796)

Schriftelijke vraag van Y. Vastersavendts aan de minister van Justitie over 'salafisten – radicalisering – screening – preventie – verklaring Duitse minister van Binnenlandse Zaken' (Senaat 2012-13, 21 januari 2013, Vr. nr. 5-7818)

Schriftelijke vraag van K. Vanlouwe aan de minister van Justitie over 'Europol – terrorismedreiging – aanslagen – statistieken 2012' (Senaat 2012-13, 2 februari 2013, Vr. nr. 5-8064)

Schriftelijke vraag van M. Taelman aan de minister van Justitie over 'Syrië – strijders – radicale terreurgroepen – Jihadreis – Nederlanders – Belgen – terugkeer naar Europa – terrorisme' (Senaat 2012-13, 25 februari 2013, Vr. nr. 5-8286)

Schriftelijke vraag van M. Taelman aan de minister van Justitie over de 'illegale en radicale scholen – Wahabisme – verspreiden van radicalisme – Staatsveiligheid – deradicaliseringsprogramma's' (Senaat 2012-13, 8 maart 2013, Vr. nr. 5-8434)

Schriftelijke vraag van M. Taelman aan de minister van Binnenlandse Zaken over 'haatpredikers – aantallen – lijst – vervolgingen en veroordelingen – Jihad – Syrië' (Senaat 2012-13, 8 maart 2013, Vr. nr. 5-8435)

Schriftelijke vraag van M. Taelman aan de minister van Binnenlandse Zaken over 'Hezbollah – lijst van terreurorganisaties – Belgen' (Senaat 2012-13, 25 maart 2013, Vr. nr. 5-8600)

Schriftelijke vraag van M. Taelman aan de minister van Justitie over 'Rusland – bedrijfsspionage – wapentechnologie – China – preventie – stand van zaken' (Senaat 2012-13, 16 april 2013, Vr. nr. 5-8727)

Schriftelijke vraag van K. Vanlouwe aan de minister van Justitie over de 'fundamentalisme in de gevangenissen – overzicht – opleiding en taken cipiers' (Senaat 2012-13, 23 april 2013, Vr. nr. 5-8856)

Schriftelijke vraag van M. Taelman aan de minister van Justitie over 'privacy – opvorderen gegevens van gebruikers van sociale media – Politie – Staatsveiligheid – Algemene Dienst inlichting en veiligheid – rechtsbescherming – akkoorden – stand van zaken' (Senaat 2012-13, 23 mei 2013, Vr. nr. 5-9087)

Schriftelijke vraag van M. Taelman aan de minister van Binnenlandse Zaken over 'veiligheidsdiensten – afluisteren van onlinecommunicatiediensten – Skype – voice-over-IP (VOIP) – wetgevend initiatief' (Senaat 2012-13, 23 mei 2013, Vr. nr. 5-9090)

Schriftelijke vraag van K. Vanlouwe aan de staatssecretaris voor Sociale Zaken over 'het Computer emergency response team en cyberdefensie' (Senaat 2012-13, 14 juni 2013, Vr. nr. 5-9329)

Schriftelijke vraag van K. Vanlouwe aan de minister van Justitie over 'de cyberveiligheid en cyberdefensie' (Senaat 2012-13, 25 juni 2013, Vr. nr. 5-9406)

Schriftelijke vraag van M. Taelman aan de minister van Landsverdediging over 'het Stratfor-rapport inzake terrorisme in Noord-Afrika' (Senaat 2012-13, 2 juli 2013, Vr. nr. 5-9453)

Schriftelijke vraag van N. Lijnen aan de minister van Landsverdediging over 'de cyberoorlogvoering' (Senaat 2012-13, 2 juli 2013, Vr. nr. 5-9455)

Schriftelijke vraag van B. De Nijn aan de minister van Binnenlandse Zaken over de 'Syriëstrijders – ambtelijke schrappingen – impact – overzicht – samenwerkingsverbanden' (Senaat 2012-13, 3 september 2013, Vr. nr. 5-9834)

Schriftelijke vraag van M. Taelman aan de minister van Buitenlandse Zaken over 'National Security Agency – PRISM – bedrijfsspionage – data van Europese bedrijven – Staatsveiligheid – onderzoek' (Senaat 2012-13, 18 september 2013, Vr. nr. 5-9875)

Schriftelijke vraag van M. Taelman aan de minister van Justitie over 'National Security Agency – PRISM – bedrijfsspionage – data van Europese bedrijven – Staatsveiligheid – onderzoek' (Senaat 2012-13, 18 september 2013, Vr. nr. 5-9876)

Schriftelijke vraag van N. Lijnen aan de minister van Landsverdediging over 'hacking cybercrime – cijfers – hacking' (Senaat 2012-13, 24 september 2013, Vr. nr. 5-9898)

Schriftelijke vraag van B. De Nijn aan de minister van Buitenlandse Zaken over 'Kenia – Al-Shabaab – Somalië – Belgische Jihad-strijders – overzicht – inhouden van paspoorten – rekruteringsgroepen – terugkomst' (Senaat 2012-13, 2 oktober 2013, Vr. nr. 5-9962)

Schriftelijke vraag van B. De Nijn aan de minister van Justitie over 'Kenia – Al-Shabaab – Somalië – Belgische Jihad-strijders – terugkeer – juridische vervolgingen' (Senaat 2012-13, 2 oktober 2013, Vr. nr. 5-9963)

Schriftelijke vraag van K. Vanlouwe aan de minister van Justitie over 'Staatsveiligheid – sociaal overleg – stakingsrecht – stakingsaanvragen' (Senaat 2012-13, 3 oktober 2013, Vr. nr. 5-9988)

Schriftelijke vraag van M. Taelman aan de eerste minister over 'National Security Agency – Belgacom – Swift – afluisterpraktijken – hacking – overzicht – onderzoek – maatregelen' (Senaat 2012-13, 4 november 2013, Vr. nr. 5-10284)

Schriftelijk vraag van N. Lijnen aan de minister van Landsverdediging over 'Syrian Electronic Army – cyberaanvallen – opvolging' (Senaat 2012-13, 18 november 2013, Vr. nr. 5-10407)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over de 'ambassades – spionagenetwerken – spionageapparatuur – personeel – persona non grata' (Senaat 2012-13, 19 november 2013, Vr. nr. 5-10418)

Schriftelijke vraag van B. Anciaux aan de minister van Binnenlandse Zaken over de 'beveiligingsfirma's – vergunnen en toekennen van private bewakingsopdrachten – reputatie – vergunning – gunningscriteria' (Senaat 2012-13, 21 november 2013, Vr. nr. 5-10430)

Schriftelijke vraag van M. Taelman aan de minister van Binnenlandse Zaken over de 'activiteitenverslag Vast Comité I – Staatsveiligheid – opvolgen veroordeelden voor terrorisme – radicalisering in gevangenissen' (Senaat 2013-14, 6 december 2013, Vr. nr. 5-10544)

Schriftelijke vraag van M. Taelman aan de minister van Justitie over het 'activiteitenverslag Vast Comité I – Staatsveiligheid – opvolgen veroordeelden voor terrorisme – radicalisering in gevangenissen' (Senaat 2013-14, 6 december 2013, Vr. nr. 5-10545)

Schriftelijke vraag van M. Taelman aan de minister van Binnenlandse Zaken over de 'inlichtingendiensten – Staatsveiligheid – inbreken op internetfora – opvolgen van internetfora – wettelijke instrumenten' (Senaat 2013-14, 6 december 2013, Vr. nr. 5-10546)

Schriftelijke vraag van K. Vanlouwe aan de minister van Justitie over de 'bezoeken van buitenlandse hoogwaardigheidsbekleders – kostprijs – delegaties van categorie A en B' (Senaat 2013-14, 9 december 2013, Vr. nr. 5-10551)

Schriftelijke vraag van M. Taelman aan de minister van Binnenlandse Zaken over de 'Veiligheid van de Staat – classificatie van documenten – motivering – transparantie' (Senaat 2013-14, 11 december 2013, Vr. nr. 5-10588)

Schriftelijke vraag van M. Taelman aan de minister van Justitie over de 'Veiligheid van de Staat – classificatie van documenten – motivering – transparantie' (Senaat 2013-14, 11 december 2013, Vr. nr. 5-10589)

Schriftelijke vraag van M. Taelman aan de minister van Binnenlandse Zaken over de 'Veiligheid van de Staat – Tshwane Principles – harmonisering – minimumnormen in de Europese Unie' (Senaat 2013-14, 11 december 2013, Vr. nr. 5-10590)

Schriftelijke vraag van M. Taelman aan de minister van Justitie over de 'Veiligheid van de Staat – Tshwane Principles – harmonisering – minimumnormen in de Europese Unie' (Senaat 2013-14, 11 december 2013, Vr. nr. 5-10591)

Schriftelijke vraag van M. Taelman aan de minister van Binnenlandse Zaken over de 'verslag Vast Comité I – inlichtingendiensten – fraude – gerechtelijke onderzoeken – veroordelingen – sancties' (Senaat 2013-14, 20 december 2013, Vr. nr. 5-10701)

Vraag om uitleg van B. Hellings aan de minister van Justitie over 'een mogelijk onderzoek van het federaal parket naar de aanwezigheid van NSA-spyware op servers van Google in Saint-Ghislain' (*Hand*. Senaat 2013-14, 8 januari 2014, nr. 5-268, 6, Vr. nr. 5-4234)

Schriftelijke vraag van B. Anciaux aan de staatssecretaris voor Ambtenarenzaken over 'cloud computing – gebruik – beveiliging – privacy' (Senaat 2013-14, 13 januari 2014, Vr. nr. 5-10855)

Schriftelijk vraag van N. Lijnen aan de eerste minister over 'Syrian Electronic Army – cyberaanvallen – opvolging – link met het Assad-regime' (Senaat 2013-14, 15 januari 2014, Vr. nr. 5-10881)

Schriftelijke vraag van K. Vanlouwe aan de minister van Binnenlandse Zaken over 'Jubelpark – Grote Moskee – islamitisch Cultureel Centrum – Saoedi-Arabië – salafisme – Staatveiligheid' (Senaat 2013-14, 15 januari 2014, Vr. nr. 5-10885)

Schriftelijke vraag van K. Vanlouwe aan de minister van Justitie over 'Jubelpark – Grote Moskee – islamitisch Cultureel Centrum – Saoedi-Arabië – salafisme – Staatveiligheid' (Senaat 2013-14, 15 januari 2014, Vr. nr. 5-10886)

Vraag om uitleg van B. Hellings en K. Vanlouwe aan de minister van Landsverdediging over 'de structurele samenwerking tussen de Algemene Dienst inlichtingen en veiligheid en het National Security Agency' (*Hand*. Senaat 2013-14, 21 januari 2014, nr. 5-274, 5, Vr. nrs. 5-3937 en 4199)

Vraag om uitleg van B. Hellings aan de minister van Landsverdediging over 'het potentiële gebruik van de toezichtinstrumenten van het NSA door de Algemene Dienst inlichtingen en veiligheid in het kader van de opdrachten van het Belgisch leger in Afghanistan' (*Hand*. Senaat 2013-14, 21 januari 2014, nr. 5-274, 8, Vr. nr. 5-3938)

Schriftelijke vraag van M. Taelman aan de minister van over 'het "cybercommando"' (Senaat 2013-14, 22 januari 2014, Vr. nr. 5-10945)

Schriftelijke vraag van M. Taelman aan minister van Landsverdediging over 'de oprichting van de "Joint Sigint Cyber Unit" in Nederland' (Senaat 2013-14, 22 januari 2014, Vr. nr. 5-10946)

Vraag om uitleg van B. De Nijn aan de minister van Binnenlandse Zaken over 'de zwarte lijst van gevaarlijke organisaties' (*Hand*. Senaat 2013-14, 28 januari 2014, nr. 5-277, 14, Vr. nr. 5-4375)

Vraag om uitleg van G. Deprez aan de minister van Binnenlandse Zaken over 'de gegevensuitwisseling tussen de sociale media en de Belgische autoriteiten in het kader van officiële onderzoeken' (*Hand*. Senaat 2013-14, 28 januari 2014, nr. 5-277, 6, Vr. nr. 5-4452)

Schriftelijke vraag van R. Miller aan de minister van Binnenlandse Zaken over 'de Europese coördinatie voor een betere bestrijding van het terrorisme' (Senaat 2013-14, 29 januari 2014, Vr. nr. 5-10994)

Schriftelijke vraag van M. Taelman aan de eerste minister over de 'economische spionage – National Security Agency – Belgische bedrijven – evolutie – maatregelen Nederland' (Senaat 2013-14, 4 februari 2014, Vr. nr. 5-11018)

Schriftelijke vraag van M. Taelman aan de minister van Landsverdediging over de 'veiligheidsdiensten – onderscheppen en delen van informatie – Nederland – National Security Agency – Veiligheid van de Staat – Algemene Dienst inlichting en veiligheid – telefoonrecords – metadata – rechtsgrond' (Senaat 2013-14, 11 februari 2014, Vr. nr. 5-11093)

Schriftelijke vraag van M. Taelman aan de minister van Binnenlandse Zaken over de 'veiligheidsdiensten – onderscheppen en delen van informatie – Nederland – National Security Agency – Veiligheid van de Staat – Algemene Dienst inlichting en veiligheid – telefoonrecords – metadata – rechtsgrond' (Senaat 2013-14, 11 februari 2014, Vr. nr. 5-11094)

Schriftelijke vraag van M. Taelman aan de minister van Justitie over de 'veiligheidsdiensten – onderscheppen en delen van informatie – Nederland – National Security Agency – Veiligheid van de Staat – Algemene Dienst inlichting en veiligheid – telefoonrecords – metadata – rechtsgrond' (Senaat 2013-14, 11 februari 2014, Vr. nr. 5-11095)

Schriftelijke vraag van F. Winckel aan de minister van Binnenlandse Zaken over de 'Olympische Winterspelen van Sotsji – Belgische burgers – veiligheid' (Senaat, 2012-2013, 13 februari 2014, Vr. n° 5-11127)

Vraag om uitleg van M. Taelman aan de minister van Binnenlandse Zaken over 'de giften aan de jihad in Jemen' (*Hand*. Senaat 2013-14, 11 februari 2014, nr. 5-284, 4, Vr. nr. 5-4297)

Mondelinge vraag van K. Vanlouwe aan de minister van Binnenlandse Zaken over 'het aantal Belgische Syriëstrijders' (*Hand*. Senaat 2013-14, 13 februari 2014, nr. 5-140, 20, Vr. nr. 5-1316)

Mondelinge vraag van Z. Khattabi aan de minister van Justitie over 'het nieuwe hoofd van de Veiligheid van de Staat' (*Hand*. Senaat 2013-14, 27 februari 2014, nr. 5-143, 21, Vr. nr. 5-1342)

Schriftelijke vraag van M. Taelman aan de minister van Binnenlandse Zaken over de 'Staatsveiligheid – Tshwane Principles – metadata – regelgeving – opslag – analyse – taps en internetfora' (Senaat, 2012-2013, 12 maart 2014, Q. n° 5-11232)

Mondelinge vraag van K. Vanlouwe aan de minister van Binnenlandse Zaken over 'de Syriëstrijders' (*Hand*. Senaat 2013-14, 13 maart 2014, nr. 5-144, 37, Vr. nr. 5-1359)

Mondelinge vraag van B. Laeremans aan de minister van Justitie over 'het dossier van de zes politieke moorden die toegeschreven zijn aan Abdelkader Belliraj' (*Hand*. Senaat 2013-14, 27 maart 2014, nr. 5-146, 26, Vr. nr. 5-1385)

Schriftelijke vraag van M. Taelman aan de minister van Werk over 'cybercrime – bedrijfsleven – maatregelen' (Senaat 2014-15, 4 december 2014, Vr. nr. 6-275)

Schriftelijke vraag van M. Taelman aan de minister van Ontwikkelingssamenwerking over 'cybercrime – bedrijfsleven – maatregelen' (Senaat 2014-15, 4 december 2014, Vr. nr. 6-276

Kamer van Volksvertegenwoordigers

Vraag van P. Dedecker aan de eerste minister over 'de spionage bij Belgacom' (*Vr. en Ant.* Kamer 2013-14, 8 januari 2014, QRVA 142, 44, Vr. nr. 123)

Samengevoegde vragen van K. Van Vaerenbergh en A. Frédéric aan de minister van Justitie over 'de algemene staking tegen het immobilisme' (*Hand.* Kamer 2013-14, 8 januari 2014, CRIV53COM890, 1, Vr. nrs. 21052 en 21151)

Samengevoegde vragen van P. Logghe aan de vice-eersteminister over 'nieuwe ronselkanalen voor jihadstrijders' (*Hand.* Kamer 2013-14, 8 januari 2014, CRIV53COM890, 21, Vr. nrs. 21258 en 21347)

Vraag van T. Veys aan de minister van Economie over 'het advies van de advocaat-generaal van het Europese Hof van Justitie omtrent de omstreden dataretentierichtlijn' (*Hand.* Kamer 2013-14, 15 januari 2014, CRIV53COM896, 15, Vr. nr. 21268)

Vraag van K. Grosemans aan de minister van Landsverdediging over 'de oprichting van het centrum voor cybersecurity in België' (*Hand.* Kamer 2013-14, 15 januari 2014, CRIV53COM898, 32, Vr. nr. 21324)

Samengevoegde vragen van A. Frédéric en B. Slegers aan de minister van Justitie over 'de wapenwet en de herdenking van WO I' (*Hand.* Kamer 2013-14, 16 januari 2014, CRIV53PLEN180, 25, Vr. nrs. 2203 en 2204)

Vraag van B. Slegers aan de minister van Binnenlandse Zaken over 'de terugkeer van jongeren uit Syrië' (*Vr. en Ant.* Kamer 2013-14, 27 januari 2014, QRVA 145, 245, Vr. nr. 1070)

Vraag van L. Devin aan de minister van Binnenlandse Zaken over 'de Syriëstrijders (*Hand.* Kamer 2013-14, 30 januari 2014, CRIV53PLEN182, 25, Vr. nr. 2249)

Vraag van R. Deseyn aan de minister van Justitie over 'het PRISM-systeem' (*Vr. en Ant.* Kamer 2013-14, 3 februari 2014, QRVA 146, 78, Vr. nr. 1165)

Vraag van Ph. Blanchart aan de minister van Justitie over de 'inlichtingendienst van de Europese Unie (SitCen)' (*Vr. en Ant.* Kamer 2013-14, 3 februari 2014, QRVA 146, 82, Vr. nr. 1115)

Gedachtewisseling met de eerste minister en toegevoegde vragen van G. Dallemagne, J. Galant, B. Weyts, R. Deseyn, M. C. Marghem, I. Emmery en R. Balcaen over 'cyberveiligheid' (*Hand.* Kamer 2013-14, 4 februari 2014, CRIV53COM915, 1, Vr. nrs. 18080, 19454, 19696, 19722, 19822, 20033, 20840, 21941 en 21977)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over de 'moslimstrijders in Syrië en berichtgeving' (*Vr. en Ant.* Kamer 2013-14, 10 februari 2014, QRVA 144, 134, Vr. nr. 929)

Vraag van B. Schoofs aan de minister van Justitie over 'het Rabia-symbool' (*Hand.* Kamer 2013-14, 11 februari 2014, CRIV53COM920, 32, Vr. nr. 22059)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over 'de Amerikaanse waarschuwingen voor aanslagen in Europa' (*Hand.* Kamer 2013-14, 12 februari 2014, CRIV53COM925, 16, Vr. nr. 22149)

Vraag van T. Francken aan de minister van Binnenlandse Zaken over de 'diensten – personeel – syndicale verlofdagen' (*Vr. en Ant.* Kamer 2013-14, 17 februari 2014, QRVA 148, 173, Vr. nr. 1184)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over de 'strijd tegen extremisme – gehanteerde lijst verenigingen en personen' (*Vr. en Ant.* Kamer 2013-14, 17 februari 2014, QRVA 148, 187, Vr. nr. 1287)

Samengevoegde vragen van T. Francken en P. Logghe aan de minister van Justitie over 'het ontnemen van de Belgische nationaliteit van Syriëstrijders' (*Hand.* Kamer 2013-14, 19 februari 2014, CRIV53COM932, 11, Vr. nrs. 22204, 22210 en 22275)

Vraag van T. Francken aan de minister van Binnenlandse Zaken over de 'inzet van de Dienst voor de Veiligheid van de Staat voor de beveiliging van de Koning en zijn entourage' (*Vr. en Ant.* Kamer 2013-14, 24 februari 2014, QRVA 149, 176, Vr. nr. 1312)

Vraag van J. Boulet aan de minister van Justitie over 'de toegang tot de omzendbrieven van het College van procureurs-generaal' (*Hand.* Kamer 2013-14, 12 maart 2014, CRIV53COM948, 2, Vr. nr. 22518)

Vraag van P. Luykx aan de minister van Buitenlandse Zaken over 'de handelsmissie in Turkije – screening van deelnemers' (*Vr. en Ant.* Kamer 2013-14, 17 maart 2014, QRVA 152, 142, Vr. nr. 834)

Samenvoegde vragen van J. Van Esbroek en P. Logghe aan de minister van Binnenlandse Zaken over 'de samenwerking tussen België en Jordanië inzake terrorisme' (*Hand.* Kamer 2013-14, 19 april 2014, CRIV53COM954, 2, Vr. nrs. 22469 en 22490)

Vraag van B. Maertens aan de minister van Landsverdediging over 'de veiligheidsverificatie voor kandidaat-militairen' (*Vr. en Ant.* Kamer 2013-14, 24 maart 2014, QRVA 153, 121, Vr. nr. 667)

Vraag van B. Maertens aan de minister van Landsverdediging over 'de veiligheidsverificatie voor militairen in functie' (*Vr. en Ant.* Kamer 2013-14, 24 maart 2014, QRVA 153, 123, Vr. nr. 666)

Samengevoegde vragen van G. Dallemagne, Ch. Lacroix en K. Grosemans aan de minister van Landsverdediging over 'de Belgian Intelligence Academy' (*Hand.* Kamer 2013-14, 2 april 2014, CRIV53COM968, 3, Vr. nrs. 22074, 22462, 22501, 22749 en 22895)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over 'telefoontaps en afnames van radioverkeer' (*Vr. en Ant.* Kamer 2013-14, 7 april 2014, QRVA 155, 111, Vr. nr. 1414)

Vraag van T. Francken aan de minister van Binnenlandse Zaken over de 'beveiliging van de Koninklijke familie' (*Vr. en Ant.* Kamer 2013-14, 7 april 2014, QRVA 155, 112, Vr. nr. 1434)

Vraag van E. Brems aan de minister van Buitenlandse Zaken over 'de hernieuwde pogingen om de gevangenis van Guantánamo te sluiten' (*Vr. en Ant.* Kamer 2013-14, 14 april 2014, QRVA 156, 91, Vr. nr. 866)

Vraag van E. Brems aan de minister van Binnenlandse Zaken over 'het bezoek van de Chinese president – het weghalen van reclame voor een dansvoorstelling' (*Vr. en Ant.* Kamer 2013-14, 14 april 2014, QRVA 156, 152, Vr. nr. 1503)

Vraag van B. Weyts aan de minister van Overheidsbedrijven over 'Federale overheidsdiensten – het gebruik van de gsm- en internetdata die bekend zijn bij Belgacom' (*Vr. en Ant.* Kamer 2013-14, 14 april 2014, QRVA 156, 188, Vr. nr. 903)

Vraag van B. Weyts aan de minister van Binnenlandse Zaken over 'radicale islamisten in Syrië' (*Vr. en Ant.* Kamer 2013-14, 22 april 2014, QRVA 157, 101, Vr. nr. 860)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over 'de financiële stromen van Arabische of radicaal-islamitische landen naar moskeeën of islamitische verenigingen op het grondgebied van België' (*Vr. en Ant.* Kamer 2013-14, 22 april 2014, QRVA 157, 161, Vr. nr. 1099)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over 'afgetapte telefoongesprekken' (*Vr. en Ant.* Kamer 2013-14, 22 april 2014, QRVA 157, 201, Vr. nr. 1264)

Vraag van B. Schoofs aan de minister van Binnenlandse Zaken over 'de activiteiten van de radicaal islamitische groepering Hizb ut Tahrir' (*Vr. en Ant.* Kamer 2013-14, 22 april 2014, QRVA 157, 218, Vr. nr. 1400)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over 'de gesneuvelde jihadstrijders in Syrië' (*Vr. en Ant.* Kamer 2013-14, 25 april 2014, QRVA 158, 62, Vr. nr. 1161)

Vraag van E. Thiébaut aan de minister van Binnenlandse Zaken over de 'inbraakpoging bij het Studiecentrum voor Kernenergie (SCK) te Mol' (*Vr. en Ant.* Kamer 2013-14, QRVA 159, 80, Vr. nr. 915)

Vraag van K. Degroote aan de minister van Binnenlandse Zaken over de 'detachering van politieambtenaren' (*Vr. en Ant.* Kamer 2013-14, QRVA 159, 175, Vr. nr. 1424)

Vraag van S. Van Hecke aan de minister van Justitie over 'de aankoop van de spionagesoftware FinFisher' (*Hand.* Kamer 2014-15, 5 november 2014, CRIV54COM012, 13, Vr. nr. 134)

Samengevoegde vragen van F. Dewinter en A. Carcaci aan de minister van Binnenlandse Zaken over 'de Moslimbeurs die van 7 tot 10 november in Brussel wordt georganiseerd' (*Hand.* Kamer 2014-15, 6 november 2014, CRIV54COM014, 21, Vr. nrs. 35 en 36)

Vraag van L. Dierick aan de minister van Binnenlandse Zaken over 'de controle op en intrekking van veiligheidsmachtigingen' (*Hand.* Kamer 2014-15, 12 november 2014, CRIV54COM015, 15, Vr. nr. 100)

Samengevoegde vragen van L. Dierick, K. Temmerman en K. Calvo aan de minister van Binnenlandse Zaken over 'de sabotage in de kerncentrale Doel 4' (*Hand.* Kamer 2014-15, 12 november 2014, CRIV54COM015, 32, Vr. nrs. 352, 382 en 444)

Vraag van H. Bonte aan de minister van Binnenlandse Zaken over 'de gevaarlijke perslekken van de veiligheidsdiensten inzake Syriëstrijders' (*Hand.* Kamer 2014-15, 20 november 2014, CRIV54COM016, 12, Vr. nr. 70)

Vraag van K. Grosemans aan de minister van Defensie over de 'veiligheidsverificatie voor kandidaat-militairen en militairen in functie' (*Vr. en Ant.* Kamer 2014-15, QRVA 002, 122, Vr. nr. 7)

Vraag van K. Grosemans aan de minister van Defensie over de 'medische ongeschiktheid in 2013' (*Vr. en Ant.* Kamer 2014-15, QRVA 002, 147, Vr. nr. 23)

Vraag van Ph. Goffin aan de minister van Justitie over 'het religieuze radicalisme in de Belgische gevangenissen' (*Hand.* Kamer 2014-15, 3 december 2014, CRIV54COM033, 33, Vr. nr. 649)

Vraag van P. Luykx aan de minister van Buitenlandse Zaken over de 'beveiliging van diplomatieke en consulaire posten' (*Vr. en Ant.* Kamer 2014-15, QRVA 003, 121, Vr. nr. 18)

Vraag van J.-M. Nollet aan de minister van Energie over het 'overvliegen van de Belgische kerncentrales – overleg tussen het FANC en het OCAD' (*Vr. en Ant.* Kamer 2014-15, QRVA 004, 195, Vr. nr. 18)

Vraag van S. Lahaye-Battheu aan de minister van Justitie over 'gevangenissen – van terreurmisdaden verdachte en voor terreurmisdrijven veroordeelde personen' (*Vr. en Ant.* Kamer 2014-15, QRVA 005, 134, Vr. nr. 31)

Vraag van S. Van Hecke aan de minister van Justitie over 'de informatieuitwisseling tussen inlichtingendiensten' (*Hand.* Kamer 2014-15, 16 december 2014, CRIV54COM040, 23, Vr. nr. 860)

Vraag van S. Van Hecke aan de minister van Justitie over 'het categoriseren van de door de VSSE vergaarde informatie' (*Hand.* Kamer 2014-15, 16 december 2014, CRIV-54COM040, 24, Vr. nr. 861)

RAPPORT D'ACTIVITÉS 2014
ACTIVITEITENVERSLAG 2014

Quis custodiet ipsos custodes ?

Quis custodiet ipsos custodes ? est une série de publications qui a pour objectif de stimuler une discussion approfondie quant au fonctionnement, aux compétences et au contrôle des services de renseignement et de sécurité et du travail de renseignement. Cette série reprend 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 renseignements et de sécurité, rue de Louvain 48, boîte 4 à 1000 Bruxelles (02 286 29 88).

Déjà parus dans cette série

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

PROEF 4

RAPPORT D'ACTIVITÉS 2014

Comité permanent de contrôle des services de renseignements et de sécurité

Comité permanent de contrôle des services
de renseignements et de sécurité

intersentia
Antwerpen – Cambridge

Le présent *Rapport d'activités 2014* a été approuvé par le Comité permanent de contrôle des services de renseignements et de sécurité lors de la réunion du 29 juin 2015.

(*soussignés*)
Guy Rapaille, président
Gérald Vande Walle, conseiller
Pieter-Alexander De Brock, conseiller
Wouter De Ridder, greffier

Rapport d'activités 2014
Comité permanent de contrôle des services de renseignements et de sécurité

ISBN 978-94-000-0614-0
D/2015/7849/123
NUR 823

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS

A.M.	Arrêté ministériel
Ann. parl.	Annales parlementaires
ANS	Autorité nationale de sécurité
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 OCAM	Arrêté royal du 28 novembre 2006 portant exécution de la Loi du 10 juillet 2006 relative à l'analyse de la menace
BIA	*Belgian Intelligence Academy*
BICS	*Belgacom International Carrier Services*
BISC	*Belgian Intelligence Studies Centre*
BSS	*British Security Service (MI5)*
CCB	Centre pour la cybersécurité Belgique
CEDH	Convention européenne des droits de l'homme
CERT	*Computer Emergency Respons Team*
CIA	*Central Intelligence Agency*
CIC	Code d'instruction criminelle
CMRS	Comité ministériel du renseignement et de la sécurité
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
CNS	Conseil national de sécurité
CP	Code pénal
CPVP	Commission de la protection de la vie privée
CRIV	Compte Rendu Intégral – Integraal Verslag
CTIVD	Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (Pays-Bas)
DCSG	Dienst Controle Strategische Goederen
DGCC	Direction générale du centre de crise
Doc. parl.	Documents parlementaires
D&A	Administration des douanes et accises
GCHQ	*Government Communications Headquarters*

HUMINT	*Human intelligence*
IMINT	*Image intelligence*
INT (réglementation)	Compétence d'interception basée sur les articles 259*bis* § 5 du Code pénal et 44*bis* L.R&S
ISTAR	Intelligence Surveillance, Target Acquisition and Reconnaissance
JIB	*Joint information box*
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
L.OCAM	Loi du 10 juillet 2006 relative à l'analyse de la menace
Loi MRD	Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité
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
L.R&S	Loi organique du 30 novembre 1998 des services de renseignement et de sécurité
M.B.	Moniteur belge
MRD	Méthodes de recueil des données
NSA	*National Security Agency*
OCAM	Organe de coordination pour l'analyse de la menace
OE	Office des Étrangers
ONU	Organisation des Nations Unies
OSINT	*Open sources intelligence*
PSE	Potentiel scientifique et économique
Q. et R.	Questions et réponses écrites (Chambre ou Sénat)
SGRS	Service général du renseignement et de la sécurité des Forces armées
SIGINT	*Signal intelligence*
SIS	*Secret Intelligence Service (MI6)*
SPF	Service public fédéral
TIC	Technologies de l'information et de la communication
UE	Union européenne
VPN	*Virtual Private Network*
VSSE	Sûreté de l'État

PRÉFACE

Début janvier 2015, un attentat à la rédaction de l'hebdomadaire satirique français « Charlie Hebdo » fait douze victimes. Presque simultanément, une prise d'otages a lieu dans un supermarché juif à l'est de Paris. Cinq personnes y perdent la vie. À peine quelques jours plus tard, la Belgique est le théâtre d'une action antiterroriste coordonnée de grande envergure, au cours de laquelle plusieurs perquisitions sont menées. Deux combattants syriens de retour en Belgique sont tués lors d'une fusillade à Verviers, et un troisième est blessé. Ces trois hommes étaient surveillés depuis longtemps déjà par les services de renseignement.

Les réactions ne se sont pas fait attendre. Le cabinet restreint a d'emblée dressé une liste de douze mesures de lutte contre le terrorisme et le radicalisme. Parmi ces mesures, la plus visible est peut-être le déploiement de l'armée pour des missions de surveillance.

Plusieurs de ces mesures ont un impact direct sur le fonctionnement des services belges de renseignement et de sécurité : la Circulaire « *foreign fighters* » de septembre 2014 sera adaptée ; le Plan d'action Radicalisme (qui date de 2005) doit être actualisé ; un Conseil national de sécurité est créé ; et les missions de protection des personnes accomplies par la Sûreté de l'État seront transférées à la Police fédérale.

Le Comité permanent R n'a pas attendu les événements de Paris et de Verviers. En 2014, il a déjà mené plusieurs enquêtes de contrôle qui cadrent avec ces décisions gouvernementales. Elles pourront assurément s'avérer utiles lors de la mise en œuvre des mesures proposées.

Ainsi, le Comité a bouclé, au début de l'année 2014, une enquête de contrôle sur la mission légale de protection des personnes par la Sûreté de l'État. Les résultats de cette enquête pourront être exploités lors de la discussion sur le transfert de cette mission de la VSSE à la Police fédérale.

En 2014 encore, l'enquête de contrôle en cours relative au suivi d'éléments extrémistes au sein de l'armée a également été élargie avec des informations sur la problématique syrienne. En outre, le Comité a terminé une enquête sur la manière dont l'Organe de coordination pour l'analyse de la menace gère, analyse et diffuse les informations stockées dans la *Joint information box* (JIB), et ce conformément aux dispositions du Plan Radicalisme.

Toujours en 2014, le Comité a ouvert une enquête sur la collaboration entre la Sûreté de l'État et l'administration pénitentiaire. Le Comité souhaite vérifier plus

particulièrement si l'échange d'informations s'est effectivement amélioré dans la pratique, comme le prévoit le protocole d'accord.

Enfin, la problématique des « *foreign fighters* » et des personnes parties combattre en Syrie ne pouvait évidemment pas être ignorée. Le Comité permanent R a ouvert une enquête sur la position d'information du Service général du renseignement et de la sécurité et de la Sûreté de l'État quant au recrutement, à l'envoi, au séjour et au retour en Belgique de jeunes qui partent ou sont partis en Syrie ou en Irak.

Le Comité permanent R est convaincu que ces enquêtes conduiront à des recommandations étayées, qui seront utiles pour la mise en œuvre des mesures nécessaires dans la lutte contre le radicalisme et le terrorisme, sans toutefois perdre de vue la protection des droits fondamentaux.

En ce qui concerne cet aspect de la protection des droits de l'homme, le Comité permanent R a d'ailleurs, en 2014, collaboré étroitement avec la Commission Libertés civiles, justice et affaires intérieures (LIBE) du Parlement européen, entre autres en vue de finaliser une Résolution faisant suite aux révélations d'Edward Snowden.

Guy Rapaille,
Président du Comité permanent de contrôle
des services de renseignement et de sécurité

1er juin 2015

CHAPITRE I
LE SUIVI DES RECOMMANDATIONS DU COMITÉ PERMANENT R

Chaque année, le Comité permanent R formule, pour les pouvoirs législatif et exécutif, des recommandations qui portent en particulier sur la légitimité, la coordination et l'efficacité de l'intervention des deux services de renseignement belges, de l'OCAM et, dans une moindre mesure, de ses services d'appui.[1] Les recommandations que le Comité a formulées en 2014 figurent au dernier chapitre du présent rapport d'activités. Ce chapitre introductif énumère les principales initiatives[2] que les différents acteurs ont prises dans la lignée des recommandations du Comité permanent R. Ensuite, une attention particulière est accordée aux recommandations que le Comité estime essentielles, mais qui n'ont pas encore été mises en œuvre.

I.1. INITIATIVES ET RÉALISATIONS DANS LA LIGNÉE DES DIFFÉRENTES RECOMMANDATIONS

I.1.1. PRIORITÉS RÉALISABLES

Jusque récemment, la VSSE énumérait, dans le volet opérationnel de ses plans d'action annuels, quelque 150 thématiques qui devaient être suivies de manière « prioritaire active » ou « active ». La VSSE est arrivée elle-même à la conclusion que l'effectif restreint dont elle dispose ne lui permettait pas de déployer les agents de renseignement nécessaires pour chacune de ces problématiques. Le Comité permanent R a estimé que l'élaboration des plans d'action devait prendre en considération l'effectif et les moyens budgétaires et techniques disponibles,

1 Les enquêtes relatives à l'OCAM et aux services d'appui sont menées conjointement avec le Comité permanent P (art. 53, 6° L.Contrôle). Lors de la discussion du Rapport d'activités 2013 du Comité permanent R, la Commission spéciale chargée de l'accompagnement du Comité permanent de contrôle des services de police et du Comité permanent de contrôle des services de renseignement et de sécurité a marqué son accord avec les recommandations qui y figurent (*Doc. parl.* Chambre 2014-15, n° 54K0720/001).

2 Cette énumération n'est pas exhaustive.

tout en se conformant aux choix politiques.[3] En d'autres termes, si les ressources disponibles sont insuffisantes, il convient de raccourcir la liste des priorités. Sinon, cette liste n'est plus qu'une énumération *a priori* irréalisable.

La VSSE a tenu compte de cette recommandation dans son Plan d'action 2014.

I.1.2. LA CRÉATION D'UN CENTRE POUR LA CYBERSÉCURITÉ

À la fin novembre 2014, l'Arrêté royal portant création du Centre pour la Cybersécurité Belgique (CCB) est paru au Moniteur belge.[4] Le CCB est placé sous l'autorité du Premier ministre et est investi de plusieurs missions: superviser, coordonner et veiller à la mise en œuvre de la stratégie belge en matière de cybersécurité; gérer par une approche intégrée et centralisée les différents projets relatifs à la cybersécurité; assurer la gestion de crise en cas de cyberincidents, en coopération avec le Centre de crise du Gouvernement… Le Centre reprend du SPF Technologie de l'Information et de Communication la gestion du service Computer Emergency Response Team (CERT), notamment chargé de détecter, d'observer et d'analyser les problèmes de sécurité en ligne.

En 2011 déjà, le Comité permanent R estimait qu'« *il est indispensable de créer une agence capable de coordonner les activités en matière de sécurité de l'information* ».[5]

I.1.3. FORMATION PERMANENTE ET CONTRÔLE RÉEL DE LA QUALITÉ DES RAPPORTS DE COLLECTE

Dans le travail de renseignement, il n'est pas toujours évident de déterminer, au moment de la collecte, quelles informations se révèleront un jour pertinentes ou non. Il n'empêche qu'il faut respecter les exigences en la matière, telles que celles décrites dans la L.R&S ainsi que dans la Loi relative à la protection de la vie privée (principe de finalité, adéquation, exactitude…). Ce qui signifie, par exemple, que le fait qu'un événement donné soit ou non repris dans un rapport

---

3 COMITÉ PERMANENT R, *Rapport d'activités 2012*, 96 (IX.2.2. La définition et la formulation de priorités réalisables).

4 A.R. du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique, *MB* 21 novembre 2014. Un budget de 719 000 euros serait réservé à cette fin pour 2015. La procédure de sélection en vue de la désignation d'un directeur et d'un directeur adjoint serait bouclée fin juin 2015.

5 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 108 et suiv. (IX.2.3. Recommandations relatives à la sécurité de l'information). Voir aussi à cet égard: Proposition de résolution visant à renforcer la cybersécurité en Belgique, *Doc. parl.* Chambre 2013-14, 54K0257/001.

de collecte, et la manière dont il y est repris, revêtent une importance cruciale. Le Comité a estimé que la procédure à suivre en matière d'input devrait faire l'objet d'une formation permanente et être soumise à un sérieux contrôle de qualité.[6] Dans ce cadre, la VSSE a organisé, en 2014, une formation interne portant sur la rédaction de rapports.

I.1.4. CONTRÔLE DES ACTIVITÉS DE SERVICES DE RENSEIGNEMENT ÉTRANGERS EN BELGIQUE

En 2012, le Comité avait rappelé qu'il soutenait la recommandation du Sénat visant à inscrire dans la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité une compétence spécifique en matière de contrôle (de la légalité) des activités de services de renseignement étrangers sur le territoire belge par la VSSE et le SGRS.[7] Début novembre 2014, une proposition de loi a été déposée à la Chambre des Représentants en vue de mentionner explicitement le contrôle des services de renseignement étrangers dans la loi, en insérant le point suivant dans les articles 7 et 11 L.R&S : *« de vérifier la légalité des activités des services de renseignement étrangers sur le territoire belge »*.[8]

I.1.5. ACCORDS DE TRAVAIL DOCUMENTÉS

La collaboration doit être plus précise, que ce soit entre les services ou entre les services de renseignement et les services de police. Le Comité permanent R a également insisté sur la conclusion d'accords de travail documentés avec d'autres autorités.[9] Dans ce sens, il convient de se réjouir de la conclusion du *« Protocolakkoord tussen de VSSE en de Diensten van de Vlaamse Onderwijsadministratie »*[10] du 27 janvier 2014. Des accords pratiques y sont stipulés pour l'échange mutuel d'informations et de données à caractère

6 COMITÉ PERMANENT R, *Rapport d'activités 2013*, 113.

7 COMITÉ PERMANENT R, *Rapport d'activités 2006*, 128, *Rapport d'activités 2008*, 2 et *Rapport d'activités 2012*, 93. En réaction à cette recommandation, le ministre de la Défense a également prôné une initiative législative qui permettrait le contrôle de la légalité des activités de services de renseignement étrangers sur le territoire belge.

8 Proposition de loi modifiant la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, concernant le contrôle des activités des services de renseignement étrangers en Belgique, *Doc. parl.* Chambre 2014-15, 54K0553/001. Il a également été proposé d'étendre l'article 18/9 L.R&S à l'*« ingérence d'un service de renseignement étranger »*.

9 COMITÉ PERMANENT R, « Aanbevelingen van het Vast Comité I in aansluiting met het Regeerakkoord. Denkpistes voor de minister van Justitie », 11 décembre 2014.

10 « Protocole d'accord entre la VSSE et les services du l'Administration flamande de l'Enseignement » (traduction libre).

personnel, afin que la Sûreté de l'État et l'Administration flamande de l'Enseignement puissent remplir plus efficacement leurs missions légales.

I.1.6. DIRECTIVES RELATIVES AU TRAVAIL HUMINT

Par le passé, entre autres dans le cadre de l'affaire Belliraj, le Comité permanent R a dû constater l'éparpillement des directives relatives au travail avec les informateurs dans différents documents. En plus, ces documents ne donnaient qu'une vue très restreinte de la thématique. C'était d'autant plus problématique que le travail avec les informateurs ne repose que sur une base légale très succincte (art. 18 L.R&S). Bien que le Comité permanent R ait plaidé à plusieurs reprises en faveur de l'élaboration d'une réglementation légale plus détaillée en la matière, aucune initiative législative n'a été prise en ce sens. Aussi le Comité permanent R a-t-il recommandé que la VSSE développe davantage ses directives internes et ses meilleures pratiques en matière de travail avec les informateurs et qu'elle les transcrive dans des notes de service claires.[11] En 2011, les « *Instructies over het werken met menselijke bronnen* »[12] et la note de service sur « *l'évaluation des informations émanant de sources humaines* »[13] ont en grande partie répondu à cette recommandation. À la fin janvier 2014, la VSSE a diffusé une nouvelle note circonstanciée sur la gestion des sources humaines. Le Comité rappelle toutefois que depuis janvier 2011, l'obligation d'édicter des directives concernant le travail avec des sources humaines incombe au Comité ministériel du renseignement et de la sécurité (art. 18 L.R&S), devenu aujourd'hui le Conseil national de sécurité.

I.1.7. PROCESSUS D'ANALYSE OPÉRATIONNELLE

Dans le cadre des recommandations que le Comité a formulées après un audit approfondi de la VSSE, il a été proposé qu'un gestionnaire de processus soit désigné pour la gestion et la mise en œuvre des processus de gestion, des processus principaux et de support. Le Comité a également recommandé de décrire à court terme tous les processus primaires et, à moyen terme, les processus principaux et de support.[14] Le Plan stratégique de la VSSE a posé le principe de l'élaboration d'un processus d'analyse opérationnelle. En janvier 2014, le groupe de travail « Analyse opérationnelle » a décrit ce processus dans une note de service.

---

11 COMITÉ PERMANENT R, *Rapport d'activités 2009*, 84-85 (VIII.2.2. Une directive claire et exhaustive en matière de travail avec les informateurs).

12 « Instructions concernant le travail avec les sources humaines » (traduction libre).

13 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 3.

14 COMITÉ PERMANENT R, *Rapport d'activités 2009*, 84 (VIII.2.1.3. Recommandations en matière de processus de travail – Gestion des processus).

I.1.8. LE STATUT DU PERSONNEL DU SGRS

Dans le cadre de l'audit mené au sein du SGRS, le Comité permanent R a formulé un grand nombre de recommandations, entre autres concernant la gestion et la direction du personnel du service. Le Comité a affirmé qu'il convenait de « *remédier aux nombreuses différences administratives et pécuniaires qui existent entre les différents groupes du personnel au sein du SGRS et entre ceux du SGRS et d'autres services du secteur du renseignement (VSSE et OCAM)* ».[15] Ces différences nuisent en effet à une bonne gestion du personnel. À la mi-juillet 2014, l'Arrêté royal qui fixe le statut des agents civils du département d'état-major Renseignement et Sécurité[16] est paru. Cet arrêté vise à revaloriser la fonction de ces agents, en alignant leur statut administratif et pécuniaire sur celui des agents des Services extérieurs de la Sûreté de l'État, qui remplissent des missions similaires. Plusieurs différences ont été abolies depuis lors.

I.2. RETOUR SUR DES RECOMMANDATIONS ANTÉRIEURES

L'article 35, alinéa 3 L.Contrôle confère au Comité permanent R la mission de faire rapport au Parlement « *lorsqu'au terme d'un délai qu'il estime raisonnable, il constate qu'aucune suite n'a été réservée à ses conclusions, ou que les mesures prises sont inappropriées ou insuffisantes* ». Dans ce cadre, le Comité reprend chaque année une ou plusieurs recommandations qu'il estime essentielles à la lumière de sa double finalité : le fonctionnement efficace des services et la garantie des droits fondamentaux.

Dans ce cadre, le Comité permanent R ne cesse d'insister sur la nécessité d'exécuter les obligations définies dans les articles 19 et 20 L.R&S. Ces articles visent en effet à réglementer l'échange d'informations et la collaboration des services de renseignement belges avec d'autres autorités, y compris étrangères.[17] Le Comité appelle l'attention du Conseil national de sécurité sur cette question délicate.

Le Comité permanent R a recommandé précédemment[18] la mise en place d'une concertation structurée entre les services de renseignement, d'une part, et les services de police (fédérale et locale), d'autre part, afin d'échanger des données par le biais de procédures bien définies. L'absence d'un accord de

15 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 104-107.

16 A.R. du 4 juillet 2014 fixant le statut de certains agents civils du département d'état-major Renseignements et Sécurité des Forces armées, *M.B.* 18 juillet 2014.

17 COMITÉ PERMANENT R, *Rapport d'activités 2010*, 3-4 et *Rapport d'activités 2011*, 5-6. Les Commissions de suivi ont également toujours souscrit à cette recommandation. Pour des informations détaillées à cet égard : COMITÉ PERMANENT R, *Rapport d'activités 2013*, 4-5.

18 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 112-113.

coopération entre ces services constitue sans aucun doute une défaillance dans le système de sécurité belge. Le Comité permanent R a attiré l'attention sur ce point à plusieurs reprises par le passé ; il le rappelle une fois encore, vu l'intérêt capital qu'il revêt.[19]

En 2010, le Comité avait déjà remarqué que le SGRS n'avait pas finalisé les descriptions de processus SIGINT des interceptions. Ce n'est toujours pas le cas. Le Comité permanent R insiste sur l'importance de ces descriptions de processus, puisqu'elles permettront notamment de procéder à des vérifications légales plus performantes. Il recommande dès lors au SGRS de boucler ces descriptions de processus.

19 COMITÉ PERMANENT R, *Rapport d'activités 2006*, 131 ; *Rapport d'activités 2007*, 75 ; et *Rapport d'activités 2009*, 86-87.

CHAPITRE II
LES ENQUÊTES DE CONTRÔLE

En 2014, tout comme en 2013, neuf enquêtes ont été clôturées. Deux enquêtes de contrôle ont été menées à la demande de la Commission de suivi ; cinq enquêtes de contrôle ont été ouvertes après une plainte ou une dénonciation et deux enquêtes ont été ouvertes d'office. Une enquête a été menée conjointement au Comité permanent de Contrôle des services de police.[20] Les sections qui suivent traitent brièvement des neuf rapports finaux (II.1 à II.9).

Ensuite sont énumérées et brièvement décrites les enquêtes toujours en cours (II.10). Dans cette dernière rubrique, il est également fait mention des cinq enquêtes de contrôle ouvertes en 2014. Trois de ces nouvelles enquêtes ont été ouvertes à la suite d'une plainte et deux l'ont été à l'initiative du Comité.

Au total, le Comité a reçu 31 plaintes ou dénonciations en 2014. Après vérification de plusieurs données objectives, le Comité a rejeté 28 de ces plaintes ou dénonciations, soit parce qu'elles étaient manifestement non fondées (art. 34 L.Contrôle), soit parce que le Comité n'était pas compétent pour en traiter les motifs. Dans ces derniers cas, les plaignants ont été renvoyés, si possible, à l'instance compétente. Dans quelques cas, les autorités policières ou judiciaires ont aussi été informées en raison d'un risque potentiel. Comme indiqué ci-dessus, trois plaintes introduites en 2014 ont donné lieu à l'ouverture d'une enquête de contrôle.

[20] Les résumés des enquêtes de contrôle communes repris dans ce rapport d'activités n'ont pas été rédigés sous les auspices des deux Comités, mais par le seul Comité permanent R.

II.1. LES RÉVÉLATIONS D'EDWARD SNOWDEN ET LA POSITION D'INFORMATION DES SERVICES DE RENSEIGNEMENT BELGES

II.1.1. INTRODUCTION

Le 6 juin 2013, *The Guardian*[21] et *The Washington Post*[22] publiaient pour la première fois des informations issues des dizaines de milliers de documents (classifiés) divulgués par Edward Snowden, qui a rempli diverses fonctions dans ou pour des services de renseignement américains. Depuis lors, de nouvelles révélations se sont succédé.

Les informations donnaient un aperçu des programmes secrets, principalement de la National Security Agency (NSA) américaine et du General Communication Headquarters (GCHQ) britannique. Elles révélaient notamment l'existence du programme PRISM, au travers duquel la NSA récoltait massivement des données et métadonnées de télécommunications, et dévoilaient que les services américains, mais aussi britanniques, avaient monté des opérations de renseignement visant certaines institutions internationales et structures de coopération (ONU, UE et G20), et où des « pays amis » étaient également ciblés.

Ces révélations ont constitué le point de départ de nombreuses enquêtes parlementaires, judiciaires et de renseignement à travers le monde, y compris en Belgique. Le 1er juillet 2013, la Commission de suivi du Sénat a demandé au Comité permanent R *« […] een update van de bestaande informatie over de praktijken op het vlak van datamining. Niet alleen de Amerikaanse inlichtingendienst NSA zou dit doen, maar ook het Verenigd Koninkrijk zou massaal gegevens onderscheppen en analyseren. In de tweede plaats wil de begeleidingscommissie dat het Comité I onderzoekt welke de gevolgen zijn voor de bescherming van het economisch en wetenschappelijk potentieel van ons land, en van de wettelijke opdrachten van onze inlichtingendiensten. Ten slotte wenst de begeleidingscommissie dat het Comité I onderzoekt hoe dergelijke praktijken worden getoetst aan de nationale en internationale rechtsregels die de privacy van burgers beschermen.* »[23]

---

21 G. GREENWALD et E. MACASKILL, *The Guardian*, 6 juin 2013 (NSA Taps in to Internet Giant's Systems to Mine User Data, Secret files Reveals).

22 B. GELLMAN et L. POITRAS, *The Washington Post*, 6 juin 2013 (US Intelligence Mining Data from Nine US Internet Companies in Broad Secret Program).

23 « *Une mise à jour des informations existantes sur les pratiques en matière de* datamining [exploration de données]. *Le service de renseignement américain ne serait pas le seul à le pratiquer, la Grande-Bretagne intercepterait et analyserait aussi massivement des données. En second lieu, la commission de suivi veut que le Comité examine quelles sont les conséquences pour la protection du potentiel scientifique et économique de notre pays, une des missions légales de nos services de renseignement. Enfin, la commission de suivi souhaite que le Comité R*

Le Comité permanent R a dès lors ouvert trois enquêtes de contrôle[24], qui sont évidemment étroitement liées. Cela vaut aussi pour une quatrième enquête[25], qui a été initiée à la suite d'une plainte du président de l'Ordre néerlandais des avocats du Barreau du Bruxelles.

La première enquête de contrôle, que résume le présent rapport, apporte une réponse aux questions suivantes :

- De quels moyens les grandes puissances telles que les États-Unis et la Grande-Bretagne disposent-elles pour intercepter et exploiter à grande échelle des données de personnes, organisations, entreprises ou instances établies en Belgique ou qui ont un lien avec la Belgique, et de quelles données s'agit-il (quantitativement *et* qualitativement) ?
- Dans quelle mesure les services de renseignement belges étaient-ils au courant des moyens dont disposent ces grandes puissances (ou dans quelle mesure devaient-ils être au courant au regard de leurs missions légales) ? Des renseignements ont-ils été recueillis à ce sujet ou cela n'a-t-il pas été jugé souhaitable ? Les services belges offrent-ils une protection suffisante en la matière ?
- 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 des services de renseignement belges ?

Dans une première phase de l'enquête, le Comité permanent R souhaitait, en se basant sur des sources ouvertes, avoir la vue la plus précise possible sur la captation massive de données par certains États et sur la manière dont ces États pratiquent l'espionnage politique l'égard d'« États amis ».[26]

Dans le même temps, les informations qui étaient déjà disponibles au Comité ont été analysées et traitées. En outre, les informations diffusées au niveau national et international ont été soigneusement conservées. Enfin, des questions

---

étudie comment de telles pratiques sont évaluées au regard des règles de droit nationales et internationales qui protègent la vie privée des citoyens. » (traduction libre).

24 Outre la présente enquête de contrôle, des enquêtes ont également été ouvertes sur les règles nationales et internationales en vigueur en Belgique en matière de protection de la vie privée à l'égard de la captation massive de données (voir Chapitre II.2) et sur les implications éventuelles du datamining pour la protection du potentiel scientifique et économique du pays (voir Chapitre II.10.7).

25 Enquête de contrôle suite à une plainte d'un Bâtonnier sur l'utilisation d'informations issues des récoltes massives de méta-data d'origine étrangère dans des affaires pénales belges. Voir à ce propos le Chapitre II.3 « L'utilisation dans des enquêtes pénales d'informations émanant de captations massives de données par des services étrangers ».

26 Cette partie de l'enquête de contrôle a été sous-traitée au doctorant Mathias Vermeulen, désigné comme expert. Mathias Vermeulen était *Research Fellow* à la European University Institute (EUI) à Florence et au Centre for Law, Science and Technology Studies à la VU Brussel. Son travail a donné lieu à l'étude intitulée « *Les révélations de Snowden, interception massive de données et espionnage politique* ». Cette étude a été intégralement reprise comme Annexe D du *Rapport d'activités 2013* (pp. 132-187) du Comité permanent R.

et réponses parlementaires, des analyses académiques (étrangères), des plateformes de discussion en ligne… ont été consultées.

Par ailleurs, plusieurs interviews ont été menées. Ainsi, par exemple, un contact a eu lieu à la mi-octobre 2013 entre le Comité permanent R et Laura Poitras (une des journalistes qui a reçu des documents d'Edward Snowden) et Jacob Appelbaum (journaliste d'investigation et développeur de logiciels). Des idées intéressantes sont ressorties de cet entretien. En outre, une tentative pour organiser un entretien avec la délégation de la NSA, qui était en visite en Belgique dans le cadre du *ad hoc EU-US Working Group on Data Protection*, n'a pas abouti. La délégation a fait savoir qu'elle ne disposait pas d'un mandat pour rencontrer le Comité permanent R.

Dans une deuxième phase, il a été demandé aux services de renseignement de répondre par écrit à une série de questions d'enquête ciblées et d'envoyer au Comité un certain nombre de documents relatifs à la thématique traitée. Par la suite, des briefings très complets[27] ont été organisés et des documents supplémentaires ont été demandés. Enfin, lors de réunions, les options stratégiques (déjà arrêtées ou futures) ont été sondées avec, respectivement, la direction de la VSSE et le personnel du SGRS.

Le fait que les deux services ont été désignés comme experts dans le cadre de l'enquête judiciaire relative au piratage du réseau Belgacom/BICS, ne constituait pas un obstacle pour cette enquête de contrôle : les services pouvaient partager avec le Comité toutes les informations utiles et jugées nécessaires.[28]

II.1.2. LES RÉVÉLATIONS D'EDWARD SNOWDEN DANS LEUR CONTEXTE

Depuis la divulgation des premiers *slides* de la NSA, de nouvelles données (extrêmement sensibles) ont été révélées sans discontinuer. Celles-ci mettaient en lumière la captation massive de données et l'espionnage politique et économique de et dans des pays amis. En outre, il est apparu très rapidement que la problématique ne se limitait pas à PRISM, à TEMPORA ou à l'espionnage du G20, comme on le pensait initialement.[29]

---

27 Le Comité a eu pas moins de quatre briefings avec le SGRS, où il a pu compter sur une grande ouverture et un grand professionnalisme de la part du personnel de ce service.

28 L'enquête de contrôle a donné lieu à un volumineux rapport pour les ministres compétents. Certaines parties du rapport ont dû être classifiées « TRÈS SECRET Loi 11.12.1998 », en ce qui concerne le SGRS, et « SECRET Loi 11.12.1998 » en ce qui concerne la VSSE. Le rapport a été soumis pour avis aux services concernés. Leurs remarques ont été examinées et des modifications ont été apportées au texte. Sur la base du rapport classifié, un rapport « Diffusion restreinte » a été rédigé pour le donneur d'ordres. Le présent rapport reprend les éléments les plus importants du rapport « Diffusion restreinte ».

29 À titre exemplatif : la 'Boundless Informant Heat Map' de mars 2013, publiée par G. GREENWALD et E. MAC ASKILL, *The Guardian*, 11 juin 2013 (Boundless Informant : the NSA's secret tool to trace global surveillance data).

Le Comité permanent R a souligné qu'il n'avait pas trouvé d'indications fondées mettant en doute l'authenticité des *slides* d'Edward Snowden. Au contraire, le Comité estimait pouvoir conclure des enquêtes déjà menées que les révélations sur l'existence de captations massives de données et d'espionnage politique et économique par des services amis, étaient, certainement « dans les grandes lignes », véridiques.[30] De plus, aussi en raison du caractère fragmentaire des révélations[31], le fait qu'il n'y avait aucune certitude sur l'interprétation donnée aux *slides* ne changeait en rien cette constatation. Il n'empêche que la prudence reste de mise quant à l'interprétation. Ainsi, par exemple, l'on présumait au départ que la NSA avait écouté des millions de conversations en Norvège et aux Pays-Bas. Or, il s'est avéré qu'il s'agissait d'interceptions de communications que les services de renseignement norvégiens et néerlandais avaient eux-mêmes effectuées à l'étranger, et ce à propos d'opérations militaires. Il est toutefois apparu que des données avaient été partagées, sans plus, avec la NSA.

Dans ce qui suit, les révélations d'Edward Snowden sont placées dans un cadre plus large.

II.1.2.1. La NSA et le GCHQ parmi d'autres…

L'enquête de contrôle s'est exclusivement concentrée sur la captation massive de données par la National Security Agency (NSA) américaine et le Government Communications Headquarters (GCHQ) britannique. Il se peut que dans ces pays, d'autres services encore fassent de la captation massive de données. Et naturellement, les États-Unis et la Grande-Bretagne ne sont pas les seules grandes puissances à procéder de la sorte.

En marge des révélations d'Edward Snowden, les activités des services de renseignement, entre autres, français, allemands et suédois sont abordées. Et bien entendu, il y a aussi les moyens susceptibles d'être déployés par, à titre d'exemple, la Russie et la Chine. Mais, ce qui est au moins aussi important dans ce cadre, ce sont les accords de coopération en matière de *Signals Intelligence* (SIGINT) qui existent entre certains pays. Le plus connu est le dénommé FIVE EYES, qui, outre les États-Unis et la Grande-Bretagne, regroupe le Canada, l'Australie et la Nouvelle-Zélande. Ces pays collaborent très étroitement depuis des décennies. Les communications de données interceptées seraient échangées de manière pratiquement illimitée. De plus, la presse a aussi mentionné, par

---

30 Il convient en outre de tenir compte du fait que ni les autorités américaines ni les autorités britanniques n'ont jusqu'à présent mis en doute l'authenticité des documents divulgués. Tout au plus, l'interprétation qui en a été parfois été donnée dans les sources ouvertes a été contestée.

31 *The Guardian* n'aurait encore publié qu'un pourcent de tous les documents qu'elle a reçus d'Edward Snowden (X, *De Standaard*, 3 décembre 2013 (Amper 1 procent van informatie Snowden gepubliceerd)).

exemple, les NINE EYES et les FOURTEEN EYES, desquels, selon des sources ouvertes, la Belgique faisait également partie.[32]

Enfin, les autorités n'ont pas l'exclusivité de la captation et de l'exploitation massives de données. De grands acteurs privés disposent parfois de moyens similaires, même si la finalité de leurs activités est d'une autre nature la plupart du temps. Pour des raisons évidentes, cette problématique n'a pas été étudiée par le Comité. En effet, elle se situe en dehors de sa sphère de compétences.

II.1.2.2. PRISM et TEMPORA. Entre autres…

Les premières révélations concernaient surtout le programme (américain) PRISM et le programme (britannique) TEMPORA. Il est apparu que ces deux programmes de renseignement sont une source très importante d'informations, mais qu'ils n'étaient certainement pas les seuls. Le Comité a distingué, un peu schématiquement, cinq formes ou techniques de captation massive de données ou « interception non ciblée » de communications et télécommunications (*infra*).

II.1.2.2.1. Interceptions non ciblées et massives

L'enquête de contrôle du Comité s'est limitée aux programmes ou techniques de renseignement, où le recueil est essentiellement « non ciblé » (aussi appelé '*fishing expedition*'). Un gigantesque filet à mailles fines est, pour ainsi dire, lancé, et ce n'est que par la suite que ce qui peut être pertinent et utile est examiné manuellement ou au moyen de processus automatisés.[33] Cela ne concernait donc *pas* la mise sur écoute du trafic téléphonique d'une personne ou d'une instance (bien qu'il puisse s'agir de données nombreuses et sensibles). Une forme pure de captation « non ciblée » est par exemple l'extraction et la conservation de *toutes* les informations qui passent par un câble internet international, pour ensuite effectuer des recherches numériques (le '*data-mining*'). Un autre exemple est la captation de tous les signaux GSM dans une région déterminée.

Cependant, toutes les techniques décrites dans les dossiers d'Edward Snowden ne font nécessairement référence à une captation « massive ». La captation, par exemple, des câbles en fibre optique, est opérée la plupart du temps avec ce que l'on appelle des '*selectors*': un numéro de GSM, une adresse IP ou un terme déterminé (p. ex. « attentat »). Cela signifie que toutes les données qui passent par le câble sont certes examinées sur la base de paramètres dictés au

---

32 E. MACASKILL et J. BALL, *The Observer*, 2 novembre 2013 (Portrait of the NSA: no detail too small in quest for total surveillance).

33 Le Comité a fait remarquer que la captation et l'enregistrement de données et métadonnées est toujours une ingérence dans la vie privée au sens de l'article 8 CEDH, et ce même si ces données ne sont pas examinées ni utilisées.

préalable, mais seules les informations qui répondent à un ou plusieurs critère(s) de sélection sont effectivement extraites et conservées. Dans ce cas, l'appréciation du caractère « ciblé » ou « non ciblé » de la captation dépend en grande partie de la quantité et de la description des '*selectors*'. Lorsque les '*selectors*' restent essentiellement limités à des numéros de GSM ou adresses IP bien déterminés, le recueil de renseignement semble alors plutôt « ciblé » (en supposant évidemment qu'un nombre limité de numéros et d'adresses soit introduit). En revanche, si des critères de sélection très larges sont utilisés (tels que l'usage de certains termes, un nom de domaine (p. ex. '@comiteri.be'), l'utilisation de certains termes sur des moteurs de recherche ou l'utilisation de certaines applications (par exemple les techniques VPN ou TOR), on ne peut alors ignorer que les données sont récoltées de manière non ciblée. Bien que toute la lumière n'ait pas été faite au moment de l'enquête, tout indiquait de façon probante que des captations non ciblées et massives avaient lieu.

En d'autres termes, le caractère « massif » des captations de données peut, dans un premier temps, révéler qu'il s'agit d'une captation « non ciblée ». Mais dans le cadre de cette enquête, le terme « massif » est aussi utilisé dans le sens où l'on capte de façon ciblée, mais d'autant de manières et à partir d'autant de points différents, que l'information qui est captée globalement est « massive ».

II.1.2.2.2. Cinq techniques

Les cinq « techniques » reprises ci-après peuvent à la fois se compléter (par exemple, parce qu'un e-mail ne peut éventuellement pas être lu dans son intégralité via un câble surveillé, il peut être utile de collecter le message entier chez le fournisseur de service) et se chevaucher (une conversation GSM peut être directement extraite des ondes et aussi être extraite d'un câble) :

1. Le recueil en amont ('*upstream*') ou la « saisie » du trafic internet ou téléphonique qui passe par des câbles (en fibre optique) (internationaux), par exemple en plaçant un appareil à des points centraux qui sont exploités par de grands opérateurs télécoms ou en surveillant directement le câble. Cela peut se faire à l'insu ou non de l'opérateur/exploitant du câble[34] ;
2. Le recueil en aval ('*downstream*'), où des données sont captées ou, sous la contrainte ou non, demandées aux opérateurs de télécommunications[35] ;

[34] TEMPORA est, selon les *slides* d'Edward Snowden, le nom de code du programme britannique pour cette forme de captation.

[35] L'exemple le plus connu est le programme PRISM : neuf grandes entreprises de technologie américaines étaient prêtes et/ou étaient/sont obligées de fournir des données d'utilisateurs de manière structurée. Il s'agit de Microsoft, Google, Yahoo !, Facebook, PalTalk, YouTube, Skype, AOL et Apple.

3. L'interception de communications sans fil (signaux radio classiques ou signaux GSM qui passent par des antennes émettrices et des satellites)[36] ;
4. Le piratage ('*hacking*') de systèmes IT d'opérateurs, par exemple, afin d'extraire à l'insu des informations utiles[37] ;
5. La coopération et l'échange de données avec des services partenaires (dans le cadre ou non d'une structure de coopération telle que FIVE EYES).[38]

Cela n'a évidemment aucun sens de capter massivement des données si ces données ne peuvent être ni conservées ni exploitées. Vu les quantités considérables de données générées par l'ensemble des programmes, un *hardware* gigantesque est non seulement nécessaire pour stocker ces données, mais il faut aussi un *software* performant qui permette de trouver l'aiguille dans la botte de foin. Le programme XKEYSCORE permet notamment aux analystes de la NSA de traiter des informations en amont. Une partie de l'analyse se fait sans aucun doute de manière automatisée : des algorithmes recherchent au préalable certains « modèles » et certaines « anomalies » dans les données. Mais il est aussi possible de transmettre des données en vrac à des pays ou à des services partenaires en vue d'une analyse ultérieure.

II.1.2.3. Métadonnées et terrorisme. Entre autres…

Les différents programmes captent non seulement les métadonnées (telles que, par exemple, l'adresse d'expéditeurs et de destinataires, l'identification de connexion, l'heure et la durée, le moyen technique utilisé, la taille d'un fichier…), mais aussi le contenu des messages, si ceux-ci sont envoyés par GSM, téléphone, boîte vocale interne, messageries instantanées, messages de forums en ligne, *clouding*, annexes d'e-mails, Skype…

Les autorités américaines prétendent depuis longtemps que seuls les messages en rapport avec le terrorisme, avec des formes graves de criminalité et avec la prolifération étaient interceptés. Mais ici aussi, les sources ouvertes ont démontré de manière convaincante que l'intérêt et la sphère de compétences, par exemple

---

36 FORNSAT serait le nom de code d'un des programmes visant une telle captation de communications, qui se fait via des satellites. Mais aussi l'interception de communications à partir de dizaines de postes diplomatiques et consulaires américains répartis aux quatre coins du monde (les « F6 SITES »), pourrait être placée sous ce dénominateur.

37 C'était le cas avec BICS, une filiale de Belgacom, qui est responsable du *roaming* de télécommunication dans de grandes zones du globe. Via l'opération SOCIALIST, les Britanniques seraient parvenus à installer un logiciel malveillant techniquement très élaboré, avec la collaboration de la NSA, et ainsi, selon toute vraisemblance, à extraire une quantité énorme de données.

38 Comme le suggèrent des sources ouvertes, il est possible que le service A fasse ce que le service B n'est pas autorisé à faire en vertu de sa législation nationale et inversement, et que les données soient échangées, si bien que les restrictions légales sont *de facto* contournées (X., De Morgen, 22 novembre 2013 (Britse burgers massaal bespioneerd)).

de la NSA, comme fournisseur de l'ensemble de la communauté américaine du renseignement, sont nettement plus larges : il apparaît que les informations économiques et politiques sont également visées.

II.1.2.4. Qu'en est-il des données de et sur des Belges et des données relatives à la Belgique ?

Le Comité permanent R était principalement intéressé par l'éventuelle interception de données qui concernent ou proviennent de personnes, organisations, entreprises ou instances établies en Belgique ou qui ont un lien avec la Belgique. Au final, il y a eu peu d'informations à ce propos. Le Comité a toutefois souligné qu'il serait naïf de conclure que la Belgique est restée hors d'atteinte, certainement en raison de la présence d'organisations internationales importantes sur son territoire. En outre, les révélations comportent toute une série d'éléments qui permettent de conclure que des « données belges » peuvent être interceptées à grande échelle, que ce soit directement (par exemple Belgacom/BICS) ou indirectement (des ressortissants belges utilisent Google, Hotmail, Facebook…).

II.1.2.5. Qu'y a-t-il d'essentiel dans les révélations ?

Il est de notoriété publique que certaines grandes puissances disposent depuis assez longtemps de moyens et de programmes très avancés pour procéder à une captation massive de données. À titre d'exemple, une référence peut être faite ici aux révélations sur le réseau ECHELON et l'affaire SWIFT.

Les révélations d'Edward Snowden font néanmoins apparaître trois nouveaux éléments.

Premièrement, l'espionnage électronique, global et massif, est réalisé à partir de centaines de SIGADS (points de recueil de données) répartis à travers le monde, et ce avec les *hardwares* et *softwares* les plus en pointe et des moyens humains et financiers colossaux. Peu de moyens de communication ou de messages semblent pouvoir échapper à une éventuelle interception. Que cela se soit produit dans un contexte de renseignement n'est pas si surprenant. Par exemple, la technologie de l'Internet, y compris toutes les formes de communications qui passent par l'Internet, offre une source rêvée de données détaillées qui étaient inaccessibles auparavant. La croissance exponentielle de la numérisation de la vie quotidienne a ouvert en même temps une nouvelle ère multidimensionnelle pour le monde du renseignement.

Deuxièmement, il est devenu de plus en plus évident que des grandes puissances pratiquent aussi l'espionnage économique et politique à l'égard de « pays amis », en s'adonnant à des captations massives de données.

Et enfin, le troisième et dernier élément nouveau est qu'aujourd'hui, avec une quasi-certitude, des éléments apportant la preuve de ces captations et de leur

ampleur sont disponibles. Ils le sont sous la forme de documents officiels internes, notamment les *slides* qui ont été divulgués.

II.1.3. ANALYSE JURIDIQUE DE LA COMPÉTENCE DE LA VSSE, DU SGRS ET DE L'OCAM

II.1.3.1. La compétence de la VSSE en matière de suivi de la captation de données et de l'espionnage politique et économique par des services étrangers

En guise de première réaction, la VSSE a déclaré que sa compétence en matière de suivi de la captation massive de données par des services étrangers ressortent des articles 7 et 8 L.R&S. Par la suite, le service a explicitement mis en question sa compétence en matière d'infractions massives à la vie privée. Dans des enquêtes de contrôle précédentes (voir, par exemple, ECHELON[39] et SWIFT[40]), le Comité avait déjà clairement affirmé qu'il incombe à la VSSE de suivre de telles pratiques d'espionnage. Le Comité a dès lors réitéré le fait que, tant en ce qui concerne « les menaces à suivre » (espionnage[41]) qu'en ce qui concerne « les intérêts à défendre » (le potentiel scientifique et économique, la sûreté intérieure sous la forme des « droits de l'homme et libertés fondamentales »[42] et de la sûreté extérieure sous la forme de « souveraineté de l'État »[43]), la Loi organique des services de renseignement offre des points de repère clairs pour suivre la captation massive de données par des services de renseignement étrangers, même s'il s'agit d'un « pays ami » ou d'un « service ami ». En outre, le Comité a souligné qu'il ne s'agissait pas ici de menaces « potentielles », mais bien de menaces « actuelles ».

En 2008, la VSSE déclarait encore « *dat […] het Amerikaanse Echelon systeem […] al geruime tijd door haar diensten [wordt] opgevolgd. Mocht echter uit de toepassing van deze nieuwe Protect America Act een activiteit voortvloeien die een inbreuk zou veroorzaken op één van de wettelijk te beschermen belangen, zal de*

---

39 COMITÉ PERMANENT R, *Rapport d'activités 1999*, 23-46. Ce qui est étonnant, c'est que la VSSE avait elle-même souligné à l'époque au Comité que le suivi du système ECHELON relevait de sa compétence.

40 COMITÉ PERMANENT R, *Rapport d'activités 2006*, 43-44.

41 L'« espionnage » concerne seulement la recherche furtive d'informations détenues par des autorités ; quiconque tente de retrouver des données confidentielles de particuliers ou d'entreprises entre en effet aussi dans le cadre de cette définition (COMITÉ PERMANENT R, *Rapport d'activités 2006*, 39-48, et COMITÉ PERMANENT R, *Rapport d'activités 2012*, 14-28).

42 À cet égard, c'est la vie privée qui est visée en premier lieu.

43 L'écoute illimitée et non autorisée pratiquée sur le territoire d'un État étranger doit également être considérée comme une violation de souveraineté, même si les opérations d'écoute sont conformes au droit de l'État qui les pratique.

VSSE binnen haar wettelijk kader haar inlichtingen mede delen aan de betrokken overheden en bevoegde instanties overeenkomstig de doelstellingen van hun opdrachten. »[44]

Enfin, le Comité a attiré l'attention sur l'article 8 CEDH, qui offre une protection contre les atteintes illégitimes à la vie privée et qui implique une obligation positive pour les États membres du Conseil de l'Europe. Une des manières de réaliser cette obligation positive pourrait consister à inciter les services de renseignement nationaux à détecter des infractions massives et à en faire rapport. Le Comité se réfère aussi à cet égard à la recommandation suivante issue du projet de rapport de la Commission LIBE du Parlement européen : « *Exhorte les États membres à satisfaire immédiatement à l'obligation positive, qui leur incombe au titre de la convention européenne des droits de l'homme, de protéger leurs citoyens des activités de surveillance contraires aux dispositions de la convention, y compris lorsque ces activités visent à garantir la sécurité nationale, réalisées par des pays tiers et à veiller à ce que l'état de droit ne soit pas affaibli par l'application extraterritoriale du droit d'un pays tiers* ».[45] Dans ce sens, les services de renseignemement, entre autres, peuvent être considérés comme un instrument entre les mains des autorités, leur permettant de remplir leur obligation positive émanant de la Convention européenne.

II.1.3.2. La compétence du SGRS en matière de suivi de la captation de données et de l'espionnage politique et économique par des services étrangers

En 1999, le Comité constatait que le « *SGR n'effectue […] pas de recherche active sur le programme 'Echelon', se fondant, d'une part sur le fait qu'il ne s'agit pas d'une de ses compétences définies dans la nouvelle loi organique du 30 novembre 1998 sur les services de renseignements […]* »[46] En 2006, ce point du vue était réitéré à la suite de l'affaire SWIFT.[47] En ce qui concerne la présente enquête de contrôle, le SGRS prétend ne pas être compétent non plus. Le Comité ne pouvait souscrire que partiellement à ce point de vue. Tout d'abord, il n'était pas exclu que les activités d'espionnage de la NSA ou d'autres services amis s'étendaient aussi à la politique de défense belge. Conformément à l'article 11 L.R&S, le SGRS doit faire son travail de renseignement en cas de tentative de « *prendre*

---

44 « que […] le système américain Echelon [est] suivi par ses services depuis un certain temps déjà. Si toutefois une activité découlant de l'application de ce nouveau *Protect America Act* venait à porter atteinte à un des intérêts légaux à protéger, la VSSE communiquerait, dans son cadre légal, ses renseignements aux autorités concernées et aux instances compétentes, conformément aux objectifs de ses missions » (traduction libre).

45 Cette recommandation a été reprise pratiquement intégralement dans le rapport définitif (European Parliament, LIBE Committee Inquiry, *Electronic mass surveillance of EU citizens. Protecting fundamental rights in a digital age. Proceedings, Outcome and Background Documents*, 2013-2014, 29-30).

46 COMITÉ PERMANENT R, *Rapport d'activités 1999*, 41.

47 COMITÉ PERMANENT R, *Rapport d'activités 2006*, 44.

connaissance par voie illicite» d'aspects de la politique de défense. Aussi le Comité a-t-il conclu que le SGRS n'était pas compétent en matière de captation massive de données comme phénomène en tant que tel, mais bien en matière d'espionnage au niveau de la politique de défense. Le Comité a toutefois souligné que pour ce dernier aspect, il n'y avait aucune indication concrète à l'égard de la Belgique dans les révélations d'Edward Snowden.

Par ailleurs, depuis 2010, le SGRS est compétent en matière de protection du PSE à l'égard des entreprises ou des institutions qui sont reprises sur une liste spécifique. À la fin 2012, un projet de liste a été établi par les ministres de la Justice et de la Défense. Malgré l'absence d'approbation formelle de cette liste par Comité ministériel, le SGRS s'estimait compétent, depuis 2013, pour la protection du PSE de ces entreprises. Par conséquent, le service ne pouvait plus faire comme s'il n'avait pas la moindre compétence en matière de suivi de captations massives de données, puisque les entreprises reprises dans la liste peuvent elles aussi être menacées par de telles pratiques.

En 2010 encore, le SGRS a reçu pour mission «*dans le cadre des cyberattaques de systèmes informatiques et de communications 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*» (art. 11 § 1er, 2° L.R&S). Le Comité a déjà attiré l'attention sur le champ d'application limité de cette disposition: si des attaques surviennent dans d'autres SPF ou infrastructures critiques nationales (telles que les réseaux de communication), la réaction ne peut être que défensive, sans que le système ennemi puisse être neutralisé.[48]

II.1.3.3. La compétence de l'OCAM

L'Organe de coordination pour l'analyse de la menace a pour mission principale de réaliser, sur demande ou d'initiative, des analyses sur des menaces ponctuelles ou stratégiques (art. 8 L.OCAM). La compétence de l'OCAM se limite toutefois au «terrorisme et [à] l'extrémisme». Dans le cadre de la présente problématique, l'OCAM n'a donc pas de tâche spécifique.

Par la Loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, l'OCAM s'est vu octroyer une mission supplémentaire: dans certains cas, il doit réaliser des analyses sur des menaces pesant sur des «infrastructures critiques». Ce concept reprend aussi «les communications électroniques publiques». Cependant, la loi cible essentiellement les «risques d'interruption du fonctionnement ou la destruction de l'infrastructure». L'OCAM a affirmé qu'il ne réalisait pas d'analyse de ce genre, ni d'initiative ni sur demande.

48 COMITÉ PERMANENT R, *Rapport d'activités 2011,* 21.

II.1.3.4. La compétence des services de renseignement belges en matière d'interception de communications

Pour les services de renseignement belges, deux réglementations prévalent en matière d'interceptions de communications : la Loi MRD, qui, depuis 2010, autorise tant la VSSE que le SGRS à utiliser des méthodes de renseignement spécifiques et exceptionnelles, et la réglementation INT (art. 259*bis* § 5 du Code pénal en combinaison avec l'art. 44*bis* L.R&S), qui octroie une compétence d'interception spécifique au SGRS.

Aucune des deux lois ne renferme une interdiction de principe à la collecte de données en amont ou en aval, à l'interception de communications sans fil ou au piratage de systèmes IT. Il en est ainsi notamment parce que la réglementation belge en matière d'utilisation de méthodes n'opère pas de distinction entre les communications par câble et les autres, comme c'est par exemple le cas aux Pays-Bas et en Suède. En outre, la loi stipule spécifiquement pour les méthodes MRD que, par exemple, l'intrusion dans des systèmes informatiques peut avoir lieu de différentes manières « *à l'aide ou non de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités* » (art. 18/16 L.R&S). Pour les autres méthodes aussi, le service de renseignement peut tenter d'obtenir les données de différentes manières : directement ou via l'opérateur. De plus, le moyen utilisé pour communiquer (une ligne fixe, un GSM, un téléphone satellite…), la nature de la communication (un message écrit, une parole, son et image), le mode de transmission (par câble ou sans fil) et la nationalité des personnes qui communiquent, n'ont aucune importance, ni dans la Loi MRD ni dans la réglementation INT.

Si une disposition d'interdiction n'est reprise explicitement dans aucune des deux lois, il convient cependant de garder à l'esprit l'existence de plusieurs limites.

Il semble tout d'abord que l'obtention de données de communications auprès d'un opérateur établi en Belgique, à son insu, n'est pas autorisée (comme cela s'est produit lors du piratage de BICS, filiale de Belgacom). L'article 18/17 § 3 L.R&S dispose en effet que « *[s]i une opération sur un réseau de communications électroniques est nécessaire l'opérateur du réseau ou le fournisseur d'un service de communications électroniques est saisi d'une demande écrite du dirigeant du service et est tenu de prêter son concours technique à la suite de cette demande* ».

Par ailleurs, il y a le fait que les communications pouvant être interceptées conformément à la réglementation INT semblent limitées à ce que l'on doit traditionnellement comprendre par une « communication entre personnes » (que ce soit oralement ou par écrit, codé ou non), si bien que, par exemple, un contrôle des sites visités par une personne n'est pas autorisé.

Ce qui est plus important, c'est que la Loi MRD et la réglementation INT comportent une restriction en matière d'application territoriale des possibilités d'interception. Cette restriction peut être résumée comme suit[49] :

- une méthode MRD ne peut pas être mise en œuvre depuis l'étranger ;
- une méthode MRD ne peut pas être mise en œuvre lorsque la communication a lieu à l'étranger[50] ;
- une méthode MRD peut être mise en œuvre depuis le territoire belge pour la partie de la communication qui a lieu en Belgique ;
- sur la base de la réglementation INT, aucune communication partant de la Belgique ne peut être écoutée[51] ;
- sur la base de la réglementation INT, des communications peuvent être écoutées depuis la Belgique quand celles-ci partent de l'étranger ;
- sur base de la réglementation INT, des communications peuvent, selon le droit belge, être écoutées à l'étranger quand celles-ci partent de l'étranger, et ce « *que ce soit dans le cadre d'un conflit armé ou lors de missions humanitaires. Dans cette dernière hypothèse, il appartiendra à la Belgique de démontrer que le dispositif est légitime eu égard aux missions qui ont été confiées à ses troupes militaires en vertu du mandat international sur la base duquel elles pénètrent sur le territoire d'un État étranger.* »[52]

Une dernière restriction réside dans le fait qu'en principe, seules les captations « ciblées » sont autorisées.

---

49 Dans les deux réglementations légales, le champ d'application territorial n'a été mentionné que de manière très sommaire.
Dans la Loi MRD, la disposition concernée (c'est-à-dire « *sur le territoire du Royaume* » – art. 18/1 L.R&S) se rapporte au *lieu d'où* ou *où* (ce n'est pas clair) la méthode peut être appliquée. Le Comité estime que cette réglementation est interprétée avec prudence, dans le sens que la méthode MRD ne peut être mise en œuvre qu'au moment où le signal de la communication à capter se trouve sur le territoire belge. Le SGRS a interprété le règlement MRD en ce sens qu'il peut mettre en œuvre des méthodes MRD à l'étranger, si c'est dans le cadre d'une mission accomplie en Belgique. Le Comité ne pouvait adhérer à ce raisonnement.
Dans le cadre de la réglementation INT, le critère est *le lieu d'où la communication est émise*, et ce indépendamment du lieu où elle arrive ou (d') où elle est interceptée. Le point de départ d'une communication détermine donc la compétence du SGRS (*Doc.parl.* Chambre, 2002-03, 50-2059/001, 9 et suiv.).

50 Cela signifie par exemple que la communication d'une personne qui appelle en Belgique depuis l'étranger peut être interceptée au moment où le signal se trouve en Belgique.

51 D'un point de vue technique, il n'est pas évident pour le SGRS de s'y conformer, vu le *roaming* (mondial) et l'évolution technologique. C'est par exemple le cas avec une conversation téléphonique qui part de la Belgique, mais est interceptée à l'étranger. La plupart du temps, le SGRS n'est pas en mesure de déterminer le point de départ.

52 Cet éclairage a été donné par le fonctionnaire délégué qui, à l'époque, a expliqué au Conseil d'État le projet du gouvernement en matière d'interceptions (*Doc.parl.* Chambre, 2002-03, 50-2059/001, 10 et suiv.). Le Comité permanent R a remarqué que chaque intervention n'entre pas dans le cadre d'un mandat international et que chaque interception n'entre pas dans le cadre d'une décision de déployer des troupes.

Ainsi, la mise en oeuvre d'une méthode MRD « cible » essentiellement une personne ou un groupement. De plus, il convient d'apporter la preuve qu'il existe un lien réel avec une des menaces énumérées dans la loi. La pratique montre elle aussi que les méthodes MRD ne sont pas utilisées de manière non ciblée : en 2012, par exemple, quelque 700 autorisations seulement ont été accordées à la VSSE et au SGRS confondus pour l'obtention de données de communication ou de localisation. Une seule méthode peut évidemment permettre d'obtenir pas mal de données (comme par exemple tout le trafic téléphonique entrant et sortant pendant plusieurs mois) mais, comme cela a été dit, la limite à laquelle les services sont confrontés se situe essentiellement dans le fait que la méthode cible une personne ou un groupement.

En ce qui concerne la possibilité pour le SGRS d'intercepter des communications émises à l'étranger, le législateur n'avait pas à l'esprit d'éventuelles interceptions « exploratoires ». Dans les travaux préparatoires qui ont donné lieu à la révision de la loi de 2003, des limites apparaissent clairement, telles que « *l'interdiction des écoutes exploratoires ou générales* » et le fait qu'il doit y avoir des « *indications sérieuses et que celles-ci soient en rapport avec la menace définie à l'article 11, § 2, de la loi du 30 novembre 1998, qu'il s'agisse selon les hypothèses que vise l'article 44* »[53], le fait que « *la possibilité d'écoute ne peut avoir qu'un caractère accessoire* » et « *doivent être dûment motivées, et il y a lieu de veiller à ce qu'un équilibre existe entre la protection de la vie privée, d'une part, et les risques majeurs en ce qui concerne la sûreté des institutions démocratiques et la perturbation éventuelle de leur fonctionnement, d'autre part.* »[54] Par ailleurs, l'article 44*bis* L.R&S impose que le « Plan d'écoutes » du SGRS mentionne les organisations et les institutions qui feront l'objet d'interceptions de leurs communications dans le courant de l'année à venir. En plus, cette liste doit reprendre la durée prévue pour chaque interception, et il doit ressortir des motivations que l'interception est en rapport avec un des motifs légitimes énumérés à l'article 44*bis* L.R&S.

La réglementation INT a été modifiée en 2010. Donnant suite à une recommandation du Comité permanent R, outre « *la captation, l'écoute, la prise de connaissance et l'enregistrement* » de télécommunications, « *la recherche* » a également été rendue possible. L'objectif était de légitimer une situation existante, illégale, mais nécessaire sur le plan opérationnel. Avant de savoir les fréquences sur lesquelles émet une cible reprise dans le Plan d'écoutes, le SGRS doit écouter toutes les fréquences. Il faut donc « chercher ». Autrement dit, chercher des fréquences ou des signaux sur lesquels émettent les cibles reprises dans le Plan d'écoutes, est légitime. Mais, en l'absence de référence concrète au préalable, il

53 *Doc. parl.* Chambre, n° 50-2059/001, 6.

54 *Doc. parl.* Chambre, 2002-03, n°50-2059/003, 7-8 – Audition de l'ancien président du Comité permanent R.

est interdit de chercher de nouvelles menaces potentielles qui ne figurent pas dans le Plan d'écoutes, en interceptant toutes les fréquences ou tous les signaux.

II.1.3.5. La compétence des services de renseignement belges en matière de recueil de données de services partenaires

L'article 20 L.R&S stipule que les services de renseignement belges doivent veiller à collaborer avec leurs homologues étrangers, ce qui signifie naturellement en premier lieu qu'ils doivent être en mesure de recevoir des informations et des renseignements de leurs partenaires étrangers. Mais cela signifie-t-il aussi que de telles données doivent pouvoir être utilisées ultérieurement si l'on sait ou soupçonne qu'elles ont été recueillies illégalement ou de manière irrégulière ? Et qu'en est-il si un service étranger a recueilli, par exemple, des données relatives à un Belge de manière légale pour ce service et le transmet à son partenaire belge qui n'aurait pas pu obtenir ces données (sans autorisation) ?

Dans le cadre de l'enquête, se posait concrètement la question de savoir si des données obtenues en violation de la vie privée pouvaient être utilisées ultérieurement dans un contexte de renseignement. La Loi du 30 novembre 1998 prévoit seulement une destruction des données quand celles-ci sont recueillies au mépris des règles MRD. Rien n'a été réglé non plus par le Comité ministériel du renseignement et de la sécurité[55], qui en vertu de la loi, doit régler les modalités pratiques de la coopération avec les services étrangers. Dans ce cadre, le Comité permanent R a fait référence à une recommandation reprise dans une Résolution du Parlement européen : *« Invite les États membres à s'abstenir d'accepter des données provenant de pays tiers et ayant été collectées illégalement, ainsi que d'accepter que des gouvernements ou agences de pays tiers effectuent sur leur territoire des activités de surveillance contraires au droit national ou ne satisfaisant pas aux garanties juridiques spécifiées dans les instruments internationaux ou européens, notamment la protection des droits de l'homme au titre du traité UE, de la CEDH et de la Charte des droits fondamentaux de l'Union européenne ».*[56] Cette résolution se situe dans le droit fil de la position adoptée par la VSSE à propos de l'affaire ECHELON : *« La Sûreté de l'État ne se prête pas à des pratiques d'espionnage, ne reçoit pas d'informations illégalement recueillies et ne les utiliserait pas ».*[57] Cela suppose bien entendu que le service destinataire

---

55 Le Comité ministériel a été remplacé par le Conseil national de sécurité, voir A.R. du 28 janvier 2015 portant création du Conseil national de sécurité, *MB* 30 janvier 2015.

56 Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA aux États-Unis, organismes de surveillance dans divers États membres et incidences sur les droits fondamentaux et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188 (INI)). Le président du Comité permanent R, Guy Rapaille, et le Sénateur et membre de l'ancienne Commission de suivi du Sénat, Armand De Decker, ont été entendus par la Commission LIBE, qui préparait cette résolution.

57 *Ann. parl. C.R.I.,* Chambre 1997-98, 16 février 1998, PLEN504, Q. n°740.

s'efforce au moins de retracer la manière dont les renseignements en question ont été obtenus. Toutefois, dans la pratique, les « services de renseignement fournisseurs » gardent en général leurs sources secrètes (et donc l'origine du renseignement), et les « services destinataires » l'acceptent également. Cette forme d'entente fait partie de la culture internationale du renseignement, tout comme la règle du tiers service, le principe du « donnant-donnant » et le devoir de réserve. Ce constat ne signifie cependant pas que le Comité adhère sans nuance à ces principes. Mais ils ne peuvent être abandonnés de manière brusque et unilatérale.

II.1.3.6. La compétence des services de renseignement belges en matière de recueil de renseignements à caractère politique ou économique à l'étranger

La VSSE a pour mission de contrer des menaces, pas en intervenant elle-même, mais en se forgeant une bonne position d'information et en informant à temps de l'existence de menaces imminentes ou actuelles. La VSSE est évidemment aussi intéressée par les informations à caractère politique, communiquées par des personnes ou instances publiques ou privées, qui constituent ou pourraient constituer une menace pour les intérêts entrant dans la sphère de compétences du service, même s'il s'agit de personnes ou d'instances étrangères. En outre, le service n'est bien entendu pas exclusivement à la recherche d'informations accessibles au public. Il a un mandat légal à cet effet. Contrairement à la plupart des services étrangers, la VSSE agit uniquement à partir du territoire belge. Mais, d'un point de vue légal, il n'y a, dans droit belge, aucune interdiction de recueillir effectivement des informations à l'étranger. Il existe cependant une exception majeure à cette règle : les méthodes MRD ne peuvent être mises en œuvre qu'en Belgique (voir II.1.3.4). Une autre différence avec certains services étrangers est que la VSSE ne recherchera pas non plus activement, par exemple, des informations économiques sur des entreprises étrangères dans le but de favoriser des entreprises belges. Cela n'entre pas dans le cadre de sa mission légale. La VSSE doit récolter des informations pour protéger le potentiel économique du pays contre, par exemple, l'espionnage ou l'ingérence par des tiers ; le service ne doit pas espionner lui-même pour aller à la recherche d'informations intéressantes pour des entreprises belges.

Le SGRS n'est pas non plus compétent pour pratiquer le recueil de renseignements à caractère économique. En ce qui concerne « l'espionnage politique », l'analyse diffère à cet égard de celle de la VSSE, en ce que le service de renseignement militaire est bel et bien actif à l'étranger, et ce principalement en soutien à des opérations militaires. Il est évident que des informations à caractère politique peuvent être récoltées à propos de telles opérations.

II.1.3.7. La collaboration avec des services étrangers

Il a déjà été fait mention de l'article 20 L.R&S, qui stipule que les services de renseignement belges doivent veiller à assurer une collaboration avec leurs homologues étrangers. Le troisième paragraphe de cette même disposition assigne au Comité ministériel du renseignement et de la sécurité la mission de définir *« les conditions de la coopération prévue au § 1er du présent article »*. Cependant, le Comité ministériel n'a pas encore édicté de directive. La VSSE a néanmoins rédigé une instruction détaillée (classifiée) relative à la collaboration bilatérale avec des correspondants. Le Comité permanent R a déjà affirmé qu'il considérait cette directive comme valable, mais a attiré l'attention sur le fait que certaines options prises par la VSSE devaient être portées par les responsables politiques, en l'occurrence les membres du Comité ministériel.[58] En outre, un des aspects les plus importants de cette collaboration – quels renseignements peuvent être communiqués à des services étrangers ? – n'a été traité que de manière sommaire.

Au moment de l'enquête, le SGRS travaillait toujours à une note similaire, avec des « critères vérifiables », dans la perspective d'une collaboration avec des services de renseignement étrangers (au sens large). La finalisation de cette note était prévue dans le courant de l'année 2014. Dans le cadre de la présente enquête, le Comité a souligné l'importance d'une telle directive pour le SGRS parce que, après l'approbation du Comité ministériel, elle pourra offrir un cadre légitime et démocratique aux plateformes de coopération desquelles le service de renseignement militaire fait déjà partie.

II.1.4. LA VSSE, LA CAPTATION MASSIVE DE DONNÉES ET L'ESPIONNAGE POLITIQUE ET ÉCONOMIQUE

II.1.4.1. La VSSE a-t-elle pris part aux programmes de la NSA ?

La VSSE n'est ou n'était en aucune manière impliquée dans la captation massive de données par la NSA et le GCHQ. Plus spécifiquement, la VSSE n'avait, par exemple, aucun accès aux programmes PRISM ou XKEYSCORE de la NSA. Elle n'était pas non plus impliquée dans l'espionnage de Belgacom/BICS. D'ailleurs, il apparaît que la VSSE, contrairement au SGRS, n'a de contacts directs avec la NSA qu'à titre exceptionnel. Ces dernières années, le Comité permanent R n'a noté que l'organisation d'une seule réunion, et ce dans le cadre d'une problématique concrète. Le peu de contacts entre la VSSE et la NSA s'explique

[58] Le Comité permanent R a recommandé à la VSSE de transmettre sa directive au Comité ministériel pour approbation (COMITÉ PERMANENT R, *Rapport d'activités 2012*, 97 et *Rapport d'activités 2013,* 4 et 111). Cette recommandation n'a pas encore été suivie d'effet.

par le fait que, en ce qui concerne les États-Unis, le service de renseignement civil correspond principalement avec le FBI et la CIA.

II.1.4.2. Était-il question de captation massive de données par la VSSE ?

Absolument aucun élément n'indique que la VSSE elle-même, ou en collaboration avec d'autres partenaires, aurait procédé à des captations massives de données, ce que la Loi MRD n'autorise d'ailleurs pas. En outre, les méthodes MRD ne peuvent être mises en œuvre à l'étranger. Enfin, il convient d'observer que la VSSE, contrairement au SGRS, n'a pas de compétences d'interception à l'étranger.

II.1.4.3. Qu'en est-il du recueil de renseignements politiques et économiques par la VSSE ?

Comme cela a déjà été expliqué (voir II.1.3.1), la VSSE recueille des informations *« à caractère politique, idéologique, confessionnel ou philosophique »* sur des personnes ou groupements belges ou étrangers qui présentent ou sont susceptibles de présenter une menace pour la sûreté intérieure et extérieure de l'État. Au cours de cette enquête, le Comité n'a pas pu constater que le service n'aurait pas opéré dans le cadre légal. Le Comité n'a pas non plus la moindre indication selon laquelle la VSSE rechercherait activement des informations à caractère économique sur des sociétés étrangères pour, par exemple, les partager avec des entreprises belges.

II.1.4.4. La position d'information de la VSSE avant et après les révélations d'Edward Snowden

Eu égard à sa compétence en la matière, la VSSE était-elle, pouvait-elle être au courant ou avoir entendu du mode opératoire de la NSA et le GCHQ avant les révélations d'Edward Snowden ? Qu'a fait la VSSE après les révélations ? La problématique a-t-elle été suivie, quelles analyses ont été réalisées, quelles autorités étaient concernées… ? Le Comité a dû conclure de la réponse à ces questions que la VSSE a adopté une attitude très passive par rapport à ces révélations.

II.1.4.4.1. La position de la VSSE avant les révélations

Lorsque l'affaire ECHELON éclate en 1998, il apparaît que la VSSE n'est pas au courant de l'existence de ce programme américain, par lequel, entre autres, le trafic européen de téléphone, fax et e-mail était intercepté. Les raisons avancées par la VSSE étaient qu'elle manquait de moyens, tant sur le plan personnel que

sur le plan matériel, et que la mission de protection du PSE venait de lui être assignée.

Un an après son premier rapport sur ECHELON, le Comité a souhaité vérifier si la VSSE avait tenté de s'informer davantage sur le réseau mondial d'écoutes. La réponse était négative. Il a notamment été signalé que le Comité ministériel du renseignement et de la sécurité n'avait pas encore défini « le potentiel scientifique et économique du pays ».

En 2006, la VSSE n'était pas non plus au courant, avant les publications dans la presse, du fait que des services américains étaient en mesure d'épier massivement les données de transactions financières qui étaient échangées via SWIFT. En guise d'explication, le service a invoqué les mêmes arguments. Le Comité permanent R n'a pu y souscrire.[59] D'ailleurs, même après la divulgation de l'affaire, la VSSE n'a pas vraiment fait preuve d'initiative.[60]

En août 2007, le Comité a interrogé la VSSE sur les conséquences éventuelles du *Protect America Act,* en vertu duquel les services de renseignement se voyaient octroyer des compétences élargies pour intercepter toutes sortes de communications. Le service a répondu qu'ECHELON était suivi depuis un certain temps, et que si de l'application de ce nouveau *Protect America Act* devait découler une activité qui porterait atteinte à un des intérêts légaux à protéger, il communiquerait ses renseignements aux autorités compétentes (voir aussi II.1.3.1).

À la fin 2008, la VSSE a informé le Comité qu'elle n'avait encore rédigé aucun rapport sur ECHELON. Selon ses dires, la VSSE surveillerait malgré tout le système ECHELON ou tout système susceptible d'intercepter des communications. Mais aucune menace n'avait encore été détectée pour la sûreté interne et externe ou pour le PSE. La VSSE affirmait néanmoins que le suivi de tels systèmes ne constituait pas une priorité.

Toujours en 2008, la VSSE mettait en garde les membres du Gouvernement contre l'usage des BlackBerry, étant donné que la communication via cet outil (alors très populaire) n'offrait aucune garantie en terme de sécurité. En effet, l'ensemble du trafic de données européen des BlackBerry transitait par la Grande-Bretagne, qui, sur la base de la législation RIPA, pouvait demander les clés de cryptage aux fins de défense de la sécurité nationale ou du bien-être économique du pays. Et la VSSE d'ajouter qu'une législation similaire aux États-Unis avait permis aux autorités américaines d'avoir accès à la base de données de SWIFT. Il s'est avéré que le raisonnement sous-jacent à cet avertissement s'appliquait à de nombreuses formes de captation de données révélées par Edward Snowden : les communications belges ou européennes passent la plupart de temps par l'étranger, où les autorités locales peuvent contraindre des personnes ou des entreprises locales à divulguer ces données. Le Comité

59 COMITE PERMANENT R, *Rapport d'activités 2006*, 47.
60 COMITE PERMANENT R, *Rapport d'activités 2006*, 47-48.

considérait que l'avertissement constituait un bon exemple d'un intérêt actif, mais a constaté qu'à ce moment-là, le service n'avait distillé aucun avertissement général concernant d'autres formes de télécommunications.

Le Comité a dû conclure qu'avant les révélations de 2013, la VSSE était certes au courant que certaines grandes puissances, y compris amies, disposaient d'énormes capacités d'interception, mais qu'elle ne s'imaginait pas que ces interceptions étaient utilisées dans le monde entier aussi massivement et qu'en outre, l'Europe était considérée comme une cible politique et économique. Le Comité a constaté que la VSSE n'avait qu'une vue limitée sur la nature et l'ampleur des pratiques de plusieurs grandes puissances amies, et ce malgré les cas antérieurs, mais aussi les informations qui étaient disponibles dans les sources ouvertes. Le Comité a noté qu'avant les révélations, la VSSE n'avait pas effectué aucune analyse globale pour les autorités, et qu'elle n'avait pas non plus rédigé de notes sur la captation massive de données. Toutefois, les citoyens et les entreprises ont été sensibilisés, par le biais de journées d'étude, d'une brochure et des médias, aux menaces éventuelles ou réelles d'espionnage économique surtout, y compris par des pays amis.

Par ailleurs, depuis l'affaire ECHELON, la hiérarchie n'a, à aucun moment, assigné la mission de suivre de tels phénomènes. Aussi ne retrouve-t-on aucune trace, dans les plans d'action annuels de la VSSE, de « la captation massive de données » ou de « l'espionnage économique et politique par des services amis ». Le thème n'a jamais été évoqué non plus avant les révélations, du moins en ce qui concerne les États-Unis ou la Grande-Bretagne, au sein d'une plateforme de concertation informelle de services de renseignement occidentaux.

II.1.4.4.2. La position de la VSSE après les révélations

Après les révélations, la VSSE a pris trois initiatives. Tout d'abord, les représentants des correspondants américains de la VSSE, de la CIA et du FBI ont été confrontés aux articles de presse. La VSSE n'a cependant jamais reçu de rapport officiel et n'a pas insisté. Deuxièmement, comme dans l'affaire ECHELON, des réponses générales ont été formulées à une série de questions ministérielles et parlementaires. Enfin, la VSSE est intervenue dans la foulée du piratage de Belgacom/BICS, et ce tant en sa qualité d'expert dans le cadre de l'enquête judiciaire que dans le cadre de sa mission de renseignement.

Le Comité a néanmoins dû constater que la VSSE n'a entrepris que peu d'actions, même après les révélations. On ne relève aucune recherche active dans les sources ouvertes, aucune analyse ni aucun compte-rendu. La direction n'a pas donné le signal de suivre cette affaire ni, par exemple, de déterminer si et dans quelle mesure les intérêts belges pourraient être menacés. La Belgique n'a même pas mis la problématique à l'agenda de la plateforme de concertation précitée. En outre, aucune question officielle n'a été adressée au SGRS, alors que ce service,

comme interlocuteur naturel de la NSA, pourrait disposer de davantage d'informations. Le Comité en a conclu que le service ne s'était pas saisi de la problématique et ne voyait pas suffisamment le lien avec ses missions légales.

II.1.4.4.3. Analyse du fonctionnement et de la position de la VSSE avant et après les révélations

Comme cela a été mentionné, tant après l'affaire ECHELON qu'après l'affaire SWIFT, la VSSE a avancé une série d'éléments qui devaient expliquer pourquoi le service n'était pas au courant ou ne pouvait pas être courant des pratiques d'espionnage. Le Comité a observé des progrès significatifs dans chacun de ces domaines : la protection du PSE et des libertés fondamentales a été reprise dans la loi, le Comité ministériel a édicté une directive sur le PSE, le cadre du personnel a été élargi au cours de la dernière décennie, et le service s'est vu octroyer la possibilité de mettre en œuvre des méthodes particulières de renseignement. Cependant, la VSSE n'a qu'à peine suivi le phénomène de la captation massive de données. Le service s'est à nouveau posé la question de savoir comment il aurait pu détecter de telles opérations menées par des services de renseignement étrangers, et si c'était possible dans le cadre légal existant et dans le cadre des moyens disponibles.

Selon le Comité, il aurait été possible pour la VSSE de suivre la captation massive de données, y compris par des pays amis, à un niveau général et pas nécessairement en détail. En outre, elle aurait pu, à intervalles réguliers, briefer et sensibiliser les autorités aux nouvelles pratiques, aux moyens techniques et aux dangers éventuels. La position d'information permettant une telle sensibilisation pouvait être élaborée sur la base de sources ouvertes, d'informations provenant du SGRS et d'autres partenaires étrangers, et ce dans le cadre des moyens disponibles et des méthodes autorisées par la loi.

Par ailleurs, le Comité était d'avis que le suivi par la VSSE de la captation massive de données était non seulement nécessaire pour informer les autorités, et, le cas échéant, pour prendre des mesures de rétorsion, mais aussi pour moderniser ses propres techniques de collecte.

Le Comité permanent R a avancé une série d'autres éléments pour expliquer l'inaction de la VSSE avant et après les révélations d'Edward Snowden.

Tout d'abord, les États-Unis et le Royaume-Uni étant des « pays amis », le service ne voyait aucune raison de modifier ses priorités en matière de contre-espionnage. Le Comité a dès lors constaté que la notion d' « État ami » exerçait une influence considérable sur la position de la VSSE. Cependant, la VSSE semble de plus en plus acquise au concept de « partenaires stratégiques » au lieu de « services amis ».

La VSSE n'a pris aucune initiative pour que cette problématique soit reprise dans le Plan d'action qui devait être approuvé par le ministre de tutelle. Le

Comité permanent R estimait qu'en la matière, les autorités politiques compétentes (c'est-à-dire le ministre de la Justice et/ou le Comité ministériel du renseignement et de la sécurité) ont un rôle à jouer au moment où la VSSE propose ses priorités annuelles. Dans le *Plan d'action 2014*, l'espionnage est à nouveau appréhendé sous l'angle d'une « menace classique ».

Parallèlement, il y a bien entendu le fait que les services américains et britanniques fournissent, selon la VSSE, beaucoup d'informations utiles, et que le service ne veut pas mettre en péril ces flux d'informations.

Par ailleurs, il y a le fait que la connaissance en matière de *signals intelligence* et de leurs moyens techniques en général est moins présente à la VSSE.

Enfin, la VSSE ne considérait pas que l'éventuelle violation massive de la vie privée des citoyens et des entreprises belges était une menace qu'elle devait suivre.

II.1.5. LE SGRS, LA CAPTATION MASSIVE DE DONNÉES ET L'ESPIONNAGE POLITIQUE ET ÉCONOMIQUE

II.1.5.1. Le SGRS a-t-il pris part aux programmes de la NSA ?

Comme pour la VSSE, le Comité permanent R a pu constater que le SGRS n'avait pas pris part au recueil en amont (*upstream*), au recueil en aval (*downstream*) ni au piratage (*hacking*) de systèmes IT. En d'autres termes, le SGRS n'a pas participé à des programmes tels que PRISM, XKEYSCORE ou TEMPORA, et le service n'a pas prêté son concours au piratage du réseau de Belgacom/BICS.[61] En outre, des membres du personnel du SGRS n'ont jamais eu un accès direct à ces programmes ou à ces opérations et n'ont pas reçu de formation.

En ce qui concerne les deux autres « techniques de captation de données » reprises dans cette enquête de contrôle (l'interception de communications sans fil et la collaboration avec des services homologues), la réponse est plus nuancée. Il existe en effet une forme de collaboration du SGRS à des programmes internationaux auxquels participe aussi la NSA, même si cette collaboration est très modeste à la lumière des dossiers d'Edward Snowden. La collaboration se limite à la participation à des interceptions dans des cas très spécifiques et exceptionnels et à la transmission d'informations SIGINT interceptées à la NSA en sa qualité de service partenaire dans le cadre bilatéral et multilatéral. La coopération entre dans le cadre de l'obligation visée à l'article 20 L.R&S (coopérer avec des services étrangers – *supra*) et vise essentiellement la lutte contre le terrorisme et la protection des troupes belges et alliées.

La coopération internationale en matière de SIGINT se concrétise de manière générale au sein de divers forums internationaux qui font l'objet d'une certaine

61 Le service l'a aussi confirmé de manière explicite au Premier ministre.

formalisation (par exemple via un *Memorandum of Understanding* (MOU), conclu au niveau des différents services SIGINT, la plupart du temps sans couverture politique explicite et officielle). Le Comité permanent R a examiné plus en détail deux plateformes de coopération multilatérales SIGINT dont le SGRS est membre : la première existe déjà depuis plusieurs décennies et visait au départ la menace dans un contexte de Guerre froide, et la seconde a été créée dans le cadre d'une opération militaire internationale spécifique en vue de partager les tâches SIGINT sur place. Le Comité est arrivé, entre autres, aux conclusions suivantes :

- La description des objectifs d'une plateforme de coopération est parfois large. Aussi autorise-t-elle en théorie des activités qui, en ce qui concerne la Belgique, pourraient se situer en dehors de la sphère de compétences légales du SGRS.
- L'adhésion à certaines plateformes est soumise au principe *do ut des* : les partenaires sont censés fournir certains efforts, investissements et renseignements. Il est évident que dans le cadre d'une coopération entre un petit et un grand service, il ne peut jamais être question d'un équilibre entre « donner et recevoir ». Mais la valeur ajoutée de la présence d'un plus petit service au sein d'une plateforme de coopération ne se situe pas (exclusivement) dans les informations qu'il peut de fournir, ni dans la prise en charge d'une partie du travail d'analyse ou des coûts. En outre, l'idée selon laquelle il est aussi intéressant pour certains pays de créer, via un réseau, un soutien international plus large pour leurs activités, est plausible.
- Au fil des années (et c'est tout à fait compréhensible), la confiance s'est renforcée entre les pays qui collaborent étroitement en matière de SIGINT. Il existe dès lors entre eux un sentiment fort de loyauté et de solidarité. Cela pourrait expliquer le ralliement immédiat à la NSA lorsqu'elle a déclaré publiquement que trois attentats avaient été évités en Belgique sur la base de ses informations.[62] Il est apparu ensuite qu'il s'agissait d'informations qui avaient utilement contribué à acquérir une meilleure position d'information dans un dossier de terrorisme concret en Belgique.
- Au sein des plateformes de coopération, le principe de non-espionnage des pays partenaires prévaut. Il s'avère que la NSA et le GCHQ ne se sont pas tenus à cette dernière règle de conduite.
- La coopération internationale est quantitativement très importante pour la section SIGINT belge. La plupart des informations transmises par cette section aux clients internes et externes, sous la forme de rapports, proviennent de partenaires étrangers.

62 K. CLERIX, *MO Magazine*, 6 août 2013 (Militaire inlichtingendienst getroffen door ernstig cyberincident).

- Malgré le fait que cette forme de coopération est qualifiée de très importante, il n'y a aucune évaluation formelle de la valeur globale des informations qui proviennent de ces plateformes de coopération.
- Dans le cadre d'une des deux plateformes de coopération, le SGRS n'a transmis, en 2013, qu'un nombre infime de rapports, dont la moitié contenait des informations relatives à des Belges. La majeure partie de ces informations était liée au terrorisme. Il en a cependant été autrement dans le cadre de la seconde plateforme de coopération. En effet, le dispositif d'interception du SGRS envoie les métadonnées de toutes les communications émises, si bien qu'elles peuvent être consultées par tous les partenaires.
- Les interceptions effectuées par le SGRS dans le contexte d'une opération militaire internationale étaient légales : elles étaient reprises dans le Plan d'écoutes, elles cadraient avec la mission du SGRS qui consiste à protéger les troupes belges et alliées actives dans le cadre d'un mandat international, et elles étaient « ciblées » du fait de l'utilisation d'un nombre limité de critères. De plus, le déploiement du personnel SIGINT était approuvé par le Gouvernement dans le cadre plus large de la décision d'envoyer des troupes. Toutefois, le Comité ministériel du renseignement et de la sécurité n'avait pas établi de directives, ni en ce qui concerne la coopération, ni en ce qui concerne la transmission de renseignements à des services tiers.[63]
- Dans un cadre bien défini, les métadonnées de *toutes* les communications d'une région déterminée étaient stockées et partagées avec les pays partenaires. Le SGRS n'avait aucune idée du volume des données stockées. Tous les pays partenaires y avaient accès et pouvaient effectuer des recherches. Le SGRS faisait également usage de cette possibilité, ce qui, sur le plan légal, était quelque peu ambigu. Indépendamment de la manière dont la recherche est effectuée (par exemple, en faisant du *datamining* pour détecter de nouvelles menaces), il est possible que le SGRS ait opéré dans un vide juridique. Le Comité est d'avis que les règles d'interception doivent être précisées en l'espèce.
- Le Comité a souligné n'avoir absolument aucune indication selon laquelle le SGRS utiliserait ces plateformes de coopération pour obtenir des informations que la loi ne lui permet pas de collecter. Toutefois, le SGRS n'effectuait pas le moindre contrôle sur l'éventuelle légitimité (en vertu du droit belge ou étranger) de la manière dont les données étaient recueillies par des partenaires étrangers. La principale raison est que c'est pratiquement impossible. En outre, les personnes qui sont amenées à voir les informations brutes (et c'est *de facto* les seules informations pouvant donner une indication sur la légitimité du recueil) n'ont pas de formation juridique.

63 Le fait que, à titre exemple, des données transmises par les pays partenaires pourraient être utilisées à d'autres fins que celles pour lesquelles elles ont été collectées, montre l'importance d'édicter de telles directives.

– Dans les plateformes de coopération, prévaut un devoir de réserve absolu, qui est étroitement surveillé. Celui-ci est d'application tant au sein du SGRS (par un strict compartimentage) qu'à l'extérieur. L'importance de cet aspect est expliquée ci-après.

Le devoir de réserve est très prégnant dans les plateformes de coopération SIGINT. Sur le plan formel, toutes les informations relatives au SIGINT sont protégées par l'exigence de disposer d'une habilitation spécifique, en sus de l'habilitation belge classique du niveau « TRÈS SECRET ». Il ne s'agit pas d'une exigence fondée sur la réglementation belge ; l'obligation émane des règlements de l'OTAN. L'obtention de cette habilitation n'est pas soumise à une enquête complémentaire ; les candidats – qui doivent déjà posséder une habilitation de sécurité du niveau « TRÈS SECRET » – reçoivent un briefing au cours duquel un accent particulier est mis sur le caractère sensible du travail avec les SIGINT. Le SGRS veille autant que possible à limiter le nombre de personnes qui reçoivent cette habilitation.

Bien que le Comité comprenne que les *signals intelligence* sont une matière très sensible pour laquelle le principe de *need to know* doit être appliqué de manière stricte et pour laquelle un certain compartimentage est indiqué, il ne voit pas de différences fondamentales avec certains autres domaines du travail de renseignement tout aussi sensibles. L'on peut penser à cet égard à l'*image intelligence* (IMINT) ou à la mise en œuvre des méthodes MRD. Quoi qu'il en soit, un tel devoir de réserve ne peut aller jusqu'à s'appliquer au niveau politique (c'est-à-dire le ministre de la Défense et/ou le Comité ministériel du renseignement et de la sécurité). Seul le ministre de la Défense disposait de l'habilitation SIGINT spécifique au moment de l'enquête. Le Comité permanent R s'est posé la question de savoir si le ministre de la Défense actuel et ses prédécesseurs étaient « suffisamment » informés (c'est-à-dire en mesure de prendre leurs responsabilités politiques à l'égard du Parlement) des éléments politiques pertinents en matière de coopération SIGINT du SGRS, et donc si la culture de stricte confidentialité qui caractérise le SIGINT n'a pas nui à la transparence. Naturellement, la question de savoir si un élément déterminé est « politiquement pertinent » est une donnée qui évolue (cf. sensibilité politique changeante, nouvelle situation géopolitique et nouvelles évolutions technologiques…).[64]

Le Comité a toutefois souligné que le devoir de réserve n'était pas invoqué en vue de pratiquer délibérément une quelconque forme de rétention.

À d'autres occasions, le SGRS a affirmé qu'en donnant les détails SIGINT au Comité permanent R, sa tâche d'information à l'égard des autorités était

64 Une forme de contrôle serait néanmoins possible par l'approbation des budgets nécessaires pour certains achats.

suffisamment (voire entièrement) remplie. Il est cependant évident que l'organe de contrôle ne peut faire office de couverture politique.

Le Comité a également fait remarquer à cet égard l'absence de directive du Comité ministériel du renseignement et de la sécurité en exécution de l'article 20 L.R&S. Une telle directive devrait reprendre au moins les grandes lignes de la coopération du SGRS en matière de SIGINT ainsi que des règles régissant l'échange d'informations SIGINT avec divers partenaires. Cet aspect sera développé dans les recommandations.

II.1.5.2. Était-il question de captation massive de données par le SGRS ?

Le Comité permanent R est arrivé à la conclusion que la captation massive de données par le SGRS lui-même ne pouvait pas être qualifiée de « massive » au moment de l'enquête, et ce vu les restrictions légales et techniques ainsi que l'effectif limité. Le Comité a cependant fait quelques observations.

Comme cela a déjà été souligné, le dispositif d'interception qui était utilisé dans le cadre de l'opération militaire visée, constituait dans un certain sens une exception à ce qui précède.

Deuxièmement, la formulation du « Plan d'écoutes 2014 » était tellement large que, théoriquement, peu de limites ont été posées aux possibilités d'écoutes du SGRS. Aussi en raison du nombre croissant de possibilités au niveau technologique et de la présence du SGRS au sein de certaines plateformes SIGINT, le Comité a formulé ses remarques à ce propos, en exécution de sa compétence reprise à l'article 44*bis* L.R&S. Lors d'une éventuelle utilisation des nouveaux moyens technologiques, le SGRS doit tenir compte des limites posées par la réglementation INT (voir II.1.3.2).

II.1.5.3. Qu'en est-il du recueil de renseignements politiques et économiques par le SGRS ?

En ce qui concerne l'étranger, le SGRS recueille uniquement des informations dans les sphères politique ou économique, dans la mesure où ces informations sont pertinentes dans le cadre de ses missions, telles que, par exemple, la protection des troupes belges et alliées.

II.1.5.4. La position d'information du SGRS avant et après les révélations d'Edward Snowden

Comme cela a déjà été mentionné, le SGRS est entre autres compétent pour l'espionnage en matière de politique de défense. À cet égard, aucune indication concrète concernant la Belgique n'a été trouvée dans les révélations d'Edward Snowden. De plus, le service était compétent depuis 2013 pour surveiller les captations massives de données, et ce dans la mesure où ces captations pouvaient

représenter une menace pour le potentiel économique ou scientifique d'une série d'entreprises et institutions reprises nommément. Par ailleurs, le Comité estime que connaître les moyens et les modes opératoires d'autres services fait partie des tâches d'un service de renseignement. L'objectif est non seulement de pouvoir informer les autorités compétentes et de pouvoir prendre des mesures de rétorsion, mais aussi de moderniser ses propres techniques de collecte. Cela indépendamment du fait qu'il s'agisse de services amis ou non.

Le Comité a dès lors estimé que la question devait être posée pour le SGRS aussi : le service était-il ou pouvait-il être au courant du mode opératoire de la NSA et du GCHQ avant les révélations ? Par ailleurs, le Comité s'est penché sur les actions entreprises par le SGRS après les révélations.

II.1.5.4.1. La position du SGRS avant les révélations

Avant l'éclatement de l'affaire ECHELON en 1998, le SGRS était au courant de la collaboration qui existait entre les dénommés FIVE EYES. Mais puisque ces pays ne constituaient pas une menace sur le plan militaire, le SGRS (à juste titre à ce moment-là, selon le Comité) estimait qu'il ne devait pas faire d'efforts particuliers en matière de renseignement.

Un an après son premier rapport ECHELON, le Comité a souhaité examiner si les services de renseignement belges avaient entrepris des démarches depuis lors. À l'époque, le service avait signalé que la numérisation croissante de la société engendrait de lourdes menaces pour la sécurité des communications.

En 2006, il est apparu que le SGRS n'était pas au courant que les services américains avaient accès aux données de SWIFT. Le Comité permanent R a conclu que c'était normal, eu égard à la compétence du SGRS.[65]

Dans la foulée de la signature du *Protect America Act* en 2007, en vertu duquel les compétences des services de renseignement américains ont été étendues à l'interception de toutes sortes de communications, le Comité a aussi interrogé le SGRS. Une division a notamment affirmé que l'on pouvait raisonnablement penser que la NSA avait procédé à des interceptions sur le territoire belge, et ce à l'encontre d'autorités belges ou étrangères et d'institutions privées. Et d'attirer l'attention sur les conséquences éventuelles des possibilités d'interceptions supplémentaires octroyées par le *Protect America Act*. Ce qui était étonnant toutefois, c'était qu'une autre division avait une tout autre perception. En effet, elle ne distinguait pas de menace, puisqu'elle travaillait en bonne entente avec les services américains et comptait sur la loyauté mutuelle.

En ce qui concerne la position d'information du SGRS avant les révélations d'Edward Snowden, le Comité a établi une distinction entre d'une part, sa compréhension théorique et réelle des capacités SIGINT appliquées par la NSA

65 COMITÉ PERMANENT R, *Rapport d'activités 2006*, 44.

et le GCHQ, et d'autre part, sa compréhension de l'ampleur et de la stratégie de ciblage SIGNIT de ces services.

Les capacités technologiques dont la NSA dispose en théorie ne constituaient pas une surprise pour le SGRS, du moins pas pour la section SIGINT qui était et est bien au courant des évolutions technologiques. En outre, cette section avait une vue sur le genre et sur l'origine des informations qui pouvaient être effectivement détectées par le biais de telles méthodes. Toutefois, la section SIGINT ne savait rien des programmes concrets ni de leurs noms de code. La section SIGINT n'a cependant mené aucune étude à ce sujet, ni rédigé le moindre rapport. En plus du devoir de réserve dont il a été question précédemment, le fait que ces possibilités n'étaient pas particulièrement surprenantes aux yeux des personnes formées à la technologie dans le domaine SIGINT, a indéniablement joué un rôle, et n'a donc pas donné lieu à une initiative spécifique.

Quant à l'ampleur des captations de données, la stratégie de ciblage de la NSA et l'intégration de nombreux moyens techniques, le Comité a pu constater que le SGRS n'était pas en mesure d'élaborer davantage, vu le peu de données avérées à sa disposition.

Enfin, il convient de mentionner qu'en ce qui concerne le genre de personnes suivies, le SGRS ne pouvait déduire que de manière globale qu'il s'agissait de personnes qui étaient soupçonnées de (liens avec le) terrorisme international. Rien n'indiquait que des citoyens lambda, des responsables politiques ou des entreprises intéressaient la NSA.

II.1.5.4.2. La position du SGRS après les révélations

Tout d'abord, le SGRS a eu plusieurs contacts avec des représentants de différents services de renseignement, dont la NSA et le GCHQ. À l'occasion de ces contacts, le SGRS a laissé paraître le mécontentement de la Belgique. De plus, lors d'une réunion avec des services homologues européens, une initiative a été prise afin de renforcer la confiance mutuelle. En adhérant à cette initiative, les participants pouvaient s'engager, sur base volontaire, à ne pas mener d'opérations SIGINT clandestines à l'égard d'autres pays de l'Union européenne. Enfin, le SGRS a attiré l'attention, au sein d'un des réseaux, sur les conséquences opérationnelles et politiques éventuelles des faits à la base des révélations d'Edward Snowden.[66]

En outre, le SGRS a organisé des briefings sur le sujet pour diverses autorités. Des réponses à de nombreuses questions parlementaires ont également été préparées.

Par ailleurs, le SGRS a prêté son concours technique dans le cadre de l'enquête judiciaire à la suite du piratage du réseau BICS. Le SGRS a aussi été impliqué dans l'analyse du logiciel malveillant.

---

66 Par conséquences politiques, on entend notamment un contrôle plus strict des services de renseignement, comme cela semble être le cas aux Pays-Bas et en Allemagne.

Enfin, le SGRS a promis une double réaction/position : une au niveau national et une au niveau international.

Au niveau national, il conviendrait d'accorder une attention accrue à la *cybersecurity*, au sein du SGRS mais aussi à l'extérieur, et à la *cyberintelligence*. Les révélations d'Edward Snowden ont mis en lumière des faiblesses dans les systèmes de sécurité. Il faut y répondre par des mesures techniques, des briefings, screening… En d'autres termes, il faut développer une gestion complète des risques à l'égard d'éventuelles fuites.

Sur le plan international, des liens de confiance doivent être retissés avec les services de renseignement concernés. Le SGRS a fait remarquer qu'un « repli sur soi » serait une erreur. La coopération internationale doit se poursuivre. Il faut cependant être bien conscient que si auparavant l'on savait clairement quels services étaient des « amis », c'est moins évident aujourd'hui. De plus, la rédaction d'une directive en matière de coopération avec des services étrangers, à l'instar de la VSSE, s'impose.

Le Comité a toutefois dû constater que le SGRS, à l'exception de la constitution d'un dossier en vue d'une réunion internationale, n'a pas mené de recherches structurées dans les sources ouvertes, n'a réalisé aucune analyse *all sources* sur les révélations et n'a pas suffisamment exploité ses propres informations.

Une seule discussion a eu lieu avec la VSSE concernant les révélations.

II.1.5.5. Analyse du fonctionnement et de la position du SGRS avant et après les révélations

Le peu d'initiatives prises en matière de renseignements par le SGRS, tant avant qu'après les révélations, s'explique surtout par le fait que les menaces sous-jacentes, telles qu'elles ressortaient des informations reçues au moment de l'enquête, ne faisaient pas partie de la sphère de compétences du service. En revanche, le Comité estime que tout service de renseignement doit avoir une vue documentée sur les moyens dont disposent des homologues étrangers, soit pour appuyer sa propre collecte, soit pour prendre des mesures de rétorsion si nécessaire (par exemple en cas d'espionnage de la politique de défense belge). Dans cette optique, un suivi de la thématique était certainement indiqué.

La position du SGRS s'expliquait bien entendu aussi par le fait qu'il s'agissait de nations amies. Dans le cadre, par exemple de l'enquête de contrôle sur la protection de systèmes de communication contre d'éventuelles interceptions étrangères et contre des cyberattaques, le Comité a pu constater que les actions menées par les services de renseignement américains ne figuraient pas dans le Plan directeur du renseignement de sécurité.[67] En effet, le SGRS comptait sur la loyauté des services partenaires au sein de l'OTAN, puisque l'application du

[67] Voir COMITÉ PERMANENT R, *Rapport d'activités 2011*, 20.

Patriot Act vise les ennemis des États-Unis.[68, 69] Le Comité a cependant pu constater qu'aujourd'hui, de plus en plus d'acteurs affirment qu'en matière de travail de renseignement, il y a certes beaucoup de partenaires, mais pas d'amis.

Un troisième élément pouvant expliquer le manque de proactivité du SGRS est sans aucun doute le fait le service de renseignement américain constitue pour lui une source importante d'informations. Dès lors, certaines activités de renseignement peuvent être considérées comme peu – voire pas du tout – problématisés.

Toutefois, le Comité a souligné les efforts du SGRS depuis la fin 2013 pour que la thématique soit discutée dans des forums SIGINT internationaux.

II.2. PROTECTION DE LA VIE PRIVÉE ET CAPTATION MASSIVE DE DONNÉES

Dans le sillage des révélations d'Edward Snowden, la Commission de suivi du Sénat de l'époque a demandé au Comité de fournir un aperçu des règles en vigueur en Belgique en matière de protection de la vie privée eu égard aux moyens qui autorisent l'interception et l'exploitation à grande échelle des données relatives à des personnes, organisations, entreprises ou instances établies en Belgique. Cette enquête devait également permettre de mieux comprendre les instruments juridiques dont disposent les États, les citoyens ou les entreprises pour introduire un recours contre des violations (éventuelles) des droits (fondamentaux).

Pour cette enquête, le Comité a fait appel à l'expertise du professeur Annemie Schaus (ULB). De son avis détaillé, qui était intégralement repris dans son rapport annuel précédent[70], le Comité a notamment retenu les éléments suivants[71] :

---

68 Cette position est aussi reprise entre autres par les services de renseignement allemands.

69 Dans une enquête précédente, le Comité a même dû noter qu'un éventuel espionnage par des services américains n'était pas considéré comme une menace immédiate qui devrait bénéficier d'une attention prioritaire (Voir COMITÉ PERMANENT R, *Rapport d'activités 2000*, 55).

70 A. SCHAUS, « Consultation sur les règles en vigueur en Belgique en matière de protection de la vie privée eu égard aux moyens autorisant l'interception et l'exploitation à grande échelle de données relatives à des personnes, organisations, entreprises ou instances établies en Belgique ou qui ont un lien avec la Belgique », COMITÉ PERMANENT R, *Rapport d'activités 2013*, 188-212.

71 Le Comité a déjà formulé certaines de ces conclusions dans le cadre de son enquête sur le réseau ECHELON (COMITÉ PERMANENT R, *Rapport d'activités* 2000, 27-57) et sur l'affaire SWIFT (COMITÉ PERMANENT R, *Rapport d'activités 2006*, 39-48). À l'époque de l'affaire ECHELON, le Parlement belge était également arrivé à la conclusion que le système constituait une violation de l'article 8 CEDH, puisqu'il ne répondait pas aux exigences de légalité, de légitimité et de nécessité (*Doc. parl.* Sénat 2001-02, n° 2-754/1 et *Doc. parl.* Chambre, 2001-02, n° 50 1660/001, 25 février 2002).

- La nature massive et arbitraire de l'interception, de la surveillance, de l'utilisation et du stockage des données à caractère personnel est en tous points contraire à la CEDH.
- Le respect de la vie privée incombe aux fournisseurs de services de réseaux sociaux qui relèvent du champ d'application territorial de la CEDH.
- La Convention n° 108 pour la protection du traitement automatisé des données à caractère personnel, qui a un caractère contraignant pour tous les États du Conseil de l'Europe, constitue l'un des meilleurs instruments juridiques pour protéger les individus contre les risques associés à la surveillance électronique.
- La directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données s'applique *rationae loci* aux fournisseurs de réseaux sociaux, même lorsque leur siège est situé en dehors de l'Espace économique européen (EEE).[72] Cette directive interdit le transfert de données personnelles à des États non membres de l'EEE si ceux-ci ne peuvent garantir au minimum le même niveau de protection.
- L'accord « Sphère de sécurité » (« *Safe Harbor* »), que les États-Unis et l'Union européenne ont conclu en matière de protection des données, a été clairement violé, puisque des entreprises certifiées « Safe Harbor » ont autorisé l'utilisation de données à caractère personnel dans le cadre du recueil de données à grande échelle par la National Security Agency (NSA).
- Les données à caractère personnel qui sont traitées dans le cadre de la collaboration policière et judiciaire dans des affaires pénales ne relèvent pas de l'application de la Directive 95/46/CE ou des principes de la Sphère de sécurité. L'échange de telles données entre l'Union européenne et les États-Unis est régi par des accords *ad hoc*, comme la convention en matière d'entraide judiciaire, l'accord sur l'utilisation et le transfert des données personnelles des passagers (PNR), l'accord relatif au traitement et au transfert de données de messagerie financière aux fins du programme de surveillance du financement du terrorisme (TFTP).
- La surveillance à grande échelle des communications électroniques sans le consentement de l'État sur le territoire duquel la surveillance a lieu viole la souveraineté de cet État, même si l'interception se déroule à partir d'une installation située sur le territoire d'un État tiers. Le fait que les écoutes soient conformes au droit de l'État qui y procède n'y change rien. Il en va de même pour les écoutes clandestines opérées au départ d'ambassades d'États tiers situées sur le territoire du pays hôte.

---

72 Voir à cet égard : Groupe 29, WP 163 « Avis 5/2009 sur les réseaux sociaux en ligne » du 12 juin 2009.

- L'État, les citoyens et les entreprises disposent de différents recours devant la Cour internationale de Justice, la Cour européenne des droits de l'homme, les tribunaux belges, etc. pour contester des violations de droits fondamentaux.
- Le recours à certaines méthodes (comme l'écoute de conversations téléphoniques ou le piratage) par un service de renseignement étranger sur le territoire belge constitue un fait répréhensible.

Sur les indications de sa Commission Libertés civiles, Justice et Affaires intérieures (ou Commission LIBE), le Parlement européen a formulé plusieurs conclusions concordantes dans sa Résolution sur « *le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures* »[73] :

- Le programme de surveillance PRISM qui a été dévoilé représente une grave entrave aux droits fondamentaux des citoyens.[74] Le Parlement souligne que la protection de la vie privée n'est pas un droit de luxe, mais constitue le fondement de toute société libre et démocratique.
- Les États membres ne peuvent pas accepter des données provenant de pays tiers et ayant été collectées illégalement. Ils doivent en outre refuser que des gouvernements de pays tiers mènent sur leur territoire des activités de surveillance contraires au droit national ou ne satisfaisant pas aux garanties juridiques spécifiées dans les instruments internationaux ou européens.
- Les États membres sont appelés à satisfaire immédiatement à l'obligation positive qui leur incombe au titre de la Convention européenne des Droits de l'Homme, à protéger leurs citoyens des activités de surveillance contraires aux dispositions de la convention, y compris lorsque ces activités visent à garantir la sécurité nationale, et à veiller à ce que l'état de droit ne soit pas affaibli par l'application extraterritoriale d'une loi d'un pays tiers.
- Les États membres doivent organiser un contrôle efficace des activités de renseignement, assuré par des parlementaires ou par des organes spécialisés juridiquement habilités à enquêter.

73 Résolution 2013/2188 (INI) du Parlement européen (12 mars 2014), P7_TA(2014)0230.

74 La Cour européenne des droits de l'homme devra elle aussi se prononcer sur l'interception à grande échelle de données. En octobre 2013, elle a été saisie par différentes associations, qui dénonçaient les pratiques révélées. Jusqu'à présent, la Cour n'a rendu aucun jugement dans cette affaire.

II.3. L'UTILISATION DANS DES AFFAIRES PÉNALES D'INFORMATIONS ISSUES D'UNE CAPTATION MASSIVE DE DONNÉES PAR DES SERVICES ÉTRANGERS

En juillet 2013, le bâtonnier de l'Ordre néerlandais des avocats du barreau de Bruxelles a déposé une plainte concernant un «*espionnage Internet étatique organisé et sans frontières utilisé massivement pendant des années*». Le bâtonnier faisait ainsi référence aux activités de captation de données via des *Signals Intelligence* (SIGINT) par les services de renseignement américains et britanniques, révélées par Edward Snowden. Il affirmait que dans la mesure où ces activités peuvent également concerner des Belges, elles sont contraires, entre autres, à l'article 8 CEDH, aux dispositions de la Convention n° 108 portant sur la protection des données[75] et aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Le bâtonnier affirmait également que la VSSE[76] n'aurait pas satisfait à l'obligation juridique positive des pouvoirs publics de défendre les droits et libertés fondamentaux des citoyens[77], et que l'utilisation devant le juge de données obtenues au moyen d'une interception massive de données est en contradiction avec l'obligation de protéger les droits et les libertés fondamentales.[78]

L'enquête du Comité permanent R a surtout porté sur cette dernière problématique, étant donné que les autres aspects de la plainte avaient déjà été traités dans deux enquêtes antérieures.[79]

II.3.1. LE CADRE LÉGAL EN MATIÈRE DE TRANSFERT D'INFORMATIONS AUX AUTORITÉS JUDICIAIRES

Plusieurs dispositions régissent le transfert d'informations depuis les services de renseignement à destination de la justice :

---

75 Conseil de l'Europe, Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ratifiée par la Belgique par la loi du 17 juin 1991.

76 Même si le plaignant visait uniquement la VSSE, le Comité permanent R a estimé que l'enquête devait également s'étendre au SGRS.

77 Voir à cet égard CEDH, n° 38478/05 du 5 mars 2009, *Jankovic c. la Croatie, et CEDH, n° 32881/04 du 28 avril 2009, KH c. la Slovaquie.*

78 Il convient de souligner que le bâtonnier, qui avait évoqué une éventuelle «percolation» d'informations provenant d'activités d'espionnage dans des affaires pénales belges, n'a pu apporter aucun dossier concret étayant cette hypothèse. La consultation des membres de son barreau n'a fait apparaître aucun dossier spécifique que le Comité aurait pu utilement examiner.

79 Voir Chapitre II.1. «Les révélations d'Edward Snowden et la position d'information des services de renseignement belges» et Chapitre II.2. «Protection de la vie privée et captation massive de données».

- L'article 29 CIC stipule que tout fonctionnaire (et donc aussi un membre de la VSSE ou du SGRS) qui, dans l'exercice de ses fonctions, acquerra la connaissance d'un crime ou d'un délit sera tenu d'en donner avis sur-le-champ aux autorités judiciaires ;
- Lorsque ces données ont été obtenues au moyen de méthodes spécifiques ou exceptionnelles, il convient d'appliquer la procédure prévue à l'article 19/1 L.R&S, qui dispose que le transfert a lieu par le biais d'un procès-verbal non classifié rédigé par la commission BIM ;
- L'article 19 L.R&S stipule que la VSSE et le SGRS peuvent (uniquement) communiquer les renseignements qu'ils ont à leur disposition, entre autres aux autorités judiciaires, lorsqu'ils sont pertinents dans le cadre de leurs missions ;
- Enfin, les services de renseignement et les autorités judiciaires s'appuient généralement sur l'article 20, § 2 L.R&S (qui prévoit une assistance technique par la VSSE et le SGRS) pour l'échange mutuel d'informations. Le Comité permanent R a toutefois déjà souligné à plusieurs reprises que cette disposition devait être interprétée de manière restrictive et ne devait donc pas servir de base à la transmission de renseignements.[80]

Ces règles ont déjà été détaillées dans les circulaires COL 9/2005 et COL 9/2012 du Collège des procureurs généraux.

II.3.2. LE CADRE LÉGAL DE L'UTILISATION DE RENSEIGNEMENTS DANS DES AFFAIRES PÉNALES

Comme stipulé dans la circulaire COL 9/2012, dans les affaires pénales, l'administration de la preuve est libre, si bien que toutes les pièces utiles peuvent être versées au dossier d'enquête à condition de ne pas être classifiées. Les renseignements de la VSSE ou du SGRS n'ont toutefois aucune valeur probante particulière.

La question suivante était cependant cruciale pour cette enquête de contrôle : qu'en est-il si les renseignements que les services de renseignement belges transmettent aux autorités judiciaires ont été obtenus par un système de collecte de données illégal au sens de la législation belge ? Le Comité faisait référence en la matière à l'avis que son expert[81] avait formulé dans une enquête de contrôle antérieure :

---

80 Voir COMITÉ PERMANENT R, *Rapport d'activités 2004*, 133 et COMITÉ PERMANENT R, *Rapport d'activités 2006*, 54-56.

81 Voir « Consultation sur les règles en vigueur en Belgique en matière de protection de la vie privée eu égard aux moyens autorisant l'interception et l'exploitation à grande échelle de données relatives à des personnes, organisations, entreprises ou instances établies en Belgique ou qui ont un lien avec la Belgique », dans COMITÉ PERMANENT R, *Rapport d'activités 2013*, 211-212.

« Le droit de la procédure pénale belge prévoit […] une règle d'exclusion des éléments de preuve obtenus de manière illégale. Cette exclusion n'est néanmoins pas absolue. En effet, la loi du 24 octobre 2013 a inséré dans le code d'instruction criminelle un nouvel article 32, qui se lit de la manière suivante :

« Art. 32. La nullité d'un élément de preuve obtenu irrégulièrement n'est décidée que si :

- *le respect des conditions formelles concernées est prescrit à peine de nullité, ou ;*
- *l'irrégularité commise a entaché la fiabilité de la preuve ou ;*
- *l'usage de la preuve est contraire au droit à un procès équitable ».*

Cette loi fait suite à la jurisprudence de la Cour de cassation belge dite « Antigone » du 14 octobre 2003. Cette jurisprudence avait déjà donné lieu à une loi du 9 décembre 2004 « sur l'entraide judiciaire internationale en matière pénale et modifiant l'article 90ter du Code d'Instruction Criminelle », qui dispose, en son article 13 :

« Art. 13. Ne peuvent être utilisés dans le cadre d'une procédure pénale menée en Belgique, les éléments de preuve :

1° recueillis irrégulièrement à l'étranger, lorsque l'irrégularité :

- *découle, selon le droit de l'État dans lequel l'élément de preuve a été recueilli, de la violation d'une règle de forme prescrite à peine de nullité ;*
- *entache la fiabilité de la preuve ;*

2° ou dont l'utilisation viole le droit à un procès équitable ».

Cette réglementation de la preuve implique donc que toute illégalité/irrégularité n'entraîne pas l'écartement automatique de cet élément de preuve. »

Il en résulte que des renseignements, qui, par hypothèse, sont recueillis en toute légalité dans le pays d'origine et ne portent pas atteinte au droit à un procès équitable, peuvent être utilisés dans des procédures pénales belges, même s'ils n'auraient pas pu être recueillis en vertu du droit belge.

II.3.3. LE TRAITEMENT ET LA TRANSMISSION DE RENSEIGNEMENTS SIGINT ÉTRANGERS PAR LA VSSE ET LE SGRS

II.3.3.1. Généralités

La VSSE n'entretient pas de contacts réguliers avec les services étrangers qui, d'après les révélations d'Edward Snowden, ont mis sur pied les programmes de captation massive de données via des Signals intelligence (SIGINT). Les partenaires internationaux de la VSSE sont les services (« civils ») américains FBI et CIA, ainsi que le *British Security Service* (MI5) et le *Secret Intelligence Service* (MI6), qui ne sont pas eux-mêmes des agences SIGINT (contrairement à la NSA et au GCHQ). Lorsque la VSSE reçoit des renseignements de ces partenaires et

les transmet éventuellement aux parquets, la source SIGINT initiale (par exemple la NSA ou le GCHQ) a disparu au cours des étapes. De même, la VSSE ne transmet pas telles quelles les données étrangères qu'elle reçoit à d'autres services belges. Les informations sont en principe évaluées et éventuellement complétées ou nuancées.

En ce qui concerne le SGRS, qui entretient bel et bien des contacts directs avec la *National Security Agency* (NSA) et avec le *Government Communications Headquarters* (GCHQ), une enquête antérieure a démontré que les données que ces services étrangers recueillent peut-être massivement ne sont pas partagées de manière proportionnelle avec le SGRS. Si l'échange d'informations entre les services est très limité, il se peut toutefois que certaines de ces données proviennent des programmes incriminés. De fait, le SGRS n'exerce aucun contrôle sur l'éventuelle légitimité de la manière dont les partenaires étrangers ont obtenu des données au regard du droit belge ou étranger. C'est d'ailleurs pratiquement impossible, vu qu'il est rare que la manière dont les informations ont été recueillies soit communiquée. Comme dans le cadre de la première enquête thématique sur « Les révélations d'Edward Snowden et la position d'information des services de renseignement belges » (voir II.1), le Comité a néanmoins affirmé que le service destinataire doit au moins s'efforcer de découvrir de quelle manière les renseignements concernés ont été obtenus. Il ressort toutefois de la pratique que les « services de renseignement fournisseurs » taisent généralement leurs sources (et donc l'origine d'un renseignement) et que les « services destinataires » l'acceptent. Cette forme d'entente fait partie de la culture internationale du renseignement, au même titre que la règle du service tiers, le principe *do ut des* et le devoir de réserve. Ce constat ne signifie toutefois pas que le Comité adhère inconditionnellement à ces principes : le Comité a réitéré le fait que ces principes ne peuvent être abandonnés de manière brutale et unilatérale.

Dans ce cadre, le Comité s'est également appuyé sur un jugement rendu par un juge néerlandais, qui devait se pencher sur la question de savoir si et dans quelle mesure un service de renseignement (néerlandais) peut accepter et utiliser des données de partenaires étrangers s'il n'est pas certain de la manière dont ces données ont été recueillies, et s'il se peut (ou du moins qu'il n'est pas exclu) qu'elles aient été recueillies à l'aide de méthodes que son propre service n'est pas en mesure ou autorisé à appliquer.[82] Le juge a notamment déclaré que : « *Gegeven het uitgangspunt van artikel 59 lid 1 Wiv 2002 en de ruime beoordelingsvrijheid van de lidstaten bij de toetsing aan artikel 8 EVRM, betoogt de Staat op toereikende gronden dat van hem niet kan worden gevergd dat hij de dringend noodzakelijke samenwerking met buitenlandse diensten, zoals die van de VS, op het spel zet louter op grond van onbekendheid met hun werkwijze en de kans dat de Nederlandse diensten informatie ontvangen die is vergaard op een in Nederland*

[82] Tribunal de La Haye, 23 juillet 2014, numéro de rôle : C/09/455237 / HA ZA 13.1325. Un recours a été introduit contre ce jugement.

niet toegelaten wijze. Het zwaarwegende belang van de nationale veiligheid geeft hier de doorslag »[83]

II.3.3.2. Concrètement

Comme mentionné ci-dessus, la consultation menée par le bâtonnier auprès des membres de son barreau n'a fait ressortir aucun dossier spécifique qui ferait apparaître que des informations reprises dans des affaires pénales proviendraient de programmes (étrangers) de captation massive de données. De même, l'enquête du Comité permanent R, qui portait en principe sur la période 2011-2013, n'a relevé que peu de données concrètes.

II.3.3.2.1. Qu'en est-il de la VSSE ?

Les données émanant de la VSSE ne concernaient que la période allant de novembre 2012 à juin 2014. En effet, ce n'est qu'à partir de novembre 2012 que la base de données de ce service a pu établir un lien entre les notes sortantes et les messages entrants qui en étaient à la base.

Durant cette période, la VSSE a reçu quelque 4 000 rapports de renseignement du FBI, de la CIA, du BSS et du SIS. Cependant, sur les quelque 550 notes que la VSSE a envoyées aux parquets au cours de cette même période, un lien direct entre les renseignements étrangers initiaux et les notes envoyées aux parquets n'a pu être établi que dans 14 cas. En outre, seules deux notes (qui portaient sur un même cas) contenaient des informations d'origine SIGINT, mais le service fournisseur n'était pas un service de renseignement. Par ailleurs, la VSSE n'a pas pu déterminer quels moyens SIGINT ont été précisément utilisés, bien que rien n'indique qu'il s'agissait en l'espèce d'une captation massive (non ciblée). Les informations SIGINT ont été reprises dans les notes adressées au parquet de manière très sommaire et sans mention de la source initiale. De surcroît, les notes contenaient d'autres renseignements émanant de la propre production de la VSSE. Dans ces notes, il n'était nullement question d'informations sur les relations entre un client et son avocat.

De manière générale, l'enquête a montré que la VSSE n'a communiqué aux autorités judiciaires que dans une mesure très limitée des données SIGINT provenant de sources américaines et britanniques.

---

83 « *Partant de l'article 59, alinéa 1, Wiv 2002 et de la large liberté d'appréciation des États membres dans l'analyse au regard de l'article 8 CEDH, l'État fait valoir par des motifs suffisants que l'on ne peut pas exiger de lui qu'il mette en jeu la collaboration absolument nécessaire avec des services étrangers, tels que ceux des États-Unis, uniquement parce que l'on ignore leur méthode de travail et que les services néerlandais risquent de recevoir des informations qui ont été recueillies d'une manière considérée comme illicite aux Pays-Bas. L'impératif de la sécurité nationale est ici prépondérant.* » (traduction libre).

II.3.3.2.2. Qu'en est-il du SGRS ?

Le SGRS lui aussi n'a transmis au parquet des données émanant d'opérations SIGINT des services américains ou britanniques que dans deux cas. Le SGRS a chaque fois envoyé un rapport classifié et un rapport non classifié.

Dans l'un des deux cas, il s'est avéré que les renseignements provenaient d'opérations SIGINT d'un des services de renseignement étrangers visés. Il ne s'agissait pas d'une opération « non ciblée », mais d'une action visant une cible bien précise. Dans l'autre cas, l'information provenait d'Internet.

II.3.4. CONCLUSION

Au cours de la période de référence, les services de renseignement belges n'ont transmis aux autorités judiciaires qu'un volume très restreint de renseignements et d'informations émanant de l'étranger.

En outre, le Comité permanent R n'a trouvé aucun élément indiquant que des renseignements proviendraient de programmes (américains ou britanniques) de captation massive de données (e.a. SIGINT). Il ne s'agissait pas non plus d'informations portant sur la relation entre des avocats et leurs clients.

Le Comité permanent R n'a dès lors trouvé, dans le cadre de cette enquête, aucun élément permettant de déduire que des informations d'origine étrangère auraient ainsi mis en péril les droits de justiciables belges.

II.4. LA VSSE ET SA MISSION LÉGALE DE PROTECTION DES PERSONNES

II.4.1. CONTEXTE

En marge d'une enquête de contrôle antérieure[84], le Comité permanent R a appris que la VSSE aurait connu des problèmes de disponibilité d'« agents de protection » pour l'exécution de missions de protection de personnes. Plusieurs missions n'auraient pas été remplies. Le Comité a dès lors décidé d'ouvrir une enquête autour des questions suivantes : la VSSE exécute-t-elle toutes les missions qui lui sont confiées en matière de protection des personnes ? À quels problèmes

84 COMITÉ PERMANENT R, *Rapport d'activités 2012*, 35 et suiv. (II.5. Enquête commune sur les évaluations de la menace effectuées par l'OCAM concernant des personnalités étrangères en visite en Belgique). Le Comité permanent R s'est déjà intéressé à plusieurs reprises à la mission de protection des personnes de la VSSE. Voir à cet égard entre autres COMITÉ PERMANENT R, *Rapport d'activités 1996*, 68-84 et 225 ; *Rapport d'activités 2003*, 155-158 et *Rapport d'activités 2011*, 42 et suiv.

est-elle confrontée dans l'accomplissement de cette tâche et quelles sont les causes de ces problèmes ?

À la mi-juillet 2013, alors que l'enquête était toujours en cours, le Gouvernement fédéral a décidé de transférer cette mission de la Sûreté de l'État à la Police fédérale.[85] Cette décision s'annonçait depuis un certain temps. En effet, à la fin mars 2013, la VSSE a soumis à la ministre de la Justice un (projet de) « Plan stratégique 2013-2016 », qui mentionnait le désengagement de la mission de protection des personnes. Ce changement s'inscrivait dans le cadre de l'orientation stratégique de la VSSE, qui donne la priorité à la mission de renseignement : la réintégration des inspecteurs actuellement employés au sein du Service Protection des personnes pouvait contribuer au renforcement de la mission de renseignement.

Les discussions sur ce transfert ont certes débuté, mais le Conseil des ministres de l'époque a finalement décidé en février 2014 de ne plus se prononcer sur ce dossier pendant la législature en cours.

La nouvelle majorité s'y est employée dans l'Accord de gouvernement fédéral d'octobre 2014 : « *Le gouvernement prendra les initiatives nécessaires pour que la police fédérale puisse reprendre intégralement les missions de protection des personnes (y compris le personnel et les moyens y afférents) de la Sûreté de l'État. Cette initiative sera neutre budgétairement* ».[86]

Lorsque le transfert sera concrétisé, plusieurs constatations de cette enquête seront sans doute moins pertinentes. Ce ne sera toutefois pas le cas pour toutes les conclusions formulées par le Comité. En effet, plusieurs problèmes pourraient subsister, et ce même si ce n'est plus la VSSE, mais la Police fédérale, qui est chargée de cette mission.

II.4.2. CADRE JURIDIQUE

La protection des personnes est une tâche de police (administrative). Cette tâche est depuis longtemps remplie par la VSSE, qui en a reçu explicitement la mission en 1998. L'article 7, 3° L.R&S stipule que la Sûreté de l'État a pour mission « *d'exécuter les tâches qui lui sont confiées par le ministre de l'Intérieur en vue de protéger des personnes* ».

L'article 5 L.R&S stipule également que : « *Pour l'exécution de ses missions, la Sûreté de l'État est placée sous l'autorité du ministre de la Justice. Toutefois, le ministre de l'Intérieur peut requérir la Sûreté de l'État pour ce qui concerne l'exécution des missions prévues à l'article 7, lorsqu'elles ont trait […] à la*

85 Selon des articles parus dans la presse le 7 octobre 2013 (*Belga, De Morgen, het Nieuwsblad*), le porte-parole de la ministre de l'Intérieur a déclaré que le transfert aurait lieu le 1er avril 2014.

86 À la clôture de la rédaction du présent rapport d'activités, le transfert n'avait pas encore eu lieu.

protection des personnes. Dans ce cas, le ministre de l'Intérieur, sans s'immiscer dans l'organisation du service, précise l'objet de la réquisition et peut faire des recommandations et donner des indications précises sur les moyens à mettre en œuvre et les ressources à utiliser. Lorsqu'il est impossible de se conformer à ces recommandations et indications parce que leur exécution porterait atteinte à l'exécution d'autres missions, le ministre de l'Intérieur en est informé dans les meilleurs délais. Cela ne dispense pas la Sûreté de l'État de l'obligation d'exécuter les réquisitions. »

L'article 8, 5° L.R&S décrit plus précisément cette mission : « « *protéger des personnes* » *: assurer la protection de la vie et de l'intégrité physique des personnes suivantes désignées par le ministre de l'Intérieur : a) les chefs d'État étrangers ; b) les chefs de gouvernement étrangers ; c) les membres de la famille des chefs d'État et de gouvernement étrangers ; d) les membres des gouvernements belges et étrangers ; e) certaines personnalités qui font l'objet de menaces résultant d'activités définies à l'article 8, 1°* ».

Ces officiers de protection sont « *les seuls agents des services extérieurs de la Sûreté de l'État habilités à exercer les missions relatives à la protection des personnes, à l'exclusion de toute autre mission* » (art. 22 L.R&S). Ils disposent à cette fin des mêmes compétences générales que tous les autres agents de la VSSE[87] et peuvent donc utiliser presque toutes les méthodes ordinaires de recueil de données. D'autre part, les officiers de protection ont également reçu des compétences purement policières (par exemple le droit de pénétrer dans des bâtiments abandonnés, de procéder à une fouille de sécurité, à un contrôle d'identité…).

Outre les dispositions de la L.R&S, plusieurs autres règles présentent également un intérêt en la matière. Ainsi, le 8 février 2000, les ministres de l'Intérieur, des Affaires étrangères et de la Justice ont signé « *un protocole d'accord concernant les mesures de police lors de visites de certaines personnalités étrangères* ». Ce protocole définit des mesures de protection qui doivent toujours être mises en œuvre dans un nombre prédéfini de cas. La mission de protection des personnes dans le cadre de ce protocole d'accord s'applique (uniquement) aux chefs d'État et de gouvernement, ainsi qu'aux ministres des Affaires étrangères. L'accord prévoit, pour les personnalités concernées, une « protection rapprochée » assurée par les officiers de protection de la VSSE. En septembre 2003, ce protocole a fait l'objet d'une évaluation, et les capacités de la VSSE concernant les différentes missions de protection ont été définies.

La Circulaire n° 6/2004 du Collège des procureurs généraux relative à la protection des personnalités, des fonctionnaires d'état et des personnes privées menacées a été édictée début mars 2004.[88] Cette circulaire développe, entre

---

87 Voir art. 24 L.R&S, qui renvoie aux articles 12 à 14 et 16 à 18 L.R&S.

88 Cette circulaire abroge la circulaire COL 1/2001 du 5 février 2001 concernant « *la fixation des modalités à prendre en considération lors de la communication d'informations relatives à la protection des personnes – Exécution de l'article 23 de la loi du 30 novembre 1998* ».

autres, les dispositions de l'article 23 L.R&S et elle régit l'échange d'informations avec les autorités judiciaires dans le cadre de la protection des personnes.

En outre, l'on peut se référer à l'instruction gouvernementale MO/100.A du 10 juin 1974. Bien que cette instruction soit surannée, son esprit conserve toute son importance, particulièrement en ce qui concerne la collaboration et la répartition des tâches entre les services.

Enfin, la VSSE a rédigé plusieurs directives internes, dont la plus récente date de février 2013.

II.4.3. DESCRIPTION DU DÉROULEMENT DES MISSIONS DE PROTECTION

Les missions de protection se subdivisent en missions « permanentes » et « ponctuelles » (également appelées « missions officielles »). Les missions permanentes concernent la protection de diplomates étrangers accrédités en Belgique qui y bénéficient d'une protection pendant leur séjour (et donc en principe en permanence). Les missions ponctuelles portent sur la protection de VIP pendant leur visite officielle en Belgique.

Dans le cadre des missions ponctuelles, la VSSE est le dernier maillon de la chaîne, dans un processus où le besoin de protection d'une personnalité en visite est évalué, et ensuite concrétisé.

Tout d'abord, le SPF Affaires étrangères est informé par voie diplomatique de la visite d'une personne à protéger. Une demande de protection est établie. Le Centre de crise du Gouvernement ouvre un dossier afin de vérifier si la personne concernée nécessite une protection et, dans l'affirmative, laquelle.[89] À cette fin, il demande à l'OCAM et à la Police fédérale, chacun selon ses compétences, d'examiner les menaces dont fait l'objet la personne concernée. Les autorités judiciaires fournissent elles aussi des informations.[90, 91] L'OCAM[92] (et la Police fédérale en cas d'éléments concrets de menace criminelle) fait part de ses constatations au Centre de crise, qui décide, à son

89 Un officier de liaison de la VSSE est détaché au Centre de crise.

90 Cf. Circulaire n° COL 6/2004 du Collège des Procureurs généraux relative à la protection des personnalités, des fonctionnaires d'État et des personnes privées menacées.

91 Si nécessaire – par exemple lorsque certains éléments ne sont pas clairs –, le Centre de crise organise une réunion de coordination avec les instances concernées par le dossier.

92 L'évaluation de la menace lors d'une visite d'une personnalité étrangère en Belgique relève des missions légales de l'OCAM. En effet, l'une de ses tâches consiste à « *effectuer ponctuellement une évaluation commune qui doit permettre d'apprécier si des menaces visées à l'article 3 se manifestent et, le cas échéant, quelles mesures s'avèrent nécessaires* » (art. 8, 2° L.OCAM). Voir en détail à cet égard : COMITÉ PERMANENT R, *Rapport d'activités 2012*, 35-37 (II.5 Enquête commune sur les évaluations de la menace effectuées par l'OCAM concernant des personnalités étrangères en visite en Belgique).

tour, des mesures qui s'imposent.[93] Le cas échéant, une mission d'intervention est adressée à la VSSE, qui exécute ensuite la mission. La Police locale ou d'autres instances (comme la Police aéroportuaire) peuvent également se voir attribuer certaines tâches.

II.4.4. LE SERVICE PROTECTION DES PERSONNES DE LA VSSE

Le Service Protection des personnes fait partie des Services extérieurs de la VSSE et relève de la compétence du Directeur Opérations.

En principe, le service est dirigé par un chef de section, assisté d'un ou de plusieurs adjoints. Depuis octobre 2011, la direction était exercée *de facto* par un chef de section adjoint (commissaire), qui, depuis septembre 2012, était assisté par un inspecteur divisionnaire. Le secrétariat du service était assuré par un groupe de six assistants de protection (et donc pas de personnel administratif ni de collaborateurs engagés pour cette tâche), qui s'occupaient du secrétariat à tour de rôle.

La mission de protection proprement dite est remplie par des officiers et des assistants de protection. Les officiers de protection ont le grade d'inspecteur (niveau B). Leur tâche consiste à assumer la direction de tout type de mission de protection ou d'occuper la fonction de *key-man*.[94] Les assistants de protection sont des collaborateurs de niveau C.[95]

Le statut des membres du personnel qui effectuent des missions de protection de personnes est régi par l'A.R. du 13 décembre 2006 portant le statut des agents des services extérieurs de la VSSE.

L'effectif du service Protection des personnes a fortement évolué au fil des années, puisqu'il a presque triplé depuis 2000. La composition du personnel a connu sa modification la plus profonde en 2009 lors du recrutement d'assistants de protection.[96] C'est en 2010, année de la présidence belge de l'Union européenne, que l'effectif était le plus important. Depuis, des inspecteurs ont

---

93 Les missions de protection ont été subdivisées en catégories en fonction du « niveau de menace », tel que décrit dans la Loi du 10 juillet 2006 relative à l'analyse de la menace (L.OCAM), et de l'Arrêté royal du 28 novembre 2006 portant exécution de cette loi (AR OCAM). L'article 11 AR OCAM décrit quatre niveaux de menace : niveau 1 ou « faible », niveau 2 ou « moyen », niveau 3 ou « grave » et niveau 4 ou « très grave ».

94 Le *key-man* est la personne qui prend place sur le siège passager avant dans le véhicule du VIP.

95 Le niveau C requiert un diplôme de l'enseignement secondaire supérieur, tandis que le niveau B requiert un diplôme de l'enseignement supérieur de type court. Un assistant de protection peut accéder au niveau B à condition de réussir une sélection comparative d'accession au niveau supérieur.

96 Auparavant, cette fonction n'existait pas, alors qu'elle représentait environ deux tiers du personnel en 2012.

été systématiquement retirés du service (environ un tiers de l'effectif) pour renforcer les rangs des sections de renseignement de la VSSE.

II.4.5. CONSTATATIONS

II.4.5.1. L'exécution ou non des missions

Au risque de se répéter, la Sûreté de l'État assure deux types de missions de protection : les missions dites « permanentes » et les missions dites « ponctuelles » ou « officielles ».

Le nombre de missions ponctuelles a fluctué au fil des années. Le Comité a constaté que plusieurs de ces missions n'ont pas été exécutées. Selon la VSSE, ce fut le cas pour une mission sur quatre environ durant la période 2010-2012. Ce nombre a diminué, puisqu'en 2012, le nombre de « refus » se situait encore entre 4 % (VSSE) ou 11 % (Centre de crise) selon les sources.[97] Il convient toutefois de constater que ces missions ne représentaient qu'une partie plutôt restreinte de la charge de travail du Service Protection des personnes. En effet, seulement un cinquième du nombre d'heures prestées était consacré à des « missions officielles ».

Les missions permanentes étaient quant à elles toujours exécutées.[98] L'impact de ces missions permanentes sur le fonctionnement du service était important. Le Comité permanent R a recommandé de réexaminer en priorité ces missions permanentes et de voir si elles peuvent être accomplies d'une autre manière afin de requérir moins de moyens (*infra*).

II.4.5.2. La question des assistants de protection et des inspecteurs

L'effectif du service se compose d'assistants de protection (niveau C) et d'officiers de protection ayant le grade d'inspecteur (niveau B). Les assistants de protection représentent plus des deux tiers de l'effectif. La délimitation des tâches entre les assistants et les officiers s'est toutefois révélée moins stricte que ce que les descriptions de fonction laissent supposer (par exemple le fait d'assumer ou non une responsabilité). Le Comité a insisté sur le fait qu'il convient de veiller à ce que cette distinction n'engendre pas de tensions.

---

97 La différence entre les deux est due aux points de référence utilisés et à la manière dont les deux institutions interprètent les articles 7 et 8 L.R&S.

98 Il apparaît toutefois que les personnes à protéger ne sont pas toujours conscientes des risques, ce qui complique parfois l'exécution de ces missions.

II.4.5.3. La problématique des heures supplémentaires

Le « congé de récupération » – octroyé lorsque les prestations calculées sur une période de quatre mois dépassent la durée moyenne normale d'une semaine de travail – et le « repos compensatoire » – octroyé, par exemple, après le dépassement du nombre maximal d'heures de travail par jour – étaient une source d'incertitude. Le nombre d'heures de congé de récupération et de repos compensatoire à prendre est très élevé. Le Comité a pu constater qu'elles ont augmenté de plus de 44 000 heures entre janvier 2010 et fin décembre 2012. Depuis lors, la tendance est à la baisse, mais à une degré limité : pendant les trois premiers mois de 2013, quelque 3 300 heures ont été récupérées, mais le solde restait quoi qu'il en soit particulièrement élevé.

C'est surtout la décision de retirer des inspecteurs du Service Protection des personnes (*infra*) qui a eu un impact négatif sur le nombre d'heures supplémentaires. L'accroissement de l'effectif et, plus particulièrement, le recrutement des assistants de protection, n'ont manifestement pas permis de résoudre ce problème. Des mesures telles que, par exemple, une rationalisation poussée des équipes ou une externalisation visant à maîtriser la problématique des heures supplémentaires, n'ont eu que des effets (très) limités. D'autres mesures, comme le paiement des heures supplémentaires et la redéfinition ou le désengagement de missions – surtout des missions permanentes –, ont été envisagées, mais n'ont jamais été concrétisées.

II.4.5.4. Les missions d'accompagnement protocolaire

L'« accompagnement protocolaire » (c'est-à-dire quand la VSSE estime qu'il n'y a pas de menace, mais que le statut du VIP requiert un accompagnement officiel) était assuré, au moment de l'enquête, par un dispositif limité, associé à un chauffeur et une limousine d'une société privée. Le Comité permanent R n'a pas pu constater que le recours à des chauffeurs et à limousines privés était financièrement plus intéressant. C'est plutôt le contraire. D'autre part, le Comité a estimé que ce choix nuisait à la qualité fonctionnelle et que le dispositif mis en place présentait des risques, tant pour les personnes à protéger que pour les membres de la VSSE. Par conséquent, le Comité permanent R a estimé qu'une évaluation approfondie de cette méthode de travail s'imposait.

II.4.5.5. Le « retrait » de la mission de renseignement aux inspecteurs

Par le passé, des inspecteurs ont été retirés du Service Protection des personnes pour renforcer les sections de renseignement. Mais l'inverse s'est également produit : des membres des sections de renseignement (Services extérieurs) de la VSSE ont été sollicités pour faire face à un surcroît de travail au sein du Service

Protection des personnes.[99] Le Comité a pu constater qu'avec le temps, la VSSE n'a pratiquement plus eu recours à cette pratique (une seule fois en 2012). Depuis 2013, le Service Protection des personnes n'a plus fait appel à des membres des sections de renseignement.

II.4.5.6. La définition des niveaux de menace

Cette enquête de contrôle n'avait pas pour objectif de se prononcer sur la manière dont les différents acteurs (la VSSE, l'OCAM et le Centre de crise) déterminent et interprètent les niveaux de menace.[100] Le Comité a cependant pu constater que l'application concrète des niveaux de menace sur le terrain n'était pas cohérente. Les dispositifs mis en place sur le terrain se sont en effet avérés très éloignés des niveaux de menace formels définis par l'OCAM.

II.4.5.7. Le désinvestissement en matériel

Enfin, le Comité permanent R a également constaté plusieurs autres problèmes, essentiellement matériels, dans le cadre de l'exécution de la mission de protection de personnes. Le Comité permanent R a recommandé de remédier systématiquement à ces points, en faisant appel aux personnes qui disposent de la connaissance idoine du terrain et qui peuvent dès lors apporter des solutions pratiques.

II.5. UNE PLAINTE DE L'ÉGLISE DE SCIENTOLOGIE CONTRE LA SÛRETÉ DE L'ÉTAT

En mars 2013, l'ASBL Église de scientologie de Belgique a introduit une plainte auprès du Comité permanent R.[101] Le plaignant faisait référence à des articles parus dans *La Dernière Heure*, *Het Laatste Nieuws* et *De Morgen,* qui se fondaient sur deux notes divulguées de la VSSE. Une de ces notes s'intitulait « *Église de scientologie – Infiltration de la communauté congolaise ou d'origine congolaise de Belgique, implantation en République démocratique du Congo* », tandis que l'autre

99 Cette pratique présentait de nombreux inconvénients: l'exécution des missions de renseignement de la VSSE ont ainsi été affaiblies et les membres des sections de renseignement, qui doivent normalement œuvrer en toute discrétion (contact avec les sources, filature…), ont été mis sous les feux de la rampe.

100 Voir à cet égard: COMITÉ PERMANENT R, *Rapport d'activités 2012*, 35-37 (II.5 Enquête commune sur les évaluations de la menace effectuées par l'OCAM concernant des personnalités étrangères en visite en Belgique).

101 L'enquête a été ouverte le 14 avril 2013 et le rapport final a été approuvé le 21 mai 2014. Elle a été suspendue pendant une longue période parce qu'une enquête similaire était en cours à la demande du Sénat.

concernait une « *Analyse de phénomène d'ingérence non étatique* ».[102] Il ressortait des articles que la VSSE a estimé que l'Église de scientologie souhaitait s'implanter en République démocratique du Congo et cherchait, à cette fin, des intermédiaires dans la communauté belgo-congolaise. Mais le mouvement religieux aurait aussi voulu offrir son soutien au groupe de rebelles de l'est de la RDC, le « Mouvement du 23 mars », également appelé « M23 ». L'Église de scientologie a posé trois questions précises au Comité :

- *« enquêter sur la réalité du fondement de ces informations et sur la manière avec laquelle ces informations ont été diffusées au public ;*
- *opérer un contrôle sur la manière avec laquelle ce rapport a été rédigé et sur la manière avec laquelle ce rapport a été diffusé ;*
- *dire si ces dénigrements portent atteinte aux droits fondamentaux conférés par la Constitution à l'association plaignante, notamment à la présomption d'innocence ».*

Le Comité permanent R a déjà répondu à certaines de ces questions dans l'enquête de contrôle « *Notes secrètes sur l'Église de scientologie dans la presse* ». Le Comité a rédigé un rapport détaillé sur la réalisation et la diffusion des notes classifiées concernées. Aussi le présent rapport ne reprend-il que sommairement ces éléments.

II.5.1. LE SUIVI DE L'ÉGLISE DE SCIENTOLOGIE PAR LA VSSE

Le Comité permanent R est conscient que la surveillance d'un mouvement religieux par un service de renseignement peut susciter certaines craintes pour la liberté religieuse et la liberté d'association.

Le Comité permanent R a conclu de son enquête qu'en surveillant les activités de l'Église de scientologie en Belgique, la VSSE agissait dans le cadre de ses compétences légales, telles que définies aux articles 7 et 8 de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Parmi les activités qui menacent ou pourraient menacer les intérêts fondamentaux de l'Etat, l'article 8 L.R&S inclut notamment l'ingérence, les organisations sectaires nuisibles et les organisations criminelles. « *La sécurité et la sauvegarde physique et morale des personnes* », de même que « *la sécurité et la sauvegarde des biens* » sont des intérêts que l'article 8 L.R&S inclut dans les notions de « *sûreté intérieure de l'État* » et de « *pérennité de l'ordre démocratique et constitutionnel* », au même titre que la sécurité et la sauvegarde de l'État, de l'État de droit et des institutions démocratiques.

---

[102] Pour plus de détails sur ces deux notes : COMITÉ PERMANENT R, *Rapport d'activités 2013*, 25-31 (II.2 Notes secrètes sur l'Église de scientologie dans la presse).

Dans une enquête précédente consacrée au suivi des organisations sectaires nuisibles par la VSSE[103], le Comité permanent R avait déjà conclu que :

- les critères de nuisibilité utilisés pour analyser les agissements d'un mouvement religieux et le qualifier de « sectaire » et de « nuisible » étaient pertinents et se référaient aux principes fondamentaux énoncés dans la Constitution, les lois et les conventions internationales en matière de protection des droits de l'homme ;
- les priorités retenues étaient également adaptées à la gravité de certaines menaces constatées en Belgique.
- les menaces identifiées concernaient non seulement l'exercice de la liberté individuelle, la santé et l'intégrité physique des individus, mais aussi l'ingérence sur le fonctionnement des autorités publiques et de l'économie.

En ce qui concerne spécifiquement l'Église de scientologie, la VSSE a mis en avant la volonté de conquête et de transformation totalitaire du monde affichée par cette secte, et a donc conclu à l'inadéquation de cet objectif avec les principes démocratiques de notre société.

Jusqu'en 2007, la VSSE estimait que la menace principale présentée par l'Église de scientologie était un danger d'atteinte à l'intégrité physique et/ou psychologique des personnes, pouvant aller jusqu'à mettre leur vie en péril. En 2008, la VSSE a recadré son travail sur l'Église de scientologie, considérant que la priorité devait dorénavant être accordée à l'ingérence pratiquée par la secte à l'égard des autorités publiques.

Le Comité permanent R a pris connaissance de l'analyse globale de la VSSE des multiples approches de l'ingérence que pratique l'Église de scientologie à l'égard des autorités publiques. Le Comité a cependant constaté que les observations propres de la VSSE n'ont jamais fait apparaître de moyens à proprement parler « *illicites* » mis en œuvre par l'Église de scientologie pour approcher les décideurs politiques. La VSSE disposait par contre de nombreuses indications laissant supposer l'utilisation de « *moyens trompeurs et clandestins* » à cet effet.

Le Comité permanent R a donc conclu que la VSSE suivait les activités de l'ASBL « *Église de scientologie de Belgique* » de manière légale, sans enfreindre les droits que la Constitution et la loi confèrent à la partie plaignante.

[103] Un résumé de cette enquête de contrôle figure dans le rapport d'activités de 2010 (COMITÉ PERMANENT R, *Rapport d'activités 2010*, 13).

II.5.2. LES INFORMATIONS À LA BASE DES NOTES DIVULGUÉES

Les informations figurant dans les deux notes ont été recueillies à l'aide de diverses méthodes de renseignement (dont une analyse de sources ouvertes et des témoignages d'anciens adeptes), et ce par plusieurs départements au sein de la VSSE. Le Comité permanent R n'a constaté aucune irrégularité en la matière.

Les informations remises aux autorités ont été évaluées et analysées dans les règles de l'art.

Les rapports que le Comité a étudiés étaient condensés et contenaient essentiellement des faits. Les réserves requises y étaient émises lorsque certaines données ne pouvaient être confirmées.

Les analyses portaient surtout sur l'idéologie, l'organisation pratique, les activités et l'implantation de l'Église de scientologie.

II.5.3. LA DIFFUSION DES DEUX NOTES ET LA PRÉSOMPTION D'INNOCENCE

Le plaignant estimait que ce n'était pas un hasard si les fuites dans la presse étaient concomitantes avec le traitement du dossier contre l'Église de scientologie devant la Chambre du Conseil. L'objectif aurait été de nuire à cette Église, ou du moins de ternir son image. En outre, le plaignant a attiré l'attention sur le fait que la VSSE était désignée en tant qu'expert technique dans cette affaire.

Eu égard à cet aspect de la plainte, le Comité a repris ses constatations de l'enquête de contrôle précédente.[104] Il a donc conclu que son enquête sur la diffusion des documents visés et leur fuite n'avait mis au jour aucun élément prépondérant indiquant la responsabilité de la VSSE en la matière.

II.6. LA POSITION D'INFORMATION DES SERVICES DE RENSEIGNEMENT ET DE L'OCAM CONCERNANT UN ÉLÈVE PILOTE

Une enquête de contrôle du Comité permanent P relative à des «*flux d'informations dans les aéroports*»[105] a notamment fait référence à une personne qui a pu suivre une formation de pilote dans un aéroport belge, alors que des signes de radicalisation avaient été relevés dans son passé. Cet exemple étant susceptible d'indiquer une défaillance dans l'échange d'informations entre les

104 COMITÉ PERMANENT R, *Rapport d'activités 2013*, 25-31.

105 www.comitep.be/AdditionalReports/2012-06-12_FR_informatiestromen_luchthavens.pdf («Flux d'informations opérationnelles au sein des aéroports»).

différents services publics concernés, les Comités P et R ont décidé d'ouvrir une enquête de contrôle commune en juin 2013 « *sur la position d'information et le suivi des services d'appui de l'OCAM – ainsi que sur l'évaluation de la menace faite par l'OCAM – à propos d'un particulier X admis à suivre des cours de pilotage en Belgique* ».[106, 107]

L'élève pilote concerné – d'origine étrangère et arrivé en Belgique au début des années '90 – s'est retrouvé dans la ligne de mire de la VSSE pour la première fois à l'époque de sa demande de naturalisation à la fin des années '90.[108] Le service était en possession d'informations sur l'appartenance de l'intéressé à une organisation donnée et sur la formation en aéronautique qu'il a reçue. L'homme a confirmé ces informations lors d'un entretien avec des agents de la VSSE. Il a également déclaré que son refus de participer à certains « actes » de cette organisation dirigés contre un autre État l'avait conduit à venir se réfugier en Belgique. Selon lui, seule son appartenance à l'organisation pouvait lui permettre de faire des études. La VSSE a estimé que ces déclarations étaient crédibles.

Cette même année, l'intéressé a posé sa candidature pour une fonction technique liée à l'entretien à l'aéroport de Zaventem. Une enquête complémentaire a été demandée au poste de la VSSE de l'aéroport, mais elle n'a rien relevé de particulier.

Ce n'est qu'en mars 2006 que l'homme attire de nouveau l'attention des services de sécurité : selon la Police aéronautique de Bruxelles-National, il aurait eu un comportement agressif – sous l'influence d'un imam radical – et se serait même radicalisé. La VSSE en est informée. Elle rencontre l'homme pour la seconde fois, toujours sans rien relever. Il apparaît toutefois que l'intéressé fréquente une mosquée connue de la VSSE.

En novembre 2007, la VSSE reçoit à nouveau des informations, cette fois de la Police aéronautique Ostende-Wevelgem : l'intéressé suit des leçons de pilotage en vue d'obtenir un brevet de pilote privé. Il est particulièrement pressé et il paie ses leçons en cash, ce qui pourrait être problématique selon les informations policières de mars 2006. La VSSE ne dispose néanmoins d'aucun élément concret indiquant une tendance à la radicalisation.[109]

---

106 Le présent rapport ne mentionne que sommairement les résultats de l'enquête qui concernent le volet policier. Pour plus de détails, le Comité permanent R renvoie aux publications du Comité permanent P.

107 Lors de la discussion de la présente enquête de contrôle au sein de la Commission de suivi de la Chambre, il a été décidé en 2015 d'approfondir un aspect dans une nouvelle enquête de contrôle « *sur la manière dont l'OCAM détermine le niveau de la menace que représente un individu ou de celle qui le vise, sur les conséquences que la détermination de ce niveau de la menace entraîne sur la répartition des tâches, les mesures à prendre et l'échange d'information entre services concernés, ainsi que sur les conséquences pratiques pour la personne concernée et son suivi* ».

108 La VSSE n'a pas gardé de copie de l'avis rendu en 1998 dans le cadre de la procédure de naturalisation. Voir aussi à cet égard : COMITÉ PERMANENT R, *Rapport d'activités 2012*, 5-14 (II.1. Le rôle de la VSSE dans le cadre des procédures d'acquisition de la nationalité belge).

109 La VSSE n'a pas mené d'investigation sur les fonds destinés à payer les cours de pilotage, jugeant une telle enquête non proportionnelle, étant donné l'absence d'éléments indiquant une quelconque radicalisation.

Toutefois, les différents services de sécurité (police, VSSE, SGRS et OCAM) échangent désormais régulièrement des informations. C'est d'ailleurs la première fois que le SGRS reçoit des informations concernant l'intéressé. Le SGRS n'a cependant pas enquêté sur lui, et ce malgré l'attention particulière qu'il disait accorder aux élèves pilotes depuis les attentats du 11 septembre 2001.

À la demande de la Police aéronautique Ostende-Wevelgem, une réunion de coordination est organisée en décembre 2007 concernant l'intéressé. Plusieurs services de police et les deux services de renseignement y assistent. La VSSE et le SGRS n'ont aucune nouvelle information à fournir.

Après la réunion, la DJP/Terro de la Police fédérale estime qu'il n'y a aucune raison de refuser à l'intéressé le badge de sécurité lui donnant accès à l'aéroport de Wevelgem. En revanche, il est décidé de signaler l'intéressé sur la base de la convention de Schengen et de demander une évaluation de la menace à l'OCAM.

À la mi-décembre 2007, l'analyse de l'OCAM est prête[110] : elle fixe la menace au niveau « 2 ».[111, 112] À la demande des Comités, l'OCAM a expliqué n'avoir jamais reçu d'informations précises quant à l'intention de l'intéressé de commettre un acte terroriste. Les seuls éléments inquiétants étant son passé dans une organisation donnée, ses leçons de pilotage et un changement de comportement (temporaire). Le niveau de menace 3 (qui équivaut à une menace « *possible et vraisemblable* ») n'était donc pas justifié. L'OCAM a néanmoins conseillé à tous les services de rester vigilants, de suivre en permanence la situation de l'intéressé, et d'être attentifs à d'éventuelles évolutions dans son comportement, qui pourraient laisser penser à une radicalisation. Dans le cas d'un « niveau 2 », l'OCAM ne suit pas le dossier activement, mais le confie aux services compétents, sans désigner un « service pilote » spécifique à cet effet. Ce n'est qu'à partir du « niveau 3 » que l'OCAM procède à un suivi actif. Les Comités ont toutefois dû constater que les différents services d'appui concernés ne savaient pas clairement qui devait se charger de la coordination, ni en quoi devait consister exactement le suivi demandé. Pour un service d'appui qui n'a pas participé à l'évaluation depuis le début, il n'était pas toujours possible de savoir si un suivi permanent avait été demandé par l'OCAM.

---

110 Il a été demandé, tant à l'Office des étrangers (OE) qu'au SPF Mobilité (c'est-à-dire deux services d'appui de l'OCAM), de fournir un complément d'informations. L'OCAM n'a toutefois reçu de ces services aucune information complémentaire susceptible d'indiquer un risque accru de danger.

111 « *Le niveau 2 ou MOYEN est attribué lorsqu'il apparaît que la menace à l'égard de la personne, du groupement ou de l'événement qui fait l'objet de l'analyse est peu vraisemblable* » (art. 11, § 6, 2° AR OCAM).

112 L'OCAM a remarqué qu'il n'y avait aucun élément indiquant que l'intéressé inciterait lui-même à la radicalisation. Dans ce sens, il ne relevait pas du Plan Radicalisme.

Début 2008, plusieurs réunions supplémentaires sont organisées avec les services de sécurité, et des informations sont régulièrement échangées. En avril 2008, la VSSE rédige une note de synthèse interne sur la menace que pourrait présenter l'intéressé. Le service conclut une nouvelle fois ne disposer d'aucune information négative.

À la mi-novembre 2008, il ressort de nouvelles informations policières que l'intéressé aurait eu un comportement étrange à l'aéroport lors de son retour de vacances. Une nouvelle réunion de coordination est organisée. Peu de temps après, la VSSE décide de s'entretenir avec l'individu pour la troisième fois. Cette fois, son employeur est également interrogé. Ces différents entretiens ne révèlent toujours aucun signe de radicalisation.

Entre 2009 et 2011, la VSSE reçoit encore plusieurs notes de la police. En juin 2010, la VSSE rédige un nouveau rapport qui mentionne que l'intéressé a obtenu son diplôme (*Private Pilot License*) et souhaite suivre une formation de pilote commercial.[113] Il n'a toutefois plus fait l'objet d'un suivi systématique par la VSSE.

II.7. ENQUÊTE DE CONTRÔLE RELATIVE AUX ÉLÉMENTS TRANSMIS PAR LA VSSE DANS LE CADRE D'UN DOSSIER DE NATURALISATION

Un procureur du Roi s'est opposé à l'octroi de la nationalité belge à un particulier, s'appuyant sur des «*faits personnels graves*» révélés par la VSSE. L'intéressé a toutefois estimé qu'il s'agissait d'un malentendu. À la fin juillet 2013, cette personne a déposé plainte auprès du Comité permanent R[114], qui a alors ouvert une enquête de contrôle. Cette enquête a été finalisée en février 2014.

II.7.1. LA PLAINTE

Le plaignant estimait être victime d'une atteinte à ses droits individuels par la VSSE. L'avis du procureur du Roi faisait effectivement état que l'intéressé était connu de la VSSE pour sa participation active à un mouvement qui figure sur la

113 À partir de mai 2012, l'intéressé ne disposait plus d'une habilitation valable. Il ne pouvait donc plus piloter d'avions.

114 En mai 2013, le plaignant s'est également adressé à la Commission de la protection de la vie privée afin d'accéder aux données à caractère personnel traitées par la VSSE. Conformément à l'art. 13 alinéa 3 de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (la Loi Vie privée), la Commission a fait savoir au plaignant qu'elle avait procédé à toutes les vérifications requises. L'intéressé a également demandé la saisine du tribunal de première instance, ce qui a entraîné la transmission du dossier à la Chambre des Représentants comme demande de naturalisation.

liste européenne d'organisations terroristes, ainsi que pour son « *implication présumée* » dans des activités d'extorsion, de corruption de fonctionnaires, de blanchiment d'argent et de financement du terrorisme avec des faux billets.

Selon le plaignant, les raisons précitées étaient totalement dénuées de fondement. Il les a qualifiées de « *très vexantes, dégradantes et insultantes* ». Et de prétendre qu'aucun des faits portés à la connaissance du procureur du Roi par la VSSE n'est étayé par le moindre élément concret. En outre, le plaignant a invoqué son casier judiciaire vierge.

II.7.2. CONSTATATIONS

Après enquête, le Comité est arrivé à la conclusion que dans le cas présent, l'évaluation, le traitement et la communication des informations par la Sûreté de l'État aux autorités judiciaires posaient effectivement problème.

Le nom du plaignant apparaît pour la première fois à la VSSE en 2009. La VSSE reçoit alors des informations indiquant que l'intéressé est un militant d'une organisation terroriste déterminée. Les informations font également mention de son implication dans des délits de droit commun. Vu que les informations disponibles ne provenaient que d'une seule source, une enquête complémentaire a été menée.

En application de l'article 29 CIC, la VSSE a communiqué, au début de l'année 2010, toutes les informations plutôt vagues et non confirmées au procureur du Roi et au procureur fédéral. Comme la VSSE n'a pas été chargée d'une mission d'expertise, le service en a déduit qu'aucune enquête judiciaire n'a été ouverte à la suite de cette communication.

Lorsque le plaignant introduit sa demande d'obtention de la nationalité belge en décembre 2012, la VSSE transmet sans réserve les mêmes informations (non actualisées) au parquet. Celles-ci ont amené le procureur du Roi compétent à émettre un avis négatif sur la demande de nationalité.

En négligeant de mettre à jour les informations sur le plaignant, la VSSE a fait preuve de légèreté et a ainsi compromis ses chances d'obtenir la nationalité belge.

À la suite de la plainte que la personne lésée avait introduite auprès du Comité permanent R, la VSSE a rectifié sa position et a actualisé les informations. Compte tenu des nouvelles informations recueillies, la VSSE a estimé que le plaignant devait être considéré comme n'étant « *pas défavorablement connu par la VSSE* ». La VSSE s'est engagée à en informer le procureur du Roi compétent.

II.8. PLAINTE RELATIVE À LA MANIÈRE DONT LA VSSE SUIT LE DIRIGEANT D'UNE ENTREPRISE D'EXPORTATION BELGE

À la mi-2013, le dirigeant d'une entreprise a adressé une plainte au Comité.[115] Certains membres de la VSSE seraient passés régulièrement chez lui depuis 2010 pour lui poser de nombreuses questions sur des clients et fournisseurs et leurs données bancaires. L'entreprise opère comme courtier (« *broker* ») et agit donc en tant que négociateur ou intermédiaire lors de la vente ou l'exportation de produits.[116] Dans ce cas-ci, il s'agissait de « *biens à double usage* » ou, en d'autres termes, de « *produits, y compris les logiciels et les technologies, susceptibles d'avoir une utilisation tant civile que militaire; ils incluent tous les biens qui peuvent à la fois être utilisés à des fins non explosives et entrer de manière quelconque dans la fabrication d'armes nucléaires ou d'autres dispositifs nucléaires explosifs* ».[117]

Les contacts entre le plaignant et la VSSE auraient été de moins en moins cordiaux au fil du temps. Le plaignant s'est même senti intimidé et menacé. Il craignait également que les informations qu'il devait fournir atterrissent dans les mains de tiers et se demandait s'il était réellement obligé de collaborer avec le service de renseignement.

II.8.1. LE RÉCIT DES FAITS

Lorsque l'Administration des Douanes et Accises (D&A) procède à un contrôle de routine au sein de l'entreprise concernée en 2010, elle est confrontée à une tentative d'exportation de marchandises visées par un embargo. L'entreprise a versé une somme substantielle pour régler la situation à l'amiable et ainsi échapper à des poursuites judiciaires.

La VSSE est néanmoins informée de l'affaire par le « Dienst Controle Strategische Goederen » (DCSG), qui contrôle les activités de ce genre d'entreprises en Flandre et entretient des contacts réguliers avec le service de renseignement. La VSSE ouvre alors un dossier. Il ressortira des contacts avec les

---

115 Le Comité a ouvert une enquête de contrôle le 3 octobre 2013 et a envoyé son rapport final à la Commission de suivi le 12 septembre 2014.

116 Étant donné qu'un courtier peut assumer différents rôles, il est difficile de se faire une idée précise de son fonctionnement. En outre, comme il arrive qu'un courtier agisse en tant que négociateur entre deux personnes (morales) établies à l'étranger, les produits négociés ne transitent jamais par la Belgique.

117 Règlement (CE) n° 1334/2000 du Conseil du 22 juin 2000 instituant un régime communautaire de contrôle des exportations de produit et technologies à double usage.

deux autorités concernées (D&A et DCSG) que d'autres « incidents »[118] s'étaient déjà produits par le passé. L'entreprise prendrait la réglementation en vigueur à la légère. Des correspondants étrangers ont également informé la VSSE de comportements suspects et de contacts entre l'entreprise et des partenaires commerciaux étrangers.

La VSSE a également contacté directement l'entreprise concernée. Au total, entre 2010 et la fin 2013, la VSSE s'est rendue sur place à douze reprises pour demander des données.

II.8.2. LES CONSTATATIONS

II.8.2.1. La compétence de la VSSE

Les activités de l'entreprise en question pouvaient être liées à la prolifération, une matière qui constitue l'une des missions principales de la VSSE (art. 8 L.R&S). En outre, cette menace méritait un « suivi prioritaire actif »[119] en vertu du plan d'action de l'époque. À la lumière des indices fournis par les services tiers, la VSSE aurait commis un manquement grave si elle n'était pas intervenue.

La plainte de l'entreprise à l'égard de la VSSE (à savoir que la VSSE l'a suivie à tort) n'était donc pas fondée. En effet, l'intervention de la VSSE n'était pas arbitraire, mais reposait sur des indices importants, et la VSSE est restée dans le cadre de ses compétences légales. En outre, lors de l'évaluation de l'affaire, il s'est avéré que la VSSE n'avait pas agi dans la précipitation ou manqué de nuance.

II.8.2.2. Les contacts directs avec le plaignant

La VSSE a assez rapidement choisi de contacter directement l'entreprise concernée. Elle est partie du principe que les irrégularités constatées ne visaient pas à enfreindre délibérément les restrictions à l'exportation, mais qu'il s'agissait plutôt d'actes d'une petite entreprise qui tentait de survivre financièrement et

---

118 Les deux administrations ont eu de nombreux contacts avec l'entreprise, qui avait apparemment des problèmes avec la gestion des documents et avec la réglementation. Plusieurs concertations ont été organisées avec le DCSG afin d'expliquer à l'entreprise la législation, les sanctions, la nécessité de fournir des données techniques, etc. Les Douanes & Accises ont notamment passé des accords avec l'entreprise pour faire exécuter un contrôle de douane complet, mais l'entreprise n'a pas honoré ces accords.

119 Il ressort d'ailleurs de rapports des Nations unies que la prolifération d'armes NRBC doit être considérée comme l'une des principales menaces. La lutte contre la prolifération est fondamentale dans la problématique de la sécurité nationale et internationale. La VSSE a une mission importante à remplir dans ce domaine. Par le passé, le Comité permanent R s'est déjà penché sur l'activité de la VSSE dans le domaine de la prolifération : COMITÉ PERMANENT R, *Rapport d'activités 2008*, 40-41, *Rapport d'activités 2011*, 37-40 et *Rapport d'activités 2013*, 48-51.

qui ne se rendait peut-être pas tout à fait compte de la portée de ses actes. Aussi la VSSE a-t-elle opté, à juste titre, pour une méthode de recueil de données ordinaire, à savoir l'approche directe de l'intéressé.

Les questions que la VSSE a posées concernant les données bancaires et celles des clients étaient justifiées et entraient dans le cadre des compétences de la VSSE. Compte tenu des circonstances, cette méthode était suffisante et proportionnelle pour recueillir des renseignements.[120] Ce genre d'informations peut être recueilli auprès de toute personne ou organisation privées (art. 16 L.R&S). L'intéressé reste toutefois lié par le secret professionnel auquel il est soumis le cas échéant, ou par les exigences posées par la législation relative à la protection de la vie privée. Ces deux réglementations imposent des restrictions quant à la communication de données à des tiers.

Les documents de la VSSE n'ont pas permis de vérifier si un membre de la VSSE avait effectivement eu un comportement intimidant à l'égard du plaignant. Interrogés expressément à ce propos, les membres de la VSSE ont nié s'être montrés intimidants. Le Comité a estimé qu'il n'était plus possible de découvrir *a posteriori* la vérité sur ce qui s'est passé, mais a souligné qu'il va de soi que l'intimidation n'est pas tolérable.

Enfin, le Comité a insisté sur le fait que le citoyen a le droit de ne pas collaborer à une enquête de renseignement.

II.8.2.3. La complexité de la lutte contre la prolifération

En marge de l'enquête, le Comité permanent R a constaté que la problématique de la prolifération est très complexe et peu transparente, tant pour les entreprises qui y sont confrontées que pour les services qui ont un rôle à jouer dans ce cadre.

De plus, il est apparu qu'un régime adéquat de contrôle et de sanction faisait toujours défaut. Bien que le rôle de la VSSE ne consiste évidemment ni à contrôler ni à sanctionner, cela implique que les problèmes de compétence qui existent en la matière entre l'État fédéral et les Régions[121] ne sont pas de nature à faciliter les missions des services concernés, et partant, celles de la VSSE, qui devrait pouvoir recevoir des informations utiles de ces services.

---

120 Étant donné que le dossier portait sur la lutte contre la prolifération, la VSSE aurait aussi pu recourir, en théorie, à des méthodes MRD exceptionnelles pour obtenir les données bancaires ou des communications avec des clients. Mais dans ce cas-ci, le recours à des méthodes exceptionnelles n'était pas nécessaire.

121 Une question parlementaire adressée au Ministre-Président du Gouvernement flamand et portant sur une collaboration structurelle entre le DCSG, la VSSE et les D&A révèle que celle-ci n'est pas encore au point. En effet, l'État fédéral et les trois Régions ont conclu un accord de coopération en 2007 concernant l'importation, l'exportation et le transit, ainsi que les produits et technologies à double usage et l'octroi de licences en la matière. Mais cet accord concernait uniquement le SPF Affaires étrangères et les Régions, et non le SPF Économie, la VSSE et les D&A (*Ann. parl.* Parlement flamand, 2013-2014, 1er avril 2014, n° C172-BUI7, 15, Q. n° 1159).

Dans les conclusions de l'enquête de contrôle sur *« Le rôle des services de renseignement dans la lutte contre la prolifération d'armes non conventionnelles et très sophistiquées »* de 2008, le Comité permanent R a déjà souligné que la détection des transactions relatives à la prolifération et à la clause « *catch all* »[122] est difficile pour plusieurs raisons. Et de citer le grand nombre de transactions à destination des pays « proliférateurs », la problématique des matériaux à double usage, le manque de fiabilité et de transparence des données fournies par les firmes, ainsi que la complexité du système de codage des biens par les services de douane.[123]

La présente enquête a montré que les problèmes précités n'ont pas encore été résolus, ce qui complique l'intervention de la VSSE dans cette matière.

II.9. UN PARTICULIER SUIVI PAR LES SERVICES DE RENSEIGNEMENT ?

À la fin novembre 2013, une plainte a été introduite auprès du Comité permanent R. Le plaignant, domicilié en Belgique depuis 1994 et détenteur de la nationalité belge, était persuadé de faire l'objet d'une surveillance physique et de filatures par « les services de renseignement ». Il y voyait plusieurs raisons possibles, entre autres son appartenance à mouvement islamique religieux. Le plaignant avait l'impression que ses communications téléphoniques et son courrier électronique étaient interceptés. Les faits se produiraient tant en Belgique que dans son pays d'origine.

Le Comité a ouvert une enquête de contrôle début février 2014 afin de répondre aux questions suivantes : l'intéressé était-il effectivement connu de la Sûreté de l'État et du SGRS ? Dans l'affirmative, depuis quand et dans quel cadre ? Des méthodes particulières de renseignement ont-elles été mises en œuvre ? Quels renseignements le concernant ont été recueillis ?… Le Comité n'était évidemment pas compétent pour examiner le rôle éventuel de services de renseignement étrangers.

L'enquête de contrôle a été clôturée à la mi-mai 2014. Il s'est avéré que les services de renseignement belges n'avaient mené aucune activité illégale à l'égard du plaignant.

---

122 Tout matériel militaire, et donc soumis à un contrôle, a été défini au niveau international et consigné dans des listes de production. Ce qui n'empêche pas plusieurs pays d'avoir prévu dans leur législation une clause permettant de placer sous licence des produits qui ne figurent pas sur la liste, pour des raisons de sécurité, par exemple parce qu'ils sont utilisés à des fins militaires. C'est le « *catch all* ».

123 COMITÉ PERMANENT R, *Rapport d'activités 2008*, 40-54, particulièrement p. 53-54.

II.10. ENQUÊTES DE CONTRÔLE POUR LESQUELLES DES DEVOIRS D'ENQUÊTE ONT ÉTÉ POSÉS EN 2014 ET ENQUÊTES QUI ONT DÉBUTÉ EN 2014

Cette section énumère et situe brièvement toutes les enquêtes que le Comité permanent R a démarrées en 2014, ainsi que les enquêtes sur lesquelles il a continué de travailler au cours de cette même année, mais qui n'ont pas encore pu être clôturées.

II.10.1. LE SUIVI D'ÉLÉMENTS EXTRÉMISTES AU SEIN DE L'ARMÉE

À l'occasion de briefings donnés par le SGRS, le Comité permanent R a pris connaissance de la problématique de militaires évoluant dans des milieux extrémistes et de militaires membres ou sympathisants de bandes de motards. Durant cette même période, les médias ont fait mention de la présence (temporaire), au sein du Bataillon de Chasseurs ardennais, d'un militant djihadiste qui aurait rédigé un manuel de combat en s'appuyant sur l'expérience acquise.

Le Comité a décidé d'ouvrir une enquête de contrôle sur «*la recherche et le suivi par le SGRS d'éléments extrémistes au sein du personnel de la Défense et des Forces armées*». L'enquête a pour but de vérifier si le SGRS aborde cette problématique de manière efficace et si ce service respecte les droits des citoyens dans ce cadre.

Au cours de l'enquête, la réglementation relative à la vérification (également appelée «screening») des candidats à la Défense a fait l'objet de modifications. Il a été décidé d'élargir l'enquête à cette matière afin de se pencher sur deux processus: le screening pendant la phase de recrutement, d'une part, et la détection et le suivi d'éléments radicaux ou extrémistes déjà recrutés, d'autre part.

Dans le courant de l'année 2014, des informations complémentaires ont notamment été demandées à l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité, et des devoirs d'enquête supplémentaires ont été effectués. Il a également été décidé de compléter les résultats provisoires de l'enquête par des informations sur la problématique syrienne.[124]

[124] En mars 2015, le ministre de la Défense a révélé, en Commission de la Défense, que deux anciens militaires belges radicalisés combattraient en Syrie.

II.10.2. LA MANIÈRE DONT LES FONDS SPÉCIAUX SONT GÉRÉS, UTILISÉS ET CONTRÔLÉS

En 2011-2012, les autorités judiciaires ont ouvert deux enquêtes judiciaires sur l'éventuelle utilisation abusive de fonds destinés à la rémunération d'informateurs. En vertu de sa mission judiciaire, le Service d'Enquêtes R a été sollicité dans les deux enquêtes.[125] Vu les éléments dont le Comité permanent R a pu disposer, mettant au jour d'éventuels problèmes structurels, il a été décidé, début septembre 2012, d'ouvrir une enquête thématique sur «*la manière de gérer, d'employer et de contrôler les fonds destinés à la rémunération des informateurs de la VSSE et du SGRS*».

Toutefois, compte tenu des enquêtes judiciaires en cours, l'enquête de contrôle a été suspendue immédiatement. À la fin mars 2014, le Comité a décidé que l'enquête de contrôle pouvait reprendre. Le rapport sera finalisé en 2015.

II.10.3. ENQUÊTE DE CONTRÔLE SUR LA *JOINT INFORMATION BOX*

La création d'une «*Joint information box*» (JIB) – approuvée par le Comité ministériel du renseignement et de la sécurité – constituait, pour ses initiateurs, le point fort du «Plan d'action Radicalisme». Il s'agit d'un fichier de travail géré au sein de l'OCAM vise notamment la collecte structurelle d'informations sur les entités suivies dans le cadre du Plan d'action Radicalisme.

Lors d'une réunion commune des Comités permanents P et R à la mi-novembre 2012, il a été décidé d'ouvrir une enquête de contrôle «*sur la manière dont l'OCAM gère, analyse et diffuse les informations stockées dans la Joint information box (JIB), en rapport avec l'exécution du Plan Radicalisme*».

En 2014, les Services d'Enquêtes P et R ont posé plusieurs actes d'enquête. Le rapport de contrôle a été finalisé en avril 2015 et a été transmis au président de la Commission de suivi et aux ministres de la Justice et de l'Intérieur.

II.10.4. AGENTS DE RENSEIGNEMENT ET MÉDIAS SOCIAUX

À la fin 2012, les médias ont évoqué la présence de collaborateurs de services de renseignement sur des réseaux sociaux tels que *Facebook* et *LinkedIn*. La Commission sénatoriale de suivi de l'époque a dès lors demandé au Comité

125 COMITÉ PERMANENT R, *Rapport d'activités 2013*, 97-98. (Chapitre VI. Les informations et instructions judiciaires).

permanent R d'ouvrir une enquête de contrôle sur «*l'ampleur du phénomène de publicité que donnent des collaborateurs de la Sûreté de l'État, mais aussi éventuellement du SGRS et de l'OCAM, de leur qualité d'agent de ces institutions sur Internet via des médias sociaux*». Le Comité a aussi reçu pour mission d'examiner les risques liés à une telle publicité et les mesures qui peuvent ou doivent être prises à cet égard.

Le Comité permanent R a démarré son enquête de contrôle concernant les collaborateurs du SGRS et de la VSSE en décembre 2012. Plusieurs actes d'enquête ont été posés. Le rapport final a été finalisé au cours du premier semestre 2015.

II.10.5. MEMBRES DU PERSONNEL DE L'OCAM ET MÉDIAS SOCIAUX

En ce qui concerne le volet relatif aux collaborateurs de l'OCAM et leur présence sur des sites de réseaux sociaux, une enquête de contrôle commune a été ouverte au début 2013 avec le Comité permanent P. En effet, en vertu de l'article 56, 6° L.Contrôle, le contrôle externe du fonctionnement de l'OCAM est exercé conjointement par les deux Comités.

Le rapport final a été approuvé en mars 2015 lors de la réunion conjointe des Comités permanents R et P et a été envoyé à la Commission de suivi de la Chambre.

II.10.6. LES CONTACTS INTERNATIONAUX DE L'OCAM

L'Organe de coordination pour l'analyse de la menace a entre autres pour mission d'entretenir des contacts avec des «services étrangers ou internationaux homologues» (art. 8, 3° L. OCAM). Lors de leur réunion commune de début mai 2013, les Comités permanents P et R ont décidé de mener une enquête sur la manière dont l'OCAM remplit cette mission.[126] Plusieurs devoirs d'enquête ont été effectués en 2013 et 2014. Cette enquête a été clôturée en juin 2015.

[126] Enquête de contrôle commune sur la manière dont l'OCAM entretient des relations internationales avec des services étrangers ou internationaux homologues en application de l'article 8, 3° de la L.OCAM du 10 juillet 2006.

II.10.7. LA PROTECTION DU POTENTIEL SCIENTIFIQUE ET ÉCONOMIQUE ET LES RÉVÉLATIONS D'EDWARD SNOWDEN

Les révélations d'Edward Snowden ont donné un aperçu du contenu de programmes extrêmement secrets principalement de la National Security Agency (NSA) américaine. Elles ont donné lieu à l'ouverture de nombreuses enquêtes (parlementaires, judiciaires et de renseignement) aux quatre coins du monde, y compris en Belgique. Le Comité permanent R a ouvert quatre enquêtes de contrôle qui sont naturellement étroitement liées.

Trois de ces quatre enquêtes ont été bouclées en 2014 (voir II.1, II.2 et II.3). La dernière enquête de contrôle[127] – qui n'a pas encore été finalisée – traite des implications éventuelles de ces programmes étrangers pour la protection du potentiel scientifique et économique du pays. Elle entend vérifier si les services de renseignement belges :

- se sont intéressés à ce phénomène ;
- ont détecté une menace réelle ou éventuelle pour le potentiel scientifique et économique belge ;
- en ont informé les autorités compétentes et ont proposé des mesures de protection ; et
- disposent de moyens suffisants et adéquats pour suivre cette problématique.

À l'époque, le Sénat avait aussi demandé d'examiner les conséquences de la captation massive de données sur le potentiel scientifique et économique belge. Toutefois, le Comité permanent R n'a ni la compétence légale, ni les moyens techniques et humains d'évaluer de son propre chef les opérations d'interceptions massives de données que des services de renseignement étrangers mèneraient à l'encontre d'entreprises et/ou de centres de recherches belges. Soucieux néanmoins de satisfaire à la demande du Sénat, le Comité permanent R a décidé de ne pas se limiter à enquêter auprès de la VSSE et du SGRS. Tout au long de l'année 2014, le Comité s'est adressé à un panel de personnalités représentatives des milieux scientifiques et économiques belges. Il a ainsi cherché à prendre connaissance de cas éventuels dans lesquels des entreprises et/ou centres de recherches belges auraient ou estimeraient avoir été victimes de telles pratiques. Le Comité a aussi veillé à compléter son information en consultant de nombreuses sources ouvertes (articles de presse, rapports officiels, documents parlementaires…) belges et étrangères, à l'affût de chiffres, d'indices et/ou de témoignages qui lui permettraient d'appréhender les implications des systèmes

127 Enquête de contrôle sur l'attention que les services de renseignement belges portent (ou non) aux menaces que peuvent représenter pour le potentiel scientifique et économique de la Belgique des programmes de surveillance électronique sur les systèmes de communication et d'information mis en œuvre à grande échelle par des puissances et/ou des services de renseignement étrangers.

de captation massive de données sur le potentiel scientifique et économique du pays. À défaut de telles indications, le Comité permanent R a décidé de tenter d'esquisser quelques pistes d'analyse théorique du phénomène.

Le rapport sera clôturé dans le courant de l'année 2015.

II.10.8. SUIVI À TORT PAR LES SERVICES DE RENSEIGNEMENT ?

À la fin février 2014, une personne d'origine nord-africaine a introduit une plainte auprès du Comité permanent R. L'intéressé, qui séjourne en Belgique avec sa famille depuis mai 2012, se plaignait d'être surveillé de « manière oppressante » par les services de renseignement. Le plaignant prétendait ignorer totalement les raisons de cette attention ; il n'a jamais eu de problème dans son pays d'origine ni dans le pays asiatique où il a travaillé pendant plusieurs années. Il n'aurait aucun antécédent judiciaire ni aucun lien avec le terrorisme ou le radicalisme. En outre, il déclarait avoir été l'objet d'opérations de surveillance, un sentiment renforcé par le traitement particulier qui lui a été réservé à deux reprises à l'aéroport de Zaventem.

Le Comité a décidé d'ouvrir une enquête de contrôle en juillet 2014. Par cette enquête, le Comité a voulu vérifier si la Sûreté de l'État ou le SGRS s'était effectivement intéressé(e) au plaignant et, dans l'affirmative, pourquoi et avec quels résultats.

Différents devoirs d'enquête ont été effectués et le rapport final a été envoyé en février 2015 au président de la Commission de suivi ainsi qu'aux ministres de la Justice et de la Défense.

II.10.9. LA VSSE ET L'APPLICATION DU RÈGLEMENT DE TRAVAIL

À la mi-2014, le Comité a décidé d'ouvrir une enquête de contrôle *« sur la manière dont la VSSE interprète et exécute la réglementation du travail, et plus en particulier les règles sur les congés de maladie, sur base d'une plainte d'un membre du personnel »*. Cette enquête faisait suite à une plainte d'un assistant de protection du Service Protection des personnes de la VSSE. L'intéressé a été mis en situation de non-activité, ce qui a donné lieu, selon lui, à un préjudice financier (absence sans solde) et administratif (retard dans la carrière). Il a en outre évoqué d'autres problèmes : la gestion des heures supplémentaires, le cadre légal vague concernant la réglementation de travail, la réglementation en matière de congés de maladie et la médecine préventive…

En février 2015, le rapport final du Comité a été envoyé au ministre de la Justice et au président de la Commission de suivi.

II.10.10. LA PROBLÉMATIQUE DES « FOREIGN FIGHTERS » ET DES PERSONNES PARTIES COMBATTRE EN SYRIE

Depuis 2013, la guerre en Syrie exerce un fort pouvoir d'attraction sur ce que l'on appelle les « *foreign fighters* » du monde entier. Il convient de noter en la matière que, proportionnellement, de nombreux combattants viennent de Belgique.

Le Comité permanent R a dès lors décidé, en octobre 2014, d'ouvrir une enquête de contrôle sur « *la position d'information des deux services de renseignement (VSSE et SGRS) sur le recrutement, l'envoi, le séjour et le retour en Belgique de jeunes (belges et étrangers résidant en Belgique) qui partent ou sont partis combattre en Syrie ou Irak et au transfert des renseignements aux diverses autorités* ». Cette enquête a cherché à répondre aux questions suivantes : quelle est la mission des services de renseignement belges dans ce cadre et quelle ligne à suivre leur a été (est) donnée ? Les services de renseignement belges ont-ils une vue sur les phases de recrutement et de départ ? Peuvent-ils se faire une idée de qui sont ces « combattants syriens » ? Sont-ils au courant des activités de ces combattants sur place ? L'évolution à l'étranger se traduit-elle par d'éventuelles menaces en Belgique et, dans l'affirmative, lesquelles ? Qu'en est-il du suivi et de l'approche lors de leur retour en Belgique ? Comment se déroule la collaboration (SGRS, VSSE, OCAM, mais aussi la police) en la matière ? Comment font-ils rapport de leurs activités et à qui ?…

Un premier rapport intermédiaire a été discuté début mars 2015 au sein de la Commission de la Chambre chargée de l'accompagnement des Comités permanents P et R. Un second rapport sera remis après les vacances parlementaires 2015.

II.10.11. LA VSSE ET LE PROTOCOLE DE COOPÉRATION AVEC LES ÉTABLISSEMENTS PÉNITENTIAIRES

Le 1er octobre 2014, le Comité a ouvert une enquête de contrôle sur la manière dont la VSSE met en application le « *protocole d'accord réglant la coopération entre la Sûreté de l'État et la Direction générale Exécution des Peines et des Mesures* ». Cette enquête découle de deux enquêtes de contrôle clôturées précédemment.[128] Elle a pour objectif d'examiner si l'accord est appliqué efficacement, si la VSSE peut y puiser les informations utiles pour l'exécution de ses missions, et de vérifier, ne fût-ce qu'en marge, si l'échange de données sur des

[128] COMITÉ PERMANENT R, *Rapport d'activités 2011*, 22-25 (II.3. La position d'information et les actions des services de renseignement concerne Lors Doukaev) et *Rapport d'activités 2012*, 28-33 (II.3. Le suivi éventuel d'un particulier pendant et après sa détention en Belgique).

détenus se déroule conformément à la protection des droits que la Constitution et la loi garantissent aux personnes.

Cette enquête sera bouclée en 2015.

II.10.12. ENVOI INJUSTIFIÉ D'INFORMATIONS PAR LE SGRS ?

Au début du mois d'octobre 2014, un particulier a déposé plainte auprès du Comité permanent R. Le plaignant affirmait avoir été licencié pour motif grave sur la base d'informations que son employeur avait obtenues précédemment d'un collaborateur du SGRS. Le Comité a décidé d'ouvrir une enquête de contrôle à la fin octobre 2014.

L'enquête devait établir de quelle manière le SGRS avait traité le dossier, si le service avait respecté dans ce cadre la réglementation en vigueur, et si des informations avaient effectivement été transmises à un tiers.

L'enquête a été clôturée en juin 2015.

CHAPITRE III
CONTRÔLE DES MÉTHODES PARTICULIÈRES DE RENSEIGNEMENT

L'article 35 § 1er, 1° L.Contrôle stipule que le Comité doit consacrer, dans son rapport d'activités annuel, « *une attention spécifique aux méthodes spécifiques et exceptionnelles de recueil de données, telles qu'elles sont visées dans l'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité [et] à l'application du chapitre IV/2 de la même loi* ».[129] Ce chapitre traite dès lors de la mise en œuvre des méthodes particulières de renseignement par les deux services de renseignement et de la manière dont le Comité permanent R exerce son rôle juridictionnel à cet égard. Ce rapport est un condensé des deux rapports semestriels que le Comité doit rédiger pour sa Commission de suivi.[130]

III.1. EN PRÉAMBULE : LE « GROUPE DE TRAVAIL MRD »

En avril 2014, les deux services de renseignement, la Commission BIM et le Service d'Enquêtes du Comité permanent R ont créé un groupe de travail dénommé « groupe de travail MRD ». Ce groupe de travail s'est réuni à quatre reprises en 2014 autour des thèmes suivants : une discussion sur la jurisprudence la plus récente tant de la Commission que du Comité ; l'éclaircissement des questions juridiques et opérationnelles *ad hoc* (par exemple les modalités de la procédure d'extrême urgence) ; la présentation d'un cas concret et l'explication de celui-ci ; et enfin le développement concret d'un sujet lié à une MRD donnée (par exemple les bonnes pratiques en matière de motivation d'une prolongation d'une méthode utilisée). Ces réunions contribuent à une bonne compréhension et stimulent la communication entre les partenaires concernés. Cette concertation informelle ne nuit évidemment en rien à l'indépendance du Comité permanent R dans son appréciation de la légalité des méthodes.

---

129 Pour une analyse des méthodes particulières de renseignement et du contrôle exercé sur celles-ci, voir : COMITÉ PERMANENT R, *Rapport d'activités 2010*, 49-61 en W. VAN LAETHEM, D. VAN DAELE et B. VANGEEBERGEN (eds.), *De Wet op de bijzondere inlichtingenmethoden*, Antwerpen, Intersentia, 2010, 299 p.

130 Art. 35 § 2 et 66*bis* § 2, alinéa 3, L.Contrôle.

III.2. LES CHIFFRES RELATIFS AUX MÉTHODES SPÉCIFIQUES ET EXCEPTIONNELLES

Entre le 1er janvier et le 31 décembre 2014, 1282 autorisations ont été accordées par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de renseignement : 1132 pour la VSSE (976 spécifiques et 156 exceptionnelles) et 150 par le SGRS (114 spécifiques et 36 exceptionnelles).

Le tableau ci-dessous établit une comparaison avec les chiffres des années précédentes. En outre, il convient de noter que depuis janvier 2013, le Comité utilise un autre mode de calcul pour une méthode particulière déterminée. Auparavant, le nombre de « Prises de connaissance de données d'identification de moyens de communication électroniques » n'était pas repris comme tel dans les totaux. C'est cette option qui avait été retenue, puisque la plupart des « Prises de connaissance de données d'identification » sont autorisées par les dirigeants des services de renseignement dans un seul document, où est aussi autorisée, par exemple, une « Prise de connaissance de données d'appel » ou une « Prise de connaissance de données de localisation ». Étant donné qu'il s'agit *stricto sensu* d'autres méthodes, le Comité permanent R a estimé qu'un calcul séparé de telles « Prises de connaissance de données d'identification » donne une vue plus juste du nombre de méthodes spécifiques effectivement mises en œuvre. En d'autres termes, lorsque le nombre de méthodes particulières mentionnées depuis 2013 est plus élevé que les années précédentes, cela tient principalement à un mode de calcul différent, et donc pas au fait que d'autant plus de méthodes ont été employées.

	SGRS		VSSE		TOTAL
	Méthodes spécifiques	Méthodes exceptionnelles	Méthodes spécifiques	Méthodes exceptionnelles	
2012	67	24	655	102	848
2013	131	23	1102	122	1378
2014	114	36	976	156	1282

Alors qu'une augmentation d'environ 13 % était encore enregistrée en 2013 (en tenant compte du nouveau mode de calcul), le nombre total de méthodes particulières de renseignement a diminué de 7 % en 2014. Cette diminution se situe, pour les deux services, au niveau des méthodes spécifiques ; les méthodes exceptionnelles ont quant à elles connu un accroissement.

Dans ce qui suit, trois grandes rubriques sont établies pour chaque service : des données chiffrées sur les méthodes spécifiques, sur les méthodes

exceptionnelles et sur les menaces visées par les différentes méthodes ainsi que les intérêts à protéger.

III.2.1. LES AUTORISATIONS RELATIVES AU SGRS

III.2.1.1. Les méthodes spécifiques

NATURE DE LA MÉTHODE SPÉCIFIQUE	NOMBRE 2012	NOMBRE 2013	NOMBRE 2014
Pénétration et observation dans des lieux accessibles au public à l'aide d'un moyen technique	8	14	7
Pénétration et inspection de lieux accessibles au public à l'aide d'un moyen technique	0	0	0
Prise de connaissance de données d'identification du trafic postal et réquisition du concours d'un opérateur postal	0	0	0
Prise de connaissance des données d'identification de moyens de communication électroniques ; réquisition du concours d'un opérateur ; ou l'accès direct à des fichiers de données	25 dossiers	66 méthodes[131]	67 méthodes
Prise de connaissance des données d'appel de moyens de communication électroniques et réquisition du concours d'un opérateur	30	15	12
Prise de connaissance des données de localisation de moyens de communication électroniques et réquisition du concours d'un opérateur	4	36	28
TOTAL	**67**[132]	**131**[133]	**114**

Là où, pour le SGRS, on notait encore l'année dernière une augmentation du nombre d' « observations » et de « localisations », ces méthodes ont été moins fréquemment appliquées en 2014.

131 En comparaison avec les années précédentes, une diminution est à noter : les 66 autorisations concernent en effet 16 dossiers.

132 Dans un cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste professionnel.

133 Dans un cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste professionnel.

III.2.1.2. Les méthodes exceptionnelles

NATURE DE LA MÉTHODE EXCEPTIONNELLE	NOMBRE 2012	NOMBRE 2013	NOMBRE 2014
Pénétration et observation, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	1	1	1
Pénétration et inspection, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	0	0	1
Création ou recours à une personne morale fictive	0	0	0
Ouverture et prise de connaissance d'un courrier confié ou non à un opérateur postal	0	0	0
Collecte de données concernant des comptes bancaires et des transactions bancaires	7	5	5
Intrusion dans un système informatique	2	0	3
Écoute, prise de connaissance et enregistrement de communications	14	17	26
TOTAL	**24**[134]	**23**[135]	**36**

En ce qui concerne les méthodes exceptionnelles, un chiffre ressort d'emblée : le nombre de mesures d'écoute a augmenté, passant de 17 à 26.

III.2.1.3. Les intérêts et les menaces justifiant le recours à des méthodes particulières[136]

Le SGRS est autorisé à utiliser les méthodes spécifiques et exceptionnelles dans le cadre de trois de ses missions, qui elles-mêmes comprennent des intérêts spécifiques à protéger :

- La mission de renseignement orientée vers les menaces visant, entre autres, l'intégrité du territoire national, les plans de défense militaires et le potentiel scientifique et économique en rapport avec la défense (art. 11, 1° L.R&S) ;
- La mission en matière de sécurité militaire qui vise par exemple le maintien de la sécurité militaire du personnel relevant de la Défense, des installations militaires et des installations militaires et des systèmes informatiques et de communications militaires (art. 11, 2° L.R&S) ;
- La protection des secrets militaires (art. 11, 3° L.R&S).

134 Dans un cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste professionnel.

135 Dans un cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste professionnel.

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

NATURE DE LA MISSION	NOMBRE 2012	NOMBRE 2013	NOMBRE 2014
Mission de renseignement	63	111	109
Sécurité militaire	7	15	5
Protection des secrets	21	28	36

NATURE DE LA MENACE	NOMBRE 2012	NOMBRE 2013	NOMBRE 2014
Espionnage	78	94	123
Terrorisme (et processus de radicalisation)	3	6	7
Extrémisme	3	24	15
Ingérence	2	1	0
Organisations criminelles	1	16	2
Autres	5	13	0

En ce qui concerne le SGRS, la menace « espionnage » requiert toujours la mise en œuvre de la plupart des méthodes MRD. Il convient de noter l'utilisation plutôt limitée des méthodes MRD dans le cadre des menaces « terrorisme » et « extrémisme » (encore 53 en 2013 et seulement 22 en 2014).

III.2.2. LES AUTORISATIONS RELATIVES À LA VSSE

III.2.2.1. Les méthodes spécifiques

NATURE DE LA MÉTHODE SPÉCIFIQUE	NOMBRE 2012	NOMBRE 2013	NOMBRE 2014
Pénétration et observation dans des lieux accessibles au public à l'aide d'un moyen technique	75	109	86
Pénétration et inspection de lieux accessibles au public à l'aide d'un moyen technique	1	0	0
Prise de connaissance de données d'identification du trafic postal et réquisition du concours d'un opérateur postal	2	0	0
Prise de connaissance des données d'identification de moyens de communication électroniques ; réquisition du concours d'un opérateur ; ou l'accès direct à des fichiers de données	254 dossiers	613[137] méthodes	554 méthodes

137 En comparaison avec les années précédentes, une diminution est à noter : les 613 autorisations concernent en effet 243 dossiers.

NATURE DE LA MÉTHODE SPÉCIFIQUE	NOMBRE 2012	NOMBRE 2013	NOMBRE 2014
Prise de connaissance des données d'appel de moyens de communication électroniques et réquisition du concours d'un opérateur	147	136	88
Prise de connaissance des données de localisation de moyens de communication électroniques et réquisition du concours d'un opérateur	176	244	248
TOTAL	**655**[138]	**1102**[139]	**976**

Le léger recul du nombre de méthodes spécifiques employées par la VSSE s'explique par une moindre utilisation d' « observations » spécifiques (86 au lieu de 109), de « Prises de connaissance de données d'identification » (554 au lieu de 613) et de « Prises de connaissance de données d'appel » (88 au lieu de 136). Seul le nombre de « Localisations » mises en œuvre est resté stable.

III.2.2.2. Les méthodes exceptionnelles

NATURE DE LA MÉTHODE EXCEPTIONNELLE	NOMBRE 2012	NOMBRE 2013	NOMBRE 2014
Pénétration et observation, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	8	6	9
Pénétration et inspection, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	6	6	21
Création ou recours à une personne morale fictive	0	0	0
Ouverture et prise de connaissance d'un courrier confié ou non à un opérateur postal	12	6	18
Collecte de données concernant des comptes bancaires et des transactions bancaires	16	11	8
Intrusion dans un système informatique	10	12	18
Écoute, prise de connaissance et enregistrement de communications	50	81	86
TOTAL	**102**[140]	**122**[141]	**156**

138 Dans dix-sept cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste professionnel. L'année dernière, il s'agissait de neuf cas.

139 Dans neuf cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste professionnel. On dénombrait le même nombre de cas l'année dernière.

140 Dans cinq cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste professionnel.

141 Dans un cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste professionnel.

Cette année, l'augmentation du nombre de méthodes exceptionnelles n'est pas à mettre exclusivement sur le compte des « mesures d'écoute » (de 81 à 86), mais principalement des « inspections » (de 6 à 21) et de l'« ouverture de courrier » (de 6 à 18).

Par ailleurs, il convient de noter que dans 19 cas (11 l'année dernière), il a été fait usage de la procédure d'extrême urgence, pour laquelle seul l'avis du président de la Commission BIM est sollicité.

III.2.2.3. 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). Des méthodes exceptionnelles ne peuvent pas être mises en œuvre dans le cadre de l'extrémisme ni de l'ingérence. Elles sont toutefois autorisées dans le cadre du processus de radicalisation menant au terrorisme (art. 3, 15° 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.

NATURE DE LA MENACE	NOMBRE 2012	NOMBRE 2013	NOMBRE 2014
Espionnage	243	359	319
Terrorisme (et processus de radicalisation)	288	580	499
Extrémisme	177	216	267
Prolifération	28	15	33
Organisations sectaires nuisibles	7	9	0
Ingérence	10	8	10
Organisations criminelles	5	9	8

Les chiffres repris ci-dessus ne montrent pas de changements notables par rapport à 2013 : le « terrorisme » et l' « extrémisme » restent tous les deux, sous l'angle des méthodes MRD, la priorité de la VSSE. Pourtant, malgré la problématique syrienne, une légère diminution du nombre de méthodes est enregistrée pour ces menaces (de 826 en 2013 à 766 en 2014). Cela tient en partie au fait que, dans le cadre du « terrorisme » et de l' « extrémisme », la VSSE s'est surtout concentrée sur les combattants en Syrie et moins sur d'autres formes d'extrémisme.

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

– 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.

– 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.
– La sauvegarde des éléments essentiels du potentiel scientifique et économique.

En considérant que plusieurs menaces peuvent figurer dans une même autorisation, les chiffres sont les suivants pour l'année 2014 :

INTÉRÊTS PROTÉGÉS	NOMBRE 2012	NOMBRE 2013	NOMBRE 2014
La sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel	704	1177	1100
La sûreté extérieure de l'État et les relations internationales	693	1160	1075
La sauvegarde des éléments essentiels du potentiel scientifique et économique	15	11	10

III.3. LES ACTIVITÉS DU COMITÉ PERMANENT R EN SA QUALITÉ D'ORGANE JURIDICTIONNEL ET D'AUTEUR D'AVIS PRÉJUDICIELS

III.3.1. LES CHIFFRES

Cette section reprend les activités du Comité permanent R relatives aux méthodes de renseignement spécifiques et exceptionnelles. Par ailleurs, l'attention sera exclusivement focalisée sur les décisions juridictionnelles prises en la matière. Toutefois, il convient 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.

En vertu de l'article 43/4 L.R&S, le Comité permanent R peut être saisi de cinq manières :
- D'initiative ;
- À la demande de la Commission de la protection de la vie privée ;
- Par le dépôt d'une plainte d'un citoyen ;
- 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 ;
- De plein droit quand le ministre compétent a donné son autorisation sur base de l'article 18/10, § 3 L.R&S.

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

TYPE DE SAISINE	NOMBRE 2012	NOMBRE 2013	NOMBRE 2014
1. D'initiative	19	16	13[142]
2. Commission Vie Privée	0	0	0
3. Plainte	0	0	0
4. Suspension par la Commission BIM	17	5	5
5. Autorisation du ministre	2	2	1
6. Auteur d'avis préjudiciel	0	0	0
TOTAL	**38**	**23**	**19**

Une fois saisi, le Comité peut prendre plusieurs types de décisions (intermédiaires). Toutefois, dans les deux cas (1. en 2. ci-après), une décision est prise avant la saisine proprement dite.
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. Décider de 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) ;

142 Dans deux cas, la décision du Comité n'a été rendue qu'en janvier 2015.

4. Demander des informations complémentaires à la Commission BIM (43/5 § 1er, alinéa 1er et alinéa 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, on ne fait pas référence aux multiples informations complémentaires recueillies par le service d'Enquêtes R avant la saisine proprement dite et donc d'une manière plutôt informelle ;
7. Procéder à l'audition des membres de la Commission BIM (art. 43/5 § 4, alinéa 1er, L.R&S) ;
8. Procéder à l'audition du dirigeant du service de renseignement ou des membres du service de renseignement concerné (art. 43/5 § 4, alinéa 1er, L.R&S) ;
9. Statuer sur les secrets relatifs à une information ou 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 sur la demande du dirigeant du service ou le membre du service de renseignement qui 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), ce qui implique que la méthode autorisée par le dirigeant du service a bien été considérée par le Comité comme (partiellement) légale, proportionnelle et subsidiaire ;
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 (articles 131*bis*, 189*quater* en 279*bis* CIC).

Le Comité permanent R doit statuer définitivement dans un délai d'un mois suivant la date à laquelle il a été saisi (art. 43/4 L.R&S). Ce délai a été respecté dans tous les dossiers.

NATURE DE LA DÉCISION	2012	DÉCISION FINALE 2012	2013	DÉCISION FINALE 2013	2014	DÉCISION FINALE 2014
1. Plainte frappée de nullité	0		0		0	
2. Plainte manifestement non fondée	0		0		0	
3. Suspension de la méthode	1		0		3	
4. Informations complémentaires de la Commission BIM	0		0		0	
5. Informations complémentaires du service de renseignement	6		0		1	
6. Mission d'enquête du Service d'Enquêtes R	11		50		54	
7. Audition membres de la Commission BIM	0		0		0	
8. Audition membres des services de renseignement	0		0		0	
9. Décision relative au secret de l'instruction	0		0		0	
10. Informations sensibles lors de l'audition	0		0		0	
11. Cessation de la méthode	4		9		3	
12. Cessation partielle de la méthode	18		5		10	
13. Levée (partielle) de l'interdiction de la Commission BIM	13	38	2[143]	23	0	17

[143] En fait, le Comité a décidé que la suspension prononcée par la Commission BIM était sans objet (voir dossier 2013/1728).

NATURE DE LA DÉCISION	2012	DÉCISION FINALE 2012	2013	DÉCISION FINALE 2013	2014	DÉCISION FINALE 2014
14. Incompétence	0		0		0	
15. Autorisation légale/ Non- cessation de la méthode/Non-fondement	3		7		4	
16. Avis préjudiciel	0		0		0	

En 2014, le Comité permanent R a pris 17 décisions. En 2013, il y en a eu 23, et en 2012 et 2011, encore respectivement 39 et 38. Une des raisons expliquant cette diminution est la constatation selon laquelle la Commission BIM a suspendu moins de méthodes (en 2011 et 2012 encore respectivement 15 et 17). S'y ajoute sans conteste le fait que toute une série de points de discussion juridiques sont définitivement éclaircis dans la jurisprudence, comme celle qui a été élaborée les années précédentes et celle qui a ensuite été mise en œuvre par les services.

III.3.2. LA JURISPRUDENCE

La substance des 17 décisions finales prises par le Comité permanent R en 2014 est reprise ci-après. Les synthèses sont expurgées des données opérationnelles. Seuls sont mentionnés les éléments qui présentent un intérêt d'un point de vue juridique. Dans quelques cas, le Comité était toutefois tenu de ne pas reprendre explicitement certains éléments juridiques dans ce rapport d'activités, et ce afin de garantir la confidentialité requise.

Les décisions ont été regroupées en cinq rubriques :

- Les exigences légales (de forme) préalables à la mise en œuvre d'une méthode ;
- La motivation de l'autorisation ;
- Les exigences de proportionnalité et de subsidiarité ;
- La légalité de la méthode concernant les techniques utilisées, les données recueillies, la durée de la mesure et la nature de la menace ;
- Les conséquences d'une méthode (mise en œuvre) illégale(ment).

Certaines décisions ont été reprises dans plusieurs rubriques lorsque cela s'avérait pertinent.

III.3.2.1. Les exigences légales (de forme) préalables à la mise en œuvre d'une méthode

III.3.2.1.1. Notification préalable à la Commission BIM

Une méthode spécifique ne peut être effectivement utilisée qu'après la notification de l'autorisation à la Commission BIM. Dans le dossier 2014/3291, la Commission a été informée de l'autorisation, alors que la mise en œuvre de la méthode, selon cette décision, aurait déjà débuté la veille. Aussi la Commission a-t-elle suspendu la méthode pour la partie précédant la notification. Le Comité a confirmé cette décision.

III.3.2.1.2. Indications obligatoires dans l'autorisation

Le service de renseignement voulait procéder à l'inspection d'une chambre d'hôtel qui était louée par une cible (dossier 2014/2898). Toutefois, le nom de l'hôtel, pas plus évidemment que le numéro de chambre, ne figurait dans l'autorisation même. Le service de renseignement a communiqué ces informations à la Commission BIM dans le courant de la journée. Le service a ajouté que si la cible devait encore changer d'hôtel, la Commission en serait avertie immédiatement. Le Comité a jugé que ce procédé était légal. Tout d'abord, la loi n'exige pas « *que la décision précise le nom de l'hôtel (et sa localisation) ni même le numéro de la chambre qui doit être inspectée […]; Attendu cependant que l'indication qu'il s'agit d'une chambre d'hôtel et non un immeuble servant de domicile ou de résidence d'une personne est indispensable pour apprécier le respect des principes de proportionnalité et de subsidiarité* ». En outre, le Comité a constaté que le président de la Commission BIM avait été informé sans délai de la localisation exacte.

III.3.2.1.3. Méthode visant un éventuel journaliste

Le service de renseignement souhaitait mettre en œuvre une méthode spécifique à l'égard d'une personne dont il « *ne serait pas exclu* » qu'elle soit journaliste (dossier 2014/2723). Le Comité a décidé que « *l'absence de précision sur l'identité de cette personne n'a pas permis de vérifier si la procédure prévue par l'article 18/2 § 3 devait ou non être mise en œuvre* ». La méthode était donc illégale.

III.3.2.2. Motivation de l'autorisation

III.3.2.2.1. Manque de précision de la motivation

Dans le dossier susmentionné, le service de renseignement voulait employer quatre méthodes afin d'identifier une personne donnée (dossier 2014/2723). En

effet, celle-ci était soupçonnée de vouloir vendre des informations secrètes à un tiers qui était en contact avec un service de renseignement étranger. Mais même le recueil de renseignements supplémentaires n'a pas vraiment permis d'en savoir davantage sur l'acquéreur et le vendeur, sur la nature des informations ni sur les intentions des personnes ou des services concernés. Il était dès lors « *difficile d'apprécier in concreto la nature de la menace réelle ou potentielle contre l'intérêt à protéger si ce n'est sur base d'une affirmation que cette menace existe bien ; que le texte et l'esprit de la loi exigent des indications plus précises que celles développées dans la décision* ».

III.3.2.2.2. Motivation renforcée en cas de deuxième prolongation

Un projet d'autorisation en vue de la mise en œuvre d'une méthode exceptionnelle doit être soumis pour avis à la Commission BIM, qui dispose d'un délai de quatre jours. Étant donné que la Commission s'est trouvée dans l'impossibilité de rendre un avis dans ce délai, l'autorisation a été accordée par le ministre compétent sur la base de l'article 18/10 § 3, alinéa 3 L.R&S. Le Comité a constaté qu'il s'agissait d'une deuxième prolongation d'une méthode exceptionnelle. Vu « *les circonstances particulières nécessitant de prolonger une deuxième fois la méthode exceptionnelle à l'égard de la cible sont indiquées à suffisance dans l'autorisation donnée par le ministre ; Que ces motifs font suffisamment apparaître la menace représentée par la cible ainsi que la subsidiarité et la proportionnalité de la méthode mise en œuvre à son égard* ».

III.3.2.3. Les exigences de proportionnalité et de subsidiarité

III.3.2.3.1. Attente des résultats de la première méthode

En 2014, le Comité permanent R est intervenu à cinq reprises dans des dossiers où le service de renseignement avait autorisé des méthodes sans avoir attendu les résultats obtenus par l'utilisation d'une méthode précédente. La problématique a été traitée pour la première fois dans le dossier 2014/2744. Un service de renseignement souhaitait vérifier, au moyen de données de communications électroniques, quels contacts une cible entretenait en Belgique. Le premier objectif était de lister à qui elle téléphonait et qui l'appelait. Mais la méthode avait aussi pour finalité de procéder immédiatement à la localisation de tous les contacts de la cible. Le Comité a toutefois estimé qu'au moment de sa décision, « *onmogelijk is vast te stellen welke telefoonnummers het voorwerp zullen uitmaken van een daarop volgende lokalisatie* »[144], et donc qu'il était dans

144 « *[il] est impossible de préciser quels numéros de téléphone feront ensuite l'objet d'une localisation.* » (traduction libre)

l'impossibilité de vérifier la subsidiarité et la proportionnalité de la localisation des numéros de téléphone qui n'avaient pas encore été identifiés.

La même problématique s'est présentée dans les dossiers 2014/2774 et 2014/2778. Le service de renseignement voulait d'abord procéder à la prise de connaissance de numéros entrants et sortants du GSM d'une cible. Ensuite, il aurait procédé à l'identification de tous les numéros, « *pour autant que cela soit nécessaire à l'enquête* ». Aucun problème ne se posait à ce stade. Mais le service voulait aussi procéder à la localisation de tous les numéros identifiés « *afin de nous donner des indices sur l'identité de celles-ci* ». Le Comité a répété qu'il « *[est] impossible de préciser actuellement quels numéros feront l'objet d'une telle localisation. Qu'il est dès lors impossible au Comité R de statuer actuellement sur la subsidiarité et la proportionnalité de la méthode de localisation visant les numéros non*-encore identifiés ».

Dans un quatrième dossier (2014/3253), un service de renseignement voulait autoriser simultanément quatre méthodes à l'égard d'une personne : l'identification de ses moyens de communications électroniques, l'« observation » de ces appareils, la localisation de toutes les données ainsi obtenues et l'identification de toutes les personnes concernées. Le Comité a estimé que le service devait d'abord utiliser la première méthode étant donné « *qu'en l'absence d'informations obtenues par la méthode sollicitée, il n'est pas permis de juger du respect des principes de proportionnalité, de subsidiarité donc de la légalité des trois autres méthodes sollicitées et qui sont la poursuite de la première méthode* ».

Enfin, dans le dossier 2014/3493, le Comité a réitéré le fait qu'il est impératif de travailler par étapes distinctes lorsque d'une part, on veut savoir quel moyen de communication est utilisé par une cible (article 18/7, 2° L.R&S[145]), et d'autre part avec qui elle a eu un entretien téléphonique à un moment donné (article 18/8, 1° – le repérage des données d'appel de moyens de communications électroniques à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés – associé à l'article 18/7, 1° – l'identification de l'abonné ou de l'utilisateur habituel d'un service de communications électroniques ou du moyen de communication électronique utilisé). Le Comité a estimé que « *het tweede gedeelte van de methode, gesteund op art. 18/8, 1°, vooralsnog niet beantwoordt aan de vereiste van proportionaliteit en subsidiariteit* ».[146]

III.3.2.3.2. Nécessité non démontrée

La problématique de la proportionnalité a encore été abordée dans un autre cas. Le service de renseignement souhaitait utiliser en extrême urgence une méthode exceptionnelle concernant un numéro de téléphone bien déterminé (dossier

145 Le service concerné s'était basé par erreur sur l'article 18/7, 1° L.R&S. dans son autorisation.

146 « *la deuxième partie de la méthode, s'appuyant sur l'article 18/8, 1°, ne répond pas jusqu'à présent aux exigences de proportionnalité et de subsidiarité.* » (traduction libre)

2014/3424). Le jour suivant l'autorisation effective, sur la base de l'avis conforme oral, le service de renseignement a toutefois constaté que le numéro n'était pas repris, par erreur, dans l'autorisation. Le numéro de téléphone concret a a encore été envoyé le jour même à la Commission, mais à cause d'une faute de frappe, c'est un numéro erroné qui a été transmis. La Commission BIM alors suspendu la méthode. Le Comité a confirmé cette décision, mais pour d'autres motifs. Il ressortait en effet des informations recueillies que la nécessité d'appliquer une méthode exceptionnelle au numéro n'était pas démontrée. Aussi le Comité a-t-il estimé que la méthode ne répondait pas à l'exigence de proportionnalité.

III.3.2.3.3. Subsidiarité

Dans le dossier 2014/2908, il n'était question que de la subsidiarité. La Commission BIM avait suspendu l'autorisation de procéder à une observation d'une personne avec une caméra parce que le service de renseignement avait omis d'expliquer concrètement quelles informations, qui émanaient d'un service étranger, l'avaient incité à vouloir procéder à cette observation. Le Comité a lui aussi estimé que la décision initiale n'était pas suffisamment motivée. Il a demandé des informations complémentaires et a reçu comme réponse « *dat er geen noodzaak was om een specifieke methode aan te wenden bij de observatie van de betrokken persoon; dat er immers geen technisch middel bij de beoogde observatie vereist was* »[147], si bien qu'une méthode ordinaire suffisait pour procéder à l'observation. En d'autres termes, la décision d'employer une méthode spécifique ne répondait pas à l'exigence de subsidiarité, si bien que le Comité a ordonné la cessation de la méthode.

III.3.2.4. Légalité de la méthode concernant les techniques utilisées, les données recueillies, la durée de la mesure et la nature de la menace

III.3.2.4.1. Collaboration de services étrangers

Le Comité avait déjà estimé que les services de renseignement belges pouvaient collaborer avec leurs homologues étrangers, y compris dans le cadre des méthodes particulières de renseignement, à condition que le service belge conserve effectivement le contrôle sur la méthode mise en œuvre.[148] Dans le dossier 2014/2723, le Comité a insisté à cet égard sur la nécessité que le Comité

147 « *qu'il n'était pas nécessaire d'employer une méthode spécifique dans le cadre de l'observation de la personne concernée; qu'en effet aucun moyen technique n'était requis pour l'observation visée.* » (traduction libre)

148 Voir par exemple COMITÉ PERMANENT R, *Rapport d'activités 2013*, 84-85 (III.3.2.4.1. Le contrôle de l'exécution de la méthode MRD).

ministériel du renseignement et de la sécurité[149] établisse des directives plus précises : « *[…] l'absence de directives du Comité ministériel du Renseignement et de la Sécurité quant aux conditions de la coopération avec les services de renseignement étranger oblige la VSSE à agir par elle-même et au cas par cas* ». « *[l]es nécessités d'assurer une coopération entre les services de renseignement belges […] et les services de renseignement étrangers, notamment lorsque des actions sont entreprises sur le territoire belge* » doivent néanmoins être prises en considération.

III.3.2.4.2. La Loi MRD et la Convention de Vienne sur les relations diplomatiques du 18 avril 1961

Au cours de la période de référence, le Comité a pris quatre décisions (dossiers 2014/2758, 2014/3148, 2014/3306 et 2014/3488), où il a notamment été question de la Convention de Vienne de 1961. Dans ce rapport d'activités, le Comité ne peut aborder le contenu de ces décisions, puisque celles-ci ont dû être classifiées au niveau « secret ». Néanmoins, le Comité insiste sur le fait que la Convention de Vienne s'applique aussi au fonctionnement des services de renseignement, qui doivent tenir compte de certaines limites, mais aussi sur le fait que des directives claires du Conseil national de sécurité sont nécessaires en raison de la responsabilité politique qui peut résulter de certaines activités des services de renseignement.

III.3.2.5. Les conséquences d'une méthode (mise en œuvre) illégale(ment)

La Commission BIM avait partiellement suspendu une méthode (dossier 2014/2724). Il ressortait de l'autorisation du dirigeant du service que le service de renseignement concerné voulait procéder à l'identification de communications électroniques de deux personnes qui n'étaient pas encore identifiables à ce moment-là. Mais cela était manifestement fondé sur une méprise : le service concerné n'avait pas l'intention d'employer la méthode. Le Comité a dès lors confirmé la décision de la Commission BIM.

149 L'A.R. du 21 juin 1996 portant création d'un Comité ministériel du renseignement et de la sécurité a été abrogé par l'A.R. du 28 janvier 2015 portant création du Conseil national de sécurité, *M.B.* 30 janvier 2015.

III.4. CONCLUSIONS

Sur la base des chiffres de l'année d'activités 2014, le Comité a formulé les conclusions générales suivantes :

- Alors qu'une augmentation d'environ 13 % était encore enregistrée en 2013, le nombre total de méthodes particulières de renseignement a diminué de 7 % en 2014. Cette diminution se situe, pour les deux services, au niveau des méthodes spécifiques ; les méthodes exceptionnelles ont quant à elles connu un léger accroissement.
- En ce qui concerne le SGRS, l'augmentation des méthodes exceptionnelles est imputable à l'augmentation du nombre de mesures d'écoute (qui sont passées de 17 à 26), même si le nombre reste limité en chiffres absolus.
- En ce qui concerne la VSSE, l'augmentation du nombre de méthodes exceptionnelles en 2014 n'est pas à mettre exclusivement sur le compte des mesures d'écoute (passées de 81 à 86), mais principalement sur les inspections (de 6 à 21) et sur l'ouverture de courrier (de 6 à 18).
- En ce qui concerne le SGRS, la menace « espionnage » requiert toujours la mise en œuvre de la plupart des méthodes MRD, tandis que l'utilisation des MRD par la VSSE vise surtout la lutte contre le « terrorisme/extrémisme ».
- Il convient en outre de noter que dans 19 cas (11 l'année dernière), il a été fait usage de la procédure d'extrême urgence, pour laquelle seul l'avis du président de la Commission BIM est sollicité pour la mise en œuvre d'une méthode exceptionnelle.
- En 2014, le Comité permanent R a rendu 17 décisions. En 2013, il y en a eu 23 et en 2012 et 2011, encore respectivement 39 et 38. Une des raisons de cette diminution est le constat selon lequel la Commission BIM a suspendu moins de méthodes (en 2011 et 2012 encore respectivement 15 et 17; en 2013 et 2014, chaque fois 5). Dans l'intervalle, il y a aussi le fait que toute une série de points de discussion juridique sont éclaircis dans la jurisprudence du Comité permanent R et dans les décisions de la Commission BIM.

CHAPITRE IV
LE CONTRÔLE DE L'INTERCEPTION DE COMMUNICATIONS ÉMISES À L'ÉTRANGER

Depuis le début de l'année 2011, la VSSE et le SGRS peuvent tous deux, dans des conditions très strictes, écouter des communications, en prendre connaissance et les enregistrer (art. 18/17, § 1er L.R&S).

Il convient toutefois d'établir une distinction claire entre les « interceptions MRD » et « *la recherche, la captation, l'écoute, la prise de connaissance ou l'enregistrement, par le Service Général du Renseignement et de la Sécurité des Forces armées de toute forme de communications émises à l'étranger.* » Cette seconde forme d'écoute est possible depuis longtemps déjà, et peut être mise en œuvre tant à des fins militaires dans le cadre des missions définies à l'article 11 § 2, 1° et 2°, L.R&S, que pour des motifs de sécurité et de protection des troupes belges et alliées lors de missions à l'étranger ainsi que des ressortissants belges établis à l'étranger (art. 11, § 2, 3° et 4°, L.R&S). Ces écoutes sont elles aussi généralement désignées sous l'appellation « interceptions de sécurité », mais elles sont soumises à un tout autre cadre de contrôle. Ce contrôle externe est en effet exclusivement confié au Comité permanent R, et ce à la fois avant, pendant et après les interceptions (art. 44*bis* L.R&S). Le Comité est chargé de faire cesser les interceptions en cours, lorsqu'il apparaît que les conditions dans lesquelles elles sont réalisées ne respectent pas les dispositions légales et/ou l'autorisation ministérielle (art. 44*ter* L.R&S). Chaque année, au début du mois de décembre, le SGRS doit en effet présenter au ministre de la Défense sa liste motivée d'organisations ou d'institutions dont les communications pourront faire l'objet d'interceptions dans le courant de l'année suivante, et ce dans le but d'octroyer à ces interceptions l'autorisation ministérielle. Le ministre doit prendre sa décision dans les dix jours ouvrables et doit la communiquer au SGRS. Ensuite, le SGRS est tenu de transmettre la liste et l'autorisation ministérielle au Comité permanent R.

En 2014, le Comité permanent R a effectué les vérifications requises.

En outre, le Comité a reçu une réponse du SGRS à ses questions relatives au choix, à la description des « organisations ou institutions » qui feront l'objet

d'interceptions et à la motivation qui les sous-tendent.[150] Le Comité a examiné la réponse et a demandé un complément d'explications, entre autres sur le cycle SIGINT et sur le matériel utilisé. Le SGRS a éclairci ces points lors d'un briefing organisé en octobre 2014. Le Comité permanent R a décidé d'assurer un suivi des questions précitées lorsqu'il procédera aux prochaines vérifications requises.

150 Voir COMITÉ PERMANENT R, *Rapport d'activités 2013*, 89-90.

CHAPITRE V
AVIS, ÉTUDES ET AUTRES ACTIVITÉS

V.1. VINGT ANS DE CONTRÔLE DÉMOCRATIQUE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ : VISITE DU ROI

En 2013, le Comité permanent R a fêté ses vingt années d'existence.[151] À l'occasion de cet anniversaire, Sa Majesté le Roi a honoré le Comité d'une visite de travail le 25 avril 2014. Les dirigeants de la VSSE, du SGRS et de l'OCAM ont également été invités. Le Roi a été informé de l'organisation et des missions du Comité. Il a ensuite reçu quelques explications sur les enquêtes de contrôle en cours, le contrôle des méthodes particulières de renseignement, ainsi que sur l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité.

V.2. AVIS AU MINISTRE DE LA JUSTICE

Ces dernières années, le Comité permanent de contrôle des services de renseignement et de sécurité a formulé des dizaines de recommandations visant un fonctionnement efficace des services de renseignement et une meilleure protection des droits et libertés des citoyens. Toutes n'ont pas fait l'objet d'un suivi adapté. Le Comité permanent R a toutefois pu constater que de nombreuses recommandations se retrouvaient directement ou indirectement dans l'Accord de gouvernement fédéral du 9 octobre 2014. À la demande du ministre de la Justice, le Comité a transmis un document[152] dans lequel il rappelait quelques-unes de ses principales recommandations.

---

151 W. VAN LAETHEM et J. VANDERBORGHT (eds.), *Regards sur le contrôle. Vingt ans de contrôle démocratique sur les services de renseignement*, Intersentia, Anvers, 2013, 565 p.

152 COMITÉ PERMANENT R, « Belangrijke aanbevelingen van het Vast Comité I in aansluiting met het Regeerakkoord Michel I. Denkpistes voor de minister van Justitie », 11 décembre 2014.

V.3. DOSSIERS D'INFORMATION

Outre les enquêtes de contrôle (pour les détails, voir le Chapitre II), le Comité permanent R ouvre également des « dossiers d'information », qui doivent permettre d'apporter une réponse structurée à des questions relatives au fonctionnement des services de renseignement et de l'OCAM.[153] Si de tels dossiers font apparaître des indices de dysfonctionnement ou des aspects du fonctionnement des services de renseignement qui requièrent un examen approfondi, le Comité peut procéder, par la suite, à l'ouverture d'une enquête de contrôle formelle.

Un dossier d'information qui a donné lieu à l'ouverture d'une enquête de contrôle concernait la problématique des « *foreign fighters* » et de la guerre en Syrie.

Les échanges de vues sur les éventuelles activités de renseignement du Bataillon ISTAR, mis sur pied au sein des Forces armées, se sont poursuivis en 2014. La Commission de suivi du Sénat avait été précédemment informée du point de vue juridique du Comité. Le Comité y reconnaissait les besoins croissants formulés par la Défense en termes de capacités de type « *battle-field intelligence* » organisées de manière performante, mais indiquait que cela donnerait lieu à des complications juridiques majeures. Le ministre de la Défense de l'époque a clarifié la vision des Forces armées. Le Comité a pu adhérer en principe aux solutions proposées, mais a demandé à discuter des modalités d'exécution. En définitive, il incombe au Parlement de juger si le règlement proposé peut recevoir son approbation.

V.4. EXPERT DANS DIVERS FORUMS

En 2014, le Comité permanent R et son personnel ont été sollicités à plusieurs reprises en tant qu'experts par des institutions publiques et privées, tant belges qu'étrangères.

Depuis 2011, le président du Comité permanent R assure la présidence du *Belgian Intelligence Studies Centre (BISC)*. Ce centre d'études sur le renseignement entend rapprocher les services de renseignement et de sécurité et la communauté scientifique, et contribuer à la réflexion sur des problèmes sociétaux en matière de renseignement.[154] En 2014, le BISC a organisé deux

---

153 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, etc.

154 www.intelligencestudies.be. Le BISC a publié son quatrième « *Cahier d'études de renseignement* » en 2014.

journées d'étude : la première partie d'une trilogie d'activités sur le mur de l'Atlantique (« Atlantikwall »), organisée en collaboration avec la province de Flandre-Occidentale (« D-Day moins x – Activités de renseignement derrière et le long du Mur de l'Atlantique », mai 2014), ainsi qu'une journée d'étude sur la cyberintelligence (« Building Belgium's Cyber Intelligence Knowledge Capacity », décembre 2014).

La fréquence des travaux du « Groupe de travail Analyse », où siègent des représentants des deux services de renseignement et du Comité permanent R, s'est ralentie en 2014. Ce groupe de travail a accompagné la mise en place de la *Belgian Intelligence Academy* (BIA)[155], une académie qui organise des formations pour analystes issus tant du service de renseignement civil que militaire. Au cours de l'année écoulée, des règlements d'ordre intérieur ont été élaborés pour les différents organes de gestion (le Comité de direction, le Comité exécutif et le Comité scientifique), et un projet de note de politique générale a été rédigé. En outre, la première formation « Intelligence and Analysis Course (IAC) » a commencé. Elle s'est déroulée en juin/juillet et en septembre/octobre 2014, à chaque fois pendant deux semaines. Le protocole d'accord officiel créant la BIA a finalement été signé début 2015.

Enfin, le Comité permanent R a également été consulté par le monde académique en 2014. Un représentant du Comité permanent R a pris part à un débat sur le rôle du FBI américain et la séparation (nécessaire) entre les tâches policières classiques et le *(counter)intelligence*.[156] Le responsable du *Sector of Information Society, Privacy and Data Protection Freedoms and Justice Department* van het *European Union Agency for Fundamental Rights*[157] a également été reçu. Ce dernier est chargé de réaliser une étude comparative du contrôle démocratique des services de renseignement dans les États membres de l'Union pour le compte du Parlement européen et dans le sillage de la Résolution du 12 mars 2014. En outre, le président du Comité permanent R et un commissaire-auditeur de son Service d'Enquêtes ont participé aux réunions préparatoires de la *Community of Interest on the Practice and Organization of Intelligence (COI POI)*.[158] Le Comité continue de participer aux réunions du *Groupe européen de recherche sur l'éthique du renseignement (GERER)*. Un groupe de travail, composé de représentants du monde universitaire et de praticiens (représentants des services de renseignement (militaires) français,

---

155 L'académie est investie de la mission suivante : « *La Belgian Intelligence Academy vise à être le moteur et la référence en matière de formation professionnelle dans le renseignement civil et militaire, et à être reconnue pour son expertise et ses compétences. Elle a pour mission de dispenser des formations communes et structurées, de qualité, au personnel des services de renseignement* ».

156 « Zonde(n) van het FBI : Politiediensten als inlichtingendiensten, politiediensten en inlichtingendiensten », Metaforum Leuven, KU Leuven, Hollands College, 4 décembre 2014.

157 http ://fra.europa.eu.

158 Voir à cet égard COMITÉ PERMANENT R, *Rapport d'activités 2008*, 85-86.

belges et luxembourgeois, du Comité permanent R, etc.), mène une réflexion sur la relation « éthique – services de renseignement ».[159] En octobre 2014, le Comité a été invité par le *Centrum voor Migraties en Interculturele Studies* (CEMIS) de l'université d'Anvers à participer à une séance de brainstorming portant sur une étude sur la radicalisation et les solutions possibles. Des chercheurs de plusieurs universités (UAntwerpen, UGent, KULeuven et VUBrussel) ont travaillé sur un projet de recherche qui s'inscrit dans le cadre du canal de financement de la recherche fondamentale stratégique de l'Agence pour l'innovation par la science et la technologie (« Agentschap voor Innovatie door Wetenschap en Technologie ») des autorités flamandes. Auparavant, un représentant du Comité permanent R a participé à la commission de suivi du projet de recherche « Radicalisation et médias sociaux : un test d'un modèle intégré (RADIMED) ».[160] Dans la même optique, le Comité a été sollicité pour collaborer à IMPACT Europe, une recherche européenne à grande échelle financée par la Commission européenne sur la prévention et la lutte contre la radicalisation.[161] Enfin, un conseiller du Comité a pris la parole lors d'une journée d'étude intitulée « Les méthodes particulières de recherches face aux nouvelles formes de cybercriminalité », organisée par le *Belgian Cybercrime Center of Excellence* (B-CCENTRE) et le Centre de Recherche Information, Droit et Société de l'Université de Namur (CRIDS).

V.5. PROTOCOLE DE COOPÉRATION « DROITS DE L'HOMME »

La Belgique est invitée depuis longtemps, par diverses instances, et avec beaucoup d'insistance, à créer, à l'instar des pays limitrophes, un institut national des droits de l'homme (INDH) indépendant.[162] En effet, jusqu'il y a peu, la Belgique ne disposait d'aucune instance publique chargée de vérifier si la législation actuelle et future est conforme aux arrêts de la Cour européenne des droits de l'homme et aux conventions internationales traitant des droits de l'homme.

---

159 Les travaux ont donné lieu à une première publication : P. KLAOUSEN et T. PICHEVIN, *Renseignement et éthique. Le moindre mal nécessaire*, Groupe européen de recherche sur l'éthique du renseignement (GERER), Lavauzelle, Panazol, 2014, 332 avec une préface du président du Comité permanent R.

160 L'équipe de recherche (UGent, Hogeschool Gent et UCL) a finalisé son étude scientifique en 2014 : L. PAUWELS, F. BRION, B. DE RUYVER et al, *Comprendre et expliquer le rôle des nouveaux médias sociaux dans la formation de l'extrémisme violent. Une recherche qualitative et quantitative (RADIMED)*, Bruxelles, Politique scientifique fédérale, 2014 (SP2586).

161 IMPACT Europe signifie « *Innovative Method and Procedure to Assess Counter-violent-radicalisation Techniques in Europe* ». Voir à cet égard : www.impacteurope.eu.

162 Voir par exemple Chambre, 2012-13, *Doc. parl.* 53-2946/001, 10 juillet 2013 (Proposition de loi portant création d'un Institut des Droits de l'homme) et www.mensenrechten.be.

L'absence d'instance publique des droits de l'homme était considérée comme une lacune majeure.[163] Les Accords de gouvernement de Verhofdstadt II (2003) et Di Rupo (2011) évoquaient sa création, mais force est de constater qu'elle est restée lettre morte.

Cette situation a changé en 2014. Le Comité a participé à différentes réunions préparatoires avec d'autres institutions ayant un mandat dans le domaine des droits de l'homme.[164] C'est ainsi qu'un protocole de coopération[165] a vu le jour le 13 janvier 2015, dans lequel toutes les instances participantes sont convenues d'échanger leurs pratiques et méthodes, d'examiner les questions communes, et de favoriser la coopération mutuelle.

V.6. CONTACTS AVEC DES ORGANES DE CONTRÔLE ÉTRANGERS

Début février 2014, le président du Comité permanent R a été invité par la *Commission luxembourgeoise de Contrôle parlementaire du Service de Renseignement de l'État*. Il était demandé au président de présenter le modèle belge de contrôle parlementaire des services de renseignement et de sécurité.

Début mai, le président du Comité permanent R a été invité par l'Assemblée nationale française à expliquer le modèle de contrôle belge.

Fin mai 2014, une visite de travail a été organisée à Bruxelles entre une représentation du Comité permanent R et la *Nederlandse Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD)*. À cette occasion, les délégations de deux institutions ont abordé les enquêtes de contrôle clôturées et en cours, les récentes évolutions dans le contrôle parlementaire, et la manière dont elles rendent compte aux donneurs d'ordres. Elles ont également débattu du thème des « décisions contraignantes ».

Dans le prolongement, la CTIVD a organisé une concertation à la mi-novembre 2014. Cette réunion a été étendue aux représentants du service suisse *Strategic Intelligence Service Supervision*, qui fait partie du Département fédéral de la défense, de la protection de la population et des sports. Les participants ont échangé leurs vues à propos des méthodes et processus de travail (Comment fixer des priorités ? Comment améliorer l'efficacité du contrôle ? Comment jongler entre la transparence et la classification ?…) et ont

163 Le Conseil des droits de l'homme des Nations unies l'a constaté en 2011 lors de son « Examen périodique universel » (EPU). La Belgique sera à nouveau soumise à cet examen en 2016.

164 Comme le Centre interfédéral pour l'égalité des chances, le Centre fédéral de la migration, l'Institut pour l'égalité des femmes et des hommes, la Commission vie privée, le Médiateur fédéral, le Conseil supérieur de la Justice, les Comités permanents P et R.

165 « Protocole de coopération entre les institutions exerçant partiellement ou entièrement un mandat d'institution chargée du respect des droits de l'Homme ».

évoqué les défis futurs (Comment préserver l'indépendance ? Que faire des *blind spots* ?…).

Toujours en novembre 2014, une rencontre s'est déroulée entre des représentants du Comité permanent R et le vice-président de l'organe de contrôle parlementaire italien (*Comitato Parlementare per la Sicurezza della Repubblica Italiana*, COPASIR). Cette réunion a surtout porté sur l'organisation du contrôle démocratique des services de renseignement et sur la présentation du modèle belge.

V.7. MEMBRE D'UN COMITÉ DE SÉLECTION

Le président du Comité permanent R a été désigné, aux côtés du président de la Cellule de traitement des informations financières (CTIF) et du directeur de l'Organe de coordination pour l'analyse de la menace (OCAM), dans le comité de sélection chargé de remettre un avis circonstancié aux ministres de l'Intérieur et de la Justice concernant les candidatures pour les postes d'administrateur général et d'administrateur général adjoint de la Sûreté de l'État.[166]

À la demande du bureau de sélection du service public fédéral SELOR, le président du Comité permanent R a également participé à la sélection des candidatures pour la fonction d'administrateur général de l'Administration des douanes et accises du SPF Finances.

V.8. CONTRÔLE DES FONDS SPÉCIAUX

Au nom de la Chambre des Représentants, la Cour des comptes contrôle l'utilisation des moyens financiers par les services publics. La Cour des comptes est amenée à contrôler la légalité et la légitimité de toutes les dépenses, y compris en principe toutes les dépenses des services de renseignement. Cependant, en raison du caractère sensible de la matière, la Cour des comptes n'examine pas 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). Pour la VSSE, le contrôle de ces dépenses est effectué par le chef de cabinet du ministre de la Justice. Depuis 2006, c'est le chef des Forces armées qui exerce seul le contrôle des fonds spéciaux du SGRS, et ce quatre fois par an. À la suggestion de

166 A.M. du 5 février 2014 modifiant l'arrêté ministériel du 4 avril 2006 portant désignation d'un comité de sélection chargé de l'évaluation des candidatures pour le poste d'administrateur général de la Sûreté de l'État, *MB* 7 février 2014. En mars 2014, le Conseil des ministres a décidé de nommer Jaak Raes en tant qu'administrateur général et Pascal Petry en tant qu'administrateur général adjoint de la VSSE.

la Cour des comptes, ce contrôle se déroule en présence du président du Comité permanent R depuis 2010.[167]

V.9. PRÉSENCE DANS LES MÉDIAS

Le Comité permanent R est de plus en plus souvent sollicité par la presse écrite et audiovisuelle pour fournir des explications sur ses travaux ou sur ceux des services de renseignement. Le Comité permanent R a accédé à plusieurs reprises à ces requêtes et a rédigé un communiqué de presse.

Date	Sujet/titre	Forum
7 février 2014	Communiqué de presse sur l'EU Intelligence Analysis Centre (EU INTCEN)	via Belga
17 mars 2014	Qui surveille les espions ?	France Culture
28 mars 2014	« Waakhond geheime diensten is tevreden over inlichtingenwerk in Afghanistan »	MO*
3 avril 2014	« Waarom onze staatsveiligheid faalde in opsporen NSA-spionage »	De Morgen
15 avril 2014	« Les mails du comité R ouverts à tout vent » et « Aucune intrusion constatée dans le système externe, indique le Comité R »	La Libre
15 avril 2014	« Le Comité R exige une rectification concernant le piratage de son système interne »	Belga
25 avril 2014	« Le Comité R qui contrôle les services de renseignements fête ses 20 ans »	RTBF Info
28 avril 2014	Espionnage à Bruxelles	RTBF (Matchpoint)
16 juillet 2014	« Renseignements : les élus ne font pas leur travail. Parlement et gouvernement mis en cause »	Le Soir
26 novembre 2014	Staatsveiligheid luistert steeds meer communicatie af	MO*
26 novembre 2014	« Belgische spionnen opereren in buitenland zonder wettelijk kader »	De Standaard

167 Plusieurs enquêtes judiciaires indiquent toutefois l'éventuelle utilisation abusive de fonds destinés à la rémunération d'informateurs. Le Comité a été informé par son Service d'Enquêtes d'éventuels problèmes structurels et a décidé d'ouvrir une enquête sur « la manière de gérer, d'employer et de contrôler les fonds destinés à la rémunération d'informateurs de la VSSE et du SGRS » (voir II.10.2).

CHAPITRE VI

LES INFORMATIONS ET INSTRUCTIONS JUDICIAIRES

Parallèlement aux enquêtes de contrôle, le Service d'Enquêtes R du Comité permanent R effectue également, à la demande des autorités judiciaires, des enquêtes sur des membres des services de renseignement soupçonnés d'avoir commis un crime ou un délit. Cette compétence est décrite à l'article 40, alinéa 3 de la Loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace. La Loi du 10 juillet 2006 relative à l'analyse de la menace a élargi cette compétence aux crimes et délits commis par des membres de l'Organe de coordination pour l'analyse de la menace (OCAM). En ce qui concerne les membres des autres « services d'appui », cette disposition s'applique uniquement à l'obligation de communiquer à l'OCAM tout renseignement pertinent (art. 6 et 14 L.OCAM).

Lorsqu'ils remplissent une mission de police judiciaire, les membres et le directeur du service d'Enquêtes R sont soumis à l'autorité du procureur général près la cour d'appel ou du procureur fédéral (art. 39 L.Contrôle) et 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, et ce pour une raison évidente : l'organe de contrôle est avant tout à la disposition du Parlement. Cette mission pourrait être mise en péril si les dossiers judiciaires requéraient trop de temps. 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). Cette concertation ne s'est encore jamais avérée nécessaire.

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

En 2014, le Service d'Enquêtes R a mené un nombre considérable de devoirs judiciaires dans le cadre de plusieurs enquêtes importantes. Ainsi, par exemple, 36 procès-verbaux ont été dressés.

Un premier dossier concernait une enquête, menée pour le compte du parquet de Marche-en-Famenne, et ensuite pour le compte de l'auditorat du

travail de Liège. Il s'agissait de faits supposés de harcèlement moral, ayant entraîné le suicide d'un membre du personnel de la VSSE. Toutefois, au début de l'année 2015, l'auditorat du travail a classé le dossier sans suite pour cause de preuves insuffisantes. Après la finalisation de l'enquête et conformément à l'article 43 L.Contrôle, le Service d'Enquêtes a fait part de ses constatations au Comité.

Un second dossier a été traité pour le compte du parquet de Charleroi. Ce dossier concernait une malversation financière présumée, qui était reprochée à un membre du personnel des Services extérieurs de la VSSE lors de l'exécution de ses missions. Après plusieurs devoirs judiciaires, ce dossier a également été classé sans suite.

Les autres dossiers ouverts en 2014 sont toujours en cours.

CHAPITRE VII
LE GREFFE DE L'ORGANE DE RECOURS EN MATIÈRE D'HABILITATIONS, D'ATTESTATIONS ET D'AVIS DE SÉCURITÉ

Le président du Comité permanent R assure également la présidence de l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité. La fonction de greffe est exercée par le greffier du Comité permanent R (ou son suppléant) et par son administration.

L'Organe de recours est compétent pour les contentieux qui portent sur des décisions 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.[168]

Ces activités de l'Organe de recours ont un impact direct tant sur le budget que sur le personnel du Comité permanent R. En effet, tous les frais de fonctionnement sont supportés par le Comité permanent R, qui met à disposition non seulement son président et son greffier, mais aussi son personnel administratif. La préparation, le traitement et le suivi des recours constituent une lourde charge de travail.

Ce chapitre mentionne 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 de ces deux dernières années sont également repris.

En 2014, le nombre de recours et de décisions a connu une légère diminution par rapport à 2013 : 171 recours contre 189 et 163 décisions contre 187. Cette légère baisse s'explique presque entièrement par un nombre moindre de recours contre des refus ou des retraits d'habilitations de sécurité.

168 Pour plus de détails, voir le *Rapport d'activités 2006* du Comité permanent R (87-115).

Tableau 1. Autorités de sécurité concernées

	2012	2013	2014
Autorité nationale de sécurité	40	98	99
Sûreté de l'État	0	1	0
Service général du renseignement et de la sécurité	27	78[169]	60
Agence fédérale de Contrôle nucléaire	11	9	8
Police fédérale	1	1	3
Police locale	2	2	1
Commission aéroportuaire locale	10	-[170]	-
TOTAL	**91**	**189**	**171**

Tableau 2. Nature des décisions contestées

	2012	2013	2014
Habilitations de sécurité			
Confidentiel	7	5	5
Secret	29	56	43
Très secret	9	5	4
Total habilitations de sécurité	45	66	52
Refus	33	41	25
Retrait	12	5	9
Refus et retrait	-	4	-
Habilitation pour une durée limitée	0	1	2
Habilitation pour un niveau inférieur	1	0	1
Pas de décision dans les délais	1	15	15
Pas de décision dans les nouveaux délais	0	0	0

169 La hausse significative du nombre de dossiers émanant du SGRS est due au système en vertu duquel les candidats militaires peuvent être soumis à une vérification de sécurité.

170 Depuis 2013, les avis dans le cadre de l'octroi de badges de sécurité donnant accès aux zones sécurisées des aéroports ne sont plus rendus par les commissions aéroportuaires locales mais par l'Autorité Nationale de Sécurité, ce qui explique aussi l'augmentation du nombre de dossiers émanant de l'ANS par rapport aux années précédentes.

	2012	2013	2014
Total habilitations de sécurité	45	66	52
SOUS-TOTAL HABILITATIONS DE SÉCURITÉ	**45**	**66**	**52**
Attestations de sécurité documents classifiés			
Refus	23	0	4
Retrait	0	0	0
Pas de décision dans les délais	0	0	0
Attestations de sécurité lieu ou événement			
Refus	0	15	16
Retrait	0	0	0
Pas de décision dans le délai	0	0	0
Avis de sécurité			
Avis négatif	23	106	99
Pas d'avis	0	2	0
« Révocation » d'un avis positif	0	0	0
Actes normatifs d'une autorité administrative	0	0	0
Décision d'une autorité publique d'exiger des attestations	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des attestations	0	0	0
Décision d'une autorité administrative d'exiger des avis	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des avis	0	0	0
SOUS-TOTAL ATTESTATIONS ET AVIS	**46**	**123**	**119**
TOTAL DÉCISIONS CONTESTÉES	**91**	**189**	**171**

Tableau 3. Nature du requérant

	2012	2013	2014
Fonctionnaire	5	4	0
Militaire	26	26	17
Particulier	54	159	145
Personne morale	6	0	6

Tableau 4. Langue du requérant

	2012	2013	2014
Français	51	92	92
Néerlandais	40	97	76
Allemand	0	0	0
Autre langue	0	0	0

Tableau 5. Nature des décisions interlocutoires prises par l'Organe de recours[171]

	2012	2013	2014
Demande du dossier complet (1)	90	187	168
Demande d'informations complémentaires (2)	5	12	16
Audition d'un membre d'une autorité (3)	10	3	11
Décision du président (4)	0	0	0
Soustraction d'informations du dossier par l'Organe de recours (5)	44	68	78
Soustraction d'informations du dossier par le service de renseignement (6)	0	0	0

(1) L'Organe de recours peut demander l'intégralité du dossier d'enquête aux autorités de sécurité. Comme ce dossier contient davantage de données que le rapport d'enquête seul, cette requête est systématique.
(2) L'Organe de recours peut également demander tout complément d'informations qu'il juge nécessaire pendant la procédure.
(3) L'Organe de recours peut décider d'entendre les membres des services de renseignement et de police ou des autorités de sécurité qui ont participé à l'enquête ou à la vérification de sécurité.
(4) Le président de l'Organe de recours peut décider de permettre au membre du service de renseignement de garder secrètes certaines données pendant son audition.
(5) Si le service de renseignement concerné le requiert, l'Organe de recours peut décider que certaines informations soient retirées du dossier communiqué au requérant.

171 Le « nombre de décisions interlocutoires » (tableau 5), les « manières dont les requérants font usage de leurs droits de défense » (tableau 6), ou encore la « nature des décisions de l'Organe de recours » (tableau 7) ne correspondent pas nécessairement au nombre de requêtes introduites (voir tableaux 1 à 4). En effet, certains dossiers ont par exemple déjà été ouverts en 2014, alors que la décision n'a été rendue qu'en 2015.

(6) Si l'information concernée provient d'un service de renseignement étranger, c'est le service de renseignement belge qui décide si elle peut être communiquée. Il s'agit d'un aspect de l'application de la « règle du tiers service ».

Tableau 6. Manière dont le requérant fait usage de ses droits de défense

	2012	2013	2014
Consultation du dossier par le requérant /l'avocat	54	103	84
Audition du requérant /avocat[172]	65	138	115

Tableau 7. Nature des décisions de l'Organe de recours

	2012	**2013**	**2014**
Habilitations de sécurité			
Recours irrecevable	0	2	0
Recours sans objet	1	3	3
Recours non fondé	19	20	12
Recours fondé (avec octroi partiel ou complet)	23	35	14
Devoir d'enquête complémentaire par l'autorité	1	0	0
Délai supplémentaire pour l'autorité	0	14	12[173]
Attestations de sécurité documents classifiés			
Recours irrecevable	0	0	0
Recours sans objet	0	0	0
Recours non fondé	0	0	2
Recours fondé (avec octroi)	0	0	0
Attestations de sécurité pour lieux ou événements			
Recours irrecevable	3	1	0
Recours sans objet	1	0	0

172 Dans le cadre de certains dossiers, le requérant/avocat est auditionné à plusieurs reprises.

173 Comme en 2013, ces dossiers concernaient principalement l'octroi d'habilitations de sécurité pour des membres du personnel du SHAPE. Vu que l'autorité belge de sécurité attendait parfois en vain des informations devant être communiquées par la France, les délais légaux ont été dépassés. Dans 12 cas, l'Organe de recours a décidé d'accorder un délai supplémentaire à l'Autorité nationale de sécurité pour encore prendre une décision.

	2012	2013	2014
Recours non fondé	8	6	6
Recours fondé (avec octroi)	6	11	8
Avis de sécurité			
Organe de recours non compétent	5	0	4
Recours irrecevable	1	4	4
Recours sans objet	0	1	4
Confirmation de l'avis négatif	9	25	53
Transformation en avis positif	4	65	41
Recours contre des actes normatifs d'une autorité administrative	0	0	0
TOTAL	**81**	**187**	**163**

CHAPITRE VIII
LE FONCTIONNEMENT INTERNE DU COMITÉ PERMANENT R

VIII.I. COMPOSITION DU COMITÉ PERMANENT R

La composition du Comité permanent R n'a subi aucune modification en 2014 : la présidence a été assurée par Guy Rapaille (F), avocat général près la cour d'appel de Liège, tandis que les fonctions de conseiller ont été remplies par Gérald Vande Walle (F) et Pieter-Alexander De Brock (N).[174]

Le Service d'Enquêtes R n'a connu, lui non plus, aucun changement. Ce service est composé de cinq commissaires-auditeurs et est dirigé par Frank Franceus (N).

Le cadre du personnel administratif du Comité permanent R, placé sous la direction du greffier Wouter De Ridder, est resté lui aussi en l'état et comptait toujours seize personnes.

VIII.2. RÉUNIONS AVEC LA OU LES COMMISSION(S) DE SUIVI

Dans le courant de l'année 2014, deux réunions ont encore été organisées avec la Commission de suivi du Sénat, à laquelle le Comité permanent R faisait rapport. Plusieurs enquêtes de contrôle ont été discutées lors de ces réunions à huis clos.

Avec le réaménagement des compétences du Sénat comme suite à la sixième réforme de l'État et conformément à la Loi du 6 janvier 2014[175], le contrôle sur les services de renseignement est passé à une unique 'Commission chargée de l'accompagnement du Comité permanent P et du Comité permanent R' au sein de la Chambre des Représentants, qui contrôlera à la fois les services de police et les services de renseignement.[176] Avant les élections de mai 2014, la majorité précédente avait décidé que la nouvelle commission parlementaire se

174 Un second membre suppléant néerlandophone a toutefois été désigné en 2014 (*Ann. parl.* Sénat 2013-14, 13 mars 2014, n°5-144, 47).

175 *M.B.* 31 janvier 2014.

176 Pour des informations détaillées à ce sujet, voir les articles suivants : W. VAN LAETHEM, *Juristenkrant*, 28 mai 2014 (Nieuwe Kamercommissie ziet toe op geheime diensten) et W.

composerait des chefs de groupes politiques. Début octobre 2014, un échange de vues a donc eu lieu avec les Comités permanents P et R au sein de cette commission, sous la présidence du Président de la Chambre *ad interim*, Patrick Dewael.

La nouvelle majorité a toutefois opté pour une représentation plus proportionnelle. Le principe selon lequel les chefs de groupes sont membres de plein droit de la Commission a donc été abandonné et l'article 149 du Règlement de la Chambre des Représentants a été modifié.[177] Désormais, la Commission compte treize membres ayant voix délibérative et est composée comme suit : Koenraad Degroote (N-VA), Peter Buysrogge (N-VA), Hendrik Vuye (N-VA), Laurette Onkelinx (PS), André Frédéric (PS), Denis Ducarme (MR), Philippe Pivin (MR), Servais Verherstraeten (CD&V), Franky Demon (CD&V), Patrick Dewael (Open Vld), Karin Temmerman (sp.a), Stefaan Van Hecke (Ecolo-Groen) et Christian Brotcorne (cdH).[178] La Commission se réunit sous la présidence du président de la Chambre Siegfried Bracke (N-VA).

Cette commission s'est réunie pour la première fois à la fin novembre 2014, avec à l'ordre du jour une discussion sur le *Rapport d'activités 2013* ainsi que trois enquêtes de contrôle.[179]

VIII.3. RÉUNIONS COMMUNES AVEC LE COMITÉ PERMANENT P

Les articles 52 à 55 L.Contrôle déterminent les cas où et la manière dont le Comité permanent R et le Comité permanent P doivent organiser des réunions communes. Ces réunions poursuivent un double objectif : échanger des informations et discuter d'enquêtes de contrôle communes en cours, telles que, en l'espèce, les enquêtes relatives à la *Joint Information Box* (II.10.3), aux membres du personnel de l'OCAM et les médias sociaux (II.10.5) et aux contacts internationaux de l'OCAM (II.10.6).

En 2014, quatre réunions communes ont eu lieu.

VAN LAETHEM, *Juristenkrant*, 8 avril 2015 (Dan toch geen geheime informatie voor het parlement).

177 Règlement de la Chambre des Représentants – Modification (1), *MB* 31 octobre 2014 : « *Conformément aux articles 157 et 158, la Chambre désigne en son sein, au début de chaque législature, les membres effectifs de la commission chargée du suivi du Comité permanent P et du Comité permanent R, prévue par l'article 66bis de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements et de l'Organe de coordination pour l'analyse de la menace. Il est procédé à autant de nominations qu'il est nécessaire pour que chaque groupe politique compte au moins un membre au sein de la commission. L'article 22 n'est pas d'application.* ».

178 *Ann. parl. C.R.I.,* Chambre, 2013-14, 13 novembre 2014, PLEN015, 32.

179 *Doc. parl.* Chambre 2014-15, n°54-720/001.

VIII.4. MOYENS FINANCIERS ET ACTIVITÉS DE GESTION

Dans un contexte général d'assainissement des finances publiques, le Comité a proposé d'initiative à son autorité de contrôle une dotation de 3,75 millions d'euros pour l'année d'activités 2014.[180] En comparaison avec les 3,86 millions d'euros demandés en 2013, cela représente une diminution de 2,82 % de son budget total de fonctionnement. Une gestion rationnelle des fonds mis à disposition pour 2013 a en outre permis de dégager un boni de 1,13 million d'euros. Ce montant a été ajouté au financement de la dotation de 2014, ce qui a permis de réduire de 14,6 % les moyens alloués par l'État au titre de financement de la dotation en vertu de l'article 57 L.Contrôle. Le Comité permanent R a signalé à la Commission de la Comptabilité que les effets cumulés d'un budget réduit à charge du budget de l'État et la diminution du boni peuvent, à terme, poser un problème de financement.

Depuis son installation dans les bâtiments du FORUM, propriété de la Chambre des Représentants, le Comité recherche et développe constamment des synergies avec la Chambre et d'autres institutions publiques afin d'optimaliser et/ou de diminuer les frais de fonctionnement.

VIII.5. FORMATION

Vu l'intérêt pour l'organisation, le Comité permanent R encourage ses collaborateurs à suivre des formations générales (informatique, management…) ou propres au secteur. Concernant cette dernière catégorie, un ou plusieurs membres (du personnel) du Comité permanent R ont assisté aux journées d'étude mentionnées ci-dessous.

DATE	TITRE	ORGANISATION	LIEU
2014-2015	Hautes études de sécurité et de défense	IRSD	Bruxelles
4 et 11 février 2014	Sociale media op de politionele werkvloer	Belgian Cybercrime Centre of Excellence for Training, Research and Education	Gand et Louvain
6 février 2014	Armed drones. Technical, legal and ethical considerations	IRSD	Bruxelles

180 Loi du 19 décembre 2013 contenant le budget général des dépenses pour l'année budgétaire 2014, *M.B.* 27 décembre 2013 et *Doc. parl.* Chambre 2013-14, n° 53-3237/001.

DATE	TITRE	ORGANISATION	LIEU
7 mars 2014	Social media intelligence (DocMint) : Intelligent ? No borders ? The egg of Colombus ? Raising Expectations ?	Netherlands Intelligence Studies Association	Amsterdam
13 mai 2014	L'avenir de la dissuasion nucléaire en Europe	IRSD	Bruxelles
19 mai 2014	Les enjeux géopolitiques du golfe arabo-persique	Métis	Paris
23 mai 2014	D-Day moins x – Activités de renseignement derrière et le long du Mur de l'Atlantique	BISC	Raversijde
10 juin 2014	Le danger des sectes en Belgique – Illusion ou réalité ?	Fédération Royale des Officiers et Hauts Fonctionnaires de la Police belge	Bruxelles
17 juin 2014	Open school Cyber security, challenges for Belgian defence	SGRS	Bruxelles
26 juin 2014	The public regulated service of the European Galileo navigation satellite system	ERM/ANS	Bruxelles
4 juillet 2014	Éthique et renseignement	GERER	Paris
7-10 juillet 2014	International Intelligence Review Agencies Conference	IIRAC	Londres
15 septembre 2014	Intelligence économique et renseignement. Quelles différences et quelles interactions ?	Métis	Paris
18-19 septembre 2014	Telling truth to power. The past, present and future of military intelligence	NISA/DISS	Amsterdam

DATE	TITRE	ORGANISATION	LIEU
25 septembre 2014	Ethische competentie : het belang van selectie en socialisatie	KUL/LINC	Louvain
24 octobre 2014	La sécurité privée, la défense et les études de renseignement	Université de Gand et Université Lille	Lille
6 novembre 2014	'Blowback' – Une relecture de la menace des combattants étrangers pour l'Europe	IRSD	Bruxelles
14 novembre 2014	Les méthodes particulières de recherches face aux nouvelles formes de cybercriminalité	B-CCENTRE/ CRIDS/Université de Namur	Bruxelles
20 novembre 2014	La sécurité privée, la défense et les études de renseignement	Université de Gand et Université Lille	Lille
2 décembre 2014	Building Belgium's cyber intelligence knowledge capacity	BISC	Bruxelles
4 décembre 2014	Éthique et renseignement	GERER	Paris

CHAPITRE IX
RECOMMANDATIONS

À la lumière des enquêtes de contrôle clôturées en 2014 et des dossiers MRD traités, le Comité permanent R formule les recommandations reprises ci-après. Elles portent plus particulièrement sur la protection des droits que la Constitution et la loi confèrent aux personnes (IX.1), sur la coordination et l'efficacité des services de renseignement, de l'OCAM et des services d'appui (IX.2) et, enfin, sur l'optimalisation des possibilités de contrôle du Comité permanent R (IX.3).

IX.1. RECOMMANDATIONS RELATIVES À LA PROTECTION DES DROITS QUE LA CONSTITUTION ET LA LOI CONFÈRENT AUX PERSONNES

IX.1.1. INTÉRÊT POUR LA CAPTATION MASSIVE DE DONNÉES ET POUR L'ESPIONNAGE POLITIQUE ET ÉCONOMIQUE[181]

Les deux services de renseignement doivent s'intéresser aux risques inhérents aux nouvelles possibilités offertes par la technologie en matière de captation massive de données et d'espionnage économique et politique, et ce même si ces risques émanent de « pays amis ». À cet égard, il conviendrait de procéder à des analyses de risques prenant également en considération la présence d'institutions internationales sur le territoire belge.

La VSSE et le SGRS doivent prêter attention à ces phénomènes afin de se forger une bonne position d'information. Cela leur permettrait de connaître les possibilités et les méthodes de travail d'autres services, non seulement pour pouvoir informer, le cas échéant, les autorités, ou prendre des contre-mesures, mais aussi pour évaluer leurs propres techniques de recueil.

---

181 Cette recommandation découle de la première enquête de contrôle sur les révélations d'Edward Snowden (II.1. Les révélations d'Edward Snowden et la position d'information des services de renseignement belges).

En ce qui concerne la VSSE, l'intérêt porté à la captation massive de données est évidemment nécessaire, puisque ce phénomène constitue une réelle menace pour au moins deux intérêts qu'elle est légalement tenue de protéger, à savoir les libertés et droits fondamentaux et la souveraineté de l'État. Elle peut, par exemple, retrouver de nombreuses informations dans les sources ouvertes ou en demander au service de renseignement militaire. À la lumière de ces éléments, elle peut déjà se faire une idée globale du phénomène et des risques y afférents, et en faire écho dans une analyse de phénomène[182], envoyée à intervalles réguliers aux autorités concernées. Les citoyens et les entreprises devraient eux aussi être davantage encore sensibilisés à la problématique.

IX.1.2. DIRECTIVES CONCERNANT LA COLLABORATION AVEC DES SERVICES ÉTRANGERS[183]

En 2012, la VSSE a rédigé une instruction détaillée sur la « collaboration bilatérale avec les correspondants ». Le Comité permanent R a certes considéré que cette directive était particulièrement positive, mais il a souligné que certaines des options prises par la VSSE devaient être portées par les responsables politiques, à savoir les membres du Comité ministériel du renseignement et de la sécurité (de l'époque). En outre, l'instruction n'évoque que de manière succincte l'un des principaux aspects de cette collaboration : quels renseignements peuvent être communiqués à des services étrangers ? Aussi le Comité permanent R recommande-t-il une fois encore[184] à la VSSE de transmettre sans délai sa directive – complétée par des règles plus précises sur l'échange d'informations – au Conseil national de sécurité, qui a succédé au Comité ministériel du renseignement et de la sécurité.

Cette recommandation est également valable pour le SGRS, d'autant que le Comité permanent R a pu constater que ce service travaille en étroite collaboration

---

182 Le Comité permanent R a déjà mis l'accent sur les atouts de ce que la VSSE appelle une « analyse de phénomène » : « *L'analyse du phénomène expose un thème actuel qui relève des sphères d'intérêt et des missions dévolues à un service de renseignement et qui représente un défi politique et social majeur, tant aujourd'hui que pour les années à venir. Elle s'attache à décrire ce problème tant au niveau de ses origines historiques, qu'au plan de l'idéologie, de l'organisation, de la structure et des activités y relatives. Elle contextualise les défis et les risques, établit une « évaluation du risque » à destination de nos responsables politiques, des autorités administratives concernées et des autorités judiciaires qui sont également confrontées à cette problématique* », comme l'explique la VSSE dans sa première analyse de phénomène. De telles analyses se prêtent particulièrement bien à la problématique de la captation massive de données, notamment parce qu'elles sont destinées à être largement diffusées.

183 Cette recommandation découle des deux enquêtes de contrôle suivantes : « II.1. Les révélations d'Edward Snowden et la position d'information des services de renseignement belges » et « II.3. L'utilisation dans des affaires pénales d'informations issues d'une captation massive de données par des services étrangers ».

184 COMITÉ PERMANENT R, *Rapport d'activités 2012*, 97.

avec des départements SIGINT étrangers, comme par exemple la NSA. À l'instar de la VSSE, le SGRS prépare une note similaire, avec des « critères vérifiables » à appliquer dans le cadre de la collaboration avec des services de renseignement étrangers (au sens large). Cette note aurait dû être finalisée dans le courant de l'année 2014. Le Comité insiste sur l'importance d'une telle directive pour le SGRS. En effet, elle peut apporter un cadre légitime – également après l'approbation du Conseil national de sécurité – pour les plateformes de coopération desquelles le service de renseignement militaire fait déjà partie.

En outre, le Comité recommande que les directives du SGRS et de la VSSE soient, dans la mesure du possible, d'un niveau concordant. Pour le Comité, le SGRS peut s'inspirer des éléments suivants, que la VSSE a avancés dans l'instruction susmentionnée :

- il convient de tenir compte des facteurs susceptibles de peser sur la collaboration (comme des problèmes d'ingérence, des intérêts contradictoires, le respect des droits fondamentaux…) ;
- la mission légale propre doit toujours être préservée, particulièrement dans des matières telles que le terrorisme et l'extrémisme, qui prennent rapidement une dimension judiciaire ;
- la collaboration avec les services étrangers doit être d'une transparence et d'une traçabilité totale (ce qui permet notamment un contrôle par le Comité permanent R) ;
- la collaboration doit faire l'objet d'une évaluation périodique.

Le Comité recommande par ailleurs que la collaboration soit effectivement évaluée à intervalles réguliers sur la base des critères prédéfinis. Les révélations d'Edward Snowden en démontrent la nécessité.

Afin de lever tout malentendu éventuel, le Comité permanent R tient toutefois à souligner qu'il est convaincu que les services de renseignement belges doivent continuer à investir dans une bonne collaboration avec les services étrangers, et ce tant au niveau bilatéral que multilatéral.

IX.1.3. LA NÉCESSITÉ D'UNE COUVERTURE POLITIQUE DES ACCORDS DE COOPÉRATION[185]

Le Comité estime 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

185 Cette recommandation découle de la première enquête de contrôle sur les révélations d'Edward Snowden (II.1. Les révélations d'Edward Snowden et la position d'information des services de renseignement belges).

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.

IX.1.4. LA NÉCESSITÉ D'UNE ORIENTATION POLITIQUE PAR LE CONSEIL NATIONAL DE SÉCURITÉ[186]

Le Comité ministériel du renseignement et de la sécurité, qui est aujourd'hui devenu le Conseil national de sécurité, a été créé dans le but d'orienter politiquement le travail de renseignement. Il a pour tâche d'établir la politique générale du renseignement, de déterminer, par des directives, les priorités des deux services de renseignement, d'assurer une coordination entre les services de renseignement, et de définir des règles en matière de coopération internationale et d'échange de données. Le Comité ministériel ne s'est toutefois pas réuni après les révélations d'Edward Snowden.

Le Comité juge souhaitable que le nouveau Conseil national de sécurité et, par extension, le Comité stratégique et le Comité de coordination du renseignement et de la sécurité assument leur rôle de « pilote » – en partie sur les indications des deux services de renseignement – à l'égard des phénomènes de captation massive de données et d'espionnage politique et économique. Le Comité estime que la Belgique remplirait ainsi au moins en partie son obligation positive qui découle de l'article 8 CEDH visant à protéger la vie privée de ses citoyens.

Par ailleurs, le Comité signale que le Comité ministériel/Conseil national de sécurité n'a pas approuvé officiellement, comme l'exige pourtant la loi, la liste, établie à la fin 2012, des entreprises dont le SGRS doit protéger le PSE.

IX.1.5. ÉVALUATION CRITIQUE DES RÈGLES DE LA CULTURE INTERNATIONALE DU RENSEIGNEMENT[187]

Dans sa première enquête de contrôle menée dans le sillage des révélations d'Edward Snowden, le Comité permanent R a fait référence à une recommandation figurant dans le projet de rapport de la Commission Libertés

186 *Idem*.

187 Cette recommandation découle de l'enquête de contrôle « II.3. L'utilisation dans des affaires pénales d'informations issues d'une captation massive de données par des services étrangers ».

civiles, justice et affaires intérieures du Parlement européen : « *Invite les États membres à s'abstenir d'accepter des données provenant de pays tiers et ayant été collectées illégalement, ainsi que d'accepter que des gouvernements ou agences de pays tiers effectuent sur leur territoire des activités de surveillance contraires au droit national ou ne satisfaisant pas aux garanties juridiques spécifiées dans les instruments internationaux ou européens, notamment la protection des droits de l'homme au titre du traité UE, de la CEDH et de la Charte des droits fondamentaux de l'Union européenne* ». Le Comité permanent R remarque toutefois que dans la pratique, les « services de renseignement fournisseurs » protègent généralement leurs sources (et donc l'origine d'un renseignement), et que les « services destinataires » l'acceptent. Cette forme d'entente fait partie de la culture internationale du renseignement, au même titre que la règle du service tiers, le principe « *do ut des* » et le devoir de réserve.

Le Comité a rappelé que ce constat ne signifie pas qu'il souscrit inconditionnellement à ces principes, mais ceux-ci ne peuvent être brusquement ou unilatéralement abandonnés.

Le Comité permanent R recommande que le Conseil national de sécurité examine dans un délai raisonnable quelles mesures peuvent être prises à cette fin.

IX.1.6. RESTRICTIONS EN MATIÈRE DE RECUEIL D'INFORMATIONS AUPRÈS DE PERSONNES (MORALES)[188]

La VSSE est autorisée à recueillir des informations relatives aux menaces qu'elle suit auprès de toute personne ou de toute organisation relevant du secteur privé (art. 16 L.R&S). Dans ce cadre, la personne concernée reste, il est vrai, liée par le secret professionnel auquel elle est tenue le cas échéant, ainsi que par les exigences de la Loi relative au traitement des données à caractère personnel. Ces réglementations imposent des restrictions quant à la communication de données à des tiers (comme la VSSE). En outre, le citoyen a le droit de ne pas collaborer à une enquête de renseignement. Aussi le Comité permanent R recommande-t-il que, dans leurs contacts avec des particuliers, les membres de la VSSE soient attentifs à la manière dont leur intervention est perçue par des personnes qui ne sont pas habituées à être en contact avec le service. Parallèlement, il convient de prêter attention, dans le cadre de la formation, à l'attitude correcte que les membres de la VSSE doivent adopter à l'égard des citoyens avec lesquels ils entrent en contact.

188 Cette recommandation découle de l'enquête de contrôle « II.8. Plainte relative à la manière dont la VSSE suit le dirigeant d'une entreprise ».

IX.1.7. ACTUALISER LES INFORMATIONS DISPONIBLES DANS LE CADRE DES NATURALISATIONS[189]

Le Comité recommande que les informations fournies par la VSSE dans le cadre de l'obtention de la nationalité belge soient systématiquement actualisées si elles portent sur des « *faits personnels graves* ». Ce genre informations est en effet susceptible de constituer une contre-indication à l'octroi de la nationalité belge.

IX.2. RECOMMANDATIONS RELATIVES À LA COORDINATION ET L'EFFICACITÉ DES SERVICES DE RENSEIGNEMENT, DE L'OCAM ET DES SERVICES D'APPUI

IX.2.1. LA MANIÈRE DE CONCEVOIR LA NOTION DE « SERVICES AMIS »[190]

Il apparaît que tant la VSSE que le SGRS se montrent plus « circonspects » à l'égard des services amis ou des services de pays amis. Le Comité peut certes le comprendre dans une certaine mesure, mais il recommande aux services de renseignement belges de prendre au sérieux *toutes* les menaces, même si elles émanent de services amis ou de services de pays amis. Le Comité permanent R rejoint la VSSE lorsqu'elle affirme qu'il est préférable de parler de « partenaires stratégiques » plutôt que de « services amis ».

IX.2.2. UNE COLLABORATION PLUS ÉTROITE ENTRE LES DEUX SERVICES DE RENSEIGNEMENT[191]

Le Comité a dû constater qu'avant les révélations d'Edward Snowden, la VSSE et le SGRS n'avaient jamais échangé d'informations sur les menaces émanant de la captation massive de données et de l'espionnage politique et économique, et que cet échange mutuel n'a été que limité par la suite. Le Comité attire toutefois l'attention sur l'obligation légale qui incombe à ces services en matière d'échange d'informations (art. 19 L.R&S). En outre, le Comité souligne l'existence d'un

189 Recommandation issue du chapitre « II.7. Enquête de contrôle relative aux éléments transmis par la VSSE dans le cadre d'un dossier de naturalisation ».

190 Cette recommandation découle de la première enquête de contrôle sur les révélations d'Edward Snowden (II.1. Les révélations d'Edward Snowden et la position d'information des services de renseignement belges).

191 *Idem.*

accord de coopération mutuel (Protocole d'accord du 12 novembre 2004), qui vise précisément la transmission spontanée d'informations relevant de la sphère de compétences de l'autre service. Au moins après les révélations, les mécanismes décrits dans ce Protocole d'accord auraient dû être utilisés pour renforcer la position d'information des deux services. Le Comité met particulièrement en exergue la possibilité qui figure dans le Protocole de créer une « plateforme de coopération *ad hoc* », au sein de laquelle des analyses communes peuvent être rédigées. Une telle plateforme aurait permis de lever la contradiction révélée dans le dossier concerné, à savoir que le SGRS disposait de nombreuses informations, mais n'était pas compétent pour le suivi de l'interception massive de données avant les révélations, tandis que la VSSE, qui était compétente, ne possédait que de peu d'informations spécifiques sur le phénomène.

IX.2.3. COLLABORATION INTERDÉPARTEMENTALE EN MATIÈRE DE CYBERSÉCURITÉ, *ICT-SECURITY* ET *CYBERINTELLIGENCE*[192]

Certains aspects des révélations d'Edward Snowden ont mis en évidence des faiblesses dans les systèmes de protection de réseaux IT d'acteurs privés et d'institutions publiques. Par conséquent, le Comité répète avec insistance sur la nécessité d'accorder plus d'attention à la cybersécurité et la sécurité des TIC (INFOSEC), et sur le fait que ces problématiques (qui ne relèvent pas uniquement des tâches des services de renseignement) requièrent une coopération interdépartementale. Le Conseil national de sécurité, par exemple, a un rôle crucial à jouer dans ce domaine.

Le Comité rappelle également à cet égard que le 19 décembre 2013, le Conseil des ministres a approuvé un projet d'arrêté qui devait donner lieu à la création d'un Centre pour la cybersécurité Belgique au sein de la Chancellerie du Premier ministre. La création de centre a été officialisée par l'A.R. du 10 octobre 2014.

À l'époque, des moyens supplémentaires ont également été alloués pour exécuter la stratégie de cybersécurité, telle qu'approuvée à la fin 2012. Une partie de ces moyens serait destinée au SGRS pour lui permettre d'accroître sa capacité et de se consacrer davantage à la *cyberintelligence*. Le Comité permanent R est toutefois convaincu que la cybersécurité et la *cyberintelligence* requerront des investissements constants dans les prochaines décennies.

192 *Idem.*

IX.2.4. LES CONSÉQUENCES NÉGATIVES DU COMPARTIMENTAGE ET DE LA CONFIDENTIALITÉ AU SEIN DU SGRS[193]

Il a peut-être été plus compliqué pour le SGRS de se faire une idée globale des capacités et des stratégies SIGINT de grandes puissances étrangères, vu le nombre très restreint de personnes bénéficiant d'un accès direct aux informations SIGINT et vu la stricte confidentialité entourant ce genre d'informations. Le Comité estime dès lors que le SGRS devrait réfléchir à la manière de mieux concilier les principes du *need to know* et du *need to share*.

IX.2.5. LE CHAMP D'APPLICATION TERRITORIAL DE LA LOI MRD[194]

Les évolutions technologiques imposent une clarification du champ d'application territorial de la Loi MRD. Dans l'attente d'une éventuelle initiative législative, le Comité interprète avec prudence la réglementation actuelle, dans le sens où la méthode MRD ne peut être utilisée pour des communications que lorsque le signal d'une communication à intercepter se trouve sur le territoire belge.

IX.2.6. UNE CLARIFICATION DE LA RÉGLEMENTATION INT[195]

La réglementation INT belge, qui permet au SGRS d'intercepter des communications étrangères, a vu le jour lorsque les interceptions concernaient essentiellement des signaux radio. Depuis lors, la technologie a connu une telle évolution que le législateur devrait réexaminer cette réglementation. Les révélations d'Edward Snowden n'ont fait que confirmer ce constat. Ce réexamen devra de toute manière porter sur les éléments suivants : dans quelle mesure les interceptions doivent être ciblées ou non, la portée exacte de la possibilité de « chercher » des signaux, le degré de précision du Plan d'écoutes annuel, la possibilité de faire du *datamining* dans informations en vrac, ainsi que la question de savoir si les opérations SIGINT étrangères doivent s'inscrire dans un « mandat international » plus large.

193 *Idem*.

194 *Idem*. Dans le même sens, COMITÉ PERMANENT R, *Rapport d'activités 2013*, 114.

195 *Idem*. Voir également Chapitre IV. Le contrôle de l'interception de communications émises à l'étranger.

IX.2.7. RECOMMANDATIONS DANS LE CADRE DE LA PROTECTION DES PERSONNES

Dans le cadre de son enquête de contrôle sur « La VSSE et sa mission légale de protection des personnes »[196], le Comité permanent R a relevé plusieurs problèmes et formulé un certain nombre de recommandations concrètes, parmi lesquelles :

- La proportion entre le nombre de dirigeants dans le Service Protection des personnes et le nombre de collaborateurs exécutants (*span of control*) est très grande. Il est impossible de travailler dans ces conditions.
- Le Comité a pu constater que certaines personnes à protéger ne sont pas toujours conscientes des risques. Or, en cas d'incident, ce sont la VSSE, et donc au final l'État belge, qui devraient rendre des comptes. Aussi convient-il de conclure d'urgence des accords clairs avec les diplomates étrangers. L'élaboration d'un canevas idoine ne relève pas seulement (et peut-être même pas dans un premier temps) de la responsabilité de la VSSE. Le Comité permanent R estime qu'il incombe également aux responsables politiques (Intérieur, Affaires étrangères, Justice) de procéder à court terme à une (ré) évaluation (et, partant, à une réorientation) en la matière.
- Le Comité permanent R recommande de réexaminer en priorité les missions permanentes de protection, et de voir s'il est possible de les mener à bien avec moins de moyens.
- Le Comité permanent R recommande de prêter une attention continue à la suppression des heures supplémentaires.
- L'enquête a démontré que l'application concrète des niveaux de menace sur le terrain n'était pas cohérente. Il s'est en effet avéré que les dispositifs mis en place sur le terrain n'avaient pas de lien évident avec le niveau de menace attribué par l'OCAM. Par conséquent, le Comité permanent R recommande que les services concernés se mettent d'accord sur un modèle ou une typologie qui pourrait être mis(e) en pratique aisément, et qu'ils l'appliquent ensuite de manière cohérente. Selon le Comité permanent R, la typologie fondée uniquement sur la « menace » ne permet pas d'introduire suffisamment de nuances. Le Comité permanent R adhère dès lors à la suggestion du Centre de crise du gouvernement, qui propose d'intégrer les concepts de « mesures de protection » et de « mesures de précaution » dans une nouvelle typologie, puisqu'il ne sera pas systématiquement question d'une menace réelle. Toutes les personnalités ne sont pas directement menacées, mais des mesures de précaution doivent être prises pour sauvegarder la réputation de la Belgique en tant que pays hôte. Il conviendrait également d'intégrer dans le modèle l'attitude des personnalités à protéger comme variable ou facteur pertinent.

196 Voir Chapitre II.4.

IX.2.8. DÉMONSTRATION ÉTAYÉE DE L'INGÉRENCE DE L'ÉGLISE DE SCIENTOLOGIE[197]

Le Comité permanent R a pris acte de l'analyse globale réalisée par la VSSE concernant les nombreuses formes d'ingérence que l'ASBL Église de scientologie de Belgique exerce à l'égard des autorités. Le Comité constate toutefois que les observations de la VSSE n'ont jamais fait apparaître de moyens « illicites » mis en œuvre par le mouvement pour approcher des décideurs politiques. En revanche, la VSSE dispose de nombreuses indications qui laissent supposer que cette organisation fait usage à cette fin de « *moyens trompeurs ou clandestins* ». Par conséquent, le Comité a recommandé que la VSSE démontre mieux l'ingérence de cette Église, en structurant son analyse relative aux moyens illicites, trompeurs et clandestins employés pour approcher les autorités et les décideurs politiques belges.

IX.2.9. ACCORDS DE COOPÉRATION CONTRE LA PROLIFÉRATION[198]

Le Comité permanent R recommande que les différentes autorités concluent des accords de coopération formels afin de garantir une approche efficace de la prolifération. Ces accords sont nécessaires en raison de la nature complexe du phénomène, et ce tant sur le plan de la technicité et de la réglementation que des compétences. Ces accords de coopération doivent, d'une part, être conclus entre les niveaux fédéral et régional pour faire concorder la réglementation et de déterminer les sanctions et, d'autre part, entre tous les services qui ont une responsabilité quelconque en matière de contrôle et de surveillance sur le terrain.

197 Cette recommandation provient de l'enquête « II.5. Une plainte de l'Église de scientologie contre la Sûreté de l'État ».

198 Recommandation extraite de l'enquête « II.8. Plainte relative à la manière dont la VSSE suit le dirigeant d'une entreprise ».

IX.3. RECOMMANDATION RELATIVE À L'EFFICACITÉ DU CONTRÔLE : APPLICATION STRICTE DE L'ARTICLE 33, § 2 L.CONTRÔLE[199]

En vue d'exercer son rôle de contrôle, le Comité permanent R a une nouvelle fois[200] souligné 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 »*. Cette obligation s'applique également aux conventions, Memorandums of Understanding (MOUs) ou accords conclus au niveau international, qu'ils soient bilatéraux ou multilatéraux.

199 Cette recommandation découle de la première enquête de contrôle sur les révélations d'Edward Snowden (II.1. Les révélations d'Edward Snowden et la position d'information des services de renseignement belges).

200 Le Comité a déjà mené plusieurs enquêtes à cet égard : COMITÉ PERMANENT R, *Rapport d'activités 1996*, 20-24 (Rapport sur l'application de l'article 33 alinéa 2 L.Contrôle par les services de renseignement) ; *Rapport d'activités 2001,* 206-207 (Les informations indispensables dont le Comité permanent R estime devoir disposer afin d'accomplir sa mission efficacement) ; *Rapport d'activités 2002,* 26-27 (La transmission d'initiative par les services de renseignement de certains documents au Comité permanent R) ; *Rapport d'activités 2006*, 12 ; *Rapport d'activités 2013*, 116.

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 2014 AU 31 DÉCEMBRE 2014)

Règlement de la Chambre des représentants. Modifications, *M.B.* 21 mai 2014
Règlement de la Chambre des représentants – Modification, *M.B.* 31 octobre 2014

Loi 13 janvier 2014 modifiant la loi du 10 avril 1990 réglementant la sécurité privée et particulière, *M.B.* 23 janvier 2014
Loi 6 janvier 2014 modifiant diverses lois suite à la réforme du Sénat, *M.B.* 31 janvier 2014
Loi 19 novembre 2013 modifiant la loi du 5 février 2007 relative à la sûreté maritime, *M.B.* 4 mars 2014
Loi 18 mars 2014 relative à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle, *M.B.* 28 mars 2014
Loi 27 mars 2014 portant des dispositions diverses en matière de communications électroniques, *M.B.* 28 avril 2014
Loi 24 mars 2014 modifiant la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de service fédéral, *M.B.* 2 mai 2014
Loi 25 avril 2014 portant des dispositions diverses, *M.B.* 7 mai 2014
Loi 5 mai 2014 visant à corriger plusieurs lois en matière de justice, *M.B.* 8 juillet 2014
Loi 15 mai 2014 modifiant la loi du 9 décembre 2004 sur l'entraide judiciaire internationale en matière pénale et modifiant l'article 90*ter* du Code d'instruction criminelle, *M.B.* 7 août 2014

A.R. 15 décembre 2013 déterminant les services de l'Administration générale des Douanes et Accises dans lesquels l'exercice d'une fonction peut requérir une vérification de sécurité, *M.B.* 19 décembre 2013
A.R. 29 janvier 2014 modifiant l'arrêté royal du 14 janvier 1994 portant statut de l'administrateur général et de l'administrateur général adjoint de la Sûreté de l'État, *M.B.* 4 février 2014
A.R. 26 janvier 2014 modifiant l'arrêté royal du 3 juin 2007 relatif à l'armement de la police intégrée, structurée à deux niveaux, ainsi qu'à l'armement des membres des

Services d'Enquêtes des Comités permanents P et R et du personnel de l'Inspection générale de la police fédérale et de la police locale, *M.B.* 7 février 2014

A.R. 16 février 2014 prévoyant la prise en considération dans le calcul de la pension des allocations de valorisation accordées à certains agents des services extérieurs de la Sûreté de l'État, *M.B.* 11 mars 2014

A.R. 10 avril 2014 modifiant l'arrêté royal du 28 septembre 1984 portant exécution de la loi du 19 décembre 1974 organisant les relations entre les autorités publiques et les syndicats des agents relevant de ces autorités, *M.B.* 30 avril 2014

A.R. 24 avril 2014 abrogeant l'arrêté royal du 3 août 1950 portant création d'un comité ministériel de défense, *M.B.* 13 mai 2014

A.R. 25 avril 2014 exécutant, pour les services extérieurs de la Sûreté de l'État, l'article 15*septies* de la loi du 8 avril 1965 instituant les règlements de travail, *M.B.* 30 juin 2014

A.R. 8 mai 2014 modifiant l'arrêté royal du 5 décembre 2006 relatif à l'administration générale et à la cellule d'appui de la Sûreté de l'État, *M.B.* 22 mai 2014

A.R. 4 juillet 2014 fixant le statut de certains agents civils du département d'état-major renseignements et sécurité des forces armées, *M.B.* 18 juillet 2014

A.R. 25 juillet 2014 modifiant l'arrêté royal du 21 décembre 2011 portant désignation des membres du Comité ministériel du renseignement et de la sécurité, *M.B.* 6 août 2014

A.R. 29 juin 2014 relatif aux professions ou activités qui ne sont pas considérées comme activités visées à l'article 1er de la loi du 10 avril 1990 réglementant la sécurité privée et particulière, *M.B.* 27 août 2014

A.R. 21 juillet modifiant l'arrêté royal du 16 mai 2004 relatif à la lutte contre le trafic et la traite des êtres humains, *M.B.* 1er septembre 2014

A.R. 23 août 2014 portant organisation de la 'Belgian Task Force for International Criminal Justice (BTF ICJ)', *M.B.* 5 septembre 2014

A.R. 4 septembre 2014 modifiant l'arrêté royal du 5 décembre 2006 relatif à l'administration générale et à la cellule d'appui de la Sûreté de l'État, *M.B.* 12 septembre 2014

A.R. 25 septembre 2014 modifiant l'arrêté royal du 21 décembre 2011 portant désignation des membres du Comité ministériel du renseignement et de la sécurité, *M.B.* 2 octobre 2014

A.R. 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique, *M.B.* 21 novembre 2014

A.R. 10 octobre 2014 modifiant l'arrêté royal du 13 décembre 2006 portant le statut des agents des services extérieurs de la Sûreté de l'État, *M.B.* 3 décembre 2014

A.R. 26 novembre 2014 portant répartition partielle du crédit provisionnel inscrit au programme 14-53-5 du budget général des dépenses pour l'année budgétaire 2014 et destiné à la compensation salariale et au remboursement aux départements d'origine des indemnités et des coûts afférents au déploiement et au fonctionnement de membres de la Police fédérale, de représentants de la Magistrature et de membres du personnel de la Justice, des Affaires étrangères, des Finances, de l'Intérieur, de l'Organe de Coordination pour l'Analyse de la Menace, de la Défense et d'autres instances publiques chargés de missions à l'étranger, *M.B.* 5 décembre 2014

A.M. 5 février 2014 modifiant l'arrêté ministériel du 4 avril 2006 portant désignation d'un comité de sélection chargé de l'évaluation des candidatures pour la fonction d'administrateur général de la Sûreté de l'État, *M.B.* 7 février 2014

A.M. 10 mars 2014 déterminant les armes et munitions faisant partie de l'équipement réglementaire des membres du personnel du Service général du Renseignement et de la Sécurité des Forces armées et fixant les dispositions particulières relatives à la détention, à la garde, au port, au transport et à l'utilisation d'armement, *M.B.* 30 avril 2014

A.M. 8 mai 2014 portant délégations de pouvoir par le ministre de la Défense en matière de passation et d'exécution des marchés publics de travaux, de fournitures et de services, en matière d'aliénation et en matière de dépenses diverses, *M.B.* 27 mai 2014

A.M. 7 octobre 2014 portant désignation d'un comité de sélection chargé de l'évaluation des candidatures pour la fonction de directeur d'encadrement de la Sûreté de l'État, *M.B.* 17 octobre 2014

Arrêté du Gouvernement de la Région de Bruxelles-Capitale du 3 avril 2014 portant exécution de l'Ordonnance du 20 juin 2013 relative à l'importation, à l'exportation, au transit et au transfert de produits liés à la défense, d'autre matériel pouvant servir à un usage militaire, de matériel lié au maintien de l'ordre, d'armes à feu à usage civil, de leurs pièces, accessoires et munitions, *M.B.* 17 juillet 2014

Circulaire GPI 78L relative au traitement de l'information au profit d'une approche intégrée du terrorisme et de la radicalisation violente par la police, *M.B. 17* février 2014

Ordonnance du 8 mai 2014 portant création et organisation d'un intégrateur de service régional, *M.B.* 6 juin 2014

Comité permanent de Contrôle des services de renseignement et de sécurité – Nomination d'un second membre suppléant d'expression néerlandaise – Appel aux candidats, *M.B.* 13 janvier 2014

Comité permanent de Contrôle des services de renseignement et de sécurité, Directeur du Service d'Enquêtes – Nomination, *M.B.* 30 janvier 2014

Emplois vacants d'administrateur général et d'administrateur général adjoint de la Sûreté de l'État, Appel aux candidats, *M.B.* 4 février 2014

Personnel – Désignation d'un titulaire d'une fonction de management, *M.B.* 10 avril 2014

Personnel – Désignation d'un titulaire d'une fonction de management, *M.B.* 28 avril 2014

Sélection comparative d'analystes (m/f) (niveau A), néerlandophones, pour la Sûreté de l'État (ANG14274), *M.B.* 5 septembre 2014

Sélection comparative d'analystes (m/f) (niveau A), francophones, pour la Sûreté de l'État (AFG14260), *M.B.* 5 septembre 2014

Emploi vacant de directeur d'encadrement de la Sûreté de l'État – Appel aux candidats, *M.B.* 7 octobre 2014

Sélection comparative d'administrateurs réseau (m/f) (niveau B), néerlandophones, pour la Sûreté de l'État (ANG14343), *M.B.* 5 novembre 2014

Sélection comparative d'analystes-programmeurs (m/f) (niveau B), néerlandophones pour le SPF Justice (ANG14354), *M.B.* 13 novembre 2014

Sélection comparative d'analystes-programmeurs (m/f) (niveau B), francophones, pour la Sûreté de l'État (AFG14295), *M.B.* 13 novembre 2014

Emploi vacant de directeur d'encadrement de la Sûreté de l'État – Appel aux candidats – Erratum, *M.B.* 23 décembre 2014

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 2014 AU 31 DÉCEMBRE 2014)

Sénat

Proposition de loi visant à corriger plusieurs lois en matière de justice, *Doc. parl.*, Sénat, 2013-2014, nos 5-2326/1 et 5-2326/2

Projet de loi relatif à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle, *Doc. parl.*, Sénat, 2013-2014, n° 5-2366/3 et *Ann. Parl.*, Sénat, 2013-2014, 6 février 2014, n° 5-139, p. 49

Proposition visant à instituer une commission d'enquête parlementaire chargée d'enquêter sur le rôle des services de renseignement dans le cyber espionnage, *Doc. parl.*, Sénat, 2013-2014, n° 5-2475/1

Projet de loi modifiant la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace, *Doc. parl.*, Sénat, 2013-2014, nos 5-2746/1 à 5-2746/3 et *Ann. Parl.*, Sénat, 2013-2014, 20 mars 2014, n° 5-145, p. 61 et *Ann. Parl.*, Sénat, 2013-2014, 3 avril 2014, n° 5-148, p. 44

Proposition de résolution relative à la collaboration avec les services de sécurité et de renseignement étrangers, *Doc. parl.*, Sénat, 2013-2014, n° 5-2849/1

Rapport d'activités 2012 du Comité Permanent R, *Doc. parl.*, Sénat, 2013-2014, n° 5-2426/1

Nomination d'un second membre suppléant d'expression néerlandaise pour le Comité permanent de contrôle des services de renseignements (Comité R), *Doc. parl.*, Sénat, 2013-2014, n° 5-2495/1 et *Ann. Parl.*, Sénat, 2013-2014, 20 février 2014, n° 5-141, p. 41 et *Ann. Parl.*, Sénat, 2013-2014, 13 mars 2014, n° 5-144, p. 47

Comité Permanent de Contrôle des services de renseignements et de sécurité – rapport d'activités pour 2013 – dépôt au Greffe, *Ann. Parl.*, Sénat, 2014-2015, 5 décembre 2014, n° 6-7, p. 42

Chambre des Représentants

Proposition de loi modifiant la loi du 29 juillet 1934 interdisant les milices privées en vue d'interdire les groupements non démocratiques, *Doc. parl.*, Chambre, 2013-2014, nº 53-0809/14

Projet de loi portant des dispositions diverses en matière de communications électroniques, projet de loi portant modification de la loi du 6 juillet 2005 relative à certaines dispositions judiciaires en matière de communications électroniques ainsi que la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, *Doc. parl.*, Chambre, 2013-2014, nºs 53-3318/1 et 53-3318/4

Proposition visant à instituer une commission d'enquête parlementaire chargée d'enquêter sur le rôle des services de renseignement dans le cyberespionnage, *Doc. parl.*, Chambre, 2013-2014, nº 53-3341/1 et *C.R.I.*, Chambre, 2013-2014, 6 février 2014, PLEN 183, p. 42

Projet de loi modifiant la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'organe de coordination pour l'analyse de la menace, *Doc. parl.*, Chambre, 2013-2014, nºs 53-3376/1 et 53-3376/2 et *C.R.I.*, Chambre, 2013-2014, 13 mars 2014, PLEN 189, p. 118

Projet de loi contenant le premier ajustement du Budget général des dépenses pour l'année budgétaire 2014, *Doc. parl.*, Chambre, 2013-2014, nº 53-3388/4

Projet de loi portant des dispositions diverses, *Doc. parl.*, Chambre, 2013-2014, nº 53-3413/7

Proposition de modifications techniques du Règlement de la Chambre des représentants à la suite de la sixième réforme de l'État, *Doc. parl.*, Chambre, 2013-2014, nº 53-3463/1

Proposition de modification des articles 39 et 149 du Règlement de la Chambre des représentants, *Doc. parl.*, Chambre, 2013-2014, nº 53-3465/1

Projet de loi visant à corriger plusieurs lois en matière de justice, *Doc. parl.*, Chambre, 2013-2014, nº 53-3531/1

Liste des rapports, bilans et comptes transmis à la Chambre en vertu des dispositions légales, *Doc. parl.*, Chambre, 2014-2015, nº 54-012/1

Exposé d'orientation politique, *Doc. parl.*, Chambre, 2014, nºs 54-020/15, 54-020/18, 54-020/32, 54-020/41 et 54-020/56

Proposition de loi visant à modifier la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, *Doc. parl.*, Chambre, 2014, nº 54-0164/1

Proposition de résolution relative à l'aide à la Nation pour une armée tournée vers la population, *Doc. parl.*, Chambre, 2014, nº 54-0226/1

Proposition de résolution visant à renforcer la cybersécurité en Belgique, *Doc. parl.*, Chambre, 2014, nº 54-0257/1

Proposition de modification de l'article 149 du Règlement de la Chambre des représentants en ce qui concerne la composition de la commission chargée du suivi du Comité permanent P et du Comité permanent R, *Doc. parl.*, Chambre, 2014-2015, nºs 54-0393/1 à 54-0393/6

Révision de la constitution – Révision de l'article 10, alinéa 2, deuxième membre de phrase, de la Constitution, *Doc. parl.*, Chambre, 2014, nº 54-0417/1

Projet du budget général des dépenses pour l'année 2015, *Doc. parl.*, Chambre, 2014-2015, nos 54-0496/1, 54-0496/4, 54-0496/14, 54-0496/35 et 54-0496/36

Justification du budget général des dépenses pour l'année budgétaire 2015, *Doc. parl.*, Chambre, 2014-2015, nos 54-0497/2, 54-0497/3, 54-0497/7, 54-0497/8, 54-0497/10 et 54-0497/13

Proposition visant à instituer une commission d'enquête parlementaire chargée d'enquêter sur le rôle des services de renseignement dans le cyberespionnage, *Doc. parl.*, Chambre, 2014-2015, n° 54-0552/1

Proposition de loi modifiant la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, concernant le contrôle des activités des services de renseignement étrangers en Belgique, *Doc. parl.*, Chambre, 2014-2015, n° 54-0553/1

Note de politique générale, *Doc. parl.*, Chambre, 2014-2015, nos 54-0588/1 et 4-0588/18, 4-0588/22 et 4-0588/29

Projet de loi contenant le budget des Voies et Moyens de l'année budgétaire 2015 (495/1-6) – Projet du budget général des dépenses pour l'année budgétaire 2015 (496/1-43) – Budgets des recettes et des dépenses pour l'année budgétaire 2015. Exposé général (494/1) – Justification du budget général des dépenses pour l'année budgétaire 2015. Liste des justifications par section (497/1-23) – Liste des notes de politique générale (588/1-36), *C.R.I.*, Chambre, 2014-2015, 17 décembre 2014, PLEN 022, p. 1

Rapport d'activités 2012 du Comité Permanent R, *Doc. parl.*, Chambre, 2013-2014, n° 53-3496/1

Nomination des commissions spéciales, *C.R.I.*, Chambre, 2014, 17 juillet 2014, PLEN 003, p. 11

Échange de vues avec la secrétaire d'État à l'Environnement et le ministre de l'Intérieur sur la problématique de l'approvisionnement, *C.R.I.*, Chambre, 2014, 22 août 2014, COM 003, p. 5

Auditions sur la problématique de l'approvisionnement en électricité et le plan de délestage, *C.R.I.*, Chambre, 2014, 23 septembre 2014, COM 007, p. 1

Échange de vues sur la situation en Irak et la participation éventuelle de la Belgique à la coalition internationale, *Doc. parl.*, Chambre, 2014, n° 54-0305/1 et *C.R.I.*, Chambre, 2014, 26 septembre 2014, PLEN 005, p. 2

Échange de vues sur le débriefing de la conférence internationale sur l'Irak, qui s'est tenue le 15 septembre 2014 à Paris, et la participation éventuelle de la Belgique à la coalition internationale, *Doc. parl.*, Chambre, 2014, n° 54-0344/1

Prise en considération de propositions, *C.R.I.*, Chambre, 2014, 7 octobre 2014, PLEN 006, p. 3

Reprise de la discussion de la déclaration du gouvernement, *C.R.I.*, Chambre, 2014-2015, 16 octobre 2014, PLEN 011, p. 1

Commission chargée du suivi du Comité permanent P et du Comité permanent R, *C.R.I.*, Chambre, 2014-2015, 13 novembre 2014, PLEN 015, p. 48

Comptes de l'année budgétaire 2013 du Comité permanent de contrôle des services de renseignements et de sécurité (680/1), *C.R.I.*, Chambre, 2014-2015, 18 décembre 2014, PLEN 024, p. 99

Comptes de l'année budgétaire 2013 de la Commission BIM (680/1), *C.R.I.*, Chambre, 2014-2015, 18 décembre 2014, PLEN 024, p. 100

Ajustement du budget de l'année budgétaire 2014 du Comité permanent de contrôle des services de renseignements et de sécurité (680/1), *C.R.I.*, Chambre, 2014-2015, 18 décembre 2014, PLEN 024, p. 101

Propositions budgétaires pour l'année budgétaire 2015 du Comité permanent de contrôle des services de renseignements et de sécurité (680/1), *C.R.I.*, Chambre, 2014-2015, 18 décembre 2014, PLEN 024, p. 103

Propositions budgétaires pour l'année budgétaire 2015 de la Commission BIM (680/1), *C.R.I.*, Chambre, 2014-2015, 18 décembre 2014, PLEN 024, p. 104

Rapport d'activités 2013 du Comité permanent de contrôle des services de renseignement et de sécurité, *Doc. parl.*, Chambre, 2014-2015, nº 54-0720/1

ANNEXE C
APERÇU DES INTERPELLATIONS, DES DEMANDES D'EXPLICATIONS ET DES QUESTIONS ORALES ET ÉCRITES RELATIVES AUX COMPÉTENCES, AU FONCTIONNEMENT ET AU CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'OCAM (1ER JANVIER 2014 AU 31 DÉCEMBRE 2014)

Sénat

Question écrite de B. Anciaux à la ministre de la Justice sur le 'commerce de diamants illégaux – pratiques de blanchiment – enquêtes et contrôle' (Sénat, 2011-2012, 28 décembre 2011, Q. nº 5-4620)

Question écrite de B. Anciaux à la ministre de la Justice sur la 'traite et trafic des êtres humains – condamnations pénales – diminution – motifs' (Sénat, 2011-2012, 28 décembre 2011, Q. nº 5-4662)

Question écrite de B. Anciaux à la ministre de la Justice sur la 'espionnage en Belgique – condamnations' (Sénat, 2011-2012, 6 février 2012, Q. nº 5-5495)

Question écrite de B. Anciaux à la ministre de la Justice sur les 'serveurs externes – informatique en nuage – services de recherche américains – Patriot Act – lois sur la vie privée – politique' (Sénat, 2012-2013, 23 octobre 2012, Q. nº 5-7189)

Question écrite de B. Anciaux à la ministre de la Justice sur la 'Sûreté de l'État – rapport annuel – services étrangers de sécurité et d'espionnage – nations amies' (Sénat, 2012-2013, 23 novembre 2012, Q. nº 5-7364)

Question écrite de N. Lijnen au premier ministre sur les 'services publics – cyberattaques – sécurisation informatique – logiciels de protection – formation du personnel' (Sénat, 2012-2013, 13 décembre 2012, Q. nº 5-7566)

Question écrite de N. Lijnen au ministre des Affaires étrangères sur les 'services publics – cyberattaques – sécurisation informatique – logiciels de protection – formation du personnel' (Sénat, 2012-2013, 13 décembre 2012, Q. nº 5-7568)

Question écrite de N. Lijnen à la ministre de l'Intérieur sur les 'services publics – cyberattaques – sécurisation informatique – logiciels de protection – formation du personnel' (Sénat, 2012-2013, 13 décembre 2012, Q. nº 5-7571)

Question écrite Y. Vastersavendts à la ministre de la Justice sur 'attentats contre des citoyens israéliens – Bulgarie – menace accrue – mesures' (Sénat, 2012-2013, 18 janvier 2013, Q. n° 5-7796)

Question écrite de Y. Vastersavendts à la ministre de la Justice sur les 'salafistes – radicalisation – détection – prévention – déclaration du ministre allemand de l'Intérieur' (Sénat, 2012-2013, 21 janvier 2013, Q. nº 5-7818)

Question écrite K. Vanlouwe à la ministre de la Justice sur 'Europol – menace terroriste – attentats – statistiques en 2012' (Sénat, 2012-2013, 8 février 2013, Q. n° 5-8064)

Question écrite de M. Taelman à la ministre de la Justice sur 'Syrie – combattants – groupes terroristes radicaux – voyage pour le jihad – Néerlandais – Belges – retour en Europe – terrorisme' (Sénat, 2012-2013, 25 février 2013, Q. nº 5-8286)

Question écrite de M. Taelman à la ministre de la Justice sur les 'écoles illégales et radicales – Wahhabisme – propagation du radicalisme – Sûreté de l'État – programmes de déradicalisation' (Sénat, 2012-2013, 8 mars 2013, Q. n° 5-8434)

Question écrite de M. Taelman à la ministre de l'Intérieur sur les 'prêcheurs de haine – nombre – liste – poursuites et condamnations – Jihad – Syrie' (Sénat, 2012-2013, 8 mars 2013, Q. n° 5-8435)

Question écrite de M. Taelman à la ministre de la Justice sur 'Hezbollah – liste d'organisations terroristes – Belges' (Sénat 2012-2013, 25 mars 2013, Q. n° 5-8600)

Question écrite de M. Taelman à la ministre de la Justice sur 'Russie – espionnage industriel – technologie d'armement – Chine – prévention – situation' (Sénat, 2012-2013, 23 avril 2013, Q. n° 5-8727)

Question écrite de K. Vanlouwe à la ministre de la Justice sur le 'fondamentalisme dans les prisons – aperçu – formation et tâches des gardiens' (Sénat, 2012-2013, 23 avril 2013, Q. n° 5- 8856)

Question écrite de M. Taelman à la ministre de la Justice sur la 'vie privée – réclamation de données d'utilisateurs des médias sociaux – Police – Sûreté de l'État – Service général du renseignement et de la sécurité – protection juridique – accords – situation' (Sénat, 2012-2013, 23 mai 2013, Q. n° 5-9087)

Question écrite de M. Taelman à la ministre de l'Intérieur sur les 'services de sécurité – écoute des services de communication en ligne – Skype – Voix sur IP (VOIP) – initiative législative' (Sénat, 2012-2013, 23 mai 2013, Q. n° 5-9090)

Question écrite de K. Vanlouwe au secrétaire d'État aux Affaires sociales sur 'la Computer emergency response team et la cyberdéfense' (Sénat, 2012-2013, 14 juin 2013, Q. n° 5-9329)

Question écrite de K. Vanlouwe à la ministre de la Justice sur 'la cybersécurité et la cyberdéfense' (Sénat, 2012-2013, 25 juin 2013, Q. n° 5-9406)

Question écrite de M. Taelman au ministre de la Défense sur 'le rapport Stratfor relatif au terrorisme en Afrique du Nord' (Sénat, 2012-2013, 2 juillet 2013, Q. n° 5-9453)

Question écrite de N. Lijnen au ministre de la Défense sur 'la cyberguerre' (Sénat, 2012-2013, 2 juillet 2013, Q. n° 5-9455)

Question écrite de B. De Nijn à la ministre de l'Intérieur sur les 'personnes parties combattre en Syrie – radiations officielles – impact – bilan – accords de coopération' (Sénat, 2012-2013, 3 septembre 2013, Q. n° 5-9834)

Question écrite de M. Taelman au ministre des Affaires étrangères sur 'National Security Agency – PRISM – espionnage d'entreprises – données d'entreprises européennes – Sûreté de l'État – enquête' (Sénat, 2012-2013, 18 septembre 2013, Q. n° 5-9875)

Question écrite de M. Taelman à la ministre de la Justice sur 'National Security Agency – PRISM – espionnage d'entreprises – données d'entreprises européennes – Sûreté de l'État – enquête' (Sénat, 2012-2013, 18 septembre 2013, Q. n° 5-9876)

Question écrite de N. Lijnen au ministre de la Défense sur la 'cybercriminalité – chiffres – hacking' (Sénat, 2012-2013, 24 septembre 2013, Q. n° 5-9898)

Question écrite de B. De Nijn au ministre des Affaires étrangères sur 'Kenya – Al-Shabaab – Somalie – combattants belges du Jihad – aperçu – confiscation de passeports – groupes de recrutement – retour' (Sénat, 2012-2013, 2 octobre 2013, Q. n° 5-9962)

Question écrite de B. De Nijn la ministre de la Justice sur 'Kenya – Al-Shabaab – Somalie – combattants belges du Jihad – retour – poursuites judiciaires' (Sénat 2012-2013, 2 octobre 2013, Q. n° 5-9963)

Question écrite de K. Vanlouwe à la ministre de la Justice sur 'la Sûreté de l'État – concertation sociale – droit de grève – demandes de grève' (Sénat, 2012-2013, 3 octobre 2013, Q. n° 5-9988)

Question écrite de M. Taelman au premier ministre sur la 'National Security Agency – Belgacom – Swift – écoutes – piratage informatique – aperçu – enquête – mesures' (Sénat, 2012-2013, 4 novembre 2013, Q. n° 5-10284)

Question écrite de N. Lijnen au premier ministre sur 'l'armée électronique syrienne – actions – cyberattaques – suivi' (Sénat, 2012-2013, 18 novembre 2013, Q. n° 5-10407)

Question écrite de B. Anciaux à la ministre de la Justice sur les 'ambassades – réseaux d'espionnage – matériel d'espionnage – personnel – persona non grata' (Sénat, 2013-2014, 19 novembre 2013, Q. n° 5-10418)

Question écrite de B. Anciaux à la ministre de l'Intérieur sur les 'sociétés de gardiennage – autorisation et attribution de missions de gardiennage privées – réputation – autorisation – critères d'agrément' (Sénat, 2013-2014, 21 novembre 2013, Q. n° 5-10430)

Question écrite de M. Taelman à la ministre de l'Intérieur sur le 'rapport d'activités du Comité permanent R – Sûreté de l'État – suivi des personnes condamnées pour terrorisme – radicalisation dans les prisons' (Sénat, 2013-2014, 6 décembre 2013, Q. n° 5-10544)

Question écrite de M. Taelman à la ministre de la Justice sur le 'rapport d'activités du Comité permanent R – Sûreté de l'État – suivi des personnes condamnées pour terrorisme – radicalisation dans les prisons' (Sénat, 2013-2014, 6 décembre 2013, Q. n° 5-10545)

Question écrite de M. Taelman à la ministre de l'Intérieur sur les 'services de renseignement – Sûreté de l'État – piratage de forums internet – suivi des forums internet – instruments légaux' (Sénat, 2013-2014, 6 décembre 2013, Q. n° 5-10546)

Question écrite de K. Vanlouwe à la ministre de la Justice sur les 'visites de personnalités étrangères – coût – délégations de catégorie A et B' (Sénat, 2013-2014, 9 décembre 2013, Q. n° 5-10551)

Question écrite de M. Taelman à la ministre de l'Intérieur sur la 'Sûreté de l'État – classification des documents – motivation – transparence' (Sénat, 2013-2014, 11 décembre 2013, Q. n° 5-10588)

Question écrite de M. Taelman à la ministre de la Justice sur la 'Sûreté de l'État – classification des documents – motivation – transparence' (Sénat, 2013-2014,
11 décembre 2013-2014, Q. n° 5-10589)

Question écrite de M. Taelman à la ministre de l'Intérieur sur la 'Sûreté de l'État – Principes de Tshwane – harmonisation – normes minimales dans l'Union européenne' (Sénat 2013-2014, 11 décembre 2013, Q. n° 5-10590)

Question écrite de M. Taelman à la ministre de la Justice sur la 'Sûreté de l'État – Principes de Tshwane – harmonisation – normes minimales dans l'Union européenne' (Sénat 2013-2014, 11 décembre 2013, Q. n° 5-10591)

Question écrite de M. Taelman à la ministre de la Justice sur le 'rapport du Comité permanent R – services de renseignement – fraude – enquêtes judiciaires – condamnations – sanctions' (Sénat 2013-2014, 20 décembre 2013, Q. n° 5-10701)

Demande d'explications de B. Hellings à la ministre de la Justice sur 'la possibilité d'une enquête du parquet fédéral sur la présence de logiciels-espions de la NSA sur les serveurs de Google à Saint-Ghislain' (*Ann. parl.,* Sénat, 2013-2014, 8 janvier 2014, n° 5-268, p. 6, Q. n° 5-4234)

Question écrite de B. Anciaux au secrétaire d'État à la Fonction publique sur 'l'informatique en nuage – utilisation – protection – vie privée' (Sénat, 2013-2014, 13 janvier 2014, Q. n° 5-10855)

Question écrite de N. Lijnen au premier ministre sur 'l'armée électronique syrienne – actions – cyberattaques – suivi – liens avec le régime Assad' (Sénat, 2013-2014, 15 janvier 2014, Q. n° 5-10881)

Question écrite de K. Vanlouwe à la ministre de l'Intérieur sur le 'Parc du Cinquantenaire – Grande mosquée – Centre islamique et culturel – Arabie Saoudite – Salafisme – Sûreté de l'État' (Sénat, 2013-2014, 15 janvier 2014, Q. n° 5-10885)

Question écrite de K. Vanlouwe à la ministre de la Justice sur le 'Parc du Cinquantenaire – Grande mosquée – Centre islamique et culturel – Arabie Saoudite – Salafisme – Sûreté de l'État' (Sénat, 2013-2014, 15 janvier 2014, Q. n° 5-10886)

Demande d'explications de B. Hellings et K. Vanlouwe au ministre de la Défense sur 'la collaboration structurelle entre le Service général du renseignement et de la sécurité et la National Security Agency' (*Ann. parl.,* Sénat, 2013-2014, 21 janvier 2014, n° 5-274, p. 5, Q. n^{os} 5-3937 et 5-4199)

Demande d'explications de B. Hellings au ministre de la Défense sur 'l'usage potentiel par le Service général du renseignement et de la sécurité des outils de surveillance de la NSA dans le cadre de la mission de l'armée belge en Afghanistan' (*Ann. parl.,* Sénat, 2013-2014, 21 janvier 2014, n° 5-274, p. 8, Q. n° 5-3938)

Question écrite de M. Taelman au ministre de la Défense sur 'le « cybercommando »' (Sénat, 2013-2014, 22 janvier 2014, Q. n° 5-10945)

Question écrite de M. Taelman au ministre de la Défense sur 'l'établissement de la « Joint Sigint Cyber Unit » aux Pays-Bas' (Sénat, 2013-2014, 22 janvier 2014, Q. n° 5-10946)

Demande d'explications de B. De Nijn à la ministre de l'Intérieur sur 'la liste noire des organisations dangereuses' (*Ann. parl.,* Sénat, 2013-2014, 28 janvier 2014, n° 5-277, p. 14, Q. n° 5-4375)

Demande d'explications de G. Deprez à la ministre de l'Intérieur sur 'la transmission d'informations entre les réseaux sociaux et les autorités belges dans le cadre

d'enquêtes officielles' (*Ann. parl.,* Sénat, 2013-2014, 28 janvier 2014, n° 5-277, p. 6, Q. n° 5-4452)

Question écrite de R. Miller à la ministre de l'Intérieur sur 'la coordination européenne pour lutter plus efficacement contre le terrorisme' (Sénat, 2013-2014, 29 janvier 2014, Q. n° 5-10994)

Question écrite de M. Taelman au premier ministre sur 'l'espionnage économique – National Security Agency – entreprises belges – évolution – mesures' (Sénat, 2012-2013, 4 février 2014, Q. n° 5-11018)

Question écrite de M. Taelman au ministre de la Défense sur les 'services de sécurité – interception et partage d'informations – Pays-Bas – National Security Agency – Sûreté de l'État – Service général de renseignement et de sécurité – enregistrements téléphoniques – métadonnées – base juridique' (Sénat, 2012-2013, 11 février 2014, Q. n° 5-11093)

Question écrite de M. Taelman à la ministre de l'Intérieur sur les 'services de sécurité – interception et partage d'informations – Pays-Bas – National Security Agency – Sûreté de l'État – Service général de renseignement et de sécurité – enregistrements téléphoniques – métadonnées – base juridique' (Sénat, 2012-2013, 11 février 2014, Q. n° 5-11094)

Question écrite de M. Taelman à la ministre de la Justice sur les 'services de sécurité – interception et partage d'informations – Pays-Bas – National Security Agency – Sûreté de l'État – Service général de renseignement et de sécurité – enregistrements téléphoniques – métadonnées – base juridique' (Sénat, 2012-2013, 11 février 2014, Q. n° 5-11095)

Question écrite de F. Winckel à la ministre de l'Intérieur sur les 'Jeux Olympiques d'hiver de Sotchi – citoyens belges – sécurité' (Sénat, 2012-2013, 11 février 2014, Q. n° 5-11127)

Demande d'explications de M. Taelman à la ministre de l'Intérieur sur 'les dons au jihad au Yémen' (*Ann. parl.,* Sénat, 2013-2014, 11 février 2014, n° 5-284, p. 4, Q. n° 5-4297)

Question orale de K. Vanlouwe à la ministre de l'Intérieur sur 'le nombre de combattants belges en Syrie' (*Ann. parl.,* Sénat, 2013-2014, 13 février 2014, n° 5-140, p. 20, Q. n° 5-1316)

Question orale de Z. Khattabi à la ministre de la Justice sur 'le nouveau patron de la Sûreté de l'État' (*Ann. parl.,* Sénat, 2013-2014, 27 février 2014, n° 5-143, p. 21, Q. n° 5-1342)

Question écrite de M. Taelman à la ministre de l'Intérieur sur 'Sûreté de l'État – principes de Tshwane – métadonnées – réglementation – augmentation – analyse – écoutes et forums internet (Sénat, 2013-2014, 12 mars 2014, Q. n° 5-11232)

Question orale de K. Vanlouwe à la ministre de l'Intérieur sur 'les combattants en Syrie' (*Ann. parl.,* Sénat, 2013-2014, 13 mars 2014, n° 5-144, p. 37, Q. n° 5-1359)

Question orale de B. Laeremans à la ministre de la Justice sur 'le dossier des six assassinats politiques attribués à Abdelkader Belliraj' (*Ann. parl.,* Sénat, 2013-2014, 27 mars 2014, n° 5-146, p. 26, Q. n° 5-1385)

Question écrite de M. Taelman au ministre de l'Emploi sur la 'cybercriminalité – entreprises – mesures' (Sénat, 2013-201, 4 décembre 2014, Q. n° 6-275)

Question écrite de M. Taelman au ministre de la Coopération au développement sur la 'cybercriminalité – entreprises – mesures' (Sénat, 2013-201, 4 décembre 2014, Q. n° 6-276)

Chambre des Représentants

Question de P. Dedecker au premier ministre sur 'l'espionnage chez Belgacom' (*Q.R.*, Chambre, 2013-2014, 8 janvier 2014, n° 142, p. 44, Q. n° 123)

Questions jointes de K. Van Vaerenbergh et A. Frédéric à la ministre de la Justice 'la grève nationale du 13 décembre' (*C.R.I.*, Chambre, 2013-2014, 8 janvier 2014, COM 890, p. 1, Q. n^{os} 21052 et 21151)

Questions jointes de P. Logghe à la vice-première ministre sur 'les nouveaux canaux de recrutement de djihadistes' (*C.R.I.*, Chambre, 2013-2014, 8 janvier 2014, COM 890, p. 20, Q. n^{os} 21258 et 21347)

Question de T. Veys au ministre de l'Économie sur 'l'avis de l'avocat général de la Cour de Justice de l'Union européenne concernant la directive controversée sur la rétention de données' (*C.R.I.*, Chambre, 2013-2014, 15 janvier 2014, COM 896, p. 15, Q. n° 21268)

Question de K. Grosemans au ministre de la Défense sur 'la mise en place du centre pour la cybersécurité en Belgique' (*C.R.I.*, Chambre, 2013-2014, 15 janvier 2014, COM 898, p. 32, Q. n° 21324)

Questions jointes d'A. Frédéric et B. Slegers à la ministre de la Justice sur 'la législation sur les armes et la commémoration de la 1ère Guerre mondiale' (*C.R.I.*, Chambre, 2013-2014, 16 janvier 2014, PLEN 180, p. 25, Q. n^{os} 2203 et 2204)

Question de B. Slegers à la ministre de l'Intérieur sur le 'retour des jeunes de Syrie' (*Q.R.*, Chambre, 2013-2014, 27 février 2014, n° 145, p. 245, Q. n° 1070)

Question de L. Devin la ministre de l'Intérieur sur 'les jeunes Belges partis combattre en Syrie' (*C.R.I.*, Chambre, 2013-2014, 30 janvier 2014, PLEN182, p. 25, Q. n° 2249)

Question de R. Deseyn à la ministre de la Justice sur 'le système PRISM' (*Q.R.*, Chambre, 2013-2014, 3 février 2014, n° 146, p. 78, Q. n° 1165)

Question de Ph. Blanchart à la ministre de la Justice sur 'l'agence de renseignements de l'Union européenne (SitCen)' (*Q.R.*, Chambre, 2013-2014, 3 février 2014, n° 146, p. 82, Q. n° 1115)

Échange de vues avec le premier ministre et questions jointes de G. Dallemagne, J. Galant, B. Weyts, R. Deseyn, M. C. Marghem, I. Emmery et R. Balcaen sur 'la cybersécurité' (*C.R.I.*, Chambre, 2013-2014, 4 février 2014, n° 915, p. 1, Q. n^{os} 18080, 19454, 19696, 19722, 19822, 20033, 20840, 21941 et 21977)

Question de P. Logghe à la ministre de l'Intérieur sur 'les combattants musulmans en Syrie et les informations les concernant' (*Q.R.*, Chambre, 2013-2014, 10 février 2014, n° 147, p. 134, Q. n° 929)

Question de B. Schoofs à la ministre de la Justice sur 'le symbole Rabia' (*C.R.I.*, Chambre, 2013-2014, 11 février 2014, n° 920, p. 32, Q. n° 22059)

Question de P. Logghe à la ministre de l'Intérieur sur 'la mise en garde des Américains contre l'éventualité d'attentats en Europe' (*C.R.I.*, Chambre, 2013-2014, 12 février 2014, n° 925, p. 16, Q. n° 22149)

Question de T. Francken à la ministre de l'Intérieur sur les 'services – personnel – jours de congé syndical' (*Q.R.*, Chambre, 2013-2014, 17 février 2014, n° 148, p. 173, Q. n° 1184)

Question de P. Logghe à la ministre de l'Intérieur sur la 'lutte contre l'extrémisme – liste d'associations et de personnes' (*Q.R.*, Chambre, 2013-2014, 17 février 2014, n° 148, p. 187, Q. n° 1287)

Questions jointes de T. Francken et P. Logghe à la ministre de la Justice sur 'le retrait de la nationalité belge des combattants en Syrie' (*C.R.I.*, Chambre, 2013-2014, 19 février 2014, n° 932, p. 11, Q. n°s 22204, 22210 et 22275)

Question de T. Francken à la ministre de l'Intérieur sur le 'personnel de la Sûreté de l'État affecté à la protection du Roi et de son entourage' (*Q.R.*, Chambre, 2013-2014, 24 février 2014, n° 149, p. 176, Q. n° 1312)

Question de J. Boulet à la ministre de la Justice sur 'l'accès aux circulaires du Collège des procureurs généraux' (*C.R.I.*, Chambre, 2013-2014, 12 mars 2014, n° 948, p. 2, Q. n° 22518)

Question de P. Luykx au ministre des Affaires étrangères sur 'la mission économique en Turquie – contrôle des participants' (*Q.R.*, Chambre, 2013-2014, 17 mars 2014, n° 152, p. 142, Q. n° 834)

Questions jointes de J. Van Esbroeck à la ministre de l'Intérieur sur 'la collaboration entre la Belgique et la Jordanie dans le cadre du terrorisme' (*C.R.I.*, Chambre, 2013-2014, 19 avril 2014, n° 954, p. 2, Q. n°s 22469 et 22490)

Question de B. Maertens au ministre de la Défense sur 'la vérification de sécurité des aspirants militaires' (*Q.R.*, Chambre, 2013-2014, 24 mars 2014, n° 153, p. 121, Q. n° 666)

Question de B. Maertens au ministre de la Défense sur 'la vérification de sécurité pour les militaires en fonction' (*Q.R.*, Chambre, 2013-2014, 24 mars 2014, n° 153, p. 123, Q. n° 667)

Questions jointes de G. Dallemagne, Ch. Lacroix et K. Grosemans au ministre de la Défense sur 'la Belgian Intelligence Academy' généraux' (*C.R.I.*, Chambre, 2013-2014, 2 avril 2014, n° 968, p. 3, Q. n°s 22074, 22462, 22501, 22749 et 22895)

Question de P. Logghe à la ministre de l'Intérieur sur 'des écoutes téléphoniques et enregistrements de communications radio' (*Q.R.*, Chambre, 2013-2014, 7 avril 2014, n° 155, p. 111, Q. n° 1414)

Question de T. Francken à la ministre de l'Intérieur sur la 'protection de la Famille royale' (*Q.R.*, Chambre, 2013-2014, 7 avril 2014, n° 155, p. 112, Q. n° 1434)

Question de E. Brems au ministre des Affaires étrangères sur 'les tentatives répétées de fermer la prison de Guantánamo' (*Q.R.*, Chambre, 2013-2014, 14 avril 2014, n° 156, p. 91, Q. n° 866)

Question de E. Brems à la ministre de l'Intérieur sur 'le retrait de la publicité pour une représentation de danse à l'occasion de la visite du président chinois' (*Q.R.*, Chambre, 2013-2014, 14 avril 2014, n° 156, p. 152, Q. n° 1503)

Question de B. Weyts au ministre des Entreprises publiques sur les 'Services publics fédéraux – l'utilisation des données GSM et internet connues chez Belgacom' (*Q.R.*, Chambre, 2013-2014, 14 avril 2014, n° 156, p. 188, Q. n° 903)

Question de B. Weyts à la ministre de l'Intérieur sur les 'islamistes radicaux en Syrie' (*Q.R.*, Chambre, 2013-2014, 22 avril 2014, n° 157, p. 101, Q. n° 860)

Question de P. Logghe à la ministre de l'Intérieur sur les 'flux financiers en provenance de pays arabes ou de régimes extrémistes musulmans et destinés à des mosquées ou à des associations musulmanes établies dans notre pays' (*Q.R.*, Chambre, 2013-2014, 22 avril 2014, n° 157, p. 161, Q. n° 1099)

Question de P. Logghe à la ministre de l'Intérieur sur 'les écoutes téléphoniques' (*Q.R.*, Chambre, 2013-2014, 22 avril 2014, n° 157, p. 201, Q. n° 1264)

Question de B. Schoofs à la ministre de l'Intérieur sur 'les activités du groupement islamique radical Hizb ut-Tahrir' (*Q.R.*, Chambre, 2013-2014, 22 avril 2014, n° 157, p. 218, Q. n° 1400)

Question de P. Logghe à la ministre de l'Intérieur sur les 'Djihadistes morts au combat en Syrie' (*Q.R.*, Chambre, 2013-2014, 25 avril 2014, n° 158, p. 62, Q. n° 1161)

Question d'E. Thiébaut à la ministre de l'Intérieur sur 'la tentative de cambriolage au Centre d'étude nucléaire (CEN) à Mol' (*Q.R.*, Chambre, 2013-2014, n° 159, p. 80, Q. n° 915)

Question K. Degroote à la ministre de l'Intérieur sur les 'détachement de fonctionnaires de police' (*Q.R.*, Chambre, 2013-2014, n° 159, p. 175, Q. n° 1424)

Question de S. Van Hecke au ministre de la Justice sur 'l'acquisition du logiciel d'espionnage FinFisher' (*C.R.I.*, Chambre, 2014-2015, 5 novembre 2014, n° 012 p. 13, Q. n° 134)

Questions jointes de F. Dewinter et A. Carcaci au ministre de l'Intérieur sur 'la Foire musulmane de Bruxelles du 7 au 10 novembre' (*C.R.I.*, Chambre, 2014-2015, 6 novembre 2014, n° 014, p. 21, Q. n°s 35 et 36)

Question de L. Dierick au ministre de l'Intérieur sur 'le contrôle et le retrait des habilitations de sécurité' (*C.R.I.*, Chambre, 2014-2015, 12 novembre 2014, n° 015, p. 32, Q. n° 100)

Questions jointes de L. Dierick, K. Temmerman et K. Calvo au ministre de l'Intérieur sur 'le sabotage de la centrale nucléaire Doel IV' (*C.R.I.*, Chambre, 2014-2015, 12 novembre 2014, n° 015, p. 32, Q. n°s 352, 382 et 444)

Question de H. Bonte au ministre de l'Intérieur sur 'le danger des fuites dans la presse des services de sécurité à propos des jeunes partis combattre en Syrie' (*C.R.I.*, Chambre, 2014-2015, 20 novembre 2014, n° 016, p. 12, Q. n° 70)

Question de K. Grosemans au ministre de la Défense sur 'la vérification de sécurité pour les candidats militaires et les militaires en fonction' (*Q.R.*, Chambre, 2014-2015, n° 002, p. 147, Q. n° 7)

Question de K. Grosemans au ministre de la Défense sur 'l'inaptitude médicale en 2013' (*Q.R.*, Chambre, 2014-2015, n° 002, p. 147, Q. n° 23)

Question de Ph. Goffin au ministre de la Justice sur 'le radicalisme religieux dans les prisons belges' (*C.R.I.*, Chambre, 2014-2015, 3 décembre 2014, n° 033, p. 33, Q. n° 649)

Question de P. Luyckx au ministre des Affaires étrangères sur le 'renforcement de la sécurité dans les postes diplomatiques et consulaires' (*Q.R.*, Chambre, 2014-2015, n° 003, p. 121, Q. n° 18)

Question de J.-M. Nollet à la ministre de l'Énergie sur 'la concertation entre l'AFCN et l'OCAM dans le cadre des survols de nos centrales nucléaires' (*Q.R.*, Chambre, 2014-2015, n° 004, p. 195, Q. n° 18)

Question de S. Lahaye-Battheu au ministre de la Justice sur les 'prisons – personnes suspectées et/ou condamnées pour délits de terrorisme' (*Q.R.*, Chambre, 2014-2015, n° 005, p. 134, Q. n° 31)

Question de S. Van Hecke au ministre de la Justice sur 'l'échange d'informations entre services de renseignements' (*C.R.I.*, Chambre, 2014-2015, 16 décembre 2014, n° 40, p. 23, Q. n° 861)

Question de S. Van Hecke au ministre de la Justice sur 'la catégorisation des informations recueillies par la VSSE' (*C.R.I.*, Chambre, 2014-2015, 16 décembre 2014, n° 40, p. 24, Q. n° 861)