ACTIVITEITENVERSLAG 2013
RAPPORT D'ACTIVITÉS 2013

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.

ACTIVITEITENVERSLAG 2013

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

intersentia
Antwerpen – Cambridge

Voorliggend *Activiteitenverslag 2013* werd door het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten goedgekeurd op de vergadering van 24 juli 2014.

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

Activiteitenverslag 2013
Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

ISBN 978-94-000-0551-8
D/2014/7849/156
NUR 823

INHOUD

LIJST MET AFKORTINGEN

ACOS-IS	*Assistant Chief of Staff Intelligence and Security*
ACOS Ops & Trg	Stafdepartement *Operations and Training*
ADIV	Algemene Dienst inlichting en veiligheid van de Krijgsmacht
BELINT	*Belgian intelligence*
BENIC	*Belgian National Intelligence Cell*
BIA	*Belgian Intelligence Academy*
BIC	*Battle Group Intelligence Cell*
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*
BOM	Bijzondere opsporingsmethoden
BS	Belgisch Staatsblad
CANVEK	Commissie van advies voor de niet-verspreiding van kernwapens
CBPL	Commissie voor de bescherming van de persoonlijke levenssfeer
CCB	Centrum voor Cybersecurity België
CFI	Cel voor Financiële Informatieverwerking
CHOD	*Chief of Defense*
CIA	*Central Intelligence Agency*
CPOE	*Comprehensive Preparation of the Operational Environment*
CRIV	Compte Rendu Intégral – Integraal Verslag
EVRM	Europees Verdrag voor de Rechten van de Mens
FragO	*Fragmentary Orders*
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*
ISAF	*International Security Assistance Force*
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 veilig-heidsadviezen
KB OCAD	Koninklijk besluit van 28 november 2006 tot uitvoering van de Wet van10 juli 2006 betreffende de analyse van de dreiging
MAT	*Military Assistance Team*
M.B.	Ministerieel besluit
MCIV	Ministerieel Comité voor inlichting en veiligheid
NAVO	Noord-Atlantische Verdragsorganisatie
NSA	*National Security Agency*
NVO	Nationale Veiligheidsoverheid
OCAD	Coördinatieorgaan voor de dreigingsanalyse
OEF	*Operation Enduring Freedom*
OSINT	*Open sources intelligence*
PRT	*Provincial Reconstruction Team*
RFI	*Request for information*
SIGINT	*Signals intelligence*
s.l.	*sine loco*
SOP	*Standing Operating Procedure*
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
Vr. en Antw.	Schriftelijke vragen en antwoorden (Kamer of Senaat)
VSSE	Veiligheid van de Staat
W.Beroepsorgaan	Wet van 11 december 1998 houdende oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veilig-heidsattesten en veiligheidsadviezen
W.C&VM	Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen

W.I&V	Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst
WEP	Wetenschappelijk en economisch potentieel
WOB	Wet van 11 april 1994 betreffende de openbaarheid van bestuur
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

2013 stond voor het Vast Comité I in het teken van twee totaal verschillende gebeurtenissen, die elk op hun manier belangrijk waren.

De eerste was zijn twintigjarig bestaan. Op 24 mei 1993 ging het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten immers effectief van start. Deze verjaardag konden wij niet onopgemerkt laten voorbij gaan. Er werd een meer dan 500 bladzijden tellende feestbundel 'Inzicht in toezicht' opgesteld, waarin omzeggens elk aspect van de democratische controle op de inlichtingendiensten aan bod kwam en waarbij alle betrokken actoren van vroeger en nu de gelegenheid kregen hun visie te belichten. Het boek werd onder auspiciën van de Senaatsvoorzitster op gepaste wijze voorgesteld in de Senaat.

Als één ding duidelijk is geworden, is het wel dat het Vast Comité I in die twintig jaar een vaste plaats heeft verworven in ons democratisch bestel. Het is een organisatie geworden die waakt over de concrete werking van de inlichtingendiensten en die met zijn verslagen en aanbevelingen een fundamentele bijdrage levert in het debat over de taken en de bevoegdheden ervan. Dit was alleen mogelijk dankzij de inzet en de expertise van eenieder die werkt of gewerkt heeft voor het Vast Comité I, ongeacht zijn of haar positie binnen de organisatie.

Het Vast Comité I van vandaag is zeker niet meer hetzelfde als het toezichtorgaan dat in 1993 van start ging. Daar hebben vele wetswijzingen en voortschrijdende inzichten in de praktijk voor gezorgd. Soms betrof het zeer kleine, technische ingrepen. Maar sommige aanpassingen hebben de gedaante van het Comité en zijn werkprocessen, danig gewijzigd. Dat die evolutie nog niet ten einde is, bewijst de Wet van 6 januari 2014: met de hervorming van de Senaat ingevolge de zesde staatshervorming, is het aanspreekpunt van het Comité in het Parlement sinds de verkiezingen van 25 mei 2014 verhuisd naar een eengemaakte 'Commissie belast met de begeleiding van het Vast Comité P en het Vast Comité I' in de Kamer die zowel de politie- als de inlichtingendiensten zal controleren. Maar er is meer. De commissie wordt anders samengesteld – de voorzitters van alle politieke fracties krijgen vanaf nu een zitje – én haar leden zouden ook kennis kunnen nemen van geclassificeerde informatie. De toekomst zal uitwijzen welke invloed die wijzigingen hebben op de parlementaire controle.

Dé andere gebeurtenis uit 2013, die vooral de tweede helft van het jaar kleurde, was het feit dat Edward Snowden, een voormalig medewerker van een Amerikaanse inlichtingendienst, er in geslaagd was tienduizenden uiterst

gevoelige documenten van de *National Security Agency* te kopiëren en door te spelen aan journalisten. Herhaaldelijk verschenen er dan ook ontluisterende berichten in de pers over wereldwijde, massale data-captatie en economische en politieke spionage door de Amerikaanse en Britse inlichtingendiensten. Het hoeft geen betoog dat hierdoor de internationale inlichtingengemeenschap behoorlijk door mekaar werd geschud. Deze onthullingen vormden het startschot van parlementaire, gerechtelijke en inlichtingenonderzoeken over de hele wereld. Zo ook in België. Het Vast Comité I startte in dit kader niet minder dan vier onderzoeken op.

Dat bepaalde grootmachten al geruime tijd over verregaande middelen en programma's beschikten om aan massale data-captatie te doen, was niet nieuw. Wel nieuw was het gegeven dat deze elektronische informatiegaring alomvattend en massaal plaatsgreep en dit met de meest geavanceerde *soft-* en *hardware* en met een ongekende inzet aan menselijke en financiële middelen. Een tweede nieuw element was dat het steeds duidelijker werd dat grootmachten niet nalieten 'bevriende landen' economisch en politiek te bespioneren door er aan massale of gerichte data-captatie te doen. Hieruit zullen door bewindslieden, inlichtingendiensten maar ook toezichthouders, de nodige lessen moeten worden getrokken.

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

1 juni 2014

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

Eén van de voornaamste taken van het Vast Comité I bestaat erin om ten behoeve van de wetgever en de uitvoerende macht aanbevelingen te formuleren 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 diens ondersteunende diensten.[1] De aanbevelingen die het Comité in 2013 formuleerde, zijn opgenomen in het laatste hoofdstuk van dit activiteitenverslag. In dit inleidende hoofdstuk worden de belangrijkste initiatieven 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. EEN FEDERALE STRATEGIE VOOR DE BEVEILIGING VAN INFORMATIE- EN COMMUNICATIESYSTEMEN

In de huidige samenleving is de beveiliging van communicatie- en informaticasystemen cruciaal. Het Comité formuleerde in dit kader eerder al aanbevelingen om te werken aan een geïntegreerd veiligheidsbeleid rond cyberaanvallen, hield een pleidooi voor de bevoegdheidsuitbreiding van de ADIV en de VSSE alsook voor de aanwerving van gekwalificeerde personeelsleden, beval de grootste omzichtigheid aan bij de keuze van beveiligde technische uitrustingen voor de verwerking van geclassificeerde informatie en wees op het tekort aan technische certificatie- en homologatiemiddelen op vlak van informatieveiligheid.[2]

---

1 Wat het OCAD en de ondersteunende diensten betreft, gebeuren de onderzoeken samen met het Vast Comité P (art. 53, 6° W.Toezicht).

2 VAST COMITÉ I, *Activiteitenverslag 2011*, 108-109 (IX.2.3. Aanbevelingen met betrekking tot de informatieveiligheid).

Verwijzend naar deze aanbevelingen, werden door de Senaat en de Kamer van Volksvertegenwoordigers diverse voorstellen van resolutie ingediend. Al in 2011 werd door de toenmalige leden van de parlementaire Begeleidingscommissie van het Vast Comité I een '*voorstel van resolutie tot het snel ontwikkelen van een federale strategie voor de beveiliging van informatie- en communicatiesystemen*'[3] geformuleerd, eind november 2012 gevolgd door een '*voorstel van resolutie ter beveiliging van elektronische informatie en bescherming tegen cyberaanvallen*'.[4] In diezelfde zin werd in juni 2013 in de Kamer een voorstel van resolutie ingediend '*waarbij de oprichting wordt gevraagd van een Centrum voor cyberbeveiliging in België*'.[5] De Ministerraad van 19 december 2013 keurde op zijn beurt het ontwerp van Koninklijk besluit goed voor de oprichting van het Centrum voor Cybersecurity België (CCB) dat onder het gezag van de eerste minister moet instaan voor de uitvoering van de Belgische strategie inzake *cybersecurity*.[6]

I.1.2. VERNIETIGING VAN OUDE DOSSIERS

Artikel 21 W.I&V bepaalt dat persoonsgegevens verwerkt door inlichtingendiensten slechts mogen bewaard worden '*voor een duur die niet langer mag zijn dan die welke noodzakelijk is om de doeleinden waarvoor ze opgeslagen worden, met uitzondering van de gegevens die een door het Rijksarchief erkend historisch karakter hebben*' en dat ze pas mogen worden '*vernietigd na een zekere termijn volgende op de laatste verwerking waarvan zij het voorwerp zijn geweest*'. De bewaartermijnen en de procedure met betrekking tot hun vernietiging dienen – reeds sinds de Wet van 30 november 1998! – te worden bepaald bij Koninklijk besluit, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer. Dergelijk besluit werd nog niet genomen en het Comité drong hierop aan[7]; niet alleen om uitvoering te geven aan een wettelijke verplichting, maar ook omdat het bijhouden door de inlichtingendiensten van oude gegevens een inbreuk kan betekenen op artikel 8 EVRM.

In 2012 stelde de minister van Justitie een ontwerpbesluit op dat aan het advies van de Privacy-commissie werd onderworpen. Het advies werd bekend gemaakt op 20 februari 2013.[8] Sindsdien is het Comité zonder nieuws over het ontwerpbesluit.

---

3 *Parl. St.* Senaat 2011-12, nr. 5-1246/1.

4 *Parl. St.* Senaat 2012-13, nr. 5-1855/1.

5 *Parl. St.* Kamer 2012-13, nr. 53K2918/001. In dezelfde zin: 'Resolutie van het Europees Parlement van 12 juni 2012 over de bescherming van kritieke informatie-infrastructuur – bereikte resultaten en volgende stappen: naar mondiale cyberveiligheid', *Publicatieblad van de Europese Unie*, C 332 E/22, 15 november 2013.

6 www.presscenter.org/nl/pressrelease/20131219/oprichting-van-het-centrum-voor-cybersecurity-belgie.

7 VAST COMITÉ I, *Activiteitenverslag 2008*, 22-33, i.h.b. 32 (II.2. 'Gereserveerde dossiers' bij de VSSE).

8 Commissie voor de bescherming van de persoonlijke levenssfeer, Advies nr. 07/2013 van 20 februari 2013 aangaande het voorontwerp van Koninklijk besluit tot uitvoering van arti-

I.1.3. EEN NIEUWE DIENSTNOTA VAN DE VSSE OVER DE OPVOLGING VAN PARLEMENTSLEDEN

Drie onderzoeken uit 2013 (zie II.2, II.3 en II.4) hadden aangetoond dat de meldingsplicht aan de minister van Justitie telkens wanneer een parlementslid in het vizier van de VSSE komt, in regel niet wordt nageleefd. Het Vast Comité I had voorheen al gewezen op het belang van dergelijke melding. Ze beval de bevoegde ministers aan om hun informatiebehoeften en de eventuele beperkingen tegenover de informatie-inwinning ten aanzien van politieke mandatarissen en politieke partijen in eenduidige richtlijnen om te zetten (IX.1.3). Daarenboven suggereerde het Comité dat beide inlichtingendiensten een gezamenlijk initiatief zouden nemen naar het Ministerieel Comité voor inlichting en veiligheid met het oog op de aanname van een richtlijn.

Kort na het afsluiten van bedoelde toezichtonderzoeken verspreidde de Veiligheid van de Staat – en dus niet de minister van Justitie en ook niet in overleg met de ADIV – een dienstnota '*omtrent het linken van parlementsleden en politieke mandatarissen in de documenten van de VSSE*'. Daarin werd onder meer opgenomen dat de minister van Justitie niet langer automatisch diende geïnformeerd te worden wanneer een parlementslid of minister opdook in een verslag van de Buitendiensten. De minister dient slechts te worden geïnformeerd wanneer deze politieke mandatarissen bij naam worden vermeld in de analysedocumenten. Hierdoor stroomt er minder informatie door naar de bevoegde minister.

I.1.4. DE FUNCTIE 'OPERATIONELE ANALIST' BIJ DE ALGEMENE DIENST INLICHTING EN VEILIGHEID

Naar aanleiding van de audit bij de ADIV[9] gaf het Comité aan dat '*er diende te worden bepaald welke samenwerking tussen en binnen de divisies opportuun én noodzakelijk is*'.[10] De ADIV nam deze aanbeveling ter harte en creëerde binnen de Divisie C(ounter) I(ntelligence)[11], de figuur van de 'operationele analist'. Deze vervult een brugfunctie tussen de analisten en de mensen op het terrein (collecte) en dit met het oog op een betere afstemming van de onderlinge behoeften.

---

kel 21 van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst (CO-A-2012-044).

9 VAST COMITÉ I, *Activiteitenverslag 2011*, 7-14 (II.1. Een audit bij de militaire inlichtingendienst).

10 VAST COMITÉ I, *Activiteitenverslag 2011*, 105.

11 De Divisie C(ounter)I(ntelligence) werd ondertussen samengevoegd met de Divisie S(ecurity) tot de Divisie CIS.

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 nu dringend 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.[12] Al bij zijn 'Overzicht van de voornaamste aanbevelingen van het Vast Comité I (1994-2005)'[13] drong het Comité aan op een reflectie hieromtrent.[14] Het wetsontwerp waarbij de bijzondere inlichtingenmethoden (de huidige BIM-Wet) zouden worden omschreven, bood hiertoe een uitgelezen kans. De wetgever heeft evenwel van deze opportuniteit geen gebruik gemaakt. In 2007 herhaalde het Comité zijn aanbeveling.[15] Naar aanleiding van het toezichtonderzoek naar de zogenaamde 'gereserveerde dossiers', werd in 2008 nogmaals gevraagd een duidelijke regeling uit te werken voor de overzending van persoonsgegevens naar buitenlandse (inlichtingen-)diensten en werd in het bijzonder verwezen naar de Nederlandse, Duitse en Noorse regeling ter zake.[16] In 2009 stelde het Comité dat de afwezigheid van richtlijnen hieromtrent '*de informatiedoorstroming discutabel [maakt] vanuit legaliteitsoogpunt*'.[17] De twee volgende jaren 2010-2011 toonden enkele BIM-dossiers aan dat de Belgische inlichtingendiensten soms opereren op aangeven van buitenlandse diensten waarna persoonsgegevens kunnen doorgegeven worden. Het Comité vraagt aandacht voor deze delicate materie, zeker nu het Ministerieel Comité ter zake nog steeds geen richtlijn heeft uitgewerkt.[18] In de

---

12 Deze aanbeveling werd ook steeds onderschreven door de Begeleidingscommissies.

13 VAST COMITÉ I, *Activiteitenverslag 2006*, 4 en 132.

14 '*Ondanks het feit dat het Vast Comité I er zich van bewust is dat de (buitenlandse) inlichtingendiensten de 'regel van de derde dienst' als onwrikbaar beschouwen, heeft het Comité diverse malen aangedrongen op een reflectie over de toepassing van deze regel en de controle erop. Immers, de toepassing van de derdenregel kan leiden tot een verkeerde interpretatie gelieerd aan een zekere 'cultuur van het geheim', of zelfs, in extreme gevallen, tot een verkeerd gebruik. Verder is het Vast Comité I altijd de mening toegedaan dat de samenwerking met de buitenlandse en vooral de Europese inlichtingendiensten moest worden versterkt, maar niet zonder te voorzien in de nodige controle*' in VAST COMITÉ I, *Activiteitenverslag 2006*, 4.

15 VAST COMITÉ I, *Activiteitenverslag 2007*, 73-74.

16 VAST COMITÉ I, *Activiteitenverslag 2008*, 6, 109-110.

17 VAST COMITÉ I, *Activiteitenverslag 2009*, 4, 106-107.

18 VAST COMITÉ I, *Activiteitenverslag 2010*, 3-4 en *Activiteitenverslag 2011*, 5-6.

aanbevelingen van het *Activiteitenverslag 2012* komt de kwestie opnieuw aan bod.[19] En zo ook in voorliggend activiteitenverslag. Twee belangrijke onderzoeken (II.1 'De rol van de Algemene Dienst inlichting en veiligheid bij de opvolging van het conflict in Afghanistan' en II.10 'Tussentijdse verslagen in de onderzoeken naar aanleiding van de Snowden-onthullingen') tonen nogmaals aan dat er dringend nood is aan regelgeving ter zake.

[19] VAST COMITÉ I, *Activiteitenverslag 2012*, 2 en 95.

HOOFDSTUK II
DE TOEZICHTONDERZOEKEN

In 2013 werden negen onderzoeken afgesloten. Tevens werd een tussentijds verslag afgerond naar een van de onderzoeken die volgende op de Snowden-onthullingen (zie II.10). Zes van de tien onderzoeken gebeurden op verzoek van de Begeleidingscommissie van de Senaat (waarvan één ook gedeeltelijk het resultaat van een initiatief van de minister van Justitie); vier toezichtonderzoeken werden opgestart na een klacht of een aangifte. In wat volgt, worden de negen eindverslagen (II.1 tot II.9) en het tussentijdse verslag toegelicht (II.10). Daarna volgt een opsomming en een korte situering van de nog lopende onderzoeken (II.11).

Onder deze laatste rubriek staan ook de tien in 2013 geopende toezichtonderzoeken vermeld. Drie van die onderzoeken gebeuren gezamenlijk met het Vast Comité P. Van de tien nieuwe onderzoeken werden er vier opgestart op verzoek van de Senaat, vijf naar aanleiding van een klacht en één op gemeenschappelijk initiatief van de Vaste Comités I en P.

In totaal ontving het Comité in 2013 28 klachten of aangiften. Na verificatie van een aantal objectieve gegevens wees het Comité 22 van deze klachten of aangiften af omdat ze kennelijk niet gegrond waren (art. 34 W.Toezicht) of omdat het Comité zich onbevoegd wist voor de opgeworpen vraag. 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 vijf klachten uit 2013 aanleiding tot het openen van een toezichtonderzoek. Eén klacht, die op het einde van het jaar werd ingediend, gaf pas begin 2014 aanleiding tot de opening van een onderzoek. Daarom blijft ze hier verder onvermeld.

II.1. DE ROL VAN DE ALGEMENE DIENST INLICHTING EN VEILIGHEID BIJ DE OPVOLGING VAN HET CONFLICT IN AFGHANISTAN

In december 2001 besliste België deel te nemen aan de 'International Security Assistance Force' (ISAF), een internationale macht voor het behoud van de vrede

in Afghanistan, die werd opgezet binnen de Verenigde Naties. Naast de NAVO (en zijn lidstaten), participeerden hieraan een twintigtal andere landen.

Het overgrote deel van het Belgische contingent was gestationeerd in Kaboel en stond in voor de bescherming van de internationale luchthaven. In de provincie Kunduz, in het noorden van het land, ondersteunden de Belgen ploegen die instonden voor de heropbouw van het land en verleenden zij technisch advies aan het Afghaanse leger. Ten slotte opereerden sinds 2008 een aantal Belgische gevechtsvliegtuigen vanuit Kandahar.

Om zich een globaal beeld te kunnen vormen van de wijze waarop de militaire inlichtingendienst werd betrokken bij deze operatie, besliste het Comité in januari 2010 een toezichtonderzoek te openen '*betreffende de rol van de ADIV in de opvolging van de situatie in Afghanistan*'.[20] Het Vast Comité I had met dit toezichtonderzoek een duidelijke finaliteit voor ogen: één van de belangrijkste opdrachten van de ADIV zo volledig mogelijk[21] in kaart brengen om op die wijze een referentiekader op te stellen voor latere missies alsook voor toezichtonderzoeken die daaromtrent kunnen worden ingesteld.

Uiteraard kon in deze niet voorbij worden gegaan aan de conclusies van de parlementaire onderzoekscommissie Rwanda[22], ingesteld in 1997 ten gevolge de tragische dood van tien Belgische para-commando's. Over het verzamelen en analyseren van inlichtingen oordeelde deze commissie onder meer het volgende:

- Het Belgische contingent moet steeds beschikken over een eigen, solied inlichtingennetwerk, bestaande uit inlichtingenofficieren die voldoende gevormd zijn en die, in de mate van het mogelijke, de taal beheersen van het land. Op zijn minst moet men beschikken over betrouwbare tolken.
- Om de inlichtingen te analyseren, moet de militaire inlichtingendienst beschikken over voldoende analisten die de inhoud van de informatie kunnen beoordelen. Bovendien moet er een systematische *feedback* worden gegeven aan de eenheden op het terrein.
- Het is noodzakelijk de militaire inlichtingendienst te hervormen, onder andere rekening houdend met de Wet van 30 november 1998 op de inlichtin-

---

20 Het Vast Comité I kon in het kader van dit onderzoek, waarvan een zeer omstandig "GEHEIM – Wet 11-12-1998" geclassificeerd eindrapport werd bezorgd aan de minister van Defensie in september 2013, rekenen op de grote openheid van de chef en de betrokken leden van de ADIV. Ook de onberispelijke organisatie van de plaatsbezoeken in Afghanistan verdient vermelding. Het verslag werd in zijn versie 'BEPERKTE VERSPREIDING' besproken op de vergadering van de Begeleidingscommissie van de Senaat van 12 maart 2014. Tijdens die vergadering en nadien (bij brief van 16 juni 2014) wenste de ADIV en de minister van Defensie enkele verduidelijkingen en nuanceringen toe te voegen aan het rapport. In voorliggend verslag is met die opmerkingen rekening gehouden.

21 Alleen het verzamelen van SIGINT in Afghanistan werd niet belicht. Dit aspect werd opgenomen in een later toezichtonderzoek (zie II.10.12. Vier toezichtonderzoeken in het kader van de Snowden-onthullingen).

22 *Parl. St.* Senaat 1997-1998, nr. 1-611/7.

gen- en veiligheidsdiensten. De dienst moet, voor alles, een efficiënt en coherent instrument worden ter ondersteuning van de verantwoordelijken van de operaties. Het is nodig dat de analysecapaciteit ter beschikking wordt gesteld van de verantwoordelijken ten einde hen toe te laten de politieke opties te bepalen. Er moet worden over gewaakt dat de informatiebronnen voldoende divers van aard zijn en dat de analyse tegensprekelijk gebeurt. Dit houdt in dat er voortdurend informatie dient uitgewisseld te worden tussen de inlichtingendienst enerzijds en de verantwoordelijken op het terrein anderzijds.

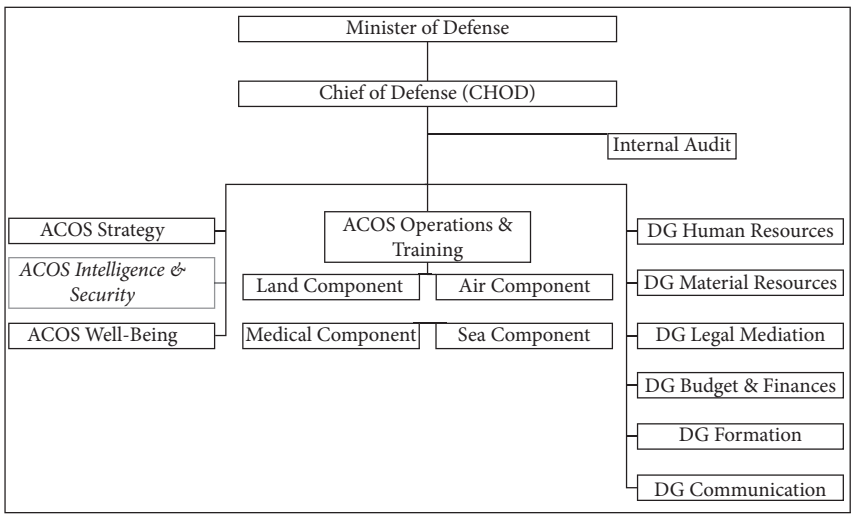
– De militaire inlichtingendienst moet zijn eenheden op het terrein op inlichtingenvlak versterken, in het bijzonder door het ter beschikking stellen van gespecialiseerd personeel of via technische middelen.

II.1.1. DE PLAATS, DE STRUCTUUR EN DE BEVOEGDHEDEN VAN DE ADIV

II.1.1.1. Plaats en structuur van de ADIV

Voor een goed begrip is van belang te weten hoe de ADIV gestructureerd is en waar de dienst zich situeert binnen de Krijgsmacht (waarin overigens nog andere componenten belast zijn met inlichtingengaring).

Structuur van de Belgische Krijgsmacht



De Algemene Dienst inlichting en veiligheid, ook de *Assistant Chief of Staff Intelligence and Security* (ACOS-IS)[23] genoemd, is één van de stafdepartementen van de Krijgsmacht.[24] De dienst was op het moment van het onderzoek opgebouwd uit vier divisies.[25]

De Divisie S(ecurity) voert veiligheidsonderzoeken uit ten aanzien van bepaalde personen of firma's en waakt over de naleving van de richtlijnen met betrekking tot de militaire veiligheid van domeinen, personen, ICT-systemen …

De Divisie A(ppui) staat onder meer in voor personeelsbeheer, budgettair beheer, ICT en logistieke aspecten die binnen de ADIV zelf worden beheerd.

De Divisie C(ounter)I(ntelligence) volgt op Belgisch grondgebied bedreigingen op tegen de militaire veiligheid of tegen andere belangen die de ADIV moet verdedigen. Deze divisie heeft echter ook een rol te vervullen bij de *force-protection* van Belgische eenheden in het buitenland: ze verleent deze eenheden steun om specifieke bedreigingen (bijvoorbeeld infiltratie door lokale groeperingen), tegen te gaan.

De Divisie I(intelligence) ten slotte vormt het grootste onderdeel van de ADIV. Ze richt zich op fenomenen die zich in het buitenland voordoen en is dan ook werkzaam op plaatsen waar Belgische troepen worden ingezet. De analysediensten van de Divisie I zijn grotendeels per regio georganiseerd, terwijl er ook bureaus voor *Naval-* en *Land-Intelligence* en transnationale aangelegenheden bestaan. Inzake collecte (gegevensverzameling) zijn binnen deze Divisie verschillende diensten actief: *Human Intelligence* (HUMINT), *Image Intelligence* (IMINT), *Signals Intelligence* (SIGINT of COMINT) en *Open Sources Intelligence* (OSINT). De opdracht om ter plaatse inlichtingen te verzamelen berust bij de Afdeling I/Ops. De onderdelen van I/Ops die in het buitenland worden ontplooid, worden aangeduid onder de benaming BENIC (*Belgian National Intelligence Cell*) of BELINT (*Belgian Intelligence*).

II.1.1.2. De opdrachten van de ADIV

De vier opdrachten van de ADIV staan omschreven in artikel 11 W.I&V: de klassieke inlichtingentaak, het zorgen voor het behoud van de militaire veiligheid, het beschermen van militaire geheimen en het uitvoeren van veiligheidsonderzoeken. Elk van deze taken kan een link hebben met buitenlandse operaties. Zo bij-

---

23 Aangezien de meeste instructies en permanente orders van deze dienst in het Engels zijn gesteld, neemt het Comité de aldus gebruikte militaire terminologie over.

24 De W.Toezicht en de W.I&V hanteren de term 'Algemene Dienst inlichting en veiligheid van de Krijgsmacht' (ADIV), het Koninklijk besluit 21 december 2001 tot bepaling van de algemene structuur van het ministerie van Landsverdediging en tot vastlegging van de bevoegdheden van bepaalde autoriteiten (KB Defensie) spreekt dan weer van het Stafdepartement Inlichtingen en Veiligheid of *Assistant Chief of Staf Intelligence and Security* (ACOS-IS). Het betreft eenzelfde dienst.

25 In 2013 werden de Divisies S(ecurity) en C(ounter) (I)ntelligence samengevoegd.

voorbeeld heeft de ADIV als opdracht het inwinnen, analyseren en verwerken van inlichtingen (met andere woorden: zijn inlichtingentaak) die betrekking hebben op elke activiteit die de vervulling van de '*opdrachten, acties of operaties in nationaal verband, in het kader van een bondgenootschap of een internationaal of supranationaal samenwerkingsverband*' van de '*Belgische Krijgsmacht, van de geallieerde strijdkrachten of van intergeallieerde defensieorganisaties*' bedreigt of zou kunnen bedreigen. Ook mag informatie worden ingewonnen over collectieve dreigingen tegen '*het leven of de lichamelijke integriteit van Belgen in het buitenland en van hun familieleden*'. Ook de tweede opdracht – het zorgen voor het behoud van de militaire veiligheid[26] van bijvoorbeeld '*het personeel dat onder de Minister van Landsverdediging ressorteert*' en '*de militaire installaties, wapens, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen*' – is van belang bij buitenlandse operaties.

II.1.1.3. De bevoegdheden van de ADIV en het territorialiteitsbeginsel

Artikel 11 W.I&V laat er geen twijfel over bestaan dat de ADIV informatie kan inzamelen *over* het buitenland. Maar kan de dienst ook informatie inzamelen *in* het buitenland? Nergens wordt uitdrukkelijk gesteld dat de ADIV in het buitenland kan optreden. Dit volgt evenwel logisch uit de omschrijving van een aantal opdrachten (bijvoorbeeld de veiligheid van operaties in het kader van een bondgenootschap en de veiligheid van Belgische onderdanen in het buitenland) die onmogelijk uitsluitend vanuit België kunnen waargenomen worden. Hetzelfde geldt voor de andere opdrachten. Zo wordt bijvoorbeeld wat betreft de 'beschermingstaak' geen onderscheid gemaakt al naargelang het personeel of materieel zich in het binnen- dan wel in het buitenland bevinden.

Maar dat de ADIV in het buitenland kan optreden, betekent nog niet dat alle inlichtingenmethoden kunnen aangewend worden. Zo is het aanwenden van specifieke of uitzonderlijke inlichtingenmethoden bij artikel 18/1, 2° W.I&V alleen toegelaten binnen het Belgische grondgebied. Het inzetten van deze methoden in het kader van een onderzoek naar een mogelijke bedreiging voor een buitenlandse missie, is dus wel mogelijk als dit gebeurt op het Belgische grondgebied.

De ADIV was van mening dat de BIM-methoden wél in het buitenland mogen worden ingezet. Het Comité is van oordeel dat dergelijke interpretatie indruist tegen de wet. Wel bestaat de mogelijkheid om in het buitenland uitgezonden communicaties te onderscheppen, bijvoorbeeld om redenen van veiligheid en bescherming van onze troepen en van deze van onze geallieerde partners tijdens de opdrachten in het buitenland. Hiervoor beschikt de ADIV immers over een specifiek wettelijk mandaat (art. 259*bis* § 5 Sw. *juncto* art. 11 § 2, 3° W.I&V.) dat ont-

[26] Deze opdracht beperkt zich tot het opstellen van richtlijnen én het garanderen van de naleving ervan, bijvoorbeeld door het uitvoeren van controles ter plaatse.

breekt voor de andere methoden. Onder meer met het oog op de naleving van mensenrechten en de operationele behoeften op het terrein, onderschreef de minister van Defensie de idee om aan deze problematiek specifiek aandacht te besteden in het kader van de evaluatie van de BIM-Wet.

II.1.1.4. De mededeling van inlichtingen aan derde landen

Een specifiek probleem vormt de mededeling van inlichtingen aan derde landen en het gebruik dat die daarvan mogelijks maken. Ingevolge de artikelen 19 en 20 W.I&V mag/moet de ADIV samenwerken en informatie uitwisselen met buitenlandse diensten. De vraag daarbij is of een dergelijke situatie tot de juridische verantwoordelijkheid van de dienst kan leiden.[27] Het Engelse *High Court of Justice* moest zich reeds uitspreken over de eis van een Pakistaans staatsburger. De Pakistaan hield voor dat de leden van het Britse GCHQ zich schuldig hadden gemaakt aan misdaden (medeplichtigheid aan moord) door het leveren van SIGINT die de NSA en de CIA vervolgens zouden gebruikt hebben bij het uitvoeren van *drone*-aanvallen waarbij zijn vader was omgekomen. De *High Court of Justice* wees de vordering af omdat het lid van de inlichtingendienst *in casu* niet in staat was om te bepalen welke inlichtingen hij eventueel wel of niet zou mogen doorspelen aan de verantwoordelijken op het terrein.[28]

II.1.1.5. Enkele andere actoren op het vlak van inlichtingengaring

ADIV is lang niet de enige entiteit binnen de Belgische Krijgsmacht die inlichtingen verzamelt en in het buitenland actief kan zijn.

Zo zijn er binnen de Land-, Zee- en Luchtcomponent[29] van het Stafdepartement *Operations and Training* (ACOS-Ops & Trg) diensten die bij de operaties en de voorbereiding ervan via allerlei bronnen (bijvoorbeeld via de ADIV of bevelhebbers op het terrein) inlichtingen inwinnen en verwerken. Hoe die diensten met elkaar moeten samenwerken, werd op het moment van het onderzoek omschreven in de *Standing Operating Procedure* (SOP) *Joint Intelligence, Counter-Intelligence and Security Structure* van 2008[30], die uitging van ACOS-Ops & Trg. Deze SOP beschreef onder meer de positie van ADIV in het geheel van de 'inlichtingenstructuur' van Defensie. Zo werd bepaald dat de ADIV richtlijnen ontvangt van de minister van Landsverdediging en van de *Chief of Defense* (CHOD), zich

---

27 Zie hierover verder voetnoot 35 met betrekking tot de uiteenzetting van de ADIV in de Senaat.

28 High Court of Justice, Queens Bench division, Administrative Court, *R – Noor Khan v Foreign Secretary* – 2012.

29 Zo bijvoorbeeld was er in Afghanistan een divisie van Air-Intel actief die gespecialiseerd is in de analyse van de operationele luchtbedreigingen.

30 Deze *Standing Operating Procedure* (SOP) werd vervangen door de SOP '*The Belgian Joint Intelligence and Security Structure*' van november 2013 (eveneens van ACOS-Ops & Trg).

moet richten op politiek-strategische en operationele inlichtingen en indien nodig een inlichtingencel in het buitenland kan ontplooien.

Verder is er in elk operationeel onderdeel van de Krijgsmacht een dusgenaamde 'S2-functie' die wordt uitgeoefend door de officier die de *Commanding Officer* bijstaat om inlichtingen te verschaffen over de situatie op het terrein. Hij levert vooral tactische informatie aan.[31]

Tijdens operaties wordt de *Commanding Officer* bijgestaan door een *Battle Group Intelligence Cell* (BIC). Sinds 2011 werd ook een verkenningsbataljon 'Intelligence, Surveillance, Target Acquistion and Reconnaissance' (ISTAR) opgericht. Dit bataljon zal missies uitvoeren met het oog op het voorbereiden van acties op het terrein en in dit kader vooral tactische informatie verzamelen.[32]

Ten slotte is er ook nog de '*Information Operations Group*' van de Landmacht waaronder de zogenaamde '*Psyops*' en de '*Human Factor Analysis*' ressorteren. *Psyops* richt zich op het verzorgen van de communicatie met de lokale bevolking en autoriteiten op plaatsen waar de Belgische troepen ontplooid zijn. De dienst moet ook reageren op eventuele anti-Belgische propaganda. De *Human Factor Analysis* bestudeert diverse menselijke factoren die een opdracht kunnen beïnvloeden, zoals *antropology* en *human geography.*

II.1.2. DE PLAATS EN DE BEVOEGDHEDEN VAN DE ADIV BINNEN DE ISAF

II.1.2.1. De ISAF-operatie

Drie dagen na de aanslagen van 9/11 nam het Amerikaanse Congres een resolutie aan waarbij het gebruik van gewapend geweld werd toegestaan tegen de verantwoordelijken voor de aanslag én tegen diegenen die aan deze laatsten een toevluchtsoord zouden hebben geboden. Op 15 september 2001 kwam de Noord-Atlantische Raad van de NATO bijeen en verklaarde op vraag van de Verenigde Staten artikel 5 van het Noord-Atlantisch Verdrag toepasselijk: het betreft het recht op bijstand van de NAVO-lidstaten aan die lidstaat die het slachtoffer werd van een gewapende aanval.[33]

Op 20 september 2011 duidden de Verenigde Staten Osama Bin Laden en zijn organisatie Al Qaida aan als verantwoordelijke voor de aanvallen van 9/11. Bin Laden verbleef op dat ogenblik in Afghanistan, waar het Taliban-regime hem de hand boven het hoofd hield en weigerde hem uit te leveren.

---

31 Tijdens de parlementaire voorbereiding van de W.I&V werd reeds een onderscheid gemaakt tussen strategische of geopolitieke inlichtingen enerzijds en de tactische inlichtingen die verband houden met de concrete werkelijkheid van het terrein en met de ontplooiing van een eenheid anderzijds (*Parl. St. Kamer* 1996-1997, 49-638 /14, 22-24 en 38).

32 Zie ook Hoofdstuk V.2.

33 Sinds het ontstaan van de NAVO is dit de enige maal dat dit artikel werd toegepast.

Vanaf oktober 2001 kwamen Amerikaanse, Britse, Franse en Australische troepen in Afghanistan in actie samen met lokale verzetsgroepen en vormden er de zogenaamde 'Noordelijke alliantie'. Deze operatie werd *Operation Enduring Freedom* (OEF) genoemd.

België – en dus ook ADIV – opereert niet binnen dit kader.[34] De activiteiten van de Belgische Krijgsmacht zijn te kaderen binnen een UNO-mandaat. Dat mandaat vond zijn oorsprong in het 'Akkoord van Bonn' van 5 november 2001 waarin de oprichting van een '*International Security Assitance Force* (ISAF)' in het vooruitzicht werd gesteld. De Afghaanse ondertekenaars van het akkoord verzochten de Veiligheidsraad van de Verenigde Naties met name '*to consider authorizing the early deployment to Afghanistan of a United Nations mandated force. This force will assist in the maintenance of security for Kabul and its surroundings. Such a force could, as appropriate, be progressively expanded to other urban centres and other areas*'.

Hieraan gevolg gevend, nam de VN-Veiligheidsraad op 20 december 2001 Resolutie 1386(2001) aan. Deze resolutie gaf het mandaat voor de ontplooiing van een ISAF '*to assist the Afghan Interim Authority in the maintenance of security for Kabul and its surrounding areas, so that the Afghan Interim Authority as well as the personnel of the United Nations can operate in a secure environment*'.

Reeds op 21 december 2001 besliste de Belgische Regering om aan deze missie deel te nemen. Eind januari 2002 werd een eerste transportvliegtuig ingezet, terwijl de inzet van troepen op het terrein ongeveer een jaar later gebeurde.

In eerste instantie viel de ISAF-missie onder een om de zes maanden wisselend commando. Sinds maart 2003 nam de NAVO het commando van ISAF over. Naast NAVO-leden zijn nog een twintigtal andere troepenmachten aanwezig.

Het is van belang te onderlijnen dat de ISAF-troepenmacht tot doel heeft de veiligheid van de bevolking te garanderen en de legitieme Afghaanse autoriteiten te ondersteunen zodat deze, samen met de UNO-autoriteiten, hun burgerlijke taken kunnen uitvoeren. Vanuit militair standpunt betekent dit dat de ISAF-troepen het terrein moeten beveiligen door de militaire krachten van de tegenstrevers te counteren en te verzwakken zodat deze niet langer in staat zouden zijn het land te destabiliseren. Niettemin vormt deze militaire taak niet de essentie van de ISAF-missie. Die missie is hoofdzakelijk gericht op wat heet *counter insurgency*. Daarbij wordt gepoogd de (al dan niet passieve) steun die de opstandelingen bij de bevolking genieten, te verminderen en op termijn te doen verdwijnen. Het is immers deze voedingsbodem die de opstandelingen toelaat hun verzet voort te zetten. De operatie is dus eigenlijk een strijd om de '*minds and hearts*' van de bevolking. De militaire inzet kan deze taak slechts faciliteren door een veiligheidssituatie te scheppen waarin de burgerlijke autoriteiten hun taak kunnen uitvoeren.

---

[34] België nam enkel in de vorm van steunoperaties deel aan *Operation Enduring Freedom* en dit buiten het Afghaanse grondgebied (onder meer door de inzet van C-130 transportvliegtuigen voor humanitaire hulp, het stationeren van een fregat in de Middellandse Zee en het leveren van bemanning voor de AWACS-toestellen boven de Verenigde Staten).

ISAF is niet alleen geen zuiver militaire operatie, het is – anders dan de *Operation Enduring Freedom* – ook geen strijd tegen terreur. In dit verband moet verwezen worden naar het *CHOD OPORDER for Bel contribution to ISAF* (zie verder onder II.1.3.3.4) die stelt dat de Belgische troepen niet aan *Counter Terrorist*-operaties zullen deelnemen. Op het vlak van de inlichtingendoorstroming is het evenwel niet uitgesloten dat inlichtingen die in het kader van de ISAF-operatie met de leden van deze coalitie gedeeld worden, via de bondgenoten die ook deel uitmaken van de *US-led coalition*, een weg vinden naar de OEF, ook al is dat laatste niet de bedoeling.[35] De nauwe verwevenheid op het terrein tussen beide missies blijkt bijvoorbeeld ook uit het feit dat het commando van ISAF en dat van de *US-forces* in Afghanistan (USFOR-A) samenvallen.

II.1.2.2. De Belgische aanwezigheid in Afghanistan met aandacht voor de ADIV

Tot 30 september 2012 stond het overgrote deel van het Belgische contingent (320 personen) in voor de bescherming van de internationale luchthaven van Kaboel (KAIA). België vervulde eveneens een rol binnen de generale staf van de ISAF in Kaboel en stationeerde een nationale steuneenheid in de Kaboul International Airport. Wat betreft Kunduz, stuurde België ongeveer 25 militairen als steun aan de provinciale wederopbouwteams (*provincial reconstruction teams*, PRT) die als opdracht hadden de omgeving te beveiligen, wederopbouwprojecten te coördineren en steun te bieden op het vlak van gezondheid, onderwijs en NGO's.

Anderzijds leverde België in het noorden van Afghanistan een *Military Assistance Team* (MAT) van ongeveer 60 militairen die als opdracht hadden technisch advies te leveren aan de generale staf van een brigade en een bataljon van het Afghaanse nationale leger.

Verder waren er Belgische F-16 gevechtsvliegtuigen op de basis in Kandahar en nam België vanaf 2008 deel aan de Operatie Guardian Falcon en leidde zij Afghaanse piloten en medisch personeel in Kandahar op.

Ten slotte waren ook een aantal militairen ontplooid in Mazar-E-Sharif.

Wat de ADIV betreft namen zowel de Divisies I, CI als S deel aan de opdrachten in Afghanistan. Uiteraard wisselde de samenstelling en getalsterkte van de personeelsleden van de ADIV in functie van de noden en beschikbaarheden. De opvolging van de strategische situatie werd uitgeoefend door personen die zijn ondergebracht in wat heet de *Belgian National Intelligence Cell* (BENIC). Daarnaast ontplooide de ADIV ook personeelsleden die bijvoorbeeld instonden voor

---

35 Voor de parlementaire Commissie Buitenlandse operaties van 19 april 2012 stelde de ADIV mondeling het volgende: *'En conclusion, nous sommes en mesure de certifier qu'en aucun cas les informations collectées, ni les analyses fournies aux unités ou aux partenaires ont un objectif de 'targeting'. Tous nos produits servent uniquement à des fins de protection, de prévention et de contextualisation du processus de décision. Mais nous ne pouvons pas nier que dans la communauté dite des Four Eyes (UK/US) ou des Five Eyes (US/UK/CAN/NZ/AUS) d'autres pratiques sont d'application'.*

de uitwisseling van inlichtingen tussen de ter plaatse ontplooide Belgische eenheden en de buitenlandse militaire bondgenoten en die informatie doorspeelden naar de *Battle Group Intelligence Cell* (BIC), de S2 en eventuele andere partners. Ook werden op punctuele basis soms analisten van de Divisie I naar Afghanistan gezonden. Het Comité stelde vast dat hun opdrachten niet steeds even duidelijk waren omschreven. De Divisie CI was aanwezig onder meer om eventuele veiligheidsproblemen voor de Belgische eenheden te detecteren, om het lokale personeel dat voor de Belgische eenheden werkt op te volgen[36] en om de graad van waardering die de Belgen genieten bij onder meer de Afghanen die met de ISAF samenwerken, te beoordelen. ADIV-S ten slotte zond een team indien een veiligheidsaudit werd aangevraagd. Desgevallend controleert dit team de uitvoering van de veiligheidsregels met betrekking tot het personeel, het materieel en de infrastructuur.

De situatie in Afghanistan werd door de ADIV uiteraard niet alleen ter plaatste opgevolgd. In Brussel is een 'bureau Afghanistan' gevestigd dat bemand wordt door analisten. Zij beantwoorden *Requests for Information* (RFI) komende vanuit ACOS-IS, de NAVO, de EU en zogenaamde 'bevriende diensten' en analyseren de informatie afkomstig van de verschillende collecte-organen (HUMINT, IMINT, SIGINT …). Het bureau verzorgt tevens de briefings voor de generale staf, voor de eenheden die zijn opgeroepen om ontplooid te worden op het terrein, voor de BENIC, alsook voor externe partners (bijvoorbeeld ambassadeurs).

Het overgrote deel van de RFI's die de analisten ontvangen, betreffen vragen van operationele of tactische aard (meestal komende van ACOS-Ops & Trg); strategische vragen vormen slechts een minderheid.

Het Comité moest vaststellen dat de analisten van het 'bureau Afghanistan' niet steeds precies wisten welk soort inlichtingen hun partners uit de inlichtingen- en militaire wereld verwachtten. Omgekeerd zijn de vragen die deze laatsten stellen vaak weinig gespecificeerd aangezien zij niet weten wat de ADIV precies kan aanleveren. De aanwezigheid van analisten op het terrein bleek belangrijk om de vraag en het aanbod beter op elkaar af te stemmen.

II.1.3. NORMEREND KADER VAN TOEPASSING OP DE ADIV IN AFGHANISTAN

II.1.3.1. Het nationale kader

Uiteraard dient in eerste instantie te worden verwezen naar artikel 11 W.I&V dat een algemene omschrijving geeft van de vier opdrachten van de ADIV (zie hoger II.1.1.2). Wat betreft de klassieke inlichtingenopdracht, moet benadrukt worden

[36] De screening van dit *'Local Employed Personnel'* wordt uitgevoerd door het bureau 'vetting' van de NAVO.

dat de wet zelf geen onderscheid maakt tussen (politiek-)strategische, operationele of tactische inlichtingen.[37] Alhoewel uit de voorbereidende werken van de wet blijkt dat het inwinnen van puur tactische informatie niet echt als opdracht van de ADIV werd gezien (zie hoger II.1.1.5), is de dienst op de drie inlichtingenterreinen bedrijvig. Inzake het opsporen van de activiteiten die een bedreiging kunnen vormen voor de vervulling van de opdrachten van de strijdkrachten, kunnen immers alle vormen van inlichtingen van belang zijn.

Verder bepaalt artikel 23 van het Koninklijk besluit van 21 december 2001 tot bepaling van de algemene structuur van het ministerie van Landsverdediging en tot vastlegging van de bevoegdheden van bepaalde autoriteiten, dat de onderstafchef inlichtingen en veiligheid (ACOS-IS), onder meer belast is met '*de organisatie van de steun inlichtingen en veiligheid aan operaties*'.

In uitvoering van de W.I&V zou het Ministerieel Comité voor inlichting en veiligheid (MCIV) bijkomende richtlijnen kunnen uitvaardigen over de werking van de militaire inlichtingendienst ingeval van buitenlandse operaties. Hiervan werd nog geen gebruik gemaakt. Ook heeft het Ministerieel Comité tot op heden geen richtlijnen uitgewerkt over de uitwisseling van inlichtingen met buitenlandse diensten. Het Vast Comité I heeft reeds meermaals op deze lacune gewezen.[38]

De prioriteiten van de ADIV staan omschreven in het Inlichtingenstuurplan (van de divisie I) en het Veiligheidsinlichtingenstuurplan (van de divisie CI). Sinds 2001 verdient Afghanistan volgens de inlichtingenstuurplannen een permanente en intensieve analyse, gebaseerd op een continue en doorgedreven opsporing van informatie door de collecte-organen. Voordien was dit niet het geval. Dezelfde evolutie zien we in de Veiligheidsinlichtingenstuurplannen.

Daarenboven is het *CHOD Operations Order for Bel contribution to ISAF* (2012) van belang. Deze richtlijn beschrijft de bijdrage van de ADIV in het kader van de militaire interventie in Afghanistan in algemene termen: de dienst komt vanuit inlichtingenstandpunt tussen bij de voorbereiding en de uitvoering van de buitenlandse operatie. De richtlijn bepaalt ook dat de Belgische inlichtingencapaciteit (BELINT) onder eigen nationaal commando blijft. De taken van de BELINT strekken zich zowel uit tot de strategische als tot de operationele en tactische inlichtingenvergaring en of –verspreiding.

Verder werden door de ADIV zelf richtlijnen uitgevaardigd die meer praktische details bevatten over alle organisatorische en operationele aspecten die van

---

37 Strategische inlichtingen zijn bestemd ter ondersteuning van de politiek-militaire besluitvormers. Operationele inlichtingen daarentegen zijn inlichtingen die nuttig zijn voor het voorbereiden en uitvoeren van campagnes op het terrein (bijvoorbeeld: Wat is de troepensterkte van de tegenstander in een regio en wat is de toestand van het terrein?). Tactische inlichtingen ten slotte zijn zeer concrete inlichtingen die slaan op zeer specifieke situaties die onmiddellijk dienstig zijn voor de personen op het terrein.

38 Zie VAST COMITÉ I, *Activiteitenverslag 2006*, 132; *Activiteitenverslag 2007*, 73, *Activiteitenverslag 2008*, 6 en 109-110; *Activiteitenverslag 2009*, 4 en 106-107; *Activiteitenverslag 2010*, 3-4 en *Activiteitenverslag 2012*, 95.

belang zijn bij het inzetten van personeel in het buitenland en waarbij meer in detail wordt ingegaan op de opdracht inzake '*force protection*'.

Ten slotte zijn er nog een aantal zogenaamde *Fragmentary Orders* (FragO) die betrekking hebben op specifieke zendingen, bijvoorbeeld van een welbepaald team binnen een bepaalde periode. Een FragO vormt in feite een verbijzondering van een algemeen *Operations Order* voor een specifieke opdracht.

II.1.3.2. Het internationale kader

Op internationaal vlak moet vooral rekening worden gehouden met het *SACEUR Operational Plan for ISAF*, dat een kader biedt voor de inlichtingendiensten van de naties die aan de ISAF operaties meewerken.[39] Als principe geldt hier dat de ADIV-componenten ter plaatse niet onder ISAF/NATO commando staat, en dit in tegenstelling tot de operationele Belgische eenheden. BELINT kan dus geen specifieke instructies krijgen om bepaalde handelingen te verrichten. Vanzelfsprekend belet dit niet dat de BELINT met de ISAF-instanties samenwerken (bijvoorbeeld onder de vorm van informatie-uitwisseling). Wel integendeel. Zo gaat het *SACEUR Operational Plan for ISAF* er van uit dat de aan de operatie deelnemende landen bereid zijn om vanwege ISAF '*Requests for Information*' te krijgen en uit te voeren. Verder zal BELINT zich ook zoveel als mogelijk inschrijven in de prioriteitenbepaling van ISAF zodat zijn inlichtingengaring bijdraagt tot de inlichtingendoelstellingen die door het *Operational Plan* werden bepaald.

II.1.3.3. Enkele verbeterpunten[40]

II.1.3.3.1. Geïntegreerde normen, een gemeenschappelijk begrippenkader en precieze inlichtingendoelen

Het Vast Comité I is van oordeel dat er in bovenstaande documenten en normen meer aandacht kon worden besteed aan onderlinge afstemming, ook al zijn ze

---

[39] Er zijn ook een aantal interne NAVO-regels van toepassing, enerzijds omdat België lid is van de NATO en anderzijds omdat ISAF opereert onder NATO-commando. Zo is er bijvoorbeeld de *NATO Human Intelligence (HUMINT) Policy IMSTAM(INT)–0157-2011(SD1)* die het algemene NATO-beleid inzake HUMINT bevat. In het document, dat niet specifiek voor de ISAF-operatie bedoeld is, wordt onder andere ingegaan op de noodzaak tot informatie-uitwisseling door de diverse Lidstaten en de '*interoperability*' van de systemen die daarvoor worden gebruikt. Verder kan verwezen worden naar de *NATO STANAG 2578 – Allied Intelligence Publication – AIntP-5 – Doctrine for Human Intelligence Procedures*. Deze richtlijn beschrijft onder andere de voorwaarden waaraan een HUMINT-operator moet voldoen en geeft aan hoe gegevens best worden verzameld en hoe een rapport wordt opgemaakt. Ook de HUMINT-organisatie en -structuur komen aan bod. Deze instructie is bedoeld om een eenvormige aanpak tussen de diverse Lidstaten tot stand te brengen en een bepaald kwaliteitsniveau te waarborgen.

[40] In de loop van het onderzoek anticipeerde de ADIV al op een aantal geformuleerde bemerkingen en voerde de dienst een aantal wijzigingen door.

niet met elkaar in tegenspraak. Zo is er tussen de internationale normen en de normen op Belgisch niveau weinig of geen integratie. Het gaat weliswaar om verschillende bevoegdheidsniveaus die van elkaar onafhankelijk zijn, maar voor de personen op het terrein biedt dit geen houvast.

Het Comité is ook van oordeel dat het op niveau van de Belgische normen mogelijk moet zijn een soort gemeenschappelijk begrippenkader te hanteren waarin alle opdrachten en taken van de militaire inlichtingendienst zouden kunnen worden gesitueerd. Dit begrippenkader zou moeten vertrekken vanuit de door de W.I&V omschreven bedreigingen. Daarop voortbouwend, zou een omschrijving moeten volgen van wat dit voor de ADIV, de bureaus én elk van de personeelsleden precies betekent. Met andere woorden: er moet gestreefd worden naar de vertaling van de taakstelling in informatiebehoeften en in te zetten middelen zodat alle medewerkers de precieze inlichtingendoelen kennen.[41] Deze vaststelling geldt zowel voorafgaand aan een operatie, als tijdens de uitvoering ervan.

Zo werd over de precieze rol van de ADIV bij de voorbereiding van de internationale interventie tot voor kort weinig of niets bepaald. Dit vertaalde zich bijvoorbeeld in het feit dat na de beslissing van de Regering in 2002 om aan de internationale interventie in Afghanistan deel te nemen, de 'inlichtingeninspanning' ten aanzien van de situatie in Afghanistan zeer beperkt bleef.

II.1.3.3.2. Gedocumenteerde methodologie bij de voorbereiding van een missie

Het Comité moest vaststellen dat er voorafgaand aan de missie geen gedocumenteerde methodologie werd gehanteerd. Dit is vandaag anders. Sinds een tweetal jaar hanteert ACOS-Ops & Trg de C*omprehensive Preparation of the Operational Environnement*-methode (CPOE) bij de voorbereiding van missies. Wat betreft de inlichtingenfunctie, blijkt er voor de ADIV een belangrijke, maar geen exclusieve, rol weggelegd. Het Comité is van mening dat het (verder) uitwerken en volgen van een dergelijke doctrine of methodologie moet gepromoot worden.

II.1.3.3.3. Gedocumenteerde methodologie tijdens de uitvoering van een missie

Ook tijdens de uitvoering van de operatie van Afghanistan waren de precieze informatie- en inlichtingendoelen van de ADIV niet altijd goed afgebakend. Idealiter zouden de informatie- en inlichtingenbehoeften en de in te zetten middelen moeten worden bepaald, vertrekkend vanuit de doelstellingen en bedreigingen uit de W.I&V.

---

[41] Ook in de audit van de ADIV van 2011 werd het ontbreken van dergelijke gestructureerde aanpak vastgesteld (VAST COMITÉ I, *Activiteitenverslag 2011*, 7-14 en 104-107).

II.1.3.3.4. Geïntegreerde aanpak voor alle divisies

Het onderzoek heeft aangetoond dat er tot eind 2012 geen document bestond waarin de Divisies I, CI en S samen en op geïntegreerde wijze werden opgenomen. Het *CHOD OPORDER for Bel contribution to ISAF* bevatte wel een aantal bepalingen in verband met de inlichtingenopdracht, maar zweeg over de bijdrage van de Divisies CI en S. In januari 2013 werd hieraan verholpen wat betreft de Divisie CI.[42]

II.1.3.3.5. Onduidelijkheid over de aard van in te winnen inlichtingen

Het Vast Comité I stelde een onduidelijkheid vast over de aard van inlichtingen waarop de ADIV zich in hoofdzaak moet richten: strategische, operationele en/of tactische. Volgens de SOP OPS *Joint Intelligence, Counter-Intelligence and Security Structure* van ACOS-Ops & Trg (zie II.1.1.5) moet de ADIV vooral politico-strategische en operationele inlichtingen aanleveren. In het CHOD OPORDER inzake Afghanistan (zie II.1.3.3.4) krijgt de ADIV echter ook een taak inzake '*tactical intelligence*' mee.

In de praktijk blijkt dat de analysediensten van de ADIV eerder op strategische *intelligence* gericht zijn, maar dat de men op het terrein vooral operationeel/tactische inlichtingen nodig heeft.

Het Vast Comité I stelt vast dat deze onduidelijkheid reeds enige tijd bestaat. Deze kwestie is niet onbelangrijk voor de manier waarop de ADIV zijn inlichtingengaring en -verwerking organiseert. Het zonder onderscheid vermengen van de verschillende typen van inlichtingen kan de efficiëntie bemoeilijken. Bovendien is er ook een weerslag op de kennisdomeinen die nodig zijn voor de collecte en analyse: de meer 'politico-civiele benadering' voor de strategische inlichtingen, tegenover de 'militaire *facts and figures*' voor de tactische en operationele inlichtingen.

II.1.4. HET OORDEEL VAN DE KLANTEN VAN DE ADIV

Het Vast Comité I heeft een bevraging gehouden van de voornaamste klanten van de ADIV: de FOD Buitenlandse Zaken (waar vooral zijn Crisiscentrum wat betreft de bescherming van Belgische onderdanen in het buitenland en de zogenaamde Veiligheidsdienst wat betreft de veiligheid in de buitenlandse diplomatieke posten betrokken partij zijn), ACOS-Ops & Trg die binnen Defensie onder meer is belast met het operationele commando van de interventietroepen en het Kabinet van de minister van Defensie.

Algemeen gesproken bleken deze 'klanten' vrij tevreden te zijn over de samenwerking met de ADIV. De dienst blijkt enerzijds flexibel en snel te reageren op

[42] Sindsdien is de gezamenlijke inzet van de divisies op het terrein een feit.

vragen die hem worden gesteld en anderzijds wordt de relevantie en de accuraatheid van de producten benadrukt. De ADIV heeft bovendien een uitstekende reputatie als het op de betrouwbaarheid van zijn producten aankomt.

De ADIV heeft zowel formele en structurele contacten met zijn partners en ter zelfde tijd heeft de dienst tal van informele contacten die zowel de flexibiliteit als de souplesse van het optreden bevorderen.

De producten van de ADIV beslaan hoofdzakelijk veiligheidsthema's op het operationele, tactische en strategische niveau en slaan in mindere mate op de politieke thema's. Nochtans heeft de ADIV ook als opdracht om economische, sociale en mediagerelateerde domeinen te behandelen zoals voorzien is in de *Comprehensive Preparation of the Operational Environnement* (CPOE). Volgens de ADIV worden deze domeinen slechts gedeeltelijk gecoverd omwille van een gebrek aan personeel. Recent werd daarom afgesproken dat Defensie zich op veiligheidsproblemen zal concentreren en Buitenlandse Zaken op voornoemde domeinen.

ACOS-Ops & Trg heeft te kennen gegeven dat ze een grotere betrokkenheid van de ADIV verwacht, in het bijzonder in het kader van de CPOE. Gezien het belang van deze opdracht zowel voor de militaire autoriteiten als voor het kabinet van de minister, komt het er voor de ADIV op aan om na te denken over zijn capaciteit om aan deze vraag tegemoet te komen.

Ten slotte moest het Comité vaststellen dat de klanten onvoldoende weten wat de ADIV kan produceren en – alhoewel ze over de bijdrage van de ADIV tevreden zijn – bijgevolg niet alle mogelijk vragen stellen. Van zijn kant betreurt de analysedienst van de ADIV een gebrek aan *feedback* over zijn producten.

II.1.5. CONCLUSIES

II.1.5.1. De wettigheidstoets en andere reglementaire aspecten

Het Comité was van oordeel dat de ADIV zijn opdrachten in Afghanistan uitvoert conform de nationale en internationale regelgeving en dit ondanks het feit dat deze normen niet alleen talrijk zijn, maar ook weinig geïntegreerd.

Het Comité betreurde evenwel dat de ADIV geen studie had gewijd aan haar eventuele verantwoordelijkheid wanneer ze informatie of inlichtingen verschaft aan een buitenlandse dienst of instantie. Het feit dat het Ministerieel Comité voor inlichting en veiligheid ter zake (nog) geen richtlijnen had opgesteld, deed daaraan geen afbreuk.

Ten slotte wees het Comité op de noodzaak van een herdefiniëring van de concepten 'operationele', 'tactische' en 'strategische' inlichtingen. De meeste internationale en nationale normen hanteren deze begrippen om de competentiedomeinen van de diverse actoren (BENIC, inlichtingenofficier S2, BIC…) af te bakenen. Maar de Wet van 30 november 1998 gebruikt deze terminologie niet; ze

bepaalt de bevoegdheid van de ADIV in functie van dreigingen die moeten worden opgevolgd. Om aan deze opdracht te voldoen, moet de ADIV alle beschikbare informatie verzamelen. Het Comité stelde bovendien vast dat deze begrippen in de praktijk niet bepalend zijn voor het verzamelen of de verspreiding van informatie. Het Comité meende derhalve dat het nuttig zou zijn om na te denken over het verband tussen deze begrippen en de wettelijke opdrachten van de ADIV. Dit lijkt des te meer noodzakelijk gezien het bestaan van het bataljon ISTAR (cf. *supra*).

II.1.5.2. De noodzaak om het risico voor het personeel in conflictzones in te schatten

Het Comité heeft meermaals kunnen vaststellen dat het personeel van de ADIV in sommige situaties risico's loopt. Vandaar dat het sterk de nadruk legde op de kwaliteit van de opleiding voorafgaand aan de ontplooiing en op de noodzaak om over adequate materiële en logistieke middelen te kunnen beschikken.

Meer in het bijzonder stelde het Comité vast dat de ADIV nog geen algemene inschatting maakte van de risico's die inherent verbonden zijn aan het inzetten van militairen of burgerpersoneel in conflictzones. Dergelijke inschatting moet bijvoorbeeld toelaten te oordelen of een ontplooiing van burgerpersoneel (analisten) te overwegen valt en zo ja, om de behoeftes inzake opleiding en materieel te bepalen. Daarenboven zou kunnen gepreciseerd worden welke rol de analisten kunnen spelen in een omgeving waarin aan informatiegaring wordt gedaan, in het bijzonder om de objectiviteit van de analysefunctie te garanderen en elke beïnvloeding te vermijden. Deze reflectie inzake risico's moet evident ook gelden voor de militairen van ADIV. Het Comité was van oordeel dat dit nog onvoldoende gebeurde.

II.1.5.3. De noodzaak om een meer systematische benadering bij de inzet van de ADIV in een conflictzone

Het Comité was van oordeel dat de ontplooiing van de ADIV in Afghanistan op pragmatische wijze gebeurde. Een dergelijke benadering is niet noodzakelijk verkeerd, maar levert het risico op dat aan een aantal meer conceptuele aspecten voorbij wordt gegaan. Een geïntegreerde benadering, waarbij vertrokken wordt van de op te volgen bedreigingen, biedt de mogelijkheid om coherente verbanden te leggen tussen de W.I&V, de *mission statement* van de ADIV, het geïntegreerde strategisch plan van I, CI en S, de Inlichtingen- en Veiligheidsinlichtingenstuurplannen, het collecteplan en vooral de menselijke en materiële middelen die moeten worden ingezet om de inlichtingendoelstellingen te bereiken. In het algemeen laat enkel een geïntegreerde benadering toe om objectief vast te stellen of de ADIV over voldoende personeel en materieel beschikt om zijn wettelijke opdrachten te vervullen.

II.1.5.4. De noodzaak om over adequaat materieel te beschikken

Het Comité heeft moeten vaststellen dat de fysieke integriteit van de personeelsleden van de ADIV gevaar kan lopen. Het is dan ook noodzakelijk dat zij over adequate, materiële middelen beschikken. In het algemeen is dit zeker ook het geval. Wel zijn de communicatiemiddelen die ter beschikking worden gesteld aan de BENIC, voor verbetering vatbaar.

II.1.5.5. De aanbevelingen van de Rwanda-commissie

II.1.5.5.1. Duidelijke regels in verband met de inzetbaarheid en de vertaling daarvan in begrijpbare richtlijnen

Het Comité wees op de verscheidenheid van nationale en internationale regels die van toepassing zijn bij de ontplooiing van het Belgische leger in Afghanistan. Daarenboven is deze regelgeving bijzonder complex, enerzijds omdat er een gebrek aan integratie is (er is geen codex voorhanden) en anderzijds omdat er een gebrek is aan 'vertaling' van de regels in begrijpbare richtlijnen. Een dergelijke complexiteit kan er toe leiden dat de regels niet gekend zijn of verkeerd geïnterpreteerd worden. Daarom pleitte het Comité voor een geïntegreerde voorstelling van de vigerende normen.

Wat de nationale regels betreft, was het Comité bovendien van oordeel dat zij beter op elkaar dienen afgestemd te worden, bijvoorbeeld vertrekkende vanuit de wettelijke opdrachten van de ADIV.

II.1.5.5.2. Een adequate voorbereiding van een opdracht

Het Comité heeft kunnen vaststellen dat de leden van de ADIV voor hun vertrek een specifieke voorbereiding genoten. Deze voorbereiding omvatte verschillende aspecten zoals het gedrag ter plaatse, de situatie in het land alsook een praktische uiteenzetting over de regels inzake de inzetbaarheid. Met uitzondering van dit laatste aspect, kon het Comité in deze recent belangrijke verbeteringen vaststellen.

II.1.5.5.3. Een solied inlichtingennetwerk

De Rwanda-commissie drong er op aan dat de ADIV in de toekomst over een eigen inlichtingennetwerk zou beschikken alsook over opgeleide en getrainde inlichtingenofficieren die de taal machtig zijn of een beroep kunnen doen op vertalers. Het Comité heeft kunnen vaststellen dat deze doelstelling bereikt was. Niettemin zag het Comité twee mogelijke verbeterpunten.

Enerzijds kon de opleiding van het ontplooide personeel van de ADIV verbeterd worden. De ADIV dient in deze een belangrijke en blijvende inspanning te leveren. De recente aanpassingen hebben ontegensprekelijk een toegevoegde waarde, maar

ze waren volgens het Comité niet voldoende. De opleiding moet praktisch en flexibel zijn en mag niet afhangen van de beschikbaarheid van de opleiders.

Anderzijds moet de rol van de ADIV in de voorbereiding van een internationale opdracht versterkt worden. In deze moet de ADIV zich inschrijven in de methodologie van de *Comprehensive Preparation of the Operational Environnement* (CPOE) en aanpassen aan de door de partners binnen het leger uitgedrukte behoeften en ter zake proactief optreden. Dit vergt onder andere dat de ADIV analyses uitvoert in de domeinen die tot haar bevoegdheid behoren.

II.1.5.5.4. Beschikken over voldoende, bekwame analisten

De Rwanda-commissie drong aan op een hervorming van de ADIV zodat de dienst voor diegenen die voor een opdracht verantwoordelijkheid dragen, een efficiënt en coherent instrument zou vormen. Het stelde ook voor de analysecapaciteit te verbeteren en deze ter beschikking te stellen voor het uitwerken van politieke opties ten behoeve van de verantwoordelijken.

Het Comité stelde vast dat deze doelstellingen in grote mate bereikt waren. De ADIV is inderdaad een onmisbare en belangrijke partner geworden bij het verzamelen en het uitbaten van informatie ten behoeve van de troepen op het terrein en in het bijzonder in het kader van de *force protection*. Ook werd zijn rol als raadgever van de hiërarchische en politieke verantwoordelijken en zijn optreden in het kader van de voorbereiding van operaties of tijdens de uitvoering ervan bevestigd.

Het Comité meent niettemin dat de rol van raadgever voor de hiërarchische en politieke verantwoordelijken nog niet ten volle kan gespeeld worden. Dit is mogelijks en ten dele het gevolg van een gebrek aan analisten binnen de ADIV. Dit gebrek zou evenwel kunnen ondervangen worden wanneer de inzet van analisten meer gebeurt in functie van duidelijke inlichtingendoelstellingen.

De klanten van de ADIV bevestigden dat ze tevreden waren over de producten van de ADIV, al werd toegegeven dat zij niet echt op de hoogte zijn welke producten precies zouden kunnen worden aangeleverd. De analisten meenden van hun kant dat zij vanwege hun klanten onvoldoende *feedback* kregen op de door hen geleverde producten. Deze vaststellingen pleiten voor een meer proactieve benadering van de ADIV naar zijn klanten toe. Concreet betekent dit dat de ADIV actief de behoeften en wensen van zowel de interne als externe klanten van Defensie zou moeten gaan bevragen, om de efficiëntie van zijn producten te kunnen optimaliseren. Wel was het Comité er zich van bewust dat ook de klanten tot deze optimalisatie moeten bijdragen.

II.1.5.5.5. De noodzaak om gespecialiseerde ploegen te ontplooien

Het Comité heeft tijdens haar missie in Afghanistan kunnen vaststellen dat de door de ADIV ontplooide ploegen zeer professioneel te werk gaan en dit tot tevredenheid van de Belgische en buitenlandse autoriteiten. De commandanten van de

Belgische onderdelen ter plaatse erkennen dat er een systematische *return* bestaat naar de eenheden op het terrein.

II.2. GEHEIME NOTA'S OVER DE SCIENTOLOGY-KERK IN DE PERS

Op 17 januari 2013 citeert de pers passages uit de nota '*Eglise de Scientologie – Infiltration de la communauté congolaise ou d'origine congolaise de Belgique, Implantation en République démocratique du Congo*' van de VSSE.[43] Deze geheim geclassificeerde nota van 11 december 2012 was door de dienst kort daarvoor verspreid onder bepaalde overheden. In de artikels wordt beweerd dat de Scientologykerk haar activiteiten probeert uit te breiden in Afrika en in dat kader tussenpersonen zoekt in de Belgisch-Congolese gemeenschap. Daarenboven worden een aantal politici bij naam genoemd[44]: Bertin Mampaka, toen ondervoorzitter van het Brussels Hoofdstedelijk Parlement en gemeenteraadslid te Brussel[45]; Justine Kasa-Vubu, voormalig minister in de eerste regering van Laurent-Désiré Kabila en nadien ambassadrice in Brussel; Gisèle Mandaila, in die periode Brussels Volksvertegenwoordiger en in 2004 Staatssecretaris voor Gezinnen en Personen met een handicap en tevens gemeenteraadslid in Etterbeek en ten slotte Pierre Migisha, ten tijde van het lek Brussels Volksvertegenwoordiger en gemeenteraadslid in Anderlecht.

Op verzoek van de Begeleidingscommissie wordt een toezichtonderzoek geopend waarbij zowel de totstandkoming als de verspreiding van de nota moet bestudeerd worden.

Amper veertien dagen later wordt in de pers gewag gemaakt van een andere nota van de VSSE.[46] Ditmaal betrof het de '*Fenomeenanalyse – Niet-staatsgestuurde inmengingsactiviteiten*'. Ook in dit geheime rapport zouden tal van politici worden geciteerd omwille van hun relaties met onder meer de Scientologykerk. Hierop werd het Comité door de minister van Justitie belast met een toezichtonderzoek. Er moest worden onderzocht of de ministeriële richtlijn van 25 mei 2009, volgens dewelke de minister van Justitie op de hoogte moet worden gebracht telkens de naam van een federaal parlementslid wordt vernoemd in een verslag, correct werd toegepast en of het al dan niet aangewezen was om parlementsleden bij naam te noemen in een fenomeenanalyse. Een dag later werd door

43 A. CLEVERS, *La Dernière Heure*, 17 januari 2013 (La Scientologie infiltre les milieux belgo-congolais); K. VAN EYCKEN en H. ADRIAEN, *Het Laatste Nieuws*, 17 januari 2013 (Scientology infiltreert in Congolese gemeenschap in Brussel).

44 De namen van deze politici kwamen uitgebreid aan bod in de media.

45 Nadien werd betrokkene door het parlement van de Franse Gemeenschap aangewezen tot Senator.

46 M. BUXANT en S. SAMYN, *De Morgen*, 2 februari 2013 (Staatsveiligheid houdt Wetstraat in de gaten).

de Begeleidingscommissie de opdracht gegeven haar eerste onderzoek uit te breiden naar de totstandkoming en de openbaarmaking van deze fenomeenanalyse en naar de vraag of de Belgische inlichtingendiensten een correcte toepassing hebben gemaakt van het *need to know*-principe.[47]

De opdrachten die de Begeleidingscommissie en de minister van Justitie toewezen aan Comité, hadden grotendeels betrekking op dezelfde problematiek. Het Comité besliste dan ook al die aspecten onder te brengen in één enkel onderzoek met als titel '*Toezichtonderzoek naar de wijze van aanmaak en verspreiding door de VSSE van de nota over de infiltratie door de Scientology-beweging van de Congolese gemeenschap in Brussel en het rapport 'Fenomeenanalyse – Niet-staatsgestuurde inmengingsactiviteiten', hierbij inbegrepen het bestuderen van de problematiek van de vermelding van de namen van politieke mandatarissen en de lijsten van bestemmelingen en hun 'need-to-know'*.[48]

II.2.1. DE GEHEIME NOTA VAN 12 DECEMBER 2012 OVER DE SCIENTOLOGYKERK

II.2.1.1. De inhoud van de nota

De VSSE moet activiteiten opvolgen die een bedreiging (kunnen) vormen voor de veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde. Bij de uitoefening van deze opdracht, stootte de VSSE op namen van politieke mandatarissen die in verband konden gebracht worden met de Scientologykerk. Dit gaf aanleiding tot het opstellen van verschillende nota's. Zo ook van de gelekte nota van 11 december 2012 waarin de relatie van de vier hogervermelde politici met de Scientologykerk werd behandeld. De nota kan als volgt worden samengevat:

– een van de vier betrokkenen wordt benaderd door de Scientologykerk;
– een tweede onderhoudt relaties met de Scientologykerk;

---

47 Tevens werd het Comité belast met een 'transversale analyse' naar de wijze waarop de inlichtingendiensten informatie inwinnen over politieke mandatarissen (II.4).

48 Niet alleen het Vast Comité I opende een onderzoek. Ingevolge de verschillende lekken, diende de VSSE begin februari 2013 klacht in met burgerlijke partijstelling tegen onbekenden wegens inbreuk op artikel 11 van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (W.C&VM). Het Comité kreeg geen inzage in het gerechtelijk onderzoek. Ook de Nationale Veiligheidsoverheid (NVO) opende bij de bestemmelingen van zowel de eerste nota als van de fenomeenanalyse een veiligheidsonderzoek. Ook de resultaten hiervan zijn bij het Vast Comité I niet gekend. Op 20 maart 2013 ten slotte, werd in naam van de Scientologykerk van België vzw, een klacht ingediend bij het Vast Comité I. Het onderzoek dat hierop volgde, werd afgerond begin 2014 (II.11.8). In het parlement werd ook een 'Voorstel tot oprichting van een parlementaire onderzoekscommissie belast met het onderzoek naar de gevallen waarin de Veiligheid van de Staat verkozen politici schaduwt' ingediend. (*Parl. St.* Kamer 2012-2013, nr. 53K2652/001 en *Parl. St.* Senaat 2012-13, nr. 5-2034/1).

– met betrekking tot de overige twee beweert de VSSE op basis van door de buitendiensten gemelde feiten dat ze zeer dicht staan bij de Scientologykerk of er zelfs lid van zijn.

Volgens het Comité handelde de VSSE bij het opstellen van deze eerste nota binnen het kader van haar wettelijke bevoegdheden zoals die staan omschreven in de Wet van 30 november 1998. Het Comité verwees meer bepaald naar artikel 8, 1° e) en g) dat betrekking heeft op 'schadelijke sektarische organisaties' en 'inmenging'. Het Comité beschikte over geen enkele aanwijzing dat er onregelmatigheden zouden hebben plaatsgevonden bij het vergaren van de inlichtingen die aan de basis lagen van de nota. Daarenboven was de nota genuanceerd in haar bewoordingen.

II.2.1.2. De bestemmelingen van de nota en hun need to know

De bewuste nota werd bezorgd aan zes bestemmelingen, te weten de ministers van Justitie en Buitenlandse Zaken, de Ambassadeur van België in Congo en de Voorzitter, het Hoofd Veiligheid en de Directeur Afrika van de FOD Buitenlandse Zaken. Ze waren allen houder van de vereiste veiligheidsmachtiging. Tevens maakte hun functie als minister, hoge functionaris of diplomaat en hun verantwoordelijkheid inzake diplomatie en internationale relaties dat voldaan was aan de vereiste van de *need to know*. De nota had namelijk betrekking op de infiltratie van de Congolese of van oorsprong Congolese gemeenschap in België door de Scientologykerk en haar vestiging in de Democratische Republiek Congo. Het Comité was de mening toegedaan dat deze inlichtingen belangrijk waren voor de overheden die belast zijn met het buitenlands beleid van België. Deze informatie moest dus bij toepassing van artikel 19 W.I&V[49] aan de betrokken overheden worden bezorgd.

II.2.1.3. De meldingsplicht

In de periode waarop het toezichtonderzoek betrekking had, bestonden er twee richtlijnen die een verplichting inhielden voor de VSSE om de minister van Justitie in kennis te stellen wanneer politici het voorwerp uitmaakten van inlichtingenactiviteiten: een ministeriële richtlijn van 25 mei 2009 – opgesteld naar aanleiding van de aanbevelingen van het Vast Comité I in het kader van een eerder toezichtonderzoek[50] – en een interne instructie van 27 maart 2012.[51]

---

49 '*De inlichtingen- en veiligheidsdiensten delen de inlichtingen bedoeld in artikel 13, tweede lid, slechts mee aan de betrokken ministers en de betrokken gerechtelijke en administratieve overheden, aan de politiediensten en aan alle bevoegde instanties en personen overeenkomstig de doelstellingen van hun opdrachten alsook aan de instanties en personen die het voorwerp zijn van een bedreiging bedoeld in de artikelen 7 en 11.*'

50 VAST COMITÉ I, *Activiteitenverslag 2008*, 22-33 (II.2. 'Gereserveerde dossiers' bij de Veiligheid van de Staat).

51 Zie hierover ook II.4.2.1.3.

De richtlijn van 25 mei 2009 stelt dat de minister van Justitie op de hoogte moet worden gebracht telkens de naam van een zetelend federaal parlementslid wordt vernoemd in een verslag. Geen van de vier betrokkenen bekleedde destijds een dergelijk mandaat. Er diende dus geen kennisgeving te gebeuren.

Het toepassingsgebied van de interne instructie van 27 maart 2012 is zowel enger als ruimer dan dat van de ministeriële instructie: ze heeft enerzijds alleen betrekking op vermeldingen in verslagen van de buitendiensten van de VSSE, maar anderzijds op alle ministers en politieke mandatarissen, ook deze van de Gemeenschappen en Gewesten.

Ten aanzien van Justine Kasa-Vubu diende ook ingevolge deze richtlijn geen kennisgeving te gebeuren aangezien zij geen Belgisch politiek mandataris was.

Ten aanzien van de drie anderen diende de minister wél te worden geïnformeerd. Met betrekking tot Bertin Mampaka had de VSSE reeds in juli 2012 een eerste nota bezorgd aan de minister van Justitie waarin gewag werd gemaakt van de contacten die hij had met de Scientologykerk. Deze nota kan dus als kennisgeving worden beschouwd. Met betrekking tot Pierre Migisha en Gisèle Mandaila kan alleen de nota van 11 december 2012 worden beschouwd als de vereiste kennisgeving. De VSSE had de minister wat deze twee laatsten betreft dus sneller moeten informeren.

II.2.2. DE FENOMEENANALYSE BETREFFENDE DE 'NIET-STAATSGESTUURDE INMENGINGSACTIVITEITEN[52]

II.2.2.1. De inhoud van de fenomeenanalyse

Het bewuste verslag vormt de vierde fenomeenanalyse die de VSSE opstelde. Het Vast Comité I benadrukte opnieuw[53] het nut van een dergelijk type van verslag dat *'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 de risque' à destination de nos responsables politiques, des autorités administratives concernées et des autorités judiciaires qui sont également confrontées à cette problématique […]'.*[54]

---

52 De problematiek van de verwittiging van de minister van Justitie in geval van inlichtingenactiviteiten ten aanzien van politieke mandatarissen werd opgenomen in het het onderzoek 'De opvolging van politieke mandatarissen door de inlichtingendiensten' (II.4).

53 VAST COMITÉ I, *Activiteitenverslag 2012*, 14-28 (II.2. De opvolging van buitenlandse inlichtingendiensten ten aanzien van hun diaspora in België).

54 Uit 'Extrémisme islamique en Belgique, Analyse du phénomène' van de VSSE.

Het Comité stelde echter vast dat de directie van de VSSE aan de opstellers ervan geen duidelijke richtlijnen had gegeven en had nagelaten de doelstellingen en de methodologie te definiëren. Het doel van deze fenomeenanalyse werd in de inleiding slechts kort toegelicht: '*de Veiligheid van de Staat tracht met deze fenomeenanalyse een beeld te schetsen van de inmengingsactiviteiten van groeperingen en/of organisaties in politieke en economische middens*'. Daarbij wees de VSSE erop dat elke organisatie het recht heeft te lobbyen om haar doelstellingen te promoten. Wordt er echter contact opgenomen met personen die verantwoordelijke functies bekleden om op die wijze beslissingsprocessen te beïnvloeden of om invloed uit te oefenen, dan wordt de grijze zone van het lobbyen overschreden en kan er sprake zijn van 'inmenging' in de zin van artikel 8, 1°g) W.I&V, aldus de VSSE.

Het Comité uitte voorts kritiek op het feit dat het rapport naliet op duidelijke wijze[55] de strategie te omschrijven die de Scientologykerk aanwendt om te trachten '*beslissingsprocessen te beïnvloeden met ongeoorloofde, bedrieglijke of clandestiene middelen*' (art. 8, 1° g) W.I&V). Evenmin werd er ingegaan op de werkelijke doelstellingen van de organisatie, noch op de wijze waarop contacten worden gelegd en onderhouden. Het Comité vond het dan ook aanbevelenswaard om in dergelijke analyse bij wijze van voorbeeld uiteen te zetten hoe een rekrutering kan verlopen: eerste contact(en) door een tussenpersoon, benaderen van parlementsleden, benadering via organisaties die hun relatie met de Scientologykerk niet onthullen, aanbieden van voordelen of hulp (bijvoorbeeld deelname aan cursussen of financiële hulp voor projecten)…

Maar het Comité was vooral kritisch voor de wijze waarop uitvoerig namen van (voormalige) politieke mandatarissen en hun medewerkers werden vermeld.[56] Ook al kwamen sommige namen meermaals voor en werd de betrokkenheid van sommige personen nader toegelicht, toch ontstond de indruk dat alle genoemde personen op eenzelfde niveau moesten worden geplaatst en dezelfde informatieve waarde bezaten. Het Comité wees er in deze op dat de vermelding bij naam in een verslag van de VSSE een 'stigmatiserend' effect heeft, zelfs indien dit verslag op beperkte schaal verspreid wordt.

Het Comité benadrukte dat, indien de opsomming van namen bedoeld was om aan te tonen wat de reikwijdte is van de contacten van de Scientologykerk en van diens activiteiten, het essentieel is te specifiëren wat de juiste band is tussen een welbepaald persoon en de Scientologykerk: zijn er één of meerdere pogingen tot toenadering geweest, waren deze pogingen succesvol, in welke context hebben ze plaatsgevonden, heeft de betrokkene op passieve of actieve wijze deelgenomen

55 Soms is wel op impliciete wijze duidelijk welke strategie wordt gevolgd. Mogelijk zijn de opstellers van de analyse te veel uitgegaan van de hypothese dat het voor de lezer om een evidentie ging.

56 Het Comité stelde vast dat de opstellers van de analyse zonder tussenkomst van de directie beslist hadden om namen te noemen. Het Vast Comité I plaatste vraagtekens bij deze beslissing.

aan activiteiten (bijvoorbeeld door een toespraak te houden op een conferentie), was de betrokkene zich bewust van het feit dat de activiteiten werden georganiseerd door de Scientologykerk… Met andere woorden, indien de VSSE het noodzakelijk acht om namen te noemen – en dat is haar verantwoordelijkheid – dan moet ze in het verslag de graad van betrokkenheid van elke persoon aangeven.

Indien het echter de bedoeling is om de ontwikkeling van de activiteiten van de Scientologykerk aan te tonen en op gedetailleerde wijze te illustreren dat er een welomschreven strategie van contactname en rekrutering wordt gevolgd (met andere woorden, indien men een fenomeen wil beschrijven), is het niet nodig om namen te noemen. In dat geval volstaan abstracte voorbeelden die aangeven hoe en waar de Scientologykerk leden rekruteert en netwerken uitbouwt.

II.2.2.2. De bestemmelingen van de fenomeenanalyse en hun need to know

Naast de verspreiding binnen de VSSE zelf, werd de fenomeenanalyse verzonden naar 33 personen.

De VSSE had vóór de verspreiding contact opgenomen met de Nationale Veiligheidsoverheid om na te gaan of de bestemmelingen houder waren van een veiligheidsmachtiging van het vereiste niveau. Dit bleek het geval, één uitzondering niet te na gesproken.[57] De VSSE liet zoals vereist een ontvangstbewijs tekenen door de bestemmeling of diens veiligheidsofficier. In een begeleidend schrijven bij de fenomeenanalyse wees de VSSE bovendien op de noodzaak tot strikte inachtneming van de Classificatiewet en op het ernstig nadeel dat kon voortvloeien uit een ongepast gebruik van het rapport.

Het Vast Comité I moest wel vaststellen dat er geen vooraf opgestelde lijst bestond van bestemmelingen voor dit soort van analyses: wie een rapport zou ontvangen en wie niet werd aan de appreciatie van de opstellers overgelaten. De hiërarchische overheid voegde er *in casu* wel enkele namen aan toe.

Het spreekt voor zich dat de ruime verspreiding die hiervan het gevolg was, het risico op lekken vergroot. Het Vast Comité I legde evenwel de nadruk op het feit dat vooreerst de perso(o)n(en) aan de oorsprong van de lekken verantwoordelijk is (zijn) (in de veronderstelling uiteraard dat er opzettelijk gelekt werd of de informatie bij de pers terecht kwam ingevolge een nalatigheid) voor de negatieve gevolgen hiervan voor de VSSE en de genoemde mandatarissen.

Bij het opstellen van de lijst met bestemmelingen was naar het oordeel van het Comité niet doordacht te werk gegaan. Ofwel werd door de VSSE in algemene termen verwezen naar de 'wettelijke bevoegdheid' van bepaalde personen (met name van de Eerste Minister, de Vice Eerste Ministers of de ministers die lid zijn van het Ministerieel Comité voor inlichting en veiligheid) ofwel, meer specifiek, naar hun veronderstelde *need to know*. Het probleem hierbij is evenwel dat de

[57] Eén bestemmeling beschikte niet over een veiligheidsmachtiging. Hij kreeg dan ook geen exemplaar van de fenomeenanalyse.

vraag wie een 'kennisnemingsbehoefte' heeft, afhankelijk is van de finaliteit van het product dat wordt verspreid. Ofwel wil het informeren over een algemeen fenomeen van inmenging, ofwel wil men de aandacht vestigen op precieze risico's waarmee een persoon of instantie in het kader van zijn of haar functie wordt of kan worden geconfronteerd. In dit laatste geval oordeelde het Comité dat het niet nodig is om het volledige verslag te bezorgen. Integendeel, op dat ogenblik is het aangewezen om de informatie te beperken tot wat nuttig is voor een welbepaalde bestemmeling. Indien het verslag echter bedoeld is om te informeren over een algemeen fenomeen, dan is het verzenden van een volledig verslag gerechtvaardigd. Maar op dat ogenblik stelt zich de vraag of het aan de VSSE zelf toekomt om dergelijk verslag te bezorgen aan veertien ambtenaren/diplomaten van de FOD Buitenlandse Zaken. Het Comité stelde zich de vraag of het niet meer aangewezen zou zijn mochten verslagen worden verzonden naar één enkele bestemmeling die als *point of contact* binnen dit departement de 'kennisnemingsbehoefte' van elk van zijn collega's kan beoordelen.[58]

Concreet wat betreft de fenomeenanalyse inmenging oordeelde het Comité dat het passender zou zijn geweest om het verslag op meer gerichte wijze te verspreiden, en dit in functie van de behoeften van elke bestemmeling. Hierdoor zouden mogelijks ook de negatieve gevolgen van het lek beperkt zijn gebleven.

II.3. EEN INFORMANT BINNEN HET VLAAMS BELANG?

Begin 2013 raken twee geheime rapporten van de Veiligheid van de Staat in de openbaarheid (zie II.2). In de parlementaire debatten die daarop volgen, verklaarde de minister van Justitie dat het '*niet de opdracht [van de VSSE] is om individuele parlementsleden te volgen. Dat is niet de opdracht van die dienst en het gebeurt in de praktijk ook niet*'.[59] Bart Debie, ex-politiecommissaris van Antwerpen en gewezen veiligheidsadviseur van Filip Dewinter (Vlaams Belang), meende dat tegen te moeten spreken. In een krantenartikel[60] liet hij optekenen: '*Wat ze met andere politici doen, weet ik niet. Maar de Staatsveiligheid heeft het Vlaams Belang jarenlang met héél véél aandacht gevolgd. En ik kan het weten, want ik was er zelf bij betrokken*'. Debie verklaart informant te zijn geweest van de VSSE van 2007 tot 2010 – periode tijdens dewelke hij woordvoerder/veiligheidsadviseur was van het Vlaams Belang. Er volgen hevige reacties van Filip Dewinter, de minister van Justitie en de administrateur-generaal van de VSSE.

---

58 Recent zou de VSSE beslist hebben om voortaan via een *point of contact* te werken.

59 *Hand.* Kamer 2012-13, 7 februari 2013, CRIV53COM666, 9 e.v. Verder: '*[…] ik herhaal ook dat het niet tot de opdracht van de Veiligheid van de Staat behoort om parlementsleden in de gaten te houden in hoofde van hun functie*'.

60 J. VAN DER AA en T. LE BACQ, *De Standaard*, 11 februari 2013 (Ik was de mol binnen Vlaams Belang).

Net daarvoor had het Vast Comité I over de thematiek van de opvolging van politieke mandatarissen een algemeen onderzoek opgestart.[61] Het Comité besliste evenwel in te gaan op deze specifieke *casus*, en een 'deelonderzoek' te voeren naar de contacten van de Veiligheid van de Staat met Bart Debie en de informatie die daaruit voortvloeide, in het bijzonder deze aangaande Filip Dewinter. Vooraf-gaand wordt overlopen of en in welke mate in de opvolging van het Vlaams Blok/ Belang werd voorzien doorheen de jaren.

II.3.1. DE OPVOLGING VAN HET VLAAMS BLOK, LATER VLAAMS BELANG

Op basis van de artikelen 7 en 8 W.I&V is de VSSE bevoegd om het extremisme[62] op te volgen wanneer dit een bedreiging vormt of zou kunnen vormen voor de interne of externe veiligheid van het land. De opvolging van politici of politieke partijen is dus mogelijk vanuit deze invalshoek. Wel moet bij de eventuele opvolging uiteraard rekening worden gehouden met de Grondwet, het EVRM en de rechtspraak van het Europees Hof voor de Rechten van de Mens inzake vrijheid van meningsuiting en vrijheid van vereniging.

Tot midden jaren '90 werd het Vlaams Blok systematisch opgenomen in de zogenaamde 'lijst met onderwerpen'. Op de lijsten van 1996 en 1999 kwam de partij niet meer voor.[63] In die periode diende er dus geen opvolging meer te gebeuren.

Daar kwam verandering in toen de minister van Justitie in 2001 de VSSE de instructie gaf om het Vlaams Blok opnieuw te beschouwen als een te behandelen onderwerp conform de Wet van 30 november 1998, met uitzondering van de activiteiten van de mandatarissen gesteld in het kader van hun parlementair mandaat. De uitoefening van een dergelijk mandaat werd daarbij gedefinieerd als '*de meningsuiting, de parlementaire vragen en interpellaties, het indienen van een wetsvoorstel, kortom wat zich in het parlementair halfrond afspeelt*'. In een interne richtlijn van juli 2001 werkte de VSSE de contouren van deze ministeriële richtlijn verder uit: de inlichtingen die over het 'Vlaams Blok' worden vergaard en verwerkt, moesten betrekking hebben op alle individuele en collectieve activiteiten die rechtstreeks verband houden met extremisme, zoals gedefinieerd in artikel 8, 1° W.I&V. Alle activiteiten zonder extremistisch karakter worden niet als dusdanig opgevolgd. De aandacht diende dus uit te gaan naar de actieve, extremistische militanten.

---

61 Zie *infra* 'II.4. De opvolging van politieke mandatarissen door die inlichtingendiensten'.

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

63 Er werd destijds niet noodzakelijk elk jaar een nieuwe lijst opgesteld.

In 2003 vraagt de VSSE – middels een bijzonder goed gemotiveerde nota – aan de Eerste Minister in zijn hoedanigheid van voorzitter van het Ministerieel Comité voor inlichting en veiligheid, om het Vlaams Blok van de lijst van op te volgen onderwerpen te verwijderen. Op deze vraag volgt geen antwoord. In 2004 wordt het Vlaams Blok het Vlaams Belang. Toch vormt dit geen aanleiding voor de VSSE om de bevoegde overheden opnieuw te bevragen omtrent hun standpunt inzake de al dan niet opvolging van de partij. Op de 'Lijst van onderwerpen' van 2006 komt het Vlaams Blok (*sic*) dan ook nog steeds voor.

Sinds 2009 maakt de VSSE geen 'lijst met onderwerpen' meer op. Vanaf dan wordt jaarlijks een zogenaamd 'actieplan' opgesteld dat door de minister van Justitie moet worden goedgekeurd. In dat plan worden de te volgen fenomenen en groeperingen[64] opgelijst en onderverdeeld in functie van een 'actieve opvolging'[65], een 'reactieve opvolging'[66] of 'geen opvolging'.[67] Zo wordt in het Actieplan 2010 onder de noemer 'reactieve behandeling' '*Extreme Rechts Nationalistische e/o identiteit bewegingen (…) nederlandstalig: Vlaams Belang*' vermeldt. De Actieplannen 2011 en 2012 maken onder meer melding van '*Vlaams Belang – interne partijwerking en nationale standpunten*', maar dan onder de noemer 'geen opvolging'. In het Actieplan 2013 wordt de partij niet meer vernoemd. De rubriek 'geen opvolging' werd sindsdien niet meer opgenomen.

II.3.2. DE CONTACTEN TUSSEN BART DEBIE EN DE VSSE

Het eerste contact tussen Bart Debie en de VSSE kwam er op initiatief van Debie zelf. Halverwege augustus 2010[68] stuurde hij een e-mailbericht naar de VSSE om zijn diensten aan te bieden omdat hij van een '*heel bekend politicus opdrachten heeft gekregen die de grenzen van het strafrecht ver overschrijden*' en waarmee hij

64 Maar nooit individuele personen *as such*.

65 Dit betekent dat de VSSE actief activiteiten ontwikkelt om de informatiepositie te verwerven, uit te bouwen of te verstevigen.

66 'Reactieve opvolging' betekent dat de VSSE activiteiten ontwikkelt om de informatiepositie te verwerven, uit te bouwen of te verstevigen, maar slechts in reactie op een uitdrukkelijke vraag daartoe.

67 'Geen opvolging' betekent dat de VSSE de opvolging niet verzekert, of desgevallend niet aan een externe vraag om inlichtingen kan voldoen. Het betreft die problematieken waarvoor de dienst zich bewust is van de noodzaak tot opvolging en/of investering, maar waarvoor gelet op de onvoldoende capaciteit een adequate informatiepositie ontbreekt en geen acties kunnen worden gepland. Dit betekent dus niet dat de VSSE geen informatie over deze thema's kan ontvangen, verzamelen of opslaan, maar wel dat de VSSE deze niet verder uitdiept en dat de opvolging ervan louter incidenteel is.

68 In de pers werd initieel gesteld dat Bart Debie reeds in 2007 in contact was met de VSSE. Dit bleek echter niet uit het onderzoek van het Vast Comité I. Wellicht ging het om een misverstand: tijdens zijn contacten met de pers sprak betrokkene over zaken die zich in 2007 hadden afgespeeld, maar die hij pas in 2010 had gemeld. De journalisten erkenden nadien overigens zelf dat zij mogelijks onnauwkeurig waren geweest (T. NAEGELS, *De Standaard*, 27 februari 2013 (Welles-nietes-nieuws).

zich '*deontologisch niet langer mee [kon] verzoenen*'. Sindsdien vonden vijf ontmoetingen plaats en werden herhaaldelijk e-mails uitgewisseld, en dit tot juli 2012.

Bart Debie verschafte informatie over de buitenlandse contacten en geplande reizen van Filip Dewinter; over zijn positie binnen het Vlaams Belang en de machtsverhoudingen binnen de partij; over zijn 'sponsors' en deze van het Vlaams Belang; over een internationale conferentie waarvan het Vlaams Belang de praktische organisatie in handen had; over de verbanden tussen het Vlaams Belang en een aantal extreemrechtse organisaties; over de terreuraanval van de Noor Anders Breivik in 2011[69] en over het bezoek van Amerikaanse zakenlui en Senatoren aan Europa waarbij Filip Dewinter de delegatie in Antwerpen ontving. Uiteraard kwamen ook de feiten die aan de basis lagen van de contactname (vermeende illegale activiteiten) aan bod.

Er wordt ook sporadisch e-mailverkeer uitgewisseld waarin Bart Debie niets bijzonders te melden heeft. Na verloop van tijd stuurt geen van beide partijen nog aan op verdere ontmoetingen. In juli 2012 ten slotte meldt Bart Debie dat hij informatie heeft over 'een lek bij het Parket'. Er wordt een ontmoeting geregeld maar betrokkene daagt niet op. Nadien vonden er geen contacten meer plaats.

Het Vast Comité I oordeelde dat de VSSE met deze contacten binnen de perken van haar jaarlijkse actieplannen was gebleven. Het Actieplan 2010 voorzag in een 'reactieve' opvolging van extreemrechts en van het Vlaams Belang wat inhoudt dat de VSSE activiteiten mag ontplooien om te reageren op een specifieke gebeurtenis of ontwikkeling. Het Vast Comité I was van mening dat de informatie die betrokkene in eerste instantie leek te zullen geven – over '*opdrachten die de grenzen van het strafrecht ver overschrijden*' – dan ook rechtvaardigde dat werd ingegaan op het aanbod van Bart Debie. Ook gelet op zijn status binnen het Vlaams Belang en zijn kennis van het extreemrechtse veld kon dergelijke bron niet zomaar aan de kant worden geschoven. In het Actieplan 2011 werd het Vlaams Belang opgenomen onder de categorie 'geen opvolging'. Dit betekende evenwel niet dat de VSSE over dit thema geen informatie meer zou mogen ontvangen. Aangezien dat jaar via de bron weinig informatie werd opgetekend die rechtstreeks betrekking had op het Vlaams Belang, was ook deze opvolging conform het actieplan. In 2012 doofden de contacten met Bart Debie uit. In het actieplan van dat jaar was het Vlaams Belang nog steeds opgenomen onder de rubriek 'geen opvolging'.

Het Comité stelde eveneens vast dat de VSSE in haar relatie met Bart Debie de instructie van 15 mei 2001 had gerespecteerd: ze had geen inlichtingen ingewonnen die te maken hadden met de uitoefening van het parlementair mandaat *as such* (het uiten van de opinie en de werkzaamheden in het Parlement) van Filip Dewinter of van andere parlementairen.

---

[69] Deze had in zijn 'manifest' naar Belgische personen verwezen en het document was ook verzonden naar een aantal Belgen, waaronder een Volksvertegenwoordiger van het Vlaams Belang. De VSSE wilde weten of er linken waren tussen de Noorse dader en de geciteerde Belgische namen.

Het Vast Comité I was in het algemeen van mening dat de manier waarop de VSSE de contacten met Bart Debie had voorbereid en afgehandeld voor weinig of geen kritiek vatbaar was. Zo werden de doelstellingen van de inlichtingengaring (bijvoorbeeld inzake de intenties van Bart Debie, de vermeende illegale activiteiten van Filip Dewinter en 'verdoken' financieringskanalen van zijn partij) door de Analysedienst duidelijk uiteengezet en door de Buitendiensten ter harte genomen. Er werd meermaals uitdrukkelijk in herinnering gebracht dat de verzamelde informatie betrekking moest hebben op activiteiten die verband (kunnen) houden met extremisme. De informatie moest bijvoorbeeld kunnen bijdragen tot het detecteren en analyseren van extremistische (xenofobe of racistische) tendensen binnen het Vlaams Belang en niet op de uitoefening van het parlementair mandaat *as such* van Filip Dewinter of van andere parlementairen. Dit werd ook meermaals duidelijk gemaakt aan de bron. In de rapporten kwamen soms wel namen voor van Vlaams Belang-parlementsleden, maar niet in relatie tot hun parlementaire activiteiten. Er werd overigens zelden of nooit verwezen naar de hoedanigheid van parlementslid. Het Comité moest wel vaststellen dat de medewerkers van de VSSE de limieten van hun optreden wat betreft parlementaire mandatarissen, niet steeds adequaat konden omschrijven, al voelden ze deze misschien intuïtief wel goed aan. De grenzen gesteld in de richtlijn van de informatie die mag ingewonnen worden als het om een politicus gaat, waren niet erg duidelijk.

Ten slotte stelde het Comité ook vast dat de materiële omstandigheden waarin de bron werd ontmoet, normaal waren. Er werden hem geen financiële voordelen gegeven, slechts één kleine attentie. In de loop van de gesprekken had Bart Debie ook persoonlijke problemen aangekaart. Hij kreeg geen erkenning om cursussen te geven aan ambulanciers en vroeg zich tevens af of hij in aanmerking zou kunnen komen voor herstel in eer en rechten voor een vroegere veroordeling. De betrokken commissaris van de VSSE liet aan zijn bron weten dat er volgens de door hem gecontacteerde persoon geen uitzonderingen werden gemaakt. Verder verstrekte hij hem enkel informatie die ook publiek toegankelijk was.

II.3.3. FILIP DEWINTER IN DE DATABANK VAN DE VSSE[70]

Uiteraard beschikte de VSSE reeds vóór haar contacten met Bart Debie over informatie met betrekking tot Filip Dewinter.[71] Zijn naam was in het datasysteem

[70] Op 11 februari 2013 was in de media een lijvig dossier te zien dat tijdens een interview op het bureau van de administrateur-generaal van de VSSE lag. Op de kaft stond de naam van 'Dewinter Philip'. Het Comité stelde vast dat het enkel ging om een bundel met procedurestukken, briefwisseling en nota's in verband met de vele procedures die de betrokkene had gevoerd om toegang te krijgen tot zijn dossier bij de VSSE.

[71] Ook de ADIV beschikte over informatie en inlichtingen met betrekking tot Filip Dewinter, maar in veel geringere mate dan de VSSE. Het 'dossier' Dewinter bij de ADIV was oud, weinig systematisch bijgehouden en voornamelijk samengesteld uit informatie afkomstig van open bronnen.

van de VSSE, dat sinds 2001 operationeel is[72], 214 maal gelinkt met bepaalde materies zoals 'extreemrechts', maar ook bijvoorbeeld met 'salafisme' of 'radicale islam'.[73] Ook de verslagen die naar aanleiding van de contacten met Bart Debie waren opgemaakt[74], werden in de databank opgenomen en gekoppeld aan *in casu* 'Extremisme' en 'Extreemrechts Nederlandstalig'. In 156 gevallen ging het om een 'pertinente link'; in 55 gevallen betrof het een link 'ter info'; drie linken waren 'te bepalen'. Het Comité stelde vragen bij de juiste betekenis van deze concepten[75] én bij de concrete toepassing ervan op het terrein.

Naast de koppeling van een naam aan een materie, zijn er ook de zogenaamde 'operationele linken' waarbij een verband wordt gelegd tussen twee namen en de relatie tussen beiden een kwalificatie krijgt in de zin van 'bevriend met', 'tegenstander van', 'kennis van', 'sympathisant van' …

Het Comité meende uit zijn analyse niet te moeten afleiden dat de VSSE een overdreven aandacht voor de betrokkene aan de dag zou hebben gelegd. Uit het relatief kleine aantal operationele linken dat werd gelegd tussen Filip Dewinter en derden – in totaal 50 op twaalf jaar tijd – blijkt dat de VSSE zeer behoedzaam tewerk is gegaan en geen belangrijke 'informatiepositie' ten aanzien van betrokkene heeft uitgebouwd. Het Vast Comité I was van mening dat de VSSE zich ter zake eerder schroomvallig heeft gedragen.

II.3.4. RAPPORTERING AAN DE MINISTER VAN JUSTITIE

Wat betreft de melding aan de minister van Justitie wanneer bepaalde politieke mandatarissen opgevolgd worden door de VSSE, waren twee richtlijnen van belang.[76] Enerzijds was er de instructie van de minister van Justitie van 25 mei 2009 inzake de rapportering van vermeldingen van federale parlementsleden. Anderzijds was er de interne instructie van 27 maart 2012 die betrekking had op ministers, de Staatssecretarissen en de verkozenen van het federale, het gemeenschaps- en het gewestelijke niveau. Op 8 juli 2010 werd betrokkene Gemeenschapssenator wat betekent dat beide richtlijnen van toepassing waren op de informatie die voortvloeide uit de contacten met Bart Debie. Eén uitzondering niet te na gesproken, werden ze echter niet opgevolgd wat betreft de informatie over Filip Dewinter.

---

72 In het informaticasysteem dat vóór 2001 operationeel was, kwam de naam van Filip Dewinter voor in 459 documenten. Mede gelet op het feit dat het verouderde informatie betrof, nam het Comité deze documenten niet op in zijn onderzoek.

73 Een link kon zowel betekenen dat men betrokken was bij een fenomeen maar ook dat men er slachtoffer van was.

74 Omdat het om een menselijke bron ging en gelet op het delicate karakter van de zaak, werden de gegevens die voortvloeiden uit de contacten opgenomen in een zogenaamde 'operatie'. Op die manier krijgen slechts die personen die uitdrukkelijk gemachtigd zijn tot het kennisnemen van een welbepaalde operatie, toegang tot de informatie uit de databank van de VSSE.

75 Zie ook II.4.2.3.

76 Zie ook Hoofstuk II.2.1.3 en II.4.2.1.3.

II.4. DE OPVOLGING VAN POLITIEKE MANDATARISSEN DOOR DE INLICHTINGENDIENSTEN

Net zoals het onderzoek naar '*Geheime nota's over Scientology in de pers*' (II.2) en '*Een informant binnen het Vlaams Belang?*' (II.3.) is ook dit toezichtonderzoek het gevolg van dezelfde twee in de pers verspreide geclassificeerde nota's van de Veiligheid van de Staat. In de (parlementaire) debatten die op de bekendmaking volgden, werd veelvuldig de vraag gesteld of en in welke mate de Belgische inlichtingendiensten politieke mandatarissen (mogen) opvolgen en welke regels ze daarbij in acht moeten nemen. Het Comité besliste daarop een thematisch onderzoek te openen '*naar de wijze waarop de inlichtingendiensten informatie verzamelen over politieke mandatarissen, de wijze waarop ze met deze informatie omgaan en analyseren en de wijze waarop ze hierover rapporteren aan de bevoegde overheden*'.

Het was overigens niet voor het eerst dat het Vast Comité I de activiteiten van de inlichtingendiensten ten aanzien van politieke mandatarissen onderzocht.

Al in 1997 werd een onderzoek geopend '*naar de manier waarop de inlichtingendiensten het onderscheid maken tussen de activiteiten van parlementsleden als milieupacifisten en als parlementsleden*'.[77] Het onderzoek kwam er na een vraag van een Ecolo-parlementslid en spitste zich toe op de inlichtingen die de VSSE en de ADIV gebeurlijk over mandatarissen van Ecolo of Agalev (thans Groen!) zouden verzamelen. Het Comité kwam tot de conclusie dat de diensten dossiers hadden op de naam van een aantal parlementsleden van deze partijen, maar dat de activiteiten van deze personen sinds 1988 niet meer in het bijzonder gevolgd werden.

Een jaar later, in 1998, startte het Vast Comité I in het verlengde van voormeld onderzoek een meer algemene enquête over '*de verzameling van gegevens over parlementsleden door de inlichtingendiensten*'.[78] Dit onderzoek had betrekking op de mandatarissen van *alle* politieke partijen. Het Comité kwam in deze tot de conclusie dat '*noch de VSSE noch SGR onderzoek instellen naar handelingen die in het kader van de eigenlijke uitoefening van het parlementair mandaat worden gesteld*'.

In 2006 ten slotte kwamen de zogenaamde 'gereserveerde dossiers' bij de VSSE aan de oppervlakte.[79] Klaarblijkelijk werden sinds het eind van de jaren '80 een aantal dossiers met gegevens over verkozenen bijgehouden door de dienst 'Affaires Générales' van de VSSE, en dit buiten het 'normale circuit'. Sommige van deze dossiers werden zelfs exclusief op het secretariaat van de toenmalige administrateur-directeur-generaal van de Openbare Veiligheid bewaard. Het Comité besloot in dit onderzoek onder meer dat '*het actueel voorkomen van politieke mandatarissen en prominenten in de nu geïnformatiseerde rapporten van een inlichtingendienst een uiterst delicaat gegeven blijft. Het Comité was echter van mening dat de hoedanigheid van een prominent of politicus geen beletsel kan zijn voor een ade-*

[77] VAST COMITÉ I, *Activiteitenverslag 1998,* 67 e.v.
[78] VAST COMITÉ I, *Activiteitenverslag 1999*, 12 e.v.
[79] VAST COMITÉ I, *Activiteitenverslag 2008*, 23 e.v.

quate opvolging en van een navenante beschikbaarheid van de rapportering hierover in het licht van de uitvoering van de wettelijke opdrachten van een inlichtingendienst. Deze activiteit dient immers te gebeuren 'zonder onderscheid des persoons'.'[80] In het verlengde hiervan deed het Comité volgende aanbeveling: *'Meer in het algemeen wenst het Vast Comité I dat de Veiligheid van de Staat klare en eenduidige richtlijnen uitwerkt met betrekking tot de inwinning, de verwerking, de raadpleging (met inbegrip van de eventuele interne afscherming), de opslag en de archivering van gegevens van bepaalde categorieën van personen die bijzondere verantwoordelijkheden dragen of droegen. Bij de uitwerking van deze richtlijnen en bij de concrete opvolging van de (gewezen) politieke mandatarissen dient de Veiligheid van de Staat rekening te houden met de krijtlijnen uitgetekend in het arrest van het Europees Hof voor de Rechten van de Mens in de zaak Segerstedt-Wiberg and others'*.[81]

II.4.1. ENKELE CIJFERGEGEVENS UIT HET NIEUWE ONDERZOEK

Op 1 maart 2013 waren er precies – dubbelmandaten buiten beschouwing gelaten – 479 personen die ofwel een ministerpost bekleedden in de federale of regionale regeringen of die verkozen waren als parlementslid van een regionale of federale, wetgevende vergadering. In zijn toezichtonderzoek vroeg het Comité aan beide inlichtingendiensten om na te gaan of en in welke mate de namen van deze personen in hun papieren dossiers en databanken voorkwamen.

Daaruit bleek dat de Buitendiensten van de VSSE vanaf juni 2010 (of met andere woorden, vanaf de start van de toenmalige federale legislatuur) tot begin 2013 727 documenten hadden opgesteld waarin telkenmale minstens één van de 479 mandatarissen werd vernoemd. In totaal werden 142 verschillende mandatarissen vernoemd.[82]

De Analysedienst van de VSSE telde over dezelfde periode 423 documenten waarin 93 verschillende politieke mandatarissen waren vermeld. Iets meer dan de helft van deze documenten waren afkomstig van externe bronnen (bijvoorbeeld

---

80 VAST COMITÉ I, *Activiteitenverslag 2008*, 30 e.v.

81 VAST COMITÉ I, *Activiteitenverslag 2008*, 110-111. In de zaak *Segerstedt-Wiberg and others* tegen Zweden van 6 juni 2006 problematiseerde het Hof het inwinnen en opslaan van gegevens over politieke opinie, verwantschap en lidmaatschap van personen en dit in het licht van artikel 8 EVRM. Het feit dat dergelijke gegevens, ook al betreffen het publiek gekende feiten, worden ingezameld of bijgehouden is een ernstige inmenging in het privéleven. Deze inmengingen kunnen – aldus het Hof – alleen gerechtvaardigd zijn wanneer zij proportioneel zijn vanuit het perspectief van de nationale veiligheid. Bij de beoordeling van deze proportionaliteit hechtte het Hof zeer veel belang aan het al dan niet gewelddadige karakter van een politieke partij. Dit karakter mag niet alleen afgeleid worden uit het politieke programma; het moet zich eveneens vertalen in de acties van de partijleiders en de posities die zij innemen.

82 Sommigen kwamen in meerdere documenten voor: 37% van de mandatarissen kreeg één vermelding, 35% twee tot vijf vermeldingen. Vier mandatarissen kwamen in meer dan 21 documenten voor. Eén verkozene werd in 91 documenten vermeld.

het OCAD, de politie of andere correspondenten); de andere helft vormde 'eigen productie'. Het betrof documenten voor intern gebruik (synthesenota's met een stand van zaken in een bepaald dossier en verslagen van vergaderingen), documenten bedoeld voor externen (nota's gericht aan Belgische autoriteiten en – slechts enkelen – aan buitenlandse overheden) en 'kantschriften' waarin de Analysedienst bepaalde vragen stelde aan de Buitendiensten.

Het Comité nam een steekproef van deze documenten[83] en bestudeerde ze om een zicht te krijgen op het collecte- en analysewerk van de VSSE ten aanzien van politieke mandatarissen (*infra*).

De ADIV[84] van zijn kant beschikte zowel over informatie op papieren als op digitale dragers. Zo bijvoorbeeld waren 115 steekkaarten beschikbaar die correspondeerden met een papieren dossier van politieke mandatarissen. Het grootste deel van de bijhorende dossiers was echter reeds vernietigd. In het zogenaamde 'levend' archief bevonden zich slecht 36 dossiers en in het 'dood' archief (omdat ze gedurende vijftien jaar niet meer waren geraadpleegd) nog 12.

In de databank van de ADIV werden de namen van 109 mandatarissen gevonden. Het Vast Comité I bestudeerde één vierde van deze dossiers. Daarbij bleek dat bijvoorbeeld nooit vermeld werd of een persoon al dan niet parlementslid was.

De ADIV had in de referteperiode van het toezichtonderzoek geen analysenota's opgesteld die specifiek op ministers of parlementaire mandatarissen betrekking hadden.

II.4.2. DE OPVOLGING VAN POLITICI DOORHEEN DE INLICHTINGENCYCLUS

Het Comité overliep bij zijn analyse van de geselecteerde dossiers alle aspecten van de inlichtingencyclus, te beginnen bij 'de sturing van de inlichtingenactiviteiten' over 'de collecte', 'de organisatie van de informatie' en 'de analyse' tot aan 'de verspreiding van de inlichtingen'.

II.4.2.1. Sturing van de inlichtingenactiviteiten

De activiteiten van de Belgische inlichtingendiensten worden op verschillende niveaus aangestuurd. Het meest algemene niveau is dat van de regelgeving – te weten wetten, besluiten en algemene instructies – waarbij bepaald wordt welke inlichtingenactiviteiten mogen worden uitgevoerd en op welke manier dit mag geschieden. Daaronder bevindt zich het niveau van de jaarlijkse actie- of inlichtingenplannen die – op voorstel van de diensten en goedgekeurd door de bevoegde

83 Eén op de vier dossiers werd bestudeerd. Hierop werd één uitzondering gemaakt: de nota's die bestemd waren voor buitenlandse overheden werden allemaal in de analyse betrokken.

84 Meer bepaald de Divisie C(ounter) I(ntelligence) die bevoegd is voor interne dreigingen.

minister – *in concreto* bepalen welke materies het komende jaar mogen of moeten bestreken worden. Ten slotte is er de *ad hoc* aansturing in concrete dossiers door het diensthoofd of de bevoegde minister. Deze drie niveaus worden hieronder besproken.

II.4.2.1.1. Regels van toepassing op het verzamelen van inlichtingen met betrekking tot politieke mandatarissen

De Wet van 30 november 1998 houdende regeling voor de inlichtingen- en veiligheidsdienst (W.I&V) bevat geen bepaling die aan een parlementslid een bijzonder statuut zou verlenen. In de wet wordt overigens geen verwijzing gemaakt naar politieke mandatarissen. Hetzelfde geldt voor de BIM-Wet van 4 februari 2010 die niet voorziet in een bijzondere bescherming voor politici, terwijl ze dat wél doet voor beroepsjournalisten, advocaten en artsen. Vanuit die optiek herhaalde het Comité zijn stelling uit 2008 dat de hoedanigheid van politicus geen beletsel kan zijn voor een adequate opvolging en rapportering. Het inlichtingenwerk dient immers te gebeuren 'zonder onderscheid des persoons'. Wel moet bij de eventuele opvolging rekening worden gehouden met de rechtspraak van het Europees Hof voor de Rechten van de Mens inzake vrijheid van meningsuiting en de vrijheid van vereniging. Er dient uiterst omzichtig te worden omgesprongen met een inmenging in deze grondrechten ten aanzien van (zelfs extreme) politieke partijen en mandatarissen.

Vanuit het besef dat de opvolging van politieke partijen of mandatarissen bijzonder gevoelig is, werd in 2001 een specifieke beperking ingebouwd voor de opvolging van parlementaire mandatarissen van het toenmalige Vlaams Blok[85]: in de ministeriële richtlijn van 15 mei 2001 waarbij de opdracht werd gegeven om die partij op te volgen, werd gesteld dat dit moet gebeuren met uitzondering van de activiteiten van de mandaterissen gesteld in het kader van hun parlementair mandaat. De VSSE definieerde deze beperking verder als volgt: '*een parlementair mandaat*' is '*de meningsuiting, de parlementaire vragen en interpellaties, het indienen van een wetsvoorstel, kortom wat zich in het parlementair halfrond afspeelt*'.

Sindsdien is deze definitie – waarvan men zich kan afvragen of ze (nog) voldoende gekend was, of ze van toepassing is buiten de mandatarissen van de betrokken partij om én of ze voldoende pertinent en duidelijk is – nooit expliciet herhaald, verfijnd of genuanceerd. Wel greep de minister van Justitie er in 2013 naar terug in haar antwoorden op enkele parlementaire vragen: activiteiten van een parlementslid '*binnen het parlement zelf*', in het kader van hun '*parlementaire functie*' of '*in hun optreden als parlementslid*' mogen niet opgevolgd worden door een inlichtingendienst.[86] Maar ook deze 'preciseringen', die dateerden van na de

[85] Zie hierover Hoofdstuk II.3.

[86] *Hand*. Senaat, 21 februari 2013, nr. 5-92, 16-18 en *Hand*. Senaat, 14 maart 2013, nr. 5-95, 17-19.

opstart van voorliggend toezichtonderzoek, namen volgens het Comité niet alle vragen weg. Immers, in de praktijk is het onderscheid tussen de activiteiten van een parlementaire mandataris binnen zijn of haar mandaat en erbuiten, moeilijk te handhaven. Daarenboven vallen bepaalde aspecten buiten de *scoop* van deze beperking (zoals bijvoorbeeld de rol van een parlementslid bij de interne partijwerking en de bepaling van de partijstrategie), terwijl ze net veel 'gevoeliger' zijn dan het louter stellen van een parlementaire vraag of het indienen van een wetsvoorstel (hetgeen informatie betreft die per definitie publiek is).

Het Comité herhaalde dan ook de aanbeveling uit zijn onderzoek 'gereserveerde dossiers'[87] om klare en eenduidige richtlijnen uit te werken met betrekking tot inlichtingenactiviteiten van bepaalde categorieën van personen die bijzondere verantwoordelijkheden dragen of droegen.

Uiteraard geldt de noodzaak van een omvattende, duidelijke richtlijn ook voor de ADIV. Immers, deze dienst hanteerde ten tijde van het onderzoek nog steeds een instructie die dateerde van vóór de Wet van 30 november 1998. In een nota van 25 juni 1998 wordt uiteengezet dat politieke mandatarissen niet opgevolgd mogen worden uit hoofde van hun mandaat, maar dat ze, net zoals ieder ander burger, de aandacht van de ADIV kunnen weerhouden wanneer ze een veiligheidsmachtiging nodig hebben, wanneer ze deel uitmaken van een organisatie die een bedreiging vormt voor de opdrachten van Defensie of wanneer ze een militair domein trachten binnen te dringen of de activiteiten van Defensie trachten te belemmeren.

II.4.2.1.2. Opname van politieke partijen in de jaarlijkse actie- of inlichtingenplannen

In 2013 kwamen geen in het Parlement vertegenwoordigde politieke partijen meer voor in de jaarlijkse actie- of inlichtingenplannen van respectievelijk de VSSE en de ADIV. Voordien werden, wat de Veiligheid van de Staat betreft, bepaalde partijen systematisch vermeld als *target*, en dit soms op expliciet verzoek van de bevoegde minister (zie II.4.2.1.1).

Ook al werden er in 2013 geen in het Parlement vertegenwoordigde politieke partijen *as such* opgevolgd, toch was het Vast Comité I van oordeel dat ook hieromtrent klare en eenduidige richtlijnen zouden moeten worden uitgewerkt.

II.4.2.1.3. *Ad hoc*-sturing door minister van Justitie: een toepassingsmodaliteit van de richtlijn van 25 mei 2009

Op 2 mei 2009 had de toenmalige minister van Justitie in het Parlement aangekondigd dat '*de Veiligheid van de Staat hem telkens een waarschuwingsnota […] ter informatie zal sturen voor een actief federaal parlementslid dat werd vermeld of*

87 VAST COMITÉ I, *Activiteitenverslag 2008*, 110-111.

gelieerd is met een specifieke materie in een dossier als onderdeel van informatie of als persoon het voorwerp uitmaakt van bedreigingen ten overstaan van zijn persoon of als een buitenlandse inlichtingendienst interesse betoont in hem'.[88] In uitvoering hiervan gaf de minister op 25 mei 2009 zijn goedkeuring aan een instructie die gebaseerd was op een ontwerp van de VSSE. Deze richtlijn hield in dat de minister een '*note d'avertissement*' zou ontvangen '*pour tout parlementaire fédéral en activité cité pour information ou lié à une matière spécifique dans un rapport, en tant qu'élément d'information, ou qui fait l'objet de l'attention de la Sûreté de L'Etat comme personne menacée ou encore comme cible de l'intérêt d'un agent de renseignement étranger, ces citations ou liens réalisés dans l'exercice des compétences de la Sûreté de l'Etat. L'avertissement serait envoyé à Monsieur le Ministre sous la forme d'une note classifiée 'Secret – Loi 11.12.1998' pour tout parlementaire fédéral cité ou lié dans un rapport produit par la Sûreté de l'Etat. […] La Sûreté de l'Etat poursuivra son activité de surveillance de manière normale (silent procedure), sauf avis contraire de Monsieur le Ministre de la Justice.*'[89]

In 2013 stelde de toenmalige administrateur-generaal van de VSSE hierover het volgende: '*Grosso modo bevat de richtlijn drie aspecten. De belangrijkste vernieuwing betrof de onmiddellijke inkennisstelling van de minister van Justitie telkens de naam van een actief federaal parlementslid in een verslag van de VSSE voorkomt. De VSSE en de minister kwamen hiermee tegemoet aan de ongerustheid die bij sommige federale parlementsleden was gerezen naar aanleiding van het toezichtonderzoek van het Vast Comité I naar de zogenaamde 'gereserveerde dossiers'.*'[90] De administrateur-generaal wees er op dat deze werkwijze tevens toelaat dat de minister zijn verantwoordelijkheid kan opnemen door desgewenst bijkomende, punctuele bevelen aan de VSSE te geven. Ook kan hij toezicht houden op het inlichtingenonderzoek, eventueel via het Vast Comité I. Ten slotte laat een in kennisstelling de minister van Justitie toe te antwoorden op vragen van parlementsleden die gebruik maken van hun grondwettelijk controlerecht. Hierdoor wordt volgens de administrateur-generaal tegemoet gekomen aan de eisen van een parlementaire democratische rechtsstaat.

---

88 VAST COMITÉ I, *Activiteitenverslag 2009*, 3.

89 *'voor elk actueel, federaal parlementslid die 'ter informatie' of die gelinkt aan een specifieke materie vermeld wordt in een rapport, als informatief element, of die voorwerp uitmaakt van de aandacht van de VSSE, als bedreigd persoon of nog, als target van een buitenlandse inlichtingenagent, moeten deze vermeldingen of verbanden gerealiseerd worden in het kader van de uitoefening van de bevoegdheden van de VSSE. De verwittiging zal naar de minister van Justitie worden gezonden onder de vorm van een 'GEHEIM – Wet 11.12.1998' geclassificeerde nota en dit voor elk federaal parlementslid die geciteerd of gelinkt wordt in een verslag opgesteld door de VSSE. […] De VSSE zal zijn opvolgingsactiviteit op een normale manier verderzetten (silent procedure), behoudens anders beslist door de Heer minister van Justitie*' (vrije vertaling).

90 A. WINANTS, '*Control in the circus*. Interne controle bij de Veiligheid van de Staat' in *Inzicht in toezicht. Twintig jaar democratische controle op de inlichtingendiensten*, W. VAN LAETHEM en J. VANDERBORGHT (eds.), Antwerpen, Intersentia 2013, 137.

Naar het oordeel van het Vast Comité I verwoordde de administrateur-generaal zeer goed het belang van de richtlijn van 2009. Het Comité had deze instructie overigens reeds positief onthaald. In zijn *Activiteitenverslag 2009* stelde het dat '*op die wijze reeds ten dele tegemoet gekomen wordt aan de bekommernissen van het Vast Comité I*', geuit in het kader van het onderzoek 'gereserveerde dossiers'.[91]

Echter, sinds juni 2010 (met andere woorden, op een ogenblik dat de instructie ongeveer één jaar van kracht was) waren binnen de VSSE al een 350-tal[92] verslagen en nota's opgesteld waarin de naam werd vermeld van op dat ogenblik actieve federale parlementsleden, terwijl hiervan slechts uitzonderlijk melding was gemaakt op de voorgeschreven wijze … Dat de instructie nauwelijks werd nageleefd, werd blijkbaar ook nooit opgemerkt, gemeld, gecontroleerd en/of geproblematiseerd intern de dienst. Het Vast Comité I wees er in zijn toezichtonderzoek overigens op dat de richtlijn niet volledig *kon* worden nageleefd alleen al omwille van het feit dat de VSSE niet beschikte over een (permanent ge-update) lijst van alle politieke mandatarissen. Gevolg was onvermijdelijk dat soms verslagen werden opgesteld over parlementsleden, zonder dat men noodzakelijkerwijs weet had van hun statuut.

In de loop van het toezichtonderzoek stelde de VSSE een aantal wijzigingen voor aan zijn werkprocessen. Zo onder meer wat betreft de verwittiging van de vermelding van parlementsleden in zijn verslagen. In dit werkdocument stelde de VSSE voor om de minister maandelijks (en dus niet langer onmiddellijk) in kennis te stellen wanneer parlementsleden vermeld worden in documenten van de Analysedienst (en dus niet langer van de Buitendiensten). Dit werkdocument resulteerde na het afsluiten van het onderzoek van het Comité in een nieuwe instructie (zie Hoofdstuk I.1.3).

II.4.2.2. De collecte

Het Vast Comité I benadrukte dat het merendeel van de meldingen van parlementsleden in collecteverslagen van de VSSE ingegeven was ofwel door het feit dat de betrokken mandataris zelf het voorwerp was van een mogelijke bedreiging, ofwel omdat hij (toevallig) in contact kwam met een persoon of een groepering die wordt opgevolgd. Het Comité vond geen aanwijzingen dat de VSSE politieke mandatarissen viseerde om redenen buiten de wettelijke opgesomde belangen en bedreigingen om.

Wat de ADIV betreft, kon dezelfde conclusie getrokken worden: de dienst vertoonde geen interesse voor politieke mandatarissen *as such*. Wanneer de ADIV uitzonderlijk aandacht besteedde aan mandatarissen, dan gebeurde dit in relatie

---

91 VAST COMITÉ I, *Activiteitenverslag 2009*, 3.

92 Het in II.4.1 vermelde aantal van 727 documenten betreffen mandatarissen van zowel federale als regionale regeringen en assemblees, terwijl het *in casu* enkel federale mandatarissen betreft.

tot een militair belang of een militaire materie. Het merendeel van de ADIV-dossiers was overigens reeds geopend lang voordat de betrokken politicus een mandaat had opgenomen. Ook dit toonde aan dat het 'politieke mandaat' niet relevant was voor de aandacht van de ADIV.

Het Vast Comité I vond bij de VSSE op het niveau van de collecte in zijn steekproef slechts één dossier waaruit kon worden opgemaakt dat gegevens waren verzameld over elementen die mogelijks kaderden 'binnen het parlementair mandaat' zoals omschreven in de bovenvermelde richtlijn van 25 mei 2001 en zich 'binnen het parlement zelf' (*in casu* weliswaar een parlement van een deelstaat) afspeelde. Het betrof informatie die de VSSE had ontvangen over een vergadering die een politieke partij had georganiseerd met een buitenlandse politieke beweging dewelke een bedreiging zou kunnen uitmaken. Dit voorbeeld illustreerde voor het Comité opnieuw dat de in de richtlijn opgesomde criteria weinig nuttig en werkbaar zijn. Immers, enerzijds beperken politieke activiteiten zich niet tot het halfrond en anderzijds lijken er geen goede redenen voorhanden te zijn om dreigingen die zouden voorbereid worden vanuit het parlement, niet op te volgen. Het Vast Comité I was dan ook van oordeel dat deze criteria moesten herbekeken worden.

Dat het Comité geen elementen vond die wezen op een onrechtmatige opvolging van parlementsleden, betekende evenwel niet dat daarmee ook het nut van alle gecollecteerde data was aangetoond. Het Comité kon niet voorbij aan het feit dat een deel van de informatie eerder 'banaal' was: politicus A gaat eerst even persoon B groeten vooraleer weg te gaan; politicus C is aanwezig op een meeting waar duizend mensen aanwezig zijn; politicus D nam deel aan de manifestatie, maar kwam pas op het eind ervan toe… Soms is de link met een van de wettelijk omschreven belangen en dreigingen op het eerste zicht dan ook onduidelijk.

Het Comité is zich weliswaar bewust van het feit dat het in het inlichtingenwerk niet steeds evident is om op het moment van de collecte zelf, meteen uit te maken welke informatie al of niet relevant zal blijken. Dit neemt niet weg dat de eisen ter zake – zoals die omschreven zijn in de W.I&V en de Privacywet (doelbindingsprincipe, adequaatheid, correctheid…) – moeten nageleefd worden. Of en op welke wijze een bepaald feit in een collecteverslag wordt opgenomen, vormt dus een cruciaal gegeven. Het Comité was van oordeel dat de wijze waarop die *input* dient te gebeuren het voorwerp zou moeten zijn van permanente vorming alsook een reële kwaliteitsbewaking. In ditzelfde kader benadrukte het Comité dat uit een verslag duidelijk moet blijken of een persoon ten aanzien van een bepaalde dreiging bijvoorbeeld 'slachtoffer', 'actor' dan wel 'passant' is.

II.4.2.3. Organisatie van de informatie

De databank van de VSSE bevat uiteraard een bijzonder groot aantal gegevens over personen, groeperingen, plaatsen en gebeurtenissen (entiteiten). Om de exploitatie van deze gegevens mogelijk te maken, worden ze 'gelinkt' aan één of meerdere van de wettelijk op te volgen dreigingen zoals extremisme, proliferatie, inmenging… Dit worden 'motiveringen' genoemd. Er zijn vier soorten 'links' mogelijk: 'Voor info', 'Te bepalen', 'Pertinente link' of 'Operationele link'. Een 'Pertinente link' geeft aan dat het verband met één van de materies of dreigingen concreet en overduidelijk is.[93] De link is 'Te bepalen' wanneer nog niet werd uitgemaakt of er al dan niet een pertinente link is. De juiste draagwijdte van de twee andere links is echter minder duidelijk. 'Voor info' wordt nu eens omschreven als een *'link voor entiteiten die geen band hebben met één van de materies of dreigingen die de VSSE behandelt'* en dan weer als *'een link die duidt op een nog niet gekwalificeerde of op een passieve betrokkenheid (bijvoorbeeld als voorwerp van de dreiging)'*. Het Comité moest dan ook vaststellen dat deze concepten niet eenduidig worden omschreven en toegepast. Hierdoor dreigt het inlichtingenwerk aan doelmatigheid en doeltreffendheid te verliezen. Immers, het risico bestaat dat niet (al) de juiste verslagen 'aan de oppervlakte komen' wanneer dit nodig is met het oog op het analysewerk. Mogelijks worden zo verkeerde conclusies getrokken. Het Vast Comité I was dan ook de mening toegedaan dat de VSSE deze concepten dringend moet herbekijken. De dienst zou daarbij ook de mogelijkheid moeten inbouwen om de (vermoedelijke) rol van een in een verslag vernoemd persoon ten aanzien van de dreiging aan te duiden: is hij een 'voorbijganger', een 'mogelijk slachtoffer', een 'sleutelfiguur', een 'actor'…

II.4.2.4. De analyse

Het Vast Comité I vond geen indicaties dat de analysediensten van beide inlichtingendiensten op onwettige wijze aandacht zouden hebben besteed aan ministers en parlementairen.[94] In twee voorgaande onderzoeken (zie II.2 en II.3) werd

---

93 Volgens de richtlijn van 27 maart 2012 mogen ministers en politieke mandatarissen in functie alleen het voorwerp zijn van een 'pertinente link' wanneer uit de informatie van het verslag blijkt dat zij actief betrokken zijn bij een dreiging tegen het voortbestaan van de democratische en van de grondwettelijke orde. Zij kunnen het voorwerp zijn van een 'link voor info' wanneer uit de informatie van het verslag blijkt dat zij het voorwerp zijn van een dreiging of wanneer zij actief betrokken zijn bij een dreiging tegen een van de andere materies waarover de VSSE inlichtingen inwint. Wanneer de opsteller van een verslag meent dat er op basis van de informatie van het verslag voor een minister of een politiek mandataris in functie een pertinente link of een link ter info moet worden gelegd, dan overlegt hij daarover met zijn sectiechef.

94 Slechts in één dossier vond het Comité een verslag dat informatie bevatte die betrekking had op 'parlementaire activiteiten in het parlement'. De informatie was opgetekend door een medewerker van de VSSE die op uitnodiging aanwezig was op een gesloten vergadering in het

reeds aangetoond dat de VSSE zich bewust was van het delicate karakter van het inlichtingenwerk wanneer het politieke mandatarissen betreft. Hetzelfde gold voor de Dienst Analyse van de ADIV-CI.

Wel merkte het Comité op dat ook de analysediensten in hun rapportage de nodige aandacht moeten besteden aan de 'positie' van een in een verslag vermeld persoon ten aanzien van de dreiging ('slachtoffer', 'actor', 'passant'…).

II.4.2.5. De verspreiding van inlichtingen

Het Comité stelde vast dat de ADIV in de referteperiode geen documenten had verspreid naar andere diensten waarin de naam van een minister of een parlementair was vermeld.

De VSSE daarentegen had wel dergelijke nota's gezonden aan Belgische autoriteiten. Het Comité wees er evenwel op dat het net een kerntaak is van deze dienst om de bevoegde autoriteiten in kennis te stellen wanneer iemand het voorwerp is van een bedreiging of zelf aan een bedreiging meewerkt (art. 19 W.I&V), ook al betreft het een Belgisch politicus. Wel moeten bij de verspreiding van deze inlichtingen buiten de VSSE de *need to know* en de eisen van voornoemd artikel 19 W.I&V richtinggevend zijn. Het Vast Comité I had dit zo reeds gesteld in een eerder onderzoek.[95] Dit principe en deze wettelijke bepaling gelden ongeacht de bestemmeling: parket, federale overheidsdiensten, Eerste minister en vakministers, ministers uit de deelregeringen, de Koning als Staatshoofd… Maar uiteraard ook wanneer een buitenlandse dienst bestemmeling is. In dit kader kon het Comité vaststellen dat de VSSE de nodige terughoudendheid aan de dag legde waar het ging om het meedelen van bedoelde verslagen aan buitenlandse diensten. Deze terughoudendheid uitte zich op verschillende manieren: het beperkte aantal mededelingen, de aard van de informatie en de landen waaraan deze informatie werd meegedeeld. Desondanks benadrukte het Comité dat steeds zorgvuldig moet worden afgewogen of namen van Belgische politieke mandatarissen (maar ook van gewone burgers) kunnen vermeld worden in documenten die bestemd zijn voor buitenlandse diensten. Het principe van de *need to know* en de eis van artikel 19 W.I&V is daarbij eens te meer richtinggevend. Maar bij doorgifte van persoonsgegevens naar het buitenland spelen nog andere eisen, zoals bijvoorbeeld deze vermeld in de Privacywet. Het Vast Comité I benadrukte in dit kader opnieuw het belang van een nadere precisering door het Ministerieel Comité voor inlichting en veiligheid van de draagwijdte van artikel 19 W.I&V.

---

parlement. Het verslag was bestemd voor de minister van Justitie. Het Comité stelde zich opnieuw de vraag of het de bedoeling kon zijn dat dergelijke verslaggeving niet toegelaten zou zijn. Het Comité oordeelde dat het de bevoegde minister toekomt om hieromtrent een beslissing te nemen.

95 Zie Hoofdstuk II.2.'Geheime nota's over de Scientologykerk in de pers'.

II.5. DE INFORMATIEPOSITIE VAN DE VEILIGHEID VAN DE STAAT TEGENOVER EEN INTERNATIONALE TRANSACTIE VAN EEN BELGISCH BEDRIJF

II.5.1. EEN KLACHT OVER EEN GEWEIGERDE UITVOERVERGUNNING

Eind 2011 beklaagden vertegenwoordigers van een firma naar Belgisch recht, gespecialiseerd in de productie van hoogtechnologisch materiaal, zich over de weigering van de bevoegde minister om een uitvoervergunning toe te kennen voor een isostatische warmtepers.[96] Nochtans was het land van bestemming partij bij het non-proliferatieverdrag.[97] Daarenboven kreeg het bedrijf volgens de klagers eerder wél een uitvoervergunning voor hetzelfde product naar hetzelfde land. De weigering zou het gevolg zijn van de druk die een buitenlandse regering uitoefende op de Belgische instanties. Naar het oordeel van de klagers was er sprake van een inmenging die nefast was voor hun economische belangen.

Begin 2012 besliste het Vast Comité I een toezichtonderzoek te openen naar de informatiepositie van de VSSE met betrekking tot deze bewuste transactie zowel in het kader van de strijd tegen proliferatie als in het kader van de bescherming van het wetenschappelijk en economisch potentieel van het land.[98]

Het betrof overigens het derde toezichtonderzoek van het Comité waarin de firma betrokken was. Reeds in 2005 werd onderzocht hoe de VSSE informatie afkomstig van een buitenlandse dienst had verwerkt met betrekking tot de uitvoer van een isostatische warmtepers naar Iran.[99] Het Vast Comité I kwam toen tot het besluit dat de VSSE blijk had gegeven van een zekere nonchalance in de manier waarop ze deze informatie had behandeld, geanalyseerd en verspreid.

In 2011 werd een tweede onderzoek afgrond naar de manier waarop de bewuste firma werd opgevolgd door de VSSE.[100] De conclusie luidde dat de dienst

---

96 Een isostatische warmtepers is een machine die tot doel heeft de weerstand en duurzaamheid van sommige materialen te versterken door ze bij hoge warmte onder zeer hoge druk te plaatsen. Dergelijke persen worden gebruikt in de luchtvaartindustrie, maar kunnen ook dienen bij de productie van raketten en kernwapens. Het betreft een zogenaamd product 'voor tweeërlei gebruik' ('*dual use*'), te weten burgerlijk en/of militair, waarvan de uitvoer is onderworpen aan de controlemaatregelen zoals voorzien in de richtlijnen 1334/2000 en 428/2009 van de Raad van de Europese Unie.

97 'Treaty on the non-proliferation of nuclear weapons', zie: www.un.org/disarmament/WMD/Nuclear/pdf/NPTEnglishText.pdf.

98 Het Comité bevroeg hierbij niet alleen de VSSE, maar ook twee belangrijke actoren op het vlak van de uitvoering van het Belgische non-proliferatiebeleid, te weten Théo Van Rentergem, voorzitter van de Commissie van advies voor de niet-verspreiding van kernwapens (CANVEK) en Werner Bauwens, speciaal gezant voor ontwapening en non-proliferatie van de FOD Buitenlandse Zaken. Het eindverslag werd goedgekeurd in november 2013.

99 VAST COMITÉ I, *Activiteitenverslag 2005*, 8-27.

100 VAST COMITÉ I, *Activiteitenverslag 2011*, 37-40.

sommige transacties met één of meerdere gevoelige landen wel aandachtig had gevolgd, maar dat deze opvolging voornamelijk reactief en *ad hoc* was: ze vond slechts plaats in functie van informatie die door buitenlandse inlichtingendiensten werd aangeleverd. Positief was evenwel dat de VSSE niet alleen oog had voor de veiligheidsbelangen in verband met de ontwikkeling van chemische, bacteriologische of nucleaire wapens, maar ook voor de problematiek van de mededinging en voor signalen die wezen op mogelijke buitenlandse inmenging.[101] Hierbij was het Comité, net zoals de VSSE, van oordeel dat in de strijd tegen proliferatie het veiligheidsbelang voorrang moet krijgen op het economisch belang van een onderneming.

II.5.2. DE VASTSTELLINGEN

Via het secretariaat van de Commissie van advies voor de niet-verspreiding van kernwapens (CANVEK)[102], kreeg de VSSE op 1 februari 2011 kennis van de geplande uitvoer van een isostatische warmtepers. Het dossier stond immers geagendeerd op de eerstvolgende vergadering van de CANVEK, en daarin zetelt een analist van de VSSE. De VSSE verwonderde er zich over dat zij niet eerder door de firma zelf op de hoogte was gesteld van de voorgenomen uitvoer. Immers, in januari 2011 had de dienst tot tweemaal toe contact met een kaderlid van de firma en dit net met de bedoeling om informatie uit te wisselen over eventuele delicate dossiers die aan de CANVEK zouden worden voorgelegd. Deze contacten wezen er volgens het Comité op dat de VSSE ondertussen een meer proactieve houding had aangenomen tegenover de betrokken firma. Maar aangezien deze laatste *in casu* had nagelaten de VSSE in kennis te stellen, was de opvolging in dit dossier opnieuw reactief.

Onmiddellijk nadat de VSSE kennis had gekregen van de geplande transactie, werden enkele verificaties verricht bij buitenlandse partnerdiensten. De informatie van deze correspondenten alsook de contextuele elementen uit een open bronnenanalyse, resulteerden in een synthesenota over de situatie bij de firma. Deze nota werd begin 2011 verzonden naar de minister van Justitie.

In maart 2011 verzond de VSSE ook twee geclassificeerde nota's naar de CANVEK en naar de FOD Economie. Daarin zette de dienst de elementen uiteen die er op wezen dat de eindgebruiker van de warmtepers in verband kon worden

---

101 De analyses van de VSSE hebben doorgaans betrekking op zowel de bescherming van het wetenschappelijk en economisch potentieel als op proliferatie. Het is echter niet de taak van de CANVEK om rekening te houden met de economische aspecten verbonden aan de dossiers die haar worden voorgelegd.

102 Zie meer over de samenstelling en de bevoegdheden van deze Commissie: Koninklijk besluit van 12 mei 1989 betreffende de overdracht aan niet-kernwapenstaten van kernmaterialen, kernuitrustingen, technologische kerngegevens en hun afgeleiden (*BS* 15 juni 1989) en het Huishoudelijk reglement van de Commissie voor advies voor de niet-verspreiding van kernwapens (*BS* 8 februari 2010).

gebracht met een entiteit die in het verleden betrokken was bij een militair nucleair programma.

Op de vergaderingen van de CANVEK liet de VSSE verstaan dat het om een delicaat exportdossier ging. In haar voorzichtige en genuanceerde analyse formuleerde zij vooral hypothesen en vermoedens, en dit bij gebrek aan nauwkeuriger informatie.[103] Uit elementen die door andere commissieleden werden aangedragen, bleek dat de overheden van het land van bestemming terughoudend waren om bijkomende inlichtingen te verstrekken en om na de levering van de isostatische pers ter plaatse een inspectie te laten uitvoeren.

Gelet op de twijfels omtrent de definitieve bestemmeling van de warmtepers en de controle op het gebruik ervan, verleende de CANVEK op 16 juni 2011 weliswaar een gunstig exportadvies, maar onder de voorwaarde dat de klant bijkomende uitleg zou verschaffen en dat de overheden van het betrokken land garanties konden geven aangaande een inspectiebezoek.

Omdat hij eveneens van mening was dat de betrokken buitenlandse overheden onvoldoende garanties boden betreffende het bezoek ter plaatse, weigerde de bevoegde minister de uitvoervergunning. Hij zond zijn dossier – waarin hij ook het advies liet opnemen dat hij ontvangen had van een buitenlandse overheid – terug naar de CANVEK.

De VSSE vroeg de betrokken correspondent bijkomende inlichtingen over het advies dat de buitenlandse overheid bij de bevoegde minister had laten toekomen.[104] Het antwoord dat de dienst kreeg, was echter zeer 'minimalistisch'. Het liet de VSSE niet toe haar oorspronkelijke analyse aan te vullen of te verfijnen.

In augustus 2011 zou de buitenlandse klant alsnog hebben ingestemd met een onvoorwaardelijk recht van toegang tot de warmtepers. Maar aangezien geen enkele Belgische overheid zich ertoe kon verbinden dit inspectiebezoek ter plaatse uit te voeren, verleende de CANVEK op 17 oktober 2011 een ongunstig advies voor de uitvoer.

De VSSE verklaarde dat de informatie die de buitenlandse overheid rechtstreeks naar de bevoegde minister had gezonden, een doorslaggevende rol heeft gespeeld in de herziening van het advies van de CANVEK. Alhoewel de VSSE de mogelijkheid van een protectionistische reflex vanwege een buitenlandse overheid nooit uitsluit wanneer dat land concurrerende ondernemingen of industrieën heeft, zag ze *in casu* geen poging tot beïnvloeding van de economische

---

103 Volgens de directeur van de CANVEK bevatten de nota's die de VSSE aan de CANVEK overzendt, doorgaans voornamelijk hypothesen en vermoedens en slechts zelden vaststaande feiten. Het is dan ook vrij moeilijk om er formele motiveringen voor haar adviezen uit te puren. Dat er doorgaans geen zekerheden kunnen meegedeeld worden, heeft vele oorzaken. De VSSE wees op de zeer hoge techniciteit van de materie, de complexiteit van de bevoorradingsnetwerken, de moeilijkheid om precieze en actuele informatie over de lopende programma's te verkrijgen, het gebrek aan toegang tot de financiële gegevens van deze netwerken en dit tegenover de beperkte menselijke middelen die zij in deze kan inzetten.

104 Nadien omschreef de VSSE dit advies als '*laconiek en negatief*'.

mededinging. Het negatieve advies zou veeleer ingegeven zijn door een algemeen wantrouwen van deze buitenlandse regering ten aanzien van bepaalde exporttransacties naar het betrokken land en door het feit dat de Belgische overheden geen effectieve controle konden uitvoeren bij de eindgebruiker. Ook benadrukte de VSSE dat zij niet anders kan dan een beroep te doen op de betrokken buitenlandse inlichtingendienst, meer bepaald wanneer ze onderzoek voert naar een buitenlandse vennootschap in een gereputeerde hoogtechnologische sector. Voorts kwam de betrokken buitenlandse overheid voor op de '*Entity List*' van het Amerikaanse ministerie van Economische Zaken (*Department of Commerce*). Dit betekent dat, voor deze administratie, de export naar de betrokken entiteit onderworpen moet zijn aan strengere voorwaarden.

Het Vast Comité I concludeerde dan ook dat de VSSE in dit dossier geen disfunctie of onwettigheid kon aangewreven verweten worden.

Wel stelde het Comité zich de vraag of en hoe de invoering van een inspectiesysteem ter plaatse bij de eindgebruikers in het buitenland de analyse- en controlecapaciteiten zou kunnen versterken op het vlak van proliferatie van massavernietigingswapens in een internationale context. Ongeacht het bevoegdheidsniveau waar dit controlesysteem wordt ondergebracht (gewestelijk, federaal of zelfs Europees) mag een dergelijke opdracht niet worden verward met het bevorderen van de economische belangen van het land.

II.6. VERMEENDE STRAFBARE FEITEN VAN EEN BUITENLANDSE INLICHTINGENDIENST EN DE INFORMATIEPOSITIE VAN DE VSSE

In januari 2010 krijgt het Vast Comité I een korte mail. De auteur ervan – die een vreemde nationaliteit heeft – beweerde dat een buitenlandse regering de ontvoering van zijn gezin op buitenlands grondgebied had georganiseerd. Het Comité verklaarde zich evenwel onbevoegd omdat er geen aanknopingspunt bleek met zijn bevoegdheden. Wel bezorgde het een kopie van de mail aan de gerechtelijke overheden en de VSSE.

Begin december 2011 legt de man opnieuw klacht neer. Bij zijn aangifte voegt hij nu een klacht met burgerlijke partijstelling bij de onderzoeksrechter. Het Comité beslist nu wel een toezichtonderzoek te openen '*naar de informatiepositie van de VSSE ten aanzien van feiten aangegeven in een klacht van een buitenlands onderdaan aan de Belgische gerechtelijke overheden ten laste van agenten van een buitenlandse inlichtingendienst*'. Nieuwe elementen duidden immers op een link met zijn opdrachten. Het onderzoek werd opgestart in januari 2012 en begin februari 2013 afgerond.

De betrokkene was tewerkgesteld op een ambassade in het buitenland. In 2003 merkte hij, naar eigen zeggen, op dat verantwoordelijken van de ambassade

en personen die werkten voor de buitenlandse veiligheidsdiensten, geregeld contact hadden met figuren die een extremistische, zelfs gewelddadige, islam verdedigden. Omdat hij geen gehoor vindt bij zijn oversten, besluit hij de media in te lichten. Hij vraagt meteen ook politiek asiel aan en krijgt een verblijfsvergunning.

In oktober 2006 zouden hij en zijn gezin onder bedreiging naar Brussel zijn gebracht en van daaruit op een vlucht naar zijn vaderland zijn gezet.

De Veiligheid van de Staat was, via het Comité (*supra*), sinds midden januari 2010 op de hoogte van de beweerde feiten. Bovendien had de dienst eind januari ook een verslag ontvangen van de Belgische ambassadeur uit het vaderland van betrokkene, die kort daarvoor een contact met hem had. De ambassadeur sprak zich daarbij niet uit over de grond van de zaak, maar gaf te kennen dat het nuttig zou zijn dat de veiligheidsdiensten een onderzoek zouden instellen. De ambassadeur sloot immers niet helemaal uit dat het om een poging ging tot compromittering van de ambassade. De VSSE deed een aantal onderzoekverrichtingen[105] die resulteerden in een beknopt informatieverslag. Daarin werd geen conclusie getrokken over de geloofwaardigheid van het verhaal. Er werd ook niet geanalyseerd of deze zaak zou zijn opgezet om de Belgische diplomatie schade te berokkenen. De VSSE achtte het niet noodzakelijk een evaluatienota op te maken voor derden '*au vu de la maigreur et de la non pertinence en termes de renseignement des éléments récoltés*'. De ambassadeur in kwestie werd niet op de hoogte gehouden van het gevolg dat de VSSE aan zijn schrijven gaf. Volgens de VSSE was dit omdat de FOD Buitenlandse Zaken de dienst VSSE nooit 'officieel' bevraagd had.

Halverwege augustus 2011 weten betrokkene en zijn gezin het land te ontvluchten.

Eind oktober 2011 dient hij klacht in bij de onderzoeksrechter nopens feiten van ontvoering, vrijheidsberoving, slagen en verwondingen, gepleegd in het buitenland en voortgezet in België en dit tegen personen die vermoedelijk deel uitmaken van een buitenlandse inlichtingendienst. Wat later herhaalt hij zijn klacht, maar dan voor het Vast Comité I.

In de loop van februari 2012 en pas na door het Comité op de hoogte te zijn gebracht van de opening van een toezichtonderzoek en de klacht bij de onderzoeksrechter, nam de VSSE contact op met het bevoegde parket. Het parket bleek nog geen kennis te hebben van bewuste klacht.

In april 2012 ging de VSSE over tot nieuwe verificaties, die evenwel geen bewijs opleverden.

De VSSE beschouwde deze zaak in alle opzichten als zeer ongeloofwaardig. De documenten en informatie die de betrokkene bezorgde evenals de formulering ervan en de manier van verzending gaven aanleiding tot ernstige twijfel over hun waarachtigheid. Ook de vanwege de buitenlandse correspondent verkregen

[105] Raadpleging van open bronnen, een vraag om informatie naar een corresponderende buitenlandse dienst, een verificatie (die negatief bleek gezien betrokkene in 2010 nog niet bekend was bij de VSSE) …

informatie leverde volgens de VSSE geen relevante elementen op die een grondige analyse en het meedelen van informatie aan een Belgische of buitenlandse partner hadden gerechtvaardigd.

Bijgevolg besloot de VSSE dat deze zaak niet relevant was in het kader van inlichtingenwerk: "*En définitive, la dénonciation d'un enlèvement, comme le dépôt d'une plainte en justice sont des dossiers judiciaires et policiers qui ne relèvent pas de la compétence légale de la VSSE.*"

Het Vast Comité I trad de positie van de VSSE in die zin bij dat de behandeling van een gerechtelijk of politioneel dossier uiteraard niet behoort tot de bevoegdheid van de dienst. Maar wanneer de gelaakte feiten verband houden met een van de wettelijk op te volgen dreigingen (*in casu* inmenging) is de opvolging ervan wél pertinent in het kader van de inlichtingenopdracht. Het Comité was tevens van oordeel dat de VSSE – zelfs voorlopige – conclusies van haar analyses schriftelijk dient vast te leggen, en dit in het kader van elke reële of potentiële bedreiging waarvan ze, op welke wijze of van wie ook, kennis krijgt.

II.7. MOGELIJKE REPUTATIESCHADE DOOR UITLATINGEN VAN DE VSSE

Midden juli 2012 ontving het Vast Comité I een klacht van een particulier die actief was in de sector van de economische inlichtingengaring.[106] Hij beweerde dat de VSSE in de sector waar hij werkzaam was zijn reputatie besmeurde en dat dit nefaste gevolgen had bij de uitbouw van zijn professionele relaties. In september 2012 besliste het Vast Comité I hierop een toezichtonderzoek te openen '*naar de informatie die de VSSE eventueel heeft verspreid over een particulier*'.[107]

Het Comité stelde vast dat de klager en zijn handelsvennootschappen gekend waren bij de VSSE en dit in het kader van een algemeen onderzoek naar private inlichtingenbedrijven. Het onderzoek was gebeurd door de dienst die binnen de VSSE instaat voor de bescherming van het wetenschappelijk en economisch potentieel van het land (WEP). Het Comité oordeelde dat de belangstelling van de VSSE voor de activiteiten van economische inlichtingengaring van de klager, legitiem was. Het Comité zelf had de VSSE overigens eerder aanbevolen dergelijke activiteiten te bestuderen.[108]

Wel gaf de informatie waarover de VSSE beschikte geen aanleiding tot welke analyse dan ook die zou moeten aantonen welke bedreiging voor het WEP zou uitgaan van de activiteiten van de klager. De ingewonnen gegevens werden dus

106 Conform artikel 40 W.Toezicht vroeg de klager om zijn anonimiteit te waarborgen.
107 Het eindverslag werd goedgekeurd in april 2013.
108 VAST COMITÉ I, *Activiteitenverslag 2003*, 24 tot 115.

bewaard in het kader van algemene informatie die wordt ingezameld over private inlichtingenbedrijven die actief zijn in België. Er werd ook geen enkel informatierapport noch enige analyse betreffende de activiteiten van de klager bezorgd aan derden.

Het Comité besloot verder dat de elementen die aan de basis lagen van de klacht, geenszins konden aangetoond worden.

II.8. VERMEENDE ONRECHTMATIGE VERSPREIDING VAN PERSOONSGEGEVENS DOOR DE VSSE

II.8.1. DE AANLEIDING

Halverwege oktober 2012 dient een particulier een klacht in bij het Vast Comité I. De inhoud van diverse krantenartikels[109] deden betrokkene vermoeden dat de VSSE beschikte over 'een geheim dossier' over hem en hij stelde zich vragen bij de wijze waarop de journalisten hiervan in het bezit waren gekomen. De klager vroeg het Comité om een kopie van alle inlichtingen die de VSSE over hem zou hebben verzameld alsook om een onderzoek naar de leden van de VSSE, die volgens hem een misdrijf begingen door geclassificeerde informatie door te geven aan de media.

Het Comité besliste daarop in april 2013 een toezichtonderzoek te openen, dat begin september 2013 werd afgerond.

Het Vast Comité I was uiteraard niet bevoegd om aan de klager de inlichtingen te verstrekken waarover de VSSE eventueel zou beschikken. Hiervoor verwees het Comité naar de verschillende mogelijkheden zoals voorzien in de Wet van 11 april 1994 betreffende de openbaarheid van bestuur (WOB) en de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer (Privacywet).

Wel kon worden nagegaan of de VSSE daadwerkelijk een dossier had aangelegd over de betrokkene en of die informatie ter kennis van de pers was gekomen[110], of de VSSE daarmee afbreuk deed aan de rechten die de Grondwet en de wet aan de klager verlenen (meer bepaald het recht op eerbied voor het privéleven) en of de bekendmaking van de vermeende informatie afbreuk deed aan de efficiënte werking van de VSSE.

---

109 PLA, LVDK en GVV, *Het Laatste Nieuws*, 22 september 2012 (Niet te temmen); JDB en JVC, *Het Nieuwsblad*, 24 september 2012 (Kopstuk Sharia4Belgium werkte even op Vlaams Kabinet).

110 Bijvoorbeeld bij toepassing van artikel 19, 2de lid van de W.I&V die de voorwaarden bepaalt inzake mededeling aan de pers van inlichtingen door de administrateur-generaal van de VSSE of door een ongepaste mededeling die strijdig zou zijn met de classificatieregels (W.C&VM).

II.8.2. ONDERZOEKSVASTSTELLINGEN

Het onderzoek wees uit dat de VSSE inderdaad – meestal 'vertrouwelijk' geclassificeerde – inlichtingen over de klager had verzameld en bewaard. Hij was bij de VSSE gekend aangezien hij in februari 2006 de aandacht had getrokken. Bovendien deelde de klager zijn (extremistische) overtuigingen en engagement op zijn *blog*. De betrokkene maakte er geen geheim van dat hij actief was binnen *Sharia4Belgium*, waarvan hij zichzelf als woordvoerder profileerde. De VSSE was dan ook de mening toegedaan dat het zeer verontrustende gedrag van de klager moest worden opgevolgd.

Het Comité vond deze opvolging gerechtvaardigd vanuit de wettelijke opdracht van de dienst die er meer bepaald in bestaat inlichtingen in te winnen, te analyseren en te verwerken die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde bedreigt of zou kunnen bedreigen.[111]

De VSSE verklaarde over de klager geen inlichtingen aan de pers te hebben meegedeeld. Buiten de verklaringen van de klager zelf vond het Comité geen enkele aanwijzing op basis waarvan kon worden bewezen of verondersteld dat een dergelijke mededeling zou hebben plaatsgevonden. Aangezien de klager zelf naar buiten trad in de media en op sociale netwerken, was het voor de pers niet moeilijk om aanwijzingen te vinden van zijn engagement binnen Sharia4Belgium. Bij gebrek aan aanwijzingen over de eventuele onrechtmatige verspreiding van (persoons)gegevens, besloot het Vast Comité I dan ook dat de VSSE geenszins afbreuk had gedaan aan de rechten die de Grondwet en de wet aan de klager verlenen.

II.9. KLACHT OVER DE ONTVREEMDING VAN EEN LAPTOP

Begin 2013 ontving de voorzitster van de Senaat een e-mail van een persoon die meldde dat zijn laptop in de loop van 2007 was ontvreemd. Hij wenste te weten of de diefstal destijds mogelijks werd gepleegd door een Belgische inlichtingendienst. De voorzitster vroeg hierop aan het Vast Comité I om een onderzoek te openen.

De klager, die als journalist actief was, schreef in de periode 2006-2007 enkele artikels over de situatie in Congo. Naar eigen zeggen werden die publicaties hem niet in dank afgenomen; hij zou er meermaals over zijn aangesproken door diverse politici. Wanneer bij hem – maar ook bij een van de in zijn artikels vermelde personen – een computer verdwijnt, doet hij daarvan aangifte bij de politie.[112] Op dat

[111] In dit verband deed het Vast Comité I ook opmerken dat de klager op 29 augustus 2013 onder aanhoudingsbevel werd geplaatst wegens het uiten van 'schriftelijke bedreigingen' ten aanzien van meerdere personen. Begin januari 2014 werd hij veroordeeld door de correctionele rechtbank van Antwerpen.

[112] Naar alle waarschijnlijkheid werd dit strafonderzoek zonder gevolg geklasseerd.

moment uit hij evenwel geen enkele verdenking met betrekking tot de mogelijke dader(s). Pas veel later geraakt hij ervan overtuigd dat een Belgische inlichtingendienst mogelijks achter de diefstal zit: een verklaring van zijn advocaat en van een derde waarvan de klager vermoedde dat hij goede banden had met een buitenlandse inlichtingendienst, deden hem hiertoe besluiten. Wanneer de pers begin 2013 gewag maakt van de opvolging van politieke verantwoordelijken door de VSSE (zie Hoofdstuk II.2), sluit hij niet uit dat ook journalisten het voorwerp zouden kunnen zijn van een bijzondere aandacht vanwege de inlichtingendiensten…

Het Vast Comité I was niet bevoegd om zich te buigen over de strafrechtelijke kant van de zaak. Het is evenwel zijn taak om klachten en aangiften over de werking, het optreden, het handelen of het nalaten te handelen van de inlichtingendiensten te behandelen. Vandaar dat het Comité de ADIV en de VSSE bevraagd heeft.

De ADIV kende de klager alleen als auteur van de vermelde persartikels.

Ook de VSSE beschikte over de persartikels omdat ze handelden over een materie die tot haar wettelijke bevoegdheid behoort en die zij opvolgt. De klager zelf maakte echter nooit het voorwerp uit van bijzondere aandacht door deze dienst. Wel had de VSSE weet van het verdwijnen van de laptop. Er werd hieromtrent zelfs een kort rapport opgesteld, zonder verdere analyse en/of commentaar.

Het Comité besloot dat de klager eind 2007 door zijn artikels een beperkte, passieve aandacht had genoten van beide inlichtingendiensten. Tevens werd geen enkel element aangetroffen dat kon wijzen op enige betrokkenheid van de ADIV noch van de VSSE bij deze feiten.[113]

II.10. TUSSENTIJDSE VERSLAGEN IN DE ONDERZOEKEN NAAR AANLEIDING VAN DE SNOWDEN-ONTHULLINGEN

De onthullingen van de Amerikaanse klokkenluider Edward Snowden vormden het startschot van diverse toezichtonderzoeken (cf. II.11.11). Het Vast Comité I kon deze onderzoeken, gezien hun complexiteit en de impact van de onthullingen, in 2013 niet afronden.

Wel werd, in het kader van zijn toezichtonderzoek '*naar de informatiepositie van de Belgische inlichtingendiensten ten aanzien van de mogelijkheden van bepaalde staten tot massale data-captatie en –mining en van de wijze waarop deze staten aan politieke spionage zouden doen van zogenaamde 'bevriende landen*", een uitgebreid tussentijds verslag afgerond en overgezonden naar de bevoegde overheden. Het tussentijds verslag bevat in essentie de open bronnen-analyse van drs. Mathias Vermeulen[114] die het Vast Comité I als deskundige had ingeschakeld op basis van arti-

113 Het toezichtonderzoek werd afgerond in oktober 2013.

114 *Research Fellow* aan het European University Institute (EUI) in Firenze en het Centre for Law, Science and Technology Studies aan de VU Brussel.

kel 48 § 3 W.Toezicht. Zijn werk resulteerde in de studie '*De Snowden-revelaties, massale data-captatie en politieke spionage*'. Het expertenverslag werd voorafgegaan door een inleiding van het Vast Comité I waarbij de Snowden-onthullingen in een breder kader werden geplaatst. Dit moest toelaten om het verslag van de expert beter te begrijpen. Omwille van het belang van het toezichtonderzoek werd het tussentijds verslag als Bijlage D van voorliggend activiteitenverslag opgenomen.

Een tweede toezichtonderzoek[115] naar aanleiding van de Snowden-onthullingen behandelt onder meer de in België geldende (inter)nationale rechtsregels 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 (of die enige link hebben met België) te onderscheppen en te exploiteren. Ook in het kader van dit onderzoek deed het Vast Comité I beroep op de inbreng van een experte (Prof. Annemie Schaus, Université Libre de Bruxelles). Haar '*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*' werd eveneens opgenomen in bijlage van onderhavig activiteitenverslag.

II.11. TOEZICHTONDERZOEKEN WAAR IN DE LOOP VAN 2013 ONDERZOEKSDADEN WERDEN GESTELD EN ONDERZOEKEN DIE IN 2013 WERDEN OPGESTART

Dit onderdeel bevat een opsomming en een korte situering van alle in 2013 opgestarte onderzoeken alsook van die onderzoeken waaraan tijdens het werkingsjaar 2013 werd verder gewerkt maar die nog niet konden worden afgerond.

II.11.1. DE OPVOLGING VAN EXTREMISTISCHE ELEMENTEN IN HET LEGER

Naar aanleiding van briefings gegeven door de ADIV in de loop van 2012, 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) aan-

115 Toezichtonderzoek *'naar 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'*. De onderzoeksresultaten werden midden februari 2014 voorgelegd aan de Senatoriële Begeleidingscommissie en aan de bevoegde ministers.

wezigheid van een militant-djihadist bij het Bataljon Ardense Jagers, die met de opgedane ervaring gevechtshandboeken zou hebben opgesteld. Het Comité besloot dan ook 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.

II.11.2. DE VSSE EN HAAR WETTELIJKE OPDRACHT VAN PERSOONSBESCHERMING

In de marge van het '*gemeenschappelijk toezichtonderzoek naar de dreigingsevaluaties van het OCAD inzake buitenlandse VIP's op bezoek in België*'[116], werden vragen gesteld met betrekking tot de beschikbaarheid van de VSSE bij het uitvoeren van bepaalde beschermingsopdrachten. De VSSE riep hiervoor meermaals dwingende redenen van overbelasting en gebrek aan middelen in.

Daarop besliste het Vast Comité I een toezichtonderzoek te openen waarin wordt bestudeerd of de Veiligheid van de Staat haar persoonsbeschermingsactiviteiten conform de wet invult en of zij daarbij doelmatig te werk gaat.

De als 'GEHEIM – Wet 11.12.1998' geclassificeerde versie van het eindrapport werd eind december 2013 aan de administrateur-generaal van de VSSE voorgelegd. Dit moest toelaten om bemerkingen en toevoegingen te maken die de volledigheid en duidelijkheid van de rapportage ten goede komen. Het onderzoek werd begin 2014 afgerond en besproken in de Begeleidingscommissie van de Senaat.

II.11.3. DE WIJZE VAN BEHEER, BESTEDING EN CONTROLE VAN DE SPECIALE FONDEN

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 (zie Hoofdstuk VI). Gezien de elementen

116 VAST COMITÉ I, *Activiteitenverslag 2012*, 35-37.

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.

II.11.4. 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 ingeplant bij het OCAD, en dat 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 2013 werden door beide Enquêtediensten P en I diverse onderzoekverrichtingen gesteld en een eerste syntheserapport opgesteld.

II.11.5. INLICHTINGENAGENTEN EN SOCIALE MEDIA

Eind november 2012 berichtte de media over profielen van medewerkers van de inlichtingendiensten op sociale netwerksites als *Facebook* en *LinkedIn*. Dienvolgens verzocht de 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 zal in 2014 gefinaliseerd worden.

II.11.6. 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 artikel 56, 6° W.Toezicht wordt de externe controle op de werking van het OCAD waargenomen door beide Comités gezamenlijk.

Ook dit verslag kan in 2014 worden afgerond.

II.11.7. DE INFORMATIEPOSITIE VAN DE INLICHTINGENDIENSTEN EN VAN HET OCAD MET BETREKKING TOT EEN LEERLING-PILOOT

In juli 2012 verschenen diverse persartikels waarin geciteerd werd uit een toezichtonderzoek van het Vast Comité P naar '*informatiestromen op de luchthavens*'. Er 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. Dit voorbeeld kon wijzen op een gebrekkige informatie-uitwisseling tussen de diverse politiediensten op de luchthavens. Na kennisname van het rapport door het Vast Comité I, werd in juni 2013 beslist 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 X die toelating verkreeg om een cursus als vliegtuigpiloot te volgen in België*'.

Het onderzoek bevindt zich in de eindfase.

II.11.8. EEN KLACHT VAN DE SCIENTOLOGYKERK TEGEN DE VEILIGHEID VAN DE STAAT

In de loop van januari en februari 2013 verschenen diverse krantenartikelen waarin wordt vermeld dat de Veiligheid van de Staat zou nagaan of en wanneer politici contact hebben met organisaties zoals de Scientologykerk (zie II.2). Daarbij wordt geciteerd uit een geclassificeerde nota en uit de 'Fenomeenanalyse van niet-staatsgestuurde inmengingsactiviteiten' van de VSSE. In maart 2013 besluit de Scientologykerk klacht neer te leggen bij het Vast Comité I. Het Comité besliste een toezichtonderzoek te openen over de wijze waarop de Veiligheid van de Staat een rapport, haar betreffend, opgesteld en verspreid heeft. In 2013 werden de meeste onderzoeksverrichtingen afgerond. Het eindverslag werd gefinaliseerd midden 2014.

II.11.9. 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.[117] In 2013 werden alle betrokken actoren uitvoerig bevraagd.

II.11.10. 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 informatie van de VSSE aangaande '*gewichtige feiten eigen aan de persoon*'. Deze informatie zou een beletsel vormen voor zijn naturalisatie. De betrokkene was daarbij van oordeel dat hij het slachtoffer was van een misverstand dat leidde tot een inbreuk op zijn individuele rechten door de Veiligheid van de Staat. Eind juli 2013 diende de man klacht in bij het Vast Comité I. Het Comité opende daarop een toezichtonderzoek dat in februari 2014 werd gefinaliseerd.

II.11.11. KLACHT OVER DE WIJZE WAAROP DE VSSE EEN ZAAKVOERDER VAN EEN BELGISCH EXPORTBEDRIJF OPVOLGT

Naar aanleiding van een klacht, opende het Vast Comité I begin oktober 2013 een toezichtonderzoek '*naar de wijze waarop de VSSE een zaakvoerder van een Belgische onderneming, die over specifieke gegevens beschikt over uitvoer naar Iran, benadert en bejegent*'. Diverse onderzoekverrichtingen werden uitgevoerd; de klager alsook vertegenwoordigers van de betrokken inlichtingendienst werden verschillende malen gehoord. Het onderzoek zal in de loop van 2014 worden afgerond.

---

117 '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'.

II.11.12. VIER TOEZICHTONDERZOEKEN IN HET KADER VAN DE SNOWDEN-ONTHULLINGEN

Op 6 juni 2013 publiceerden *The Guardian*[118] en *The Washington Post*[119] 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 snel op.

De berichten gaven een inkijk in uitermate geheime programma's van voornamelijk de Amerikaanse *National Security Agency* (NSA). Ze onthulden onder meer het bestaan van het zogenaamde 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) waarbij ook zogenaamde 'bevriende landen' werden geviseerd.

Deze onthullingen waren het startschot voor vele (parlementaire, gerechtelijke en inlichtingen) onderzoeken 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. 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.*'

Het Vast Comité I heeft daarop drie toezichtonderzoeken geopend die uiteraard nauw met elkaar verweven zijn. Dit geldt ook voor een vierde onderzoek[120] dat werd geïnitieerd na klacht van de voorzitter van de Nederlandse Orde van advocaten bij de Balie van Brussel.

Het eerste toezichtonderzoek[121] – dat begin 2014 in de Begeleidingscommissie van de Senaat werd besproken – 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

---

118 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).

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

120 'Toezichtonderzoek ingevolge een klacht van een stafhouder naar het gebruik van informatie afkomstig van massale buitenlandse data-captatie in Belgische strafzaken'.

121 'Toezichtonderzoek naar de informatiepositie van de Belgische inlichtingendiensten ten aanzien van de mogelijkheden van bepaalde staten tot massale data-captatie en –mining en van de wijze waarop deze staten aan politieke spionage zouden doen van zogenaamde 'bevriende lan-

personen, organisaties, ondernemingen of instanties (of die een 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 gecollecteerd 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? Alhoewel dit aspect van de onthullingen (met name bepaalde operaties van inlichtingendiensten van zogenaamde 'bevriende landen' ten aanzien van internationale of supranationale instellingen waarin België vertegenwoordigd is of ten aanzien van Belgische belangen) niet expliciet in de vraagstelling van de Begeleidingscommissie was opgenomen, heeft het Vast Comité I beslist om ook hieraan aandacht te besteden, en dit gelet op het intrinsieke belang van deze vraag.

Het tweede toezichtonderzoek[122] – dat ook reeds werd besproken in de Senaatscommissie – behandelt de in België geldende (inter)nationale rechtsregels 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 (of die enige link hebben met België) te onderscheppen en te exploiteren. Qua internationale regels was er daarbij uiteraard aandacht voor artikel 8 EVRM (waarbij zowel de 'horizontale werking' van deze bepalingen en de eventuele 'positieve verplichtingen' die eruit voortvloeien voor een Staat, belicht werden), artikel 17 van het Verdrag inzake burgerrechten en politieke rechter (BUPO-verdrag), Richtlijn 95/46/EC van 24 oktober 1995, Verdrag nr. 108 van 28 januari 1981 van de Raad van Europa en de artikelen 7 en 8 van het Handvest van de Grondrechten van de Europese Unie. Maar ook meer specifieke regels kwamen aan bod: de regels inzake *Passenger Name Record*, Swift, Safe Harbour … Ten slotte werden de interne rechtsregels die betrekking hebben op de privacybescherming en dataprotectie, belicht: de Wet Verwerking Persoonsgegevens en haar uitvoeringsbesluit en de bepalingen die specifiek zijn voor de werking van inlichtingendiensten. Daarnaast biedt dit tweede toezichtonderzoek ook een overzicht van de juridische mogelijkheden waarover Staten, burgers of bedrijven

---

den'. De onderzoeksresultaten werden midden april 2014 besproken met de Senatoriële Begeleidingscommissie en voorgelegd aan de bevoegde ministers.

122 Toezichtonderzoek 'naar 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'. De onderzoeksresultaten werden midden februari 2014 voorgelegd aan de Senatoriële Begeleidingscommissie en aan de bevoegde ministers.

beschikken om actie te ondernemen tegen (mogelijke) inbreuken op (grond)rechten.

Het derde toezichtonderzoek[123] – dat nog niet werd gefinaliseerd – behandelt de mogelijke implicaties van data-mining 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;
- 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.

Het vierde onderzoek, opgestart na aangifte van een stafhouder, betreft voornamelijk het eventuele gebruik in strafzaken van gegevens die op massale (en illegale) wijze zijn gecapteerd.

123 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'.

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'*.[124] 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.[125] In deze zesmaandelijkse verslagen moet naast een aantal kwantitatieve gegevens (aantal machtigingen, duur van de methoden, betrokken personen), ook worden ingegaan op de door de BIM-methoden 'behaalde resultaten'. Omwille van het belang ervan hield het Comité er aan zijn analyse in dit verband verkort weer te geven in dit activiteitenverslag.

III.1. BEHAALDE RESULTATEN

'Although the financial costs of an intelligence operation are often tangible, the benefits that it produces are often intangible … This is especially true when the object of an operation is the non-occurrence of an event, such as a terrorist attack'.[126] Dit citaat vat meteen samen hoe moeilijk het is om in een inlichtingencontext te meten wat het behaalde resultaat is van een welbepaalde operatie of methode. Het probleem van het meten van 'resultaten' is trouwens niet eigen aan de inlichtingenwereld. Het geldt ook voor de gerechtelijke wereld wanneer die de resultaten van haar bijzondere opsporingsmethoden (BOM) wil meten. We stel-

124 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.

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

126 H. BORN en A. WILLS, *Overseeing Intelligence Services – A Toolkit*, DCAF, 2012.

len dan ook vast dat de gerechtelijke overheden dergelijke analyse niet opmaakt, ondanks de bewoordingen van artikel 90*decies* Wetboek van Strafvordering.[127]

Ondanks deze moeilijkheid heeft het Comité getracht een zicht te krijgen op het 'nut' van de ingezette BIM-methoden, vooreerst door een eenvoudige bevraging te houden bij de twee inlichtingendiensten zelf en vervolgens door een diepgaande analyse van vier omvangrijke casussen.

De bevraging bij de inlichtingendiensten had betrekking op 238 BIM-beslissingen en -machtigingen uit de periode van september 2010 tot december 2012, of met andere woorden op iets meer dan 9% van het totale aantal toelatingen.[128] Beide diensten werd de vraag gesteld hoe ze de doeltreffendheid van uitgevoerde methoden evalueerden in functie van de in de toelating beoogde doelstellingen. De VSSE was van mening dat in 84% van de gevallen alle beoogde doelstellingen bereikt werden, in 8,5% een deel van de doelstellingen, en in 7,5% geen van de doelstellingen. De ADIV gaf volgend antwoord: in 72% van de gevallen was de dienst van mening dat de alle beoogde doelstellingen bereikt werden, in 16% een deel van de doelstellingen, in 12% geen van de doelstellingen.

Voortbouwend op deze zelfevaluatie voerde het Comité een inhoudelijk onderzoek waarbij alle methoden die werden ingezet ten aanzien van vier verschillende 'targets' (zijnde een persoon of organisatie) in detail werden onderzocht. Voor elke target werd bekeken welke BIM-methoden opeenvolgend werden ingezet en wat dit inhoudelijk opleverde, dit in functie van de finaliteit van de methode (bijv. het netwerk van een persoon blootleggen of zekerheid bekomen over zijn betrokkenheid bij een dreiging). In totaal werden op de vier targets 160 methoden toegepast.

De eerste target was in totaal 18 maal het voorwerp van een BIM-methode. De behaalde resultaten lieten evenwel niet toe het vermoeden van de dienst te bevestigen, wel om het te versterken, onder andere omdat de dienst een beter zicht kreeg op het netwerk van de persoon. Dit was trouwens ook het vooropgestelde doel. De BIM-methoden leverden ter zake informatie op die met 'gewone' inlichtingenmethoden niet konden worden verkregen. Deze casus toonde ook aan dat de opvolging van de betrokkene werd gestart op aangeven van een buitenlandse inlichtingendienst. De bekomen informatie werd, overeenkomstig artikel 20 Wet I&V, met deze inlichtingendienst gedeeld.

---

127 *'Tot slot moet nog een opmerking gemaakt worden bij de weging van het 'resultaat' van de diverse maatregelen. In de praktijk blijkt het zeer moeilijk om 'het resultaat' van de diverse maatregelen enerzijds voldoende adequaat te definiëren en anderzijds het resultaat 'geïsoleerd' (per maatregel) na te gaan, gezien er (veelal) sprake is van parallel gebruik van verscheidene opsporings- en onderzoeksmethoden. Bovendien is het onmogelijk om het "resultaat" correct of minstens op afdoende wijze weer te geven zonder enige bijkomende informatie betreffende de context waarin de maatregelen aangewend werden en zonder informatie over de beoordeling door de bodemrechter.'* (Dienst voor het Strafrechtelijk beleid, *Verslag 2013 in uitvoering van artikel 90decies Wetboek van Strafvordering (2012), s.l.*, 6).

128 Waarvan voor de VSSE 94 specifieke en 71 uitzonderlijke methoden en voor de ADIV 48 specifieke en 25 uitzonderlijke methoden.

Een tweede target – een organisatie – was het voorwerp van 47 methoden. Om bloot te leggen wie met wie in contact staat, werd veelvuldig gewerkt met de identificatie van abonnees van elektronische communicatiemiddelen. Tevens hanteerde men de mogelijkheid om personen te lokaliseren aan de hand van hun telecommunicatie en werden ze geschaduwd. In deze casus kan gesteld worden dat globaal genomen de door de BIM-methoden vooropgestelde doelstellingen bereikt werden. Bovendien illustreerde deze casus ook zeer goed de samenhang tussen de 'gewone' methoden en de BIM-methoden, en de tussen de diverse BIM-methoden onderling waarbij de ene methode voortbouwde op de andere.

In een derde casus werden 79 BIM-methoden toegepast. Het merendeel betrof ook hier identificaties en lokalisaties. En ook hier werd de target door een partnerdienst 'aangebracht' bij de Belgische inlichtingendienst. De methoden hebben echter niet toegelaten te bevestigen dat deze persoon ook effectief een bedreiging vormde. Wel bleek hij contacten te hebben met personen die een reële bedreiging uitmaakten. Bovendien kon, via toegang tot bankgegevens, aangetoond worden dat bepaalde financiële stromen in de tijd samenvielen met sommige activiteiten van personen die eveneens in de kijker van de inlichtingendiensten liepen. Het Comité moest in dit dossier vaststellen dat de informatiepositie van de betrokken dienst al bij al niet in grote mate was versterkt, ondanks de inzet van 79-methoden.

De laatste casus berustte op 16 BIM-methodes die werden ingezet ten aanzien van een bepaalde organisatie. Het betrof voornamelijk de (langdurige) observatie met behulp van technische middelen en de inzage van bankgegevens. Het onderzoek had tot doel na te gaan wie tot het netwerk van de organisatie kon gerekend worden. Het Comité stelde vast dat de technische middelen die ingezet waren, soms defecten vertoonden, zodat de resultaten ontbraken. Daarenboven kon een deel van de bekomen gegevens (beeldmateriaal) bij gebrek aan tijd en mensen slechts gedeeltelijk worden verwerkt. De gegevens die wél geanalyseerd konden worden, werden verwerkt in vele tientallen inlichtingenrapporten. De studie van het Comité leerde dat de observaties en de analyse van de financiële gegevens zeker hebben bijgedragen tot de realisatie van het vooropgestelde doel.

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

Tussen 1 januari en 31 december 2013 werden door de twee inlichtingendiensten samen 1378 toelatingen verleend tot het aanwenden van bijzondere inlichtingen-

methoden, 1224 door de VSSE (waarvan 1102 specifieke en 122 uitzonderlijke) en 154 door de ADIV (waarvan 131 specifieke en 23 uitzonderlijke).

Onderstaande tabel maakt een vergelijking met de cijfers van 2011 en 2012. 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' in voetnoot vermeld maar 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 in dit rapport vermelde aantal bijzondere methoden hoger ligt dan dezelfde periode van vorig jaar dan is dit grotendeels te wijten aan een andere manier van tellen en dus niet aan het feit dat er zoveel meer methoden werden aangewend. De impact van die nieuwe telwijze wordt meteen duidelijk in onderstaande tabel.

	ADIV		VSSE		TOTAAL
	Specifieke methode	Uitzonderlijke methode	Specifieke methode	Uitzonderlijke methode	
2011	60	7	731	33	831
2012	67	24	655	102	848
2013	131	23	1102	122	1378

De op het eerste gezicht uitgesproken stijging moet dus worden genuanceerd. Op basis van de telling zoals die gevoerd werd in de voorgaande jaren zou 2013 slechts 960 methoden hebben geteld. Er werden dus ten opzicht van 2012 ongeveer 13% meer BIM-methoden ingezet. Onderstaande tabellen maken duidelijk waar die stijging te situeren is.

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 2011	AANTAL 2012	AANTAL 2013
Betreden van en observeren op of in publiek toegankelijke plaatsen met een technisch middel	7	8	14
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	23 dossiers	25 dossiers	66 methoden[129]
Kennisnemen van oproepgegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	17	30	15
Kennisnemen van lokalisatiegegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	13	4	36
TOTAAL	60	67[130]	131[131]

Wat betreft de specifieke methoden ingezet door de ADIV, toont de vergelijking met voorgaande jaren twee opvallende tendensen: het aantal observaties en lokalisaties is sterk toegenomen.

III.2.1.2. De uitzonderlijke methoden

AARD UITZONDERLIJKE METHODE	AANTAL 2011	AANTAL 2012	AANTAL 2013
Betreden van en observeren in niet publiek toegankelijke plaatsen met of zonder een technisch middel	0	1	1
Betreden en doorzoeken van niet publiek toegankelijke plaatsen met of zonder een technisch middel	0	0	0

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

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

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

AARD UITZONDERLIJKE METHODE	AANTAL 2011	AANTAL 2012	AANTAL 2013
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	5	7	5
Binnendringen in een informaticasysteem	0	2	0
Afluisteren, kennisnemen en opnemen van communicaties	2	14	17
TOTAAL	7	24[132]	23[133]

III.2.1.3. De belangen en dreigingen die de inzet van de bijzondere methoden rechtvaardigen[134]

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 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 2011	AANTAL 2012	AANTAL 2013
Inlichtingenopdracht	38	63	183
Militaire veiligheid	8	7	26
Bescherming geheimen	19	21	50

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

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

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

Anders dan voor de VSSE, staan de dreigingen waaraan de ADIV aandacht mag of moet besteden, niet in de wet omschreven. Toch vermeldt deze dienst in zijn toelatingen systematisch welke bedreiging wordt geviseerd. Dergelijke transparantie verdient inderdaad aanbeveling. De cijfers tonen aan dat, wat betreft de inzet van bijzondere methoden, de strijd tegen spionage de eerste prioriteit van de militaire inlichtingendienst is gebleven.

AARD DREIGING	AANTAL 2011	AANTAL 2012	AANTAL 2013
Spionage	54	78	157
Terrorisme (en radicaliseringsproces)	10	3	11
Extremisme	3	3	42
Inmenging	0	2	2
Criminele organisatie	0	1	28
Andere	0	5	29

III.2.2. TOELATINGEN MET BETREKKING TOT DE VSSE

III.2.2.1. De specifieke methoden

AARD SPECIFIEKE METHODE	AANTAL 2011	AANTAL 2012	AANTAL 2013
Betreden van en observeren op of in publiek toegankelijke plaatsen met een technisch middel	89	75	109
Betreden en doorzoeken van publiek toegankelijke plaatsen met een technisch middel	0	1	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator	4	2	0
Kennisnemen van identificatiegegevens van elektronisch communicatie-verkeer; het vorderen van de medewerking van een operator; of de rechtstreekse toegang tot gegevensbestanden	355 dossiers	254 dossiers	613[135] methoden
Kennisnemen van oproepgegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	237	147	136

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

AARD SPECIFIEKE METHODE	AANTAL 2011	AANTAL 2012	AANTAL 2013
Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator	46	176	244
TOTAAL	**731**	**655**[136]	**1102**[137]

Wat betreft de specifieke methoden, ingezet door de VSSE, toont de vergelijking met voorgaande jaren twee opvallende tendensen: het aantal observaties en lokalisaties is sterk toegenomen.

III.2.2.2. De uitzonderlijke methoden

AARD UITZONDERLIJKE METHODE	AANTAL 2011	AANTAL 2012	AANTAL 2013
Betreden van en observeren in niet publiek toegankelijke plaatsen met of zonder een technisch middel	2	8	6
Betreden en doorzoeken van niet publiek toegankelijke plaatsen met of zonder een technisch middel	3	6	6
Oprichten en gebruiken van een fictieve rechtspersoon	0	0	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post	4	12	6
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen	10	16	11
Binnendringen in een informaticasysteem	3	10	12
Afluisteren, kennisnemen en opnemen van communicaties	11	50	81
TOTAAL	33	102[138]	122[139]

De cijfers tonen opnieuw een opvallende stijging van het aantal tapmaatregelen: van 11 in 2011 over 50 in 2012 tegenover 81 in 2013. Voor de andere uitzonderlijke methoden werden geen significante verschillen vastgesteld.

---

136 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.

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

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

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

III.2.2.3. De belangen en dreigingen die de inzet van de bijzondere methoden rechtvaardigen[140]

De VSSE mag slechts optreden ter vrijwaring van volgende belangen:
- de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde;
- de uitwendige veiligheid van de Staat en de internationale betrekkingen;
- de vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel.

AARD BELANG	AANTAL 2011	AANTAL 2012	AANTAL 2013
De inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde	694	704	1994
De uitwendige veiligheid van de Staat en de internationale betrekkingen	571	693	1965
De vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel	24	15	18

Volgende tabel geeft een beeld van de (potentiële) dreigingen die de VSSE viseerde bij de inzet van specifieke en uitzonderlijke methoden. 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).

AARD DREIGING	AANTAL 2011	AANTAL 2012	AANTAL 2013
Spionage	193	243	561
Terrorisme (en radicaliseringsproces)	371	288	1086
Extremisme	319	177	602
Proliferatie	17	28	27
Schadelijke sektarische organisaties	4	7	15
Inmenging	3	10	27
Criminele organisaties	3	5	18

[140] Per toelating kunnen meerdere belangen en dreigingen aan de orde zijn.

Deze cijfers tonen aan dat terrorisme en extremisme, maar ook spionage dé aandachtspunten blijven van de VSSE, minstens qua inzet van BIM-methoden.

III.3. DE ACTIVITEITEN VAN HET VAST COMITÉ I ALS JURISDICTIONEEL ORGAAN EN ALS PREJUDICIEEL ADVIESVERLENER INZAKE BIM-METHODEN

III.3.1. DE CIJFERS

Het Vast Comité I kan op vijf manieren worden gevat om zich uit te spreken over de wettelijkheid van bijzondere inlichtingenmethoden (art. 43/4 W.I&V):
- 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.). Desgevraagd 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 2011	AANTAL 2012	AANTAL 2013
1. Op eigen initiatief	13	19	16
2. Privacycommissie	0	0	0
3. Klacht	0	0	0
4. Schorsing door BIM-Commissie	15	17	5
5. Toelating minister	0	2	2
6. Prejudicieel adviesverlener	0	0	0
TOTAAL	28	38	23

De cijfers tonen aan dat de daling van het aantal vattingen toe te schrijven is aan het lagere aantal schorsingen uitgesproken door de BIM-Commissie.

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 en 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 geadieerd een definitieve uitspraak doen (art. 43/4 W.I&V). In alle dossiers werd die termijn gerespecteerd.

AARD VAN DE BESLISSING	**2011**	**EINDBESLISSING 2011**	**2012**	**EINDBESLISSING 2012**	**2013**	**EINDBESLISSING 2013**
1. Nietige klacht	0		0		0	
2. Kennelijk ongegronde klacht	1		0		0	
3. Schorsing methode	3		1		0	
4. Bijkomende informatie van BIM-Commissie	4		0		0	
5. Bijkomende informatie van inlichtingendienst	9		6		**0**	
6. Onderzoeksopdracht Dienst Enquêtes	17		11		50	
7. Horen BIM-Commissieleden	0		0		0	
8. Horen leden inlichtingendiensten	1		0		0	
9. Beslissing mbt geheim van onderzoek	0		0		0	
10. Gevoelige informatie tijdens verhoor	0		0		0	
11. Stopzetting methode	12		4		9	
12. Gedeeltelijke stopzetting methode	7		18		5	
13. (Gedeeltelijke) opheffing verbod van BIM-Commissie	5	**39**	13	**38**	2[141]	**23**
14. Onbevoegd	0		0		0	
15. Wettige toelating / Geen stopzetting methode / Ongegrond	15		3		7	
16. Prejudicieel advies	0		0		0	

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

III.3.2. DE RECHTSPRAAK

Hieronder wordt de essentie weergegeven van de 23 eindbeslissingen die het Vast Comité I in 2013 nam. De samenvattingen zijn ontdaan van operationele gegevens. Alleen die elementen die van belang zijn voor het juridische vraagstuk worden opgenomen.[142]

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

Geen bijzondere methode mag aangewend worden zonder voorafgaande schriftelijke toelating van het diensthoofd. In geval van een uitzonderlijke methode dient er daarenboven een ontwerp van machtiging en een eensluidend advies van de BIM-Commissie voor te liggen. Indien methoden worden ingezet zonder schriftelijke toelating of eensluidend advies, kan het Comité uiteraard optreden.

III.3.2.1.1. Geen bevoegdheid voor de inlichtingendienst

Een inlichtingendienst wil overgaan tot de opsporing van de in- en uitgaande oproepen van een bepaald gsm-nummer (dossier 2013/1835). Immers, uit een andere BIM-methode was eerder toevallig gebleken dat de target wellicht betrokken was bij een internationale smokkel of zwendel. De dienst wou hierover zekerheid. Hij wenste ook na te gaan of de buitenlandse overheid waarvan de target deel uitmaakte, bij de zaak betrokken was. Bij de omschrijving van de bedreiging maakte dienst enkel gewag van de '*schade aangericht door criminele organisaties en het clandestien karakter van de beschreven zwendel die ten minste een potentiële bedreiging vormen voor de economische belangen van België*'. Het Comité merkte echter op dat de bevoegdheid tot opvolging van criminele organisaties, zich beperkt tot die organisaties '*die wezenlijk betrekking hebben op de activiteiten van*

[142] Alle beslissingen van het Comité in deze materie worden gemerkt met de vermelding 'beperkte verspreiding'. Eén beslissing werd als 'vertrouwelijk' geclassificeerd en één als 'geheim'.

spionage, terrorisme, extremisme, proliferatie, schadelijke sektarische organisaties en inmenging' (art. 8, 1°, f W.I&V.). Aangezien dit niet genoegzaam aannemelijk werd gemaakt in de machtiging, werd de methode onwettelijk bevonden.

III.3.2.1.2. Toelating door de bevoegde minister

Net zoals vorig jaar[143] vatte de inlichtingendienst tweemaal zijn minister op basis van artikel 18/10 § 3, derde lid, W.I&V omdat de BIM-commissie omwille van de vakantieperiode niet rechtsgeldig kon vergaderen (dossiers 2013/2327 en 2013/2328). Het wetsartikel laat toe dat, indien de commissie geen advies uitbrengt binnen de termijn van vier dagen na ontvangst van het ontwerp van machtiging voor een uitzonderlijke methode, de inlichtingendienst zijn minister kan vragen de methode alsnog toe te laten. Het Comité had reeds beslist dat het, gelet op de concrete omstandigheden en op de noodzaak voor de dienst om zijn wettelijke opdrachten te kunnen blijven uitoefenen, geen bezwaar had tegen het feit dat de minister onmiddellijk werd gevat. In de twee nieuwe dossiers had de minister het ontwerp van machtiging gehandtekend, maar niet gedagtekend. Eveneens ontbrak een aanduiding van het tijdstip waarop het diensthoofd verslag had moeten uitbrengen over het verloop van de methode en liet de minister na de beslissing mee te delen aan het Comité. Beide verplichtingen zijn nochtans opgenomen in artikel 18/10 § 3, derde en vierde lid, W.I&V. Het Comité oordeelde evenwel dat de methode geldig was. Het herhaalde dat, gezien de omstandigheden en gelet de noodzaak om de inlichtingendienst toe te laten zijn wettelijke opdrachten naar behoren te vervullen, er geen bezwaar is om een beroep te doen op artikel 18/10 § 3, derde lid, W.I&V. Daarenboven merkte het Comité op dat deze bepaling eenvoudigweg de toelating van de bevoegde minister vereist zonder daarbij andere verplichtingen op te leggen dan deze voorzien in artikel 18/10 § 1 W.I&V. Het Comité voegde hieraan toe dat het '*niet-bestaan van dergelijke vermelding* [bedoeld wordt de vermelding van het tijdstip waarop het diensthoofd verslag moet uitbrengen, nvda] *de wettigheid van de beslissing niet aantast, noch afbreuk doet aan de toelating van de Minister*'.

III.3.2.1.3. Methode niet gedekt door de (vereiste) toelating of machtiging

Wanneer een observatie met een technisch middel voor de tweede maal wordt verlengd, merkt het Comité dat die verlenging bij vergissing zeven dagen te laat is aangevraagd (dossier 2013/2653). Met andere woorden: de camera draaide gedurende die korte periode verder zonder de vereiste toelating. De inlichtingendienst ging er van uit dat het Comité niet moest ingrijpen aangezien hij de opgenomen beelden niet zou opslaan in zijn bestanden en dus ook niet zou kunnen exploiteren. Het Comité stelde evenwel dat de beslissing van de dienst om de beelden niet

143 VAST COMITÉ I, *Activiteitenverslag 2012*, 55.

op te slaan '*ne peut avoir pour effet de priver le Comité des prérogatives que la loi lui a octroyées quant au sort à réserver aux données qui ont été recueillies et enregistrées sans une autorisation légale*.'[144] De beelden dienden dus te worden vernietigd.

In een ander dossiers was net hetzelfde aan de hand: tussen de tweede en de derde verlenging van de methode in had de camera gedurende 25 dagen gedraaid zonder de vereiste toelating (dossier 2013/2663). Ook hier kon het Comité niet ingaan op het verzoek om de gegevens niet te vernietigen omdat ze toch niet konden/zouden geëxploiteerd worden. Het Comité benadrukte ook dat '*la mise en œuvre illégale d'une méthode visée par l'article 18/17 L. R&S est susceptible de constituer une infraction visée à l'article 259bis du code pénal*.'[145]

In een derde dossier (2013/1760) besliste het hoofd van de betrokken inlichtingendienst een korte observatie te verrichten met een camera op de toegangspoort van een voor het publiek toegankelijke zaal waar een bepaald evenement zou plaatsgrijpen. De inlichtingendienst was de mening toegedaan dat het om een specifieke methode ging. Maar uit bijkomende informatie die door de BIM-Commissie was ingewonnen, bleek dat de toegangspoort '*est séparée de la voie publique par une bande de terrain pourvue d'une grille pouvant être fermée, et qu'elle est par conséquent située dans un lieu privé qui n'est pas accessible au public*.'[146] Het betrof met andere woorden een uitzonderlijke methode waarvoor de vereiste procedure niet was gevolgd. Het Comité onderschreef dan ook het oordeel van de BIM-Commissie en verklaarde de methode onwettelijk.

III.3.2.2. Motivering van de toelating

In 2013 trof het Comité vijf beslissingen die wezen op een gebrek aan (afdoende of coherente) motivering van de toelating.

Een inlichtingendienst wil overgaan tot de opsporing, identificatie en lokalisatie van de oproepgegevens van drie toestellen (dossier 2013/2618). Nochtans wordt in de toelating alleen de lokalisatie van één toestel expliciet gemotiveerd. Desgevraagd meldt de inlichtingendienst aan de BIM-Commissie dat het de bedoeling was slechts één van de drie toestellen te lokaliseren. De vermelding van de lokalisatie van de drie toestellen zowel in de toelating zelf als in de vordering naar de operator zou een administratieve vergissing zijn geweest. De BIM-Commissie sprak dan ook een gedeeltelijke schorsing uit. Het Comité dat was '*saisi*

144 '*niet voor gevolg kan hebben om het Comité de prerogatieven te ontnemen die de wet hem heeft verleend met betrekking tot het lot dat moet worden verbonden aan gegevens die verzameld en opgenomen zijn zonder wettelijk mandaat.*' (vrije vertaling).

145 '*de illegale uitvoering van een methode voorzien in artikel 18/17 W.I&V kan de inbreuk uitmaken bedoeld in artikel 259bis van het Strafwetboek.*' (vrije vertaling).

146 '*is gescheiden van de openbare weg door een stuk terrein voorzien van een hek dat kan gesloten worden, en dat de zaal bijgevolg gesitueerd is op een niet voor het publiek toegankelijke plaats.*' (vrije vertaling).

d'office de l'ensemble de la décision'[147] oordeelde echter anders. Het was immers niet mogelijk uit te maken of het werkelijk om een administratieve vergissing ging. Daarom werd de aanvraag voor de lokalisatie van de twee nummers waarvoor geen motivering werd opgegeven, als onwettelijke beschouwd.

In een ander dossier (2013/1912) wil de inlichtingendienst de titularis van een gsm-nummer identificeren. Hij zou immers zeer regelmatig contact hebben met een actief lid van een welbepaalde buitenlandse extremistische organisatie die onder meer tegen de NATO zou gericht zijn. Maar volgens het Comité '*l'examen des pièces ne fait pas apparaître que la condition de légalité de la méthode ainsi que les principes de subsidiarité et de proportionnalité, comme déterminés dans l'article 18/3, § 1 premier alinéa de la L. R&S, ont été respectés.*'[148] Immers, de dreiging die zou uitgaan van de organisatie werd door geen enkel concreet element gepreciseerd in de beslissing. Met het oog op bijkomende informatie vatte het Comité zich in deze zaak. Het wou meer aanduidingen over '*le caractère potentiellement menaçant de la cible de la méthode spécifique concernée*'[149] en '*le degré de priorité qu'occupe la (les) problématique(s) […] dans son Plan d'action.*'[150] Aangezien de betrokken dienst op beide vragen concrete antwoorden kon geven, oordeelde het Comité dat de toegelaten methode wettelijk, proportioneel en subsidiair was.

Een inlichtingendienst wil via een observatie te weten komen wie er zal deelnemen aan een vergadering waarin vermoedelijk zal gesproken worden over een nieuw politiek initiatief en een nieuw bewind in een bepaald land (dossier 2013/2420). Tevens verwacht men dat er leden van de betrokken buitenlandse inlichtingendienst zullen aanwezig zijn. In zijn toelating stelt de dienst dat volgende belangen bedreigd zijn: '*de uitwendige veiligheid van de Staat en de internationale betrekkingen, spionage, inmenging.*' De motivering van de ernst van de bedreigingen blijft beperkt tot het volgende: '*een reële mogelijkheid [dat] inlichtingenofficieren clandestiene activiteiten ontplooien op Belgisch grondgebied*'. '*Considérant qu'à défaut de constituer une mission en soi [du service de renseignement], la surveillance des activités que déploient les services de renseignement étrangers sur le territoire national ne se justifie que par une menace concrète pour la sûreté de l'Etat belge et ses relations internationales*'[151], aldus het Comité. Aangezien ook uit

147 '*van rechtswege gevat voor het geheel van de beslissing*' (vrije vertaling).

148 '*liet het onderzoek van de stukken niet blijken dat de voorwaarde van de wettelijkheid van de methode evenals de principes van subsidiariteit en proportionaliteit zoals bepaald in artikel 18/3, § 1, eerste lid W.I&V, werden nageleefd.*' (vrije vertaling).

149 '*het potentieel bedreigend karakter uitgaand van het voorwerp van de betrokken specifieke methode*' (vrije vertaling).

150 '*de graad van prioriteit die de problematiek(en) inneemt (innemen) in zijn Actieplan.*' (vrije vertaling).

151 '*Overwegende dat de opvolging van de activiteiten die buitenlandse inlichtingendiensten ontplooien op het nationale grondgebied alleen gerechtvaardigd is in geval van een concrete dreiging voor de veiligheid van de Belgische Staat en zijn internationale relaties, aangezien dergelijke opvolging op zich geen eigenlijke taak is van de inlichtingendiensten.*' (vrije vertaling).

de bijkomende informatie niet blijkt hoe die eventuele clandestiene activiteiten een bedreiging kunnen zijn voor de veiligheid van de Staat en de internationale betrekkingen, is de methode niet wettig.

In een laatste dossier oordeelde het Comité dat de methode niet kon toegelaten worden omdat '*la motivation de la méthode, est incohérente d'une part et insuffisante d'autre part et ne permet pas au Comité d'en apprécier la légalité*'[152] (dossier 2013/2447). De inlichtingendienst had voorgenomen een observatie te verrichten met '*bewakingscamera's gericht op niet-besloten en voor het publiek toegankelijke besloten plaatsen, zoals luchthavens of treinstations.*' De dienst verwees hiervoor naar artikel 18/4 W.I&V dat voorziet in de observatie met technische middelen in publieke plaatsen of in private plaatsen die toegankelijk zijn voor het publiek. Uit de motivering van de beslissing bleek echter dat het de bedoeling was om na te gaan welke personen er woonden of bezoek brachten aan een woonst waarvan de eigenaar op dat ogenblik van zijn vrijheid was beroofd. Aangezien de woonst deel uitmaakte van een complex van woningen, vroeg het Comité bijkomende uitleg over de wijze waarop de observatie *in concreto* zou gebeuren. Daaruit bleek duidelijk dat het geenszins de bedoeling was om plaatsen zoals stations en luchthaven te observeren. '*Les renseignements fournis au Comité, suite à sa demande, vont au-delà d'une simple explication complémentaire, mais révèle l'objectif réel de la méthode*'.[153] De gewraakte methode was namelijk bedoeld om een andere methode (met name de observatie van de personen die toegang hadden tot de woonst) voor te bereiden.

III.3.2.3. De proportionaliteits- en de subsidiariteitseis

Er werden zes beslissingen genomen waarbij de proportionaliteits- en/of de subsidiariteitseis bepalend was.

In twee dossiers (die op eenzelfde operatie betrekking hadden) wenste een inlichtingendienst over te gaan tot de opsporing en de identificatie van de oproepgegevens van de telefoonnummers van vier personen (dossier 2013/2067) en tegelijkertijd tot hun lokalisatie (dossier 2013/2068). De nummers waren op dat ogenblik echter nog niet gekend. Zij zouden verkregen worden via een andere methode. Het Comité stelde dat '*en l'absence d'informations obtenues par cette première méthode, il n'est pas permis de juger du respect des principes de subsidiarité et de proportionnalité et donc de la légalité de la présente méthode*'.[154] Het Comité beveelt dan ook de stopzetting.

---

152 '*de motivering van de methode enerzijds incoherent is en anderzijds onvoldoende en het Comité niet toelaat er de wettelijkheid van te beoordelen.*' (vrije vertaling).

153 '*de op verzoek van het Comité meegedeelde inlichtingen overstijgen een eenvoudige bijkomende uitleg maar onthullen de ware finaliteit van de methode.*' (vrije vertaling).

154 '*bij gebrek aan inlichtingen verkregen door deze eerste methode, kan geen oordeel gevormd worden over de naleving van de principes van subsidiariteit en proportionaliteit en dus over de wettelijkheid van de huidige methode.*' (vrije vertaling).

In een later dossier (2013/2337) kwam het Comité tot hetzelfde oordeel. De betrokken inlichtingendienst wou overgaan tot het afluisteren van een aantal gsm-nummers. Maar een aantal nummers waren op het moment van de toelating nog onbekend. De dienst wou immers ook een aantal nummers afluisteren die gelinkt waren of zouden kunnen zijn aan een welbepaald en gekend gsm-toestel. Om hoeveel en om welke nummers het uiteindelijk precies zou gaan, kon pas geweten zijn op het ogenblik dat de methode effectief werd aangewend. Aangezien de methode aldus sloeg '*sur un nombre indéterminé de numéros de GSM; qu'en l'absence d'information sur le nombre de ces numéros et sur les numéros eux-mêmes qui devraient être écoutés*'[155] was het onmogelijk om de subsidiariteit of de proportionaliteit te beoordelen. De methode werd dan ook stopgezet met betrekking tot de ongekende nummers.

Wanneer een inlichtingendienst wil overgaan tot de opsporing van de oproepgegevens van de gsm van een specifiek persoon en tegelijkertijd de lokalisatiegegevens wil bekomen (dossier 2013/2417), schorts de BIM-Commissie de methoden: '*Men beschikt evenwel over geen verdere informatie over deze [persoon]. Zijn profiel en zijn activiteiten blijken moeilijk te evalueren … Ook wordt in de beslissing niet aannemelijk gemaakt dat er een effectieve bedreiging van deze persoon zou uitgaan.*' In haar toelating had de inlichtingendienst een aantal overwegingen opgenomen die betrekking hadden op de persoon zelf maar ook een aantal meer algemene aspecten van geopolitieke aard. Het Comité vroeg de dienst om bijkomende informatie. Daaruit bleek dat er een zekere tegenspraak bestond tussen verklaringen die de persoon destijds had afgelegd voor een Belgische overheid en zijn activiteiten. '*Attendu que ce comportement étrange et ambigu permet de le considérer comme constituant une menace potentielle pour la sécurité intérieure et extérieure du pays*'.[156] Maar anderzijds stelde het Comité dat '*en l'absence de renseignements plus précis sur ses activités effectives, la demande de données de localisation apparait à ce stade disproportionnée*.'[157] De eerste methode (opsporing oproepgegevens) werd daarom wettelijk verklaard, terwijl de tweede methode (lokalisatie) werd vernietigd.

Ter ondersteuning van een filature wil de inlichtingendienst gedurende één jaar beelden kunnen maken tijdens de observaties (dossier 2013/2446). Het Comité stelde zich vragen bij de duur van deze specifieke methode. Het Comité had reeds toelatingen gehonoreerd voor het gebruik van camera's gedurende één jaar maar toen betrof het een vaste camera die bijvoorbeeld gericht was op een aan de openbare weg gelegen ingang. *In casu* betrof het echter een filature. '*Attendu que même si la filature est une mesure ordinaire, non susceptible de contrôle juri-*

155 '*op een onbepaald aantal gsm-nummers; dat bij gebrek aan informatie over het aantal nummers en over de nummers zelf die zouden moeten beluisterd worden*' (vrije vertaling).

156 '*Overwegende dat dit vreemde en ambigue gedrag toelaat hem te beschouwen als een potentiële bedreiging voor de in- en externe veiligheid van het land.*' (vrije vertaling).

157 '*bij afwezigheid van meer precieze inlichtingen over zijn effectieve activiteiten, lijkt het verzoek om lokalisatiegegevens op dit ogenblik disproportioneel.*' (vrije vertaling).

dictionnel par le Comité permanent R, l'utilisation d'une méthode spécifique pendant une période d'un an doit être justifiée, eu égard aux principes de légalité en ce compris les principes de proportionnalité et de subsidiarité; Attendu que la seule explication fournie quant à la durée, dans ce cas précis, est que pour des raisons pratiques, sur le plan opérationnel, une période longue permet la planification de filatures (et donc des observations au moyen d'une caméra) en tenant compte d'autres opérations de filatures en cours ou à venir'.[158] Het Comité oordeelde dat dergelijke motivering niet beantwoordt aan de principes van proportionaliteit en subsidiariteit en dat de observatie die accessoir is aan de filature moet beperkt worden tot een redelijke termijn van vier maanden.

In een laatste dossier (2013/2662) wenste een inlichtingendienst over te gaan tot de observatie met technische middelen van verschillende leden van een welbepaalde buitenlandse organisatie die actief is in België. De observatie was bedoeld voor de duur van één jaar. De dienst wou niet alleen de medewerkers observeren die in België verblijven maar ook personen die af toe naar België komen en die deel uitmaken van de directe omgeving van de beweging. De bedoeling van de methode bestond er in '*identifier les contacts et activités des membres influents de* [mouvement surveillé] *présents en Belgique.*'[159] Zo gesteld, werden personen die niet in Belgiê verblijven, niet gevat door de toelating. Bovendien bleek niet duidelijk of de personen die deel uitmaken van de directe omgeving, tevens invloedrijke personen zijn. Daar bovenop was gebleken dat de methode nog niet in uitvoering was, alhoewel dit volgens de toelating van het diensthoofd reeds bijna een volledig jaar mogelijk was. Ten slotte oordeelde het Comité dat de toelating om de personen die soms in België verbleven gedurende één jaar te kunnen observeren, niet proportioneel. Wat hen betreft, moet de duur van de toelating beperkt blijven tot de tijd die zij in België doorbrengen.

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 de dreiging

III.3.2.4.1. De controle over de uitvoering van de BIM-methode

De Wet van 30 november 1998 bepaalt dat alleen een Belgische inlichtingenagent zoals die omschreven wordt in artikel 3, 2° W.I&V, effectief een specifieke of uit-

158 '*Overwegende dat ook al vormt de filature een gewone methode die niet onderworpen is aan de jurisdictionele controle door het Vast Comité I, dan nog moet de aanwending van een specifieke methode gedurende een periode van één jaar gerechtvaardigd zijn gelet op de wettigheidsprincipes waaronder begrepen de principes van proportionaliteit en subsidiariteit; Overwegende dat de enige uitleg die in deze casus verschaft wordt wat betreft de duur van de methode, is dat dit nodig is vanuit praktische overwegingen op operationeel vlak aangezien een lange periode de planning van de filatures (en dus van de observaties met een camera) toelaat rekening houdend met andere lopende of toekomstige schaduwingsoperaties*'. (vrije vertaling).

159 '*de contacten en activiteiten identificeren van de invloedrijke leden van de opgevolgde beweging die aanwezig zijn in België*' (vrije vertaling).

zonderlijke methode mag uitvoeren. Wel voorziet artikel 13/1 § 2, vijfde lid W.I&V in de mogelijkheid om de hulp of bijstand van andere personen in te roepen. Zolang een of meerdere Belgische inlichtingenagenten *'gardant le contrôle direct de la méthode'*[160] is er geen probleem. Dit criterium werd tweemaal *in concreto* getoest door het Comité.

In het eerste dossier (2013/1950) wenste de dienst een observatie te houden in een private plaats. De methode zou uitgevoerd worden door een agent van een buitenlandse inlichtingendienst en een particulier. Aangezien de dienst '*n'a pas le contrôle direct de cette méthode comme voulu par le législateur*'[161], wordt de methode stopgezet.[162]

Het tweede dossier (2013/2226) was in dit opzicht anders. De inlichtingendienst riep de hulp in van drie buitenlandse inlichtingenagenten om een toestel uit een wagen te verwijderen. Dat toestel was via een eerdere methode geplaatst. Aangezien er slechts bijstand werd verleend door de buitenlandse agenten die over de nuttige technische ervaring beschikten en de eigen agenten dus de directe controle bewaarden, was de methode wettelijk.

III.3.2.4.2. Schorsing van een stopgezette methode

In dossier 2013/1728 was een andere problematiek aan de orde. De dag zelf waarop een tapmaatregel wordt toegelaten, beslist het hoofd van de betrokken inlichtingendienst de maatregel stop te zetten. Er was immers gebleken dat het gsm-nummer dat men wou afluisteren, niet aan de target toebehoorde. Daarop schorste de BIM-Commissie de betrokken methode en beval ze de stopzetting ervan. Het Comité oordeelde echter dat *'la constatation du fait que l'un des numéros de GSM interceptés n'est pas utilisé par la cible de la méthode concernée, n'est pas de nature, en soi, à rendre illégale la dite méthode, celle-ci ayant été décidée et exécutée en parfaite conformité avec la loi'*.[163] Het diensthoofd reageerde correct door de methode stop te zetten vanaf het ogenblik dat ze niet meer nuttig is vanuit de vooropgestelde finaliteit. Dit vormt een toepassing van artikel 18/10 W.I&V. Het Comité oordeelde dat de bevoegdheid van de BIM-Commissie om een methode te schorsen of stop te zetten (art. 18/10, § 6 W.I&V) alleen betekenisvol was geweest indien het diensthoofd zou nagelaten hebben de maatregel stop te zetten. Volgens het Comité was de beslissing van de commissie dan ook zonder voorwerp.

---

160 '*de dienst controle over de methode behouden*' (vrije vertaling).

161 '*niet de directe controle heeft over deze methode zoals gewild door de wetgever*' (vrije vertaling).

162 Daarenboven had de dienst nagelaten te onderzoeken of de locatie waar de observatie zou plaatsvinden niet aan een bijzonder juridisch statuut was onderworpen op basis van het internationaal recht.

163 '*de feitelijke vaststelling dat een van de geïntercepteerde gsm-nummers niet door de target wordt gebruikt is op zich niet van die aard dat de methode die in volledige conformiteit met de wet tot stand is gekomen en uitgevoerd, onwettelijk zou zijn*' (vrije vertaling).

III.3.2.4.3. Het statuut van advocaat

In drie dossiers (2013/2518, 2013/2519 en 2013/2536) beslist een inlichtingendienst om een uitzonderlijke methode aan te wenden ten aanzien van een advocaat die als dusdanig actief is in een niet-EU-land maar op het ogenblik van de aanwending van de methoden in België aanwezig was. Het Comité stelde zich de vraag of de betrokkene de bescherming kon genieten voorzien in de artikelen 2 § 2[164] en 18/2 § 3 W. I&V.[165] Het Comité stelde, zich baserend op de artikelen 428 en 428*bis* van het Gerechtelijk Wetboek.[166] dat de bescherming niet van toepassing kan zijn op betrokkene die '*het beroep van advocaat in België niet kan uitvoeren, noch de titel van advocaat dragen*'.

III.3.2.4.4. De duur van een uitzonderlijke methode

De BIM-commissie verleende een eensluidend advies voor de doorzoeking van bagage op een private plaats die niet toegankelijk is voor het publiek (dossier 2013/2520). Ze formuleerde evenwel een voorbehoud: de machtiging mocht niet langer duren dan vijf dagen, en niet twee maanden zoals in het ontwerp van machtiging vermeld. Die drempel is voorzien in artikel 18/12 § 1 W.I&V. Toch werd hiermee geen rekening gehouden in de machtiging zelf; die was twee maan-

164 *'Het is de inlichtingen- en veiligheidsdiensten verboden gegevens die worden beschermd door ofwel het beroepsgeheim van een advocaat of een arts, ofwel door het bronnengeheim van een journalist te verkrijgen, te analyseren of te exploiteren.*
Bij uitzondering en ingeval de betrokken dienst vooraf over ernstige aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van de potentiële bedreiging, zoals bedoeld in de artikelen 7, 1°, 8, 1° tot 4°, en 11, kunnen deze beschermde gegevens worden verkregen, geanalyseerd of geëxploiteerd worden.'

165 *'Als een in §§ 1 en 2 bedoelde methode aangewend wordt ten opzichte van een advocaat, een arts of een journalist, of van hun lokalen of communicatiemiddelen die zij voor beroepsdoeleinden gebruiken, of van hun woonplaats of verblijfplaats, mag deze methode niet uitgevoerd worden zonder dat, naargelang het geval, de voorzitter van de Orde van de Vlaamse balies, van de Ordre des barreaux francophone et germanophone, van de Nationale Raad van de Orde van Geneesheren of van de Vereniging van Beroepsjournalisten hiervan vooraf op de hoogte is gebracht door de voorzitter van de commissie bedoeld in artikel 3, 6°. De voorzitter van de commissie is verplicht om de nodige inlichtingen te verstrekken aan de voorzitter van de Orde of van de Vereniging van Beroepsjournalisten, waarvan de advocaat, de arts of de journalist deel uitmaakt. De betrokken voorzitter is tot geheimhouding verplicht. De straffen bepaald in artikel 458 van het Strafwetboek zijn van toepassing voor inbreuken op deze verplichting tot geheimhouding.'*

166 *Art. 428. 'Niemand kan de titel van advocaat voeren of het beroep van advocaat uitoefenen indien hij geen Belg of onderdaan van een lidstaat van de Europese Unie is, niet in het bezit is van het diploma van doctor of licentiaat in de rechten, niet de eed heeft afgelegd bedoeld in artikel 429 en niet is ingeschreven op het tableau van de Orde of op de lijst van de stagiairs. Er kan afgeweken worden van de voorwaarde van nationaliteit in de gevallen die de Koning bepaalt op advies van de Orde van Vlaamse balies en de Ordre des barreaux francophones et germanophone. Behoudens de afwijkingen die de wet vaststelt, mag geen nadere bepaling aan de titel van advocaat worden toegevoegd'.*

den geldig. De BIM-Commissie ging dan ook over tot de gedeeltelijke schorsing. Het Comité bevestigde het oordeel van de BIM-Commissie.

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

In dossier 2013/1728 besliste het Comité dat de tapmaatregel op een gsm die niet aan de target toebehoorde, wettig was (zie III.3.2.4.2). Nochtans was duidelijk dat het niet de bedoeling was die gegevens te verzamelen. Toch oordeelde het Comité dat het *'n'est pas compétent pour apprécier l'utilité pour un service de renseignement de conserver ou non des données recueillies au moyen d'une méthode exceptionnelle légalement mise en œuvre; que ce pouvoir d'appréciation appartient au service de renseignement lui-même en vertu de l'art. 13 L. R&S et 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'*.'[167]

In dossier 2013/1835 werd de opsporing van de communicatie van een bepaald gsm-nummer onwettelijk bevonden (zie II.3.2.1.1). Het Comité beval de stopzetting van deze methode voor zover ze nog in uitvoering was. Tevens oordeelde het ze dat '*de gegevens, verkregen en gebeurlijk nog te verkrijgen ingevolge de onwettig bevonden methoden*' niet mochten worden geëxploiteerd en dienden te worden vernietigd.

In dossier 2013/2446, waar de methode disproportioneel werd bevonden (zie II.3.2.3), stelde het Comité dat de gevraagde observatie, die accessoir was aan de filature, moet beperkt worden tot een redelijke termijn van vier maanden en *'que la méthode est illégale pour la période de temps au délà des 4 mois*'.[168]

Wanneer de inlichtingendienst in zijn machtiging geen rekening houdt met het feit dat een bepaalde uitzonderlijke methode maximaal voor vijf dagen kan worden ingezet (dossier 2013/2520 – zie ook II.3.2.4.4), stelt het Comité de onwettigheid vast van de methode '*DOCH SLECHTS voor zover zij zou zijn uitgevoerd NA het verstrijken van een periode van vijf dagen, te rekenen vanaf de machtiging van het diensthoofd*'. Met andere woorden: alleen de '*de gegevens, verkregen en gebeurlijk nog te verkrijgen op basis van het onwettig bevonden gedeelte van de methode, […] mogen [niet] worden geëxploiteerd en moeten worden vernietigd*.'

In een laatste dossier (2013/2662 – zie ook II.3.2.3) wenste een inlichtingendienst over te gaan tot de observatie met technische middelen van verschillende leden van een welbepaalde buitenlandse organisatie die actief is in België. De observatie was bedoeld voor de duur van één jaar. Het Comité oordeelde dat dit niet proportioneel was ten aanzien van de targets die zich slechts sporadisch in België bevonden en '*qu'il conviendrait dès lors de limiter leur observation à la*

167 *'niet bevoegd is om het nut te beoordeelden voor een inlichtingendienst om ja dan neen via een wettelijk uitgevoerde uitzonderlijke methode ingezamelde gegevens, te bewaren; dat die appreciatie toekomt aan de inlichtingendienst zelf en dit in functie van artikel 13 W.I&V en van de wet verwerking persoonsgegevens van 8 december 1992'* (vrij vertaling).

168 '*dat de methode onwettelijk is voor de periode boven de vier maanden'* (vrij vertaling).

durée de leur séjour en Belgique et d'utiliser la procédure d'urgence si nécessaire […] Déclare la méthode illégale en ce qu'elle concerne les "anciens responsables" qui ne résident plus en Belgique mais qui reviennent "parfois" [et] les personnes faisant "partie de l'entourage direct" du mouvement ciblé; La méthode n'ayant pas encore été mise en œuvre, il n'y a pas lieu d'en ordonner la cessation ni la destruction des données recueillies sur ces dernières personnes.'[169]

III.4. CONCLUSIES

Wat betreft het werkingsjaar 2013, formuleert het Comité volgende conclusies:

- het aantal ingezette methoden is in vergelijking met 2011 en 2012 gestegen. Men mag echter niet gewagen van een groei die zou wijzen op een ongebreidelde inzet van bijzondere methoden;
- de stijging is grotendeels het gevolg van het feit dat het aantal observaties en lokalisaties door de VSSE sterk toegenomen is;
- voor het derde jaar op rij viel er een stijging te noteren van het aantal gemachtigde tapmaatregelen;
- uit het onderzoek naar de behaalde resultaten blijkt dat één bepaalde target het voorwerp kan zijn van zeer veel methoden;
- voor de ADIV blijft de strijd tegen 'spionage' de meeste bijzondere methoden opeisen. Ook wat betreft de VSSE nam de aandacht voor deze dreiging (althans wat betreft de BIM) toe. Anderzijds werden beide diensten minder methoden gemachtigd in de strijd tegen het terrorisme;
- twaalf specifieke en uitzonderlijke methoden werden ingezet ten aanzien van een advocaat, arts of beroepsjournalist. Vorig jaar waren dit er nog 24. Aangezien op één persoon meerdere BIM-methoden kunnen worden toegepast, zegt dit cijfer niets over het aantal beroepsbeoefenaars dat het voorwerp was van een BIM-methode;
- het Vast Comité I werd in 2013 23 keer gevat in plaats van 38 het jaar voordien. Deze daling is toe te schrijven is aan het lagere aantal schorsingen uitgesproken door de BIM-Commissie.

[169] '*dat het dus vereist is hun observatie te beperken tot de duur van hun verblijf in België en indien noodzakelijk de hoogdringendheidsprocedure te hanteren. […] Verklaart de methode onwettelijk wat betreft de "vroegere verantwoordelijken" die niet meer in België verblijven maar die "soms" terugkeren [en] de personen die "deel uitmalen van de directe omgeving" van de geviseerde beweging; Aangezien de methode nog niet ten uitvoer werd gelegd dient de stopzetting, noch de vernietiging van de ten aanzien van deze personen verzamelde gegevens te worden uitgesproken'* (vrij vertaling).

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 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 2013 heeft het Vast Comité I de door de wetgever vereiste verificaties verricht. Daarenboven werd eind december 2013 een omstandige brief gericht naar de ADIV en dit in verband met het Afluisterplan voor het werkingsjaar 2014. Daarin heeft het Comité vragen tot verduidelijk gesteld met betrekking tot de limieten die zowel art. 259*bis* § 5 Strafwetboek als art. 44*bis* W.I&V stellen aan het

intercepteren in het buitenland. De vragen hadden onder meer betrekking op de keuze en de omschrijving van mogelijks te intercepteren 'organisaties of instellingen' en op de motivering ervan vanuit de wettelijke opdrachten van de militaire inlichtingendienst zoals omschreven in artikel 11 W.I&V. Het Vast Comité I ontving in maart 2014 een omstandig antwoord dat werd geanalyseerd met het oog op eventueel verder onderzoek.

HOOFDSTUK V
ADVIEZEN, STUDIES EN ANDERE ACTIVITEITEN

V.1. TWINTIG JAAR DEMOCRATISCH TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

Het Vast Comité I vierde in 2013 zijn twintigjarig bestaan. Ter gelegenheid van deze verjaardag werden een feestbundel uitgegeven en een academische zitting georganiseerd.

Voor de jubileumuitgave '*Inzicht in toezicht. Twintig jaar democratische controle op de inlichtingendiensten*'[170] werden niet minder dan 38 binnen- en buitenlandse academici, politici en practici bereid gevonden om – ieder vanuit zijn of haar ervaring, expertise en interesses – te schrijven over het toezicht op inlichtingendiensten. Daarbij werden alle behandelde thema's in vijf hoofdstukken ondergebracht: (1) Democratische controle op de inlichtingendiensten van 1830 tot 2013; (2) De controle op de inlichtingendiensten in een breder kader; (3) Het Vast Comité I voor het voetlicht; (4) Het Vast Comité I en zijn relatie met de gecontroleerde diensten en de vier machten; en (5) Het gras is (niet altijd) groener aan de overkant (waarin een aantal buitenlandse auteurs hun licht werpen op het Belgische controlesysteem). Er werd afgesloten met een epiloog van de hand van professor emeritus Cyrille Fijnaut.

Het boek werd op 24 mei 2013 in het Federaal parlement voorgesteld tijdens een plechtige zitting. Talrijke vertegenwoordigers uit de hoogste gezagsinstanties van het land, uit de inlichtingengemeenschap, de media, de academische wereld en enkele buitenlandse toezichtorganen tekenden present.

V.2. INFORMATIEDOSSIERS

Naast toezichtonderzoeken (zie hierover uitvoerig Hoofdstuk II), opent het Vast Comité I ook zogenaamde 'informatiedossiers' die moeten toelaten om een

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

gestructureerde respons te bieden op vragen met betrekking tot de werking van de inlichtingendiensten en het OCAD.[171] Indien dergelijke dossiers aanwijzingen van disfuncties aan het licht brengen of van aspecten van de werking van inlichtingendiensten die nader onderzoek behoeven, kan het Comité overgaan tot het initiëren van een toezichtonderzoek. Indien echter duidelijk is dat een dergelijk onderzoek geen meerwaarde ressorteert vanuit de doelstellingen van het Vast Comité I, wordt het informatiedossier gesloten.

In 2013 werd bijvoorbeeld een informatiedossier geopend naar de problematiek van de naleving van de classificatiewetgeving bij de verzending van documenten, naar de plannen om bepaalde (buiten)diensten van de ADIV te centraliseren en naar de mogelijke inlichtingenactiviteiten van het recent opgerichte ISTAR-Bataljon binnen de Krijgsmacht. Wat betreft ISTAR werd de Begeleidingscommissie van de Senaat in kennis gesteld van het juridisch standpunt van het Comité.

V.3. EXPERT OP DIVERSE FORA

Vertegenwoordigers van het Vast Comité I werden in 2013 diverse malen als expert geconsulteerd door binnen- en buitenlandse publieke en private instellingen.

Zo werd de voorzitter van het Comité op 20 februari 2013 uitgenodigd in de Kamercommissie voor de Binnenlandse Zaken waar hoorzittingen werden georganiseerd over de Wet van 19 juli 1991 houdende regeling van het beroep van privédetective. De voorzitter lichtte de positie van het Comité toe ten aanzien van de vraag welke rol het toezichtorgaan kan spelen bij de controle op de private inlichtingensector.[172]

De voorzitter werd op 18 juni 2013 ook gehoord door de Commissie Binnenlandse Zaken en Administratieve Aangelegenheden van de Senaat. Eerder was in de Senaat een voorstel van resolutie ingediend met betrekking tot het snel ontwikkelen van een federale strategie voor de beveiliging van informatie- en communicatiesystemen.[173] Het voorstel vond zijn oorsprong in de vaststellingen en conclusies van het toezichtonderzoek dat het Comité voerde naar de houding van de Belgische inlichtingendiensten tegenover de noodzaak om informatie- en

---

171 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…

172 *Par. St.* Kamer 2012-13, 53-2711/001, 7-9.

173 Parl. St. *Senaat* 2010-11, 4 oktober 2011, nr. 5-1246/1 en Parl. St. Senaat 2012-13, 28 november 2012, nr. 5-1855/1.

communicatiesystemen te beschermen tegen intercepties en cyberaanvallen uit het buitenland. De hoorzittingen kaderden in dit thema.

Begin juni 2013 nam een vertegenwoordiger van het Vast Comité I deel aan de door het *Democratic Centre of Armed Forces* (DCAF) in Tunis georganiseerde rondetafel over 'La transition démocratique et la réforme des services de renseignement'.[174] Door zijn expertise ter beschikking te stellen in dergelijke fora, tracht het Comité een bijdrage te leveren aan het democratiseringsproces van bepaalde landen. De bijeenkomst mondde uit in de oprichting van een interministeriële werkgroep onder leiding van de premier om tot nieuwe wettelijke regelingen te komen voor de Tunesische inlichtingendiensten. In het verlengde hiervan brachten de voorzitter van de 'Instance Nationale de la Protection des Donées Personnelles' en een magistraat verbonden aan het 'Tribunal Administratif' een werkbezoek aan het Vast Comité I.

Op de Litouwse ambassade in Brussel vond een ontmoeting plaats tussen de voorzitters van het *Comité de la Défense et de la Sécurité* enerzijds en van het Vast Comité I anderzijds. Ook hier stond de organisatie van de democratische controle op de inlichtingendiensten en een kennismaking met het Belgische model centraal.

Zoals hierboven aangegeven (Hoofdstuk II.10 en II.11.12), vormden de Snowden-onthullingen het startschot voor vele onderzoeken over heel de wereld. Zo ook in het Europees Parlement. Naar aanleiding van de Resolutie van het Europees Parlement van 4 juli 2013 organiseerde de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken van het Europees Parlement, kortweg de LIBE-Commissie, een reeks hoorzittingen om informatie te verzamelen en om de weerslag van de spionageactiviteiten op de grondrechten en gegevensbeschermingsregels te beoordelen. De voorzitter van het Vast Comité I, Guy Rapaille, werd samen met Senator en lid van de Senatoriële Begeleidingscommissie, Armand De Decker, midden november 2013 in dit kader uitgenodigd. De lopende Belgische onderzoeken werden er kort toegelicht.[175]

Sinds 2011 oefent de voorzitter van het Vast Comité I het voorzitterschap uit van het *Belgian Intelligence Studies Centre (BISC)*. Dit centrum voor inlichtingenstudies wil de inlichtingen- en veiligheidsdiensten en de wetenschappelijke wereld dichter bij elkaar brengen en een bijdrage leveren aan de reflectie over inlichtingenvraagstukken.[176] In 2013 organiseerde het BISC drie studiedagen: 'Kroniek van mijn verborgen oorlog, 1941-1944' (maart 2013), 'Spionage tijdens de Koude Oorlog revisited' (juni 2013) en 'Open source and social media intelligence' (december 2013).

---

174 www.dcaf-tunisie.org.

175 European Parliament, LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, The role of parliamentary oversight of intelligence services at national level in an era of mass surveillance, Statement by Mr Guy Rapaille, Chair of the Belgian Intelligence Services Oversight Committee, 14 november 2013 (www.europarl.europa.eu).

176 www.intelligencestudies.be.

In 2013 werd de frequentie van de werkzaamheden van de zogenaamde 'Werkgroep Analyse', waarin vertegenwoordigers van de twee inlichtingendiensten én het Vast Comité zetelen, opgevoerd. Deze werkgroep trof de voorbereidingen voor de verdere ontwikkeling van de *Belgian Intelligence Academy* (BIA)[177], een academie die opleidingen voor analisten uit zowel de burgerlijke als de militaire inlichtingendienst zal organiseren. Ten behoeve van deze inlichtingenacademie werden ondertussen ook de beheersorganen opgericht: een Directiecomité, een Uitvoerend Comité met aanstelling van een directeur en een secretariaat en een Wetenschappelijk Comité. De voorzitter van het Vast Comité I treedt op als waarnemer bij het Directiecomité en ook minstens één vertegenwoordiger van het Comité maakt deel uit van het Wetenschappelijk Comité. Een eerste 'test case Intelligence and Analysis Course (IAC)' die liep van half juni tot half juli 2013, werd geëvalueerd en een protocolakkoord tussen de betrokken ministers voorbereid. Tevens werd begin juni 2013 door vertegenwoordigers van de VSSE, ADIV en het Vast Comité I in Parijs een werkbezoek gebracht aan de 'Académie française du Renseignement'.

Ten slotte werd het Vast Comité I in 2013 ook vanuit de academische wereld geconsulteerd. De voorzitter van het Comité maakte deel uit te maken van een jury van het Franse 'Centre des Hautes Etudes du Ministère de l'Intérieur' voor een thesisverdediging.[178] Verder neemt het Comité als expert deel aan een onderzoek over de 'nieuwe uitdagingen voor het inlichtingenbeleid in Frankrijk' dat wordt uitgevoerd door Prof. Sébastien Laurent, verbonden aan de Universiteit van Bordeaux. Ook werden gastcolleges gegeven aan de universiteiten van Luik en Louvain-la-Neuve, werd deelgenomen aan de Jobday van de faculteit Rechten, Politieke Wetenschappen en Criminologie van de universiteit van Luik alsook aan een panelgesprek van de Vlaamse Liga voor Mensenrechten over privacy en veiligheid.

V.4. LID VAN EEN SELECTIECOMITÉ

De voorzitter van het Vast Comité I werd, samen met de voorzitter van de Cel voor Financiële Informatieverwerking (CFI) en de directeur van het Coördinatieorgaan voor de dreigingsanalyse (OCAD), aangesteld als lid van het selectiecomité belast met het geven van een omstandig advies aan de ministers van Binnenlandse Zaken en Justitie omtrent de kandidaturen voor de post van adjunct-directeur van het Coördinatieorgaan voor de dreigingsanalyse.[179]

---

177 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'.*

178 De thesis had betrekking op 'L'action des services de renseignement à l'épreuve du droit: quelles insuffisances, quelles améliorations?'.

179 M.B. van 29 maart 2013 houdende aanwijzing van een selectiecomité belast met de evaluatie van de kandidaturen voor de post van adjunct-directeur van het Coördinatieorgaan voor de dreigingsanalyse, *BS* 8 april 2013.

V.5. ONTWERP VAN WETSVOORSTEL TOT WIJZIGING VAN DE CLASSIFICATIEWET

De Begeleidingscommissie van de Senaat droeg het Comité midden 2013 op om een wetsvoorstel uit te werken om de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (W.C&VM) aan te passen. Dit met het oog op een *overruling*-procedure of een automatische declassificatie wanneer een bepaalde classificatie niet voldoende verantwoord lijkt. De vraag van de Senaat kaderde in eerdere aanbevelingen van het Comité.[180] Gelet op andere prioriteiten, kon het Comité dit voorstel niet finaliseren. Een voorstel zal worden uitgewerkt en overgezonden aan de nieuwe Begeleidingscommissie van de Kamer van Volksvertegenwoordigers.

V.6. CONTROLE SPECIALE FONDSEN ADIV

Het Rekenhof houdt namens de Kamer van Volksvertegenwoordigers toezicht op het gebruik van de financiële middelen door overheidsdiensten. Het moet daarbij de wettigheid en de rechtmatigheid van alle uitgaven controleren. 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.

V.7. 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.

180 VAST COMITÉ I, *Activiteitenverslag 2006*, 137.

Datum	Onderwerp/titel	Forum
Voorjaar 2013	Interview met Guy Rapaille, voorzitter van het Vast Comité I	Diplomatic World nr. 38
4 april 2013	'Filip Dewinter et le Vlaams Belang visés par la Surêté'	L'Echo
4 april 2013	'Staatsveiligheid stak dossier Dewinter niet in doofpot'	De Tijd
6 mei 2013	'Nieuw gezicht in controlecomité inlichtingendiensten'	MO*
24 mei 2013	'De cultuur van het geheim neemt toe'	MO*
25 mei 2013	'Leger in opspraak over 'geheime' geheime dienst'	De Tijd
6 juni 2013	'Staatsveiligheid gecontroleerd'	VRT, Radio 1, Joos
10 juni 2013	'Les renseignements belges'	RTBF, Radio Première, Face à l'info
27 juni 2013	'Des renseignements plus professionnels'	Le Soir
5 augustus 2013	'Controlecomité inlichtingendiensten start groot Prism-onderzoek'	MO*
18 september 2013	'NSA kreeg blanco cheque in België'	De Morgen
22 september 2013	'Vision stratégique de la cyber-sécurité: un désintérêt général'	RTBF-TV, Mise au point
23 oktober 2013	'Staatsveiligheid leeft meldingsplicht aan minister niet na'	De Morgen
23 oktober 2013	'142 namen van politici in dossiers Staatsveiligheid'	MO*
31 oktober 2013	'A quoi sert l'espionnage?'	RTBF, Radio Première, Le forum du midi

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). Op dat ogenblik 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 2013 voerde de Dienst Enquêtes I een aanzienlijk aantal onderzoeksdaden uit in het kader van twee belangrijke onderzoeken. Zo werden bijvoorbeeld 56 processen-verbaal opgesteld.

Een eerste onderzoek, opgestart eind 2011 en uitgevoerd in opdracht van het Federaal Parket naar mogelijke geldverduistering door inlichtingenagenten, werd afgerond in 2013. Het dossier werd door het Federaal Parket zonder gevolg geklasseerd. Niettemin heeft het toegelaten om de noodzaak te benadrukken om werk te maken van een fundamentele aanpassing van het fondsenbeheer bestemd voor de uitbetaling van bronnen van inlichtingendiensten.

Het tweede dossier, waaraan gelijkaardige feiten ten grondslag lagen en dat in handen was van het parket van Antwerpen, kon niet worden afgerond in 2013.

Deze twee gerechtelijke dossiers toonden de noodzaak aan om in detail de geldende regels en praktijk te analyseren met betrekking tot het beheer van fondsen voor de uitbetaling van informanten, en dit bij beide inlichtingendiensten. Het Comité besliste dan ook hieromtrent een toezichtonderzoek te openen (zie II.10.3).

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 (of zijn plaatsvervanger) 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 treedt het Beroepsorgaan ook op 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.[181]

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 2013 kende het aantal beroepen en beslissingen een spectaculaire groei in vergelijking met 2012: 189 beroepen tegenover 91 en 187 beslissingen tegenover 81. Deze stijging is vooral toe te schrijven aan het feit dat er in de loop van 2013 veel beroepen werden aangetekend door kandidaat-militairen die een negatief veilig-

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

heidsadvies kregen van de ADIV, die in deze optreedt als veiligheidsoverheid in een nieuwe procedure van selectie en aanwerving.[182] Daarnaast viel er ook een sterke aangroei te noteren van het aantal beroepen tegen negatieve veiligheidsadviezen in het kader van de toekenning van luchthavenidentificatiebadges.

Tabel 1. Betrokken veiligheidsoverheid

	2011	2012	2013
Nationale Veiligheidsoverheid	21	40	98
Veiligheid van de Staat	2	0	1
Algemene Dienst inlichting en veiligheid	39	27	78[183]
Crisiscentrum van de Regering	0	0	0
Federaal Agentschap voor Nucleaire Controle	7	11	9
Federale politie	1	1	1
Lokale politie	0	2	2
Lokale luchthavencommissie	1	10	–[184]
TOTAAL	**71**	**91**	**189**

Tabel 2. Aard van de bestreden beslissing

	2011	2012	2013
Veiligheidsmachtigingen			
Vertrouwelijk	14	7	5
Geheim	31	29	56
Zeer geheim	9	9	5
Totaal veiligheidsmachtigingen	54	45	66

182 Zie art. 9 Wet 28 februari 2007 tot vaststelling van het statuut van de militairen van het actief kader van de Krijgsmacht en tot wijziging van sommige bepalingen betreffende het statuut van het militair personeel zoals gewijzigd bij art. 24 Wet 31 juli 2013 (*BS* 20 september 2013).

183 Zoals uiteengezet in de inleiding bij dit hoofdstuk is de sterke stijging van het aantal dossiers komende van de ADIV te wijten aan het systeem waarbij kandidaat-militairen kunnen onderworpen worden aan een veiligheidsverificatie.

184 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.

	2011	2012	2013
Weigering	32	33	41
Intrekking	21	12	5
Weigering en intrekking	–	–	4
Machtiging voor beperkte duur	0	0	1
Machtiging voor lager niveau	1	1	0
Geen beslissing binnen termijn	0	1	15
Geen beslissing binnen verlengde termijn	0	0	0
Totaal veiligheidsmachtigingen	54	45	66
SUBTOTAAL VEILIGHEIDSMACHTIGINGEN	**54**	**45**	**66**
Veiligheidsattesten geclassificeerde documenten			
Weigering	0	23	0
Intrekking	0	0	0
Geen beslissing binnen termijn	0	0	0
Veiligheidsattesten plaats of gebeurtenis			
Weigering	14	0	15
Intrekking	0	0	0
Geen beslissing binnen termijn	0	0	0
Veiligheidsadviezen			
Negatief advies	3	23	106
Geen advies	0	0	2
'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	**17**	**46**	**123**
TOTAAL BESTREDEN BESLISSINGEN	**71**	**91**	**189**

Tabel 3. Hoedanigheid van de verzoeker

	2011	2012	2013
Ambtenaar	4	5	4
Militair	37	26	26
Particulier	29	54	159
Rechtspersoon	1	6	0

Tabel 4. Taal van de verzoeker

	2011	2012	2013
Franstalig	32	51	92
Nederlandstalig	39	40	97
Duitstalig	0	0	0
Anderstalig	0	0	0

Tabel 5. Aard van de door het Beroepsorgaan genomen voorbereidende beslissingen[185]

	2011	2012	2013
Volledig dossier opvragen (1)	68	90	187
Aanvullende informatie opvragen (2)	5	5	12
Horen lid overheid (3)	4	10	3
Beslissing voorzitter (4)	0	0	0
Informatie uit dossier halen door Beroepsorgaan (5)	24	44	68
Informatie uit dossier halen door inlichtingendienst (6)	0	0	0

185 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 2012, terwijl de beslissing pas viel in 2013.

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

	2011	2012	2013
Dossierinzage door klager / advocaat	48	54	103
Horen van de klager / advocaat[186]	55	65	138

Tabel 7. Aard van de beslissingen van het beroepsorgaan

	2011	2012	2013
Veiligheidsmachtigingen			
Beroep onontvankelijk	5	0	2
Beroep zonder voorwerp	1	1	3
Beroep ongegrond	29	19	20
Beroep gegrond (volledige of gedeeltelijke toekenning)	19	23	35
Bijkomende onderzoeksdaden door overheid	1	1	0
Bijkomende termijn voor overheid	0	0	14[187]

186 In bepaalde dossiers wordt de klager/advocaat meermaals gehoord.
187 Deze dossiers hadden 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 14 gevallen de NVO een bijkomende termijn te verlenen om alsnog een beslissing te nemen.

	2011	2012	2013
Veiligheidsattesten geclassificeerde documenten			
Beroep onontvankelijk	0	0	0
Beroep zonder voorwerp	0	0	0
Beroep ongegrond	0	0	0
Beroep gegrond (toekenning)	0	0	0
Veiligheidsattesten plaats of gebeurtenis			
Beroep onontvankelijk	1	3	1
Beroep zonder voorwerp	0	1	0
Beroep ongegrond	7	8	6
Beroep gegrond (toekenning)	4	6	11
Veiligheidsadviezen			
Beroep onbevoegd	0	5	0
Beroep onontvankelijk	0	1	4
Beroep zonder voorwerp	0	0	1
Bevestiging negatief advies	0	9	25
Omvorming in positief advies	3	4	65[188]
Beroep tegen normatieve rechtshandelingen	0	0	0
TOTAAL	**70**	**81**	**187**

188 Zoals uiteengezet in de inleiding bij dit hoofdstuk is de stijging van het aantal dossiers inzake veiligheidsadviezen toe te schrijven aan de beroepen van kandidaat-militairen en aan personen die een luchthavenidentificatiebadge moeten bekomen.

HOOFDSTUK VIII
DE INTERNE WERKING VAN HET VAST COMITÉ I

VIII.1. SAMENSTELLING VAN HET VAST COMITÉ I

Tijdens zijn plenaire vergadering van 2 mei 2013 is de Senaat overgegaan tot de benoeming van twee werkende leden, van twee plaatsvervangende voorzitters en van vier plaatsvervangende leden van het Vast Comité I.[189] Gérald Vande Walle werd opnieuw verkozen tot Franstalig werkend lid. Pieter-Alexander De Brock, gedetacheerd expert bij het Coördinatieorgaan voor de dreigingsanalyse, werd verkozen tot Nederlandstalig raadsheer. Zij legden op 8 mei 2013 de eed af in handen van de voorzitster van de Senaat. Guy Rapaille, advocaat-generaal bij het hof van beroep te Luik, werd reeds eerder herbenoemd.

Ook bij de Dienst Enquêtes I vielen er verschuivingen te noteren. Een Nederlandstalige en Franstalige commissaris-auditor besloten de dienst te verlaten. Zij werden respectievelijk in maart 2013 en januari 2014 vervangen. Eind 2013 besloot ook directeur Pierre Nivelle de Dienst Enquêtes I te verlaten. Hij werd op 2 december 2013 vervangen door Frank Franceus, die tot dan werkzaam was als commissaris-auditor. Hij werd benoemd voor een termijn van vijf jaar met aanvang op 1 januari 2014. Het personeelsbestand van deze dienst viel terug op vijf *fulltime* equivalenten.

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

VIII.2. VERGADERINGEN MET DE BEGELEIDINGSCOMMISSIE(S)

In de loop van 2013 vonden zes vergaderingen plaats met de Senatoriële Begeleidingscommissie aan wie het Vast Comité I rapporteert. Tijdens deze vergaderingen werden – achter gesloten deuren – de toezichtonderzoeken besproken. Ook het

189 *BS* 21 mei 2013. Pierre Vanderheyden, advocaat-generaal bij het hof van beroep van Luik, werd aangeduid als eerste plaatsvervangend voorzitter; Emile Dejehansart, raadsheer bij het hof van beroep van Bergen, werd tweede plaatsvervangend voorzitter. Carmelo Zaïti, Philippe Meire, Herman Daens en Frank Franceus, werden aangesteld als plaatsvervangende leden.

'zesmaandelijkse verslag over de toepassing van de specifieke en uitzonderlijke methoden door de inlichtingen- en veiligheidsdiensten en de controle hierop door het Vast Comité I voor het werkingsjaar 2012', kwam aan bod. Tevens vond er in oktober 2013 een vergadering plaats met de Begeleidingscommissies van zowel de Kamer van Volksvertegenwoordigers als van de Senaat. Tijdens deze vergadering werd het *Activiteitenverslag 2012* van het Vast Comité I besproken[190] en stond een gemeenschappelijk toezichtonderzoek van de Vaste Comités I en P geagendeerd.

De samenstelling van de Senaatscommissie onderging een wijziging. Sabine de Bethune (CD&V) nam het voorzitterschap van de commissie waar. Verder maakten Dirk Claes (CD&V), Armand De Decker (MR), Philippe Mahoux (PS) deel uit van de commissie. Danny Pieters (N-VA) werd op 17 juli 2013 vervangen door Karl Vanlouwe (N-VA).[191]

Ingevolge de Wet van 6 januari 2014[192], verhuisde de begeleiding van het Vast Comité I van de Senaat naar een ééngemaakte 'Commissie belast met de begeleiding van het Vast Comité P en het Vast Comité I' in de Kamer, die zowel de politie- als de inlichtingendiensten zal controleren.

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 gemeenschappelijke toezichtonderzoeken. In 2013 vonden vijf gemeenschappelijke vergaderingen plaats.

VIII.4. FINANCIËLE MIDDELEN EN BEHEERSACTIVITEITEN

Voor het werkingsjaar 2013 werd aan het Vast Comité I een dotatie toegekend van 3,86 miljoen euro tegenover 3,93 miljoen euro in 2012.[193] In 2013 kon het Vast Comité I ten volle zijn voordeel halen uit de kostenbesparing door schaalvergroting als uitloper van zijn verhuis naar het FORUM-gebouw van de Kamer van Volksvertegenwoordigers. Inzake werkingskosten werden bovendien nieuwe synergiën met de Kamer ontwikkeld.

---

190 *Parl. St.* Senaat 2013-14, nr. 5-2426/1 en *Parl. St.* Kamer 2013-14, nr. 53K3496/1.
191 *Hand.* Senaat 2012-13, 17 juli 2013, nr. 5-113, 7.
192 *B.S.* 31 januari 2014.
193 Wet van 4 maart 2013 houdende de algemene uitgavenbegroting voor het begrotingsjaar 2013, *BS* 15 maart 2013 en *Parl. St.* Kamer 2012-2013, nr. 53K2578/001.

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
2012-2013 2013-2014	Hogere Studies Veiligheid en Defensie	KHID	Brussel
14 januari 2013	Le renseignement en réseaux	Métis	Parijs
17 januari 2013	Renseignement de sources ouvertes: sommes-nous tous des capteurs?	KHID	Brussel
1 maart 2013	Cybercriminalité – Enjeux et actualités	Université de Namur – B-CCentre – CRIDS	Namen
19 maart 2013	Kroniek van mijn verborgen oorlog, 1941-1944	BISC	Brussel
26 maart 2013	De conflicten tussen het Belgische recht en het lokaal recht	Studiecentrum voor Militair recht en Oorlogsrecht	Brussel
26 maart 2013	Le paysage nucléaire militaire en mutation	Académie royale de Belgique	Brussel
27 maart 2013	Cybercrime – Risks to Operative Derived from Smart Phones, the Internet en Social Media	Ambassade Verenigd Koninkrijk	Brussel
4 april 2013	Modernisation et cadre juridique du renseignement en France	Université de Lille	Rijsel
29 april 2013	Le renseignement en question: les sources ouvertes	Métis	Parijs
22-23 mei 2013	Changing Intelligence Challenges	GFF – CATS – Swedish National Defence College – SUPO	Stockholm
3 juni 2013	Rencontre coordination du renseignement	BIA	Parijs
10 juni 2013	Spionage tijdens en na de Koude Oorlog revisited	BISC	Brussel

DATUM	TITEL	ORGANISATIE	PLAATS
13 juni 2013	L'action des services de renseignement à l'épreuve du droit	Centre des hautes études du Ministère de l'Intérieur	Paris
13 juni 2013	Intelligence stratégique	HEC Liège – BISC	Seraing
21 juni 2013	Diplomatic security conference	ECSA	Brussel
24 juni 2013	Le renseignement en question: les sources ouvertes	Métis	Parijs
27 juni 2013	Security & Defence Day Conference	Security & Defence– SDA – CEIS – KAS	Brussel
10 juli 2013	Le rapport Urvoas: quel contrôle des services de renseignement?	HCFDC	Parijs
19 september 2013	Beyond the security vs privacy debate	Security & Defence	Brussel
20 september 2013	Single table lunch meeting (Mr Leonard H. Schrank)	ECSA	Brussel
30 september 2013	Ethique et renseignement	GERER	Parijs
16 oktober 2013	TIGFI Finance Lunch	The Institute for Global Financial Integrity	Luxemburg
21 oktober 2013	De Belgische wapenhandel	Vlaams Vredesinstituut – GRIP	Brussel
24 oktober 2013	Single table lunch meeting (Mr André Vandoren)	ECSA	Brussel
15 november 2013	Les Assises de l'Intelligence Stratégique	Agence de Stimulation économique – Université Louvain-la-Neuve	Louvain-la-Neuve
21 november 2013	Avonddebat 'Privacy'	Liga voor Mensenrechten	Brussel
27 november 2013	10 jaar BOM – balans en uitdagingen	Federale politie (DJO/BTS)	Brussel
6 december 2013	Open source & social media intelligence	BISC	Brussel
16 december 2013	Ethique et renseignement	GERER	Parijs

VIII.6. EVALUATIE VAN DE INTERNE WERKPROCESSEN

Het Vast Comité I heeft – net zoals in 2009 – zijn interne werkprocessen grondig geëvalueerd. Het betreft meer specifiek de werkstromen in het kader van de uitvoering van toezichtonderzoeken, de afhandeling van BIM-dossiers of nog, de behandeling van de dossiers van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en –adviezen. Aan de hand van de bevindingen hieromtrent kon het Vast Comité I zijn interne werking optimaliseren.

HOOFDSTUK IX
AANBEVELINGEN

Op basis van de in 2013 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. UITVOERING VAN DE ARTIKELEN 19 EN 20 W.I&V[194]

Het Comité herhaalt opnieuw dat het, conform artikelen 19 en 20 W.I&V, aan de bevoegde ministers en aan het Ministerieel Comité voor inlichtingen en veiligheid toekomt om te bepalen onder welke voorwaarden de Belgische inlichtingendiensten moeten of kunnen samenwerken met buitenlandse inlichtingendiensten. Het Vast Comité I acht het hiertoe noodzakelijk dat de beide inlichtingendiensten ten laatste midden 2015 gezamenlijk een voorstel zouden formuleren aan het Ministerieel Comité waarin alle aspecten van de problematiek aan bod komen.

Specifiek aan de ADIV beveelt het Vast Comité I aan dat een studie zou worden uitgevoerd over de eventuele verantwoordelijkheid wanneer de dienst informatie en/of inlichtingen met een buitenlandse inlichtingendienst of instantie uitwisselt.

---

194 Deze aanbeveling stamt uit de onderzoeken naar 'De rol van de Algemene Dienst inlichting en veiligheid bij de opvolging van het conflict in Afghanistan' (zie II.1) en 'De opvolging van politieke mandatarissen door de inlichtingendiensten' (II.4).

IX.1.2. EEN RICHTLIJN OVER INLICHTINGENWERK T.A.V. PERSONEN MET BIJZONDERE VERANTWOORDELIJKHEDEN EN POLITIEKE PARTIJEN[195]

Het Vast Comité I wenst dat de Veiligheid van de Staat én de Algemene Dienst inlichting en veiligheid een gezamenlijk initiatief nemen naar het Ministerieel Comité voor inlichting en veiligheid met het oog op de aanname van een uniforme richtlijn met klare en eenduidige regels met betrekking tot de inwinning, de verwerking, de raadpleging (met inbegrip van de eventuele interne afscherming), de opslag en de archivering van gegevens van bepaalde categorieën van personen die bijzondere verantwoordelijkheden dragen of droegen evenals van politieke partijen. Bij het uitwerken van deze richtlijn moet rekening worden gehouden met de vrijheid van vereniging, de vrijheid van meningsuiting en de krijtlijnen uitgetekend in het arrest van het Europees Hof voor de Rechten van de Mens in de zaak 'Segerstedt-Wiberg and others' en moet gestalte gegeven worden aan het in artikel 2 van de Wet van 30 november 1998 gestelde principe: '*Bij het vervullen van hun opdrachten zorgen die diensten voor de naleving van, en dragen bij tot de bescherming van de individuele rechten en vrijheden alsook tot de democratische ontwikkeling van de maatschappij*'.

Het Comité wijst er ten slotte op dat het aan de wetgever toekomt om desgewenst bijzondere waarborgen in te bouwen voor politieke mandatarissen door een eventuele aanpassing van de wetgeving (bijvoorbeeld in de BIM-wet) en/of door een bijzonder toezicht op te dragen aan het Vast Comité I. Daarbij dient evenwel rekening te worden gehouden met het belang van een normale werking en ontwikkeling van de democratische instellingen alsook met de wettelijke opdrachten van de inlichtingendiensten.

IX.1.3. EENDUIDIGE RICHTLIJNEN OMTRENT HET MELDEN VAN DE OPVOLGING VAN POLITICI

Aansluitend bij de vorige aanbeveling, is het Comité van oordeel dat het aan de bevoegde ministers – als hiërarchisch en politiek verantwoordelijke overheid – toekomt om te bepalen in welke gevallen en wanneer zij in kennis wensen te worden gesteld. Daarbij is van belang dat de ministers duidelijk de finaliteit en de modaliteiten[196] van dergelijke kennisgeving omschrijven.

---

195 Deze aanbeveling werd geformuleerd naar aanleiding van de toezichtonderzoeken 'Geheime nota's over de Scientologykerk in de pers (II.2.), 'Een informant binnen het Vlaamse Belang?' (II.3) en 'De opvolging van politieke mandatarissen door de inlichtingendiensten (II.4). Het Comité herneemt daarmee de aanbeveling uit zijn onderzoek 'gereserveerde dossiers', zie VAST COMITÉ I, *Activiteitenverslag 2008*, 110-111.

196 Onmiddellijk of periodieke melding; alleen melding van collectedocumenten, analyseverslagen en/of verslagen die bestemd zijn voor externe diensten; melding ook voor regionale minis-

IX.1.4. PERMANENTE VORMING EN REËLE KWALITEITSBEWAKING INZAKE COLLECTEVERSLAGEN[197]

Het Comité is zich bewust van het feit dat het in het inlichtingenwerk niet steeds evident is 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 of en op welke wijze een bepaald feit in een collecteverslag wordt opgenomen een cruciaal gegeven vormt. De wijze waarop die *input* dient te gebeuren zou het voorwerp moeten zijn van permanente vorming en onderworpen worden aan een ernstige kwaliteitsbewaking.

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

IX.2.1. AANBEVELINGEN IN HET KADER VAN BUITENLANDSE MISSIES VAN DE ADIV

In het kader van zijn toezichtonderzoek naar 'De rol van de Algemene Dienst inlichting en veiligheid bij de opvolging van het conflict in Afghanistan (II.1), werden diverse punctuele aanbevelingen geformuleerd.[198] Het Vast Comité I:

– beveelt aan dat de ADIV de verbanden definieert die tussen operationele, tactische en strategische inlichtingen en de wettelijke opdrachten beschreven in de W.I&V, moeten gelegd worden;
– raadt de ADIV aan om een bundel op te maken van de teksten die toepasselijk zijn tijdens een ontplooiing van de ADIV, met daarin zowel de internationale als de nationale regels. Wat deze laatste betreft, dringt een betere integratie en grotere coherentie van de inhoud zich op;

---

ters en parlementsleden en/of hoogwaardigheidsbekleders van de rechterlijke macht; eventuele controle hierop door het Vast Comité I via een autonome toegang tot de database …

197 Deze aanbeveling komt voort uit het toezichtonderzoek naar 'vermeende strafbare feiten van een buitenlandse inlichtingendienst en de informatiepositie van de VSSE' (II.6).

198 In reactie op het verslag stelde dat ADIV dat de aanbevelingen '*een wezenlijke bijdrage kunnen leveren voor de optimalisatie van organisatie en werking van ADIV. Hoewel het onderzoek zich focust op één operatie, die in meer dan 10 jaren grondige wijzigingen heeft ondergaan, blijft het zeker representatief voor het actuele inlichtingenwerk van ADIV.*' Ook blijkt dat de dienst reeds een aanvang heeft genomen met de implementatie van verschillende aanbevelingen. Het Comité kan zich hierover alleen maar verheugen.

- meent dat het noodzakelijk is om de opleiding van het personeel voorafgaand aan het vertrek voor een opdracht te versterken, en spoort de ADIV aan de al ondernomen verbeteringen voort te zetten;
- meent dat het noodzakelijk is dat de ADIV de C*omprehensive Preparation of the Operational Environnement*-methode toepast (of elke andere methodologie die hetzelfde doel beoogt) en vooral rekening houdt met de behoeften die de militaire partners in het kader van de voorbereiding van opdrachten uitdrukken;
- beveelt aan dat de ADIV ten aanzien van zijn klanten een proactieve houding zou aannemen, om zo meer precies te kunnen bepalen welke hun verwachtingen zijn maar ook om de klanten een duidelijk beeld te verschaffen over wat de ADIV kan aanleveren;
- raadt de ADIV aan een algemene inschatting te maken van de risico's voor het in de conflictzone ontplooide militair en burgerlijk personeel, en voorstellen te formuleren om met die risico's om te gaan;
- spoort de ADIV aan om nader de rol te bepalen van analisten die ingezet worden in een omgeving waar aan collecte wordt gedaan, in het bijzonder met het oog op het garanderen van de objectiviteit van de analysefunctie;
- raadt de ADIV een meer systematische benadering aan bij het inzetten van het personeel in de conflictzone. Een dergelijke benadering, waarbij vertrokken wordt van de bedreigingen die de ADIV in het kader van de W.I&V moet opvolgen, is fundamenteel ten einde te bepalen welke de in te zetten menselijke en materiële middelen zijn;
- meent dat het ontplooide ADIV-personeel in de conflictzone over geschikt materieel moet beschikken, in het bijzonder wat betreft de communicatiemiddelen en de voertuigen die ter beschikking van de BENIC worden gesteld.

IX.2.2. EEN DEBAT OVER DE INZET VAN BIM-METHODEN IN HET BUITENLAND

Om in het buitenland uitgezonden communicaties te onderscheppen, bijvoorbeeld om redenen van veiligheid en bescherming van onze troepen en van deze van onze geallieerde partners tijdens de opdrachten in het buitenland, beschikt de ADIV over een specifiek wettelijk mandaat (art. 259*bis* § 5 Sw. *juncto* art. 11 § 2, 3° W.I&V). Dat ontbreekt voor de inzet van bijzondere inlichtingenmethoden. Het Comité beveelt aan dat de wetgever een debat zou voeren over de noodzaak om bepaalde BIM-methoden mogelijk te maken in het buitenland. De minister van Defensie onderschreef de idee – onder meer met het oog op de naleving van de mensenrechten en de operationele behoeften op het terrein – om aan deze problematiek specifiek aandacht te besteden en koppelde dit aan een evaluatie van de BIM-Wet.

IX.2.3. EENDUIDIGE CONCEPTEN VOOR DE ORGANISATIE VAN DE DATABANK

In zijn toezichtonderzoek naar de opvolging van politieke mandatarissen (II.4), heeft het Vast Comité I moeten vaststellen dat de concepten die aan de basis van de organisatie van de databank van de VSSE liggen, fundamentele problemen met zich meebrengen omdat ze niet eenduidig worden geïnterpreteerd of als dusdanig worden toegepast. Hierdoor dreigt het inlichtingenwerk aan doelmatigheid en doeltreffendheid te verliezen omdat het risico bestaat dat niet (al) de juiste verslagen 'aan de oppervlakte komen' wanneer dit nodig is met het oog op het analysewerk. Ook bestaat het risico dat verkeerde conclusies worden getrokken. Het Vast Comité I is dan ook van mening dat de VSSE deze concepten dringend zou moeten herbekijken, zeker wanneer ze voorkomen in documenten die buiten de VSSE verspreid worden.

Het Vast Comité I is daarenboven van mening dat er actueel een concept ontbreekt: de aanduiding van de (vermoedelijke) rol van een in een verslag vernoemd persoon ten aanzien van de dreiging: is hij een 'voorbijganger', een 'mogelijk slachtoffer', een 'sleutelfiguur', een 'actor'…?

IX.2.4. CONCLUSIES VAN HET ANALYSEWERK SCHRIFTELIJK VASTLEGGEN[199]

Het Comité beveelt aan dat de VSSE elke analyse systematisch afsluit met een (weze het beknopte of voorlopige) conclusie, teneinde vast te leggen óf en op welke wijze en met welke intensiteit het voorwerp van de analyse (een persoon, groepering, gebeurtenis of fenomeen) verder moet worden opgevolgd.

IX.2.5. DE CONTROLE OP BUITENLANDSE INLICHTINGENDIENSTEN

Opnieuw is de noodzaak gebleken voor een uitbreiding van de bevoegdheden van de inlichtingendiensten inzake de controle op buitenlandse inlichtingendiensten.[200] Het Comité herinnert dan ook aan zijn aanbeveling en die van de Senaat om in de Wet houdende regeling van de inlichtingen- en veiligheidsdiensten een specifieke bevoegdheid op te nemen betreffende de controle van de wettelijkheid van de activiteiten van de buitenlandse inlichtingendiensten op Belgisch grondgebied.[201]

---

199 Deze aanbeveling komt voort uit het toezichtonderzoek naar 'vermeende strafbare feiten van een buitenlandse inlichtingendienst en de informatiepositie van de VSSE' (II.6).

200 *Ibid.*

201 VAST COMITÉ I, *Activiteitenverslag 2006*, 132.

IX.2.6. HOOGDRINGENDHEIDPROCEDURE IN GEVAL VAN ARTIKEL 13/1, § 2 W.I&V

Artikel 13/1 § 2, derde lid W.I&V verleent de (voltallige) BIM-Commissie de mogelijkheid om aan inlichtingenagenten de uitdrukkelijke toelating te verlenen om strafbare feiten te begaan die strikt noodzakelijk zijn voor de efficiëntie van de uitvoering van een BIM-methode of ter verzekering van hun eigen veiligheid of die van andere personen. De wet heeft hierbij echter niet voorzien in een procedure van hoogdringendheid. Het Comité is van oordeel dat wanneer de bijzondere methode zelf bij hoogdringendheid kan worden ingezet, ook in de mogelijkheid moet worden voorzien dat de accessoire bevoegdheid uit artikel 13/1 § 2, derde lid, W.I&V bij hoogdringendheid kan worden uitgeoefend.

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

'*De inlichtingendiensten, het Coördinatieorgaan voor de dreigingsanalyse en de andere ondersteunende diensten, zenden uit eigen beweging aan het Vast Comité I de interne reglementen en richtlijnen over, alsook alle documenten die de handelswijze van de diensten regelen*', aldus artikel 33 § 2 W.Toezicht. Het is niet de eerste maal[202] dat het Vast Comité I heeft moeten vaststellen dat deze verplichting niet strikt wordt nageleefd, in het bijzonder wat betreft de ADIV, het OCAD en de ondersteunende diensten. De nauwgezette toepassing door de gecontroleerde diensten van dit artikel vormt een *conditio sine qua non* met het oog op een doeltreffende uitvoering van de opdracht van het Comité. Om deze reden onderlijnt het Comité andermaal het belang van de tijdige, volledige en ambtshalve toezending van deze gegevens.

[202] 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.

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 2013 TOT 31 DECEMBER 2013)

Wet 30 juli 2013 houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van strafvordering, *BS* 23 augustus 2013

Wet 31 juli 2013 tot wijziging van de wet van 28 februari 2007 tot vaststelling van het statuut van de militairen van het actief kader van de Krijgsmacht en tot wijziging van sommige bepalingen betreffende het statuut van het militair personeel, *BS* 20 september 2013

K.B. 14 januari 2013 besluit tot uitvoering van de wet van 4 december 2012 tot wijziging van het Wetboek van de Belgische nationaliteit teneinde het verkrijgen van de Belgische nationaliteit migratieneutraal te maken, *BS* 21 januari 2013

K.B. 23 juli 2013 tot wijziging van het koninklijk besluit van 21 juni 1996 houdende oprichting van een Ministerieel Comité voor inlichting en veiligheid, *BS* 30 juli 2013

K.B. 4 september 2013 tot vaststelling van de bedragen van de retributies verschuldigd zijn voor het afgeven van veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, *BS* 7 oktober 2013

K.B. 4 september 2013 tot vaststelling van de samenstelling, de werkwijze en de bevoegdheden van het Beheerscomité van de Nationale Veiligheidsoverheid, een Staatsdienst met afzonderlijk beheer, *BS* 7 oktober 2013

K.B. 7 oktober 2013 tot bepaling van de inwerkingtredigen van sommige bepalingen van de wet van 15 augutus 2012 houdende oprichting en organisatie van een federale dienstenintegrator, *BS* 23 oktober 2013

M.B. 7 januari 2013 betreffende de samenstelling van de examencommissies voor de taalexamens voor de zittijd van december 2012-januari 2013, *BS* 13 februari 2013

M.B. 29 maart 2013 houdende aanwijzing van een selectiecomité belast met de evaluatie van de kandidaturen voor de post van adjunct-directeur van het Coördinatieorgaan voor de dreigingsanalyse, *BS* 8 april 2013

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten – Directeur van de Dienst Enquêtes – Benoeming, *BS* 30 januari 2013

Omzendbrief 8 maart 2013 betreffende bepaalde aspecten van de wet van 4 december 2012 tot wijziging van het Wetboek van de Belgische nationaliteit teneinde het verkrijgen van de Belgische nationaliteit migratieneutraal te maken, *BS* 14 maart 2013

Benoeming van de twee werkende leden, twee plaatsvervangende voorzitters en vier plaatsvervangende leden van het Vast Comité van toezicht op de inlichtingendiensten (Comité I), *BS* 25 mei 2013

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 2013 TOT 31 DECEMBER 2013)

Senaat

Wetsvoorstel tot wijziging van artikelen 137 en 138 van het Strafwetboek, teneinde de strijd tegen het terrorisme op te voeren, *Parl. St.* Senaat 2012-13, nr. 5-1655/2 en *Hand.* Senaat 2012-13, 7 februari 2013, nr. 5-91, 17

Wetsontwerp tot wijziging van boek II, titel I*ter* van het Strafwetboek, *Parl. St.* Senaat 2012-13, nrs. 5-1905/2 et 5-1905/3

Wetsvoorstel tot aanvulling van de wet van 11 januari 1993 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme, met het oog op de uitbreiding van de controlebevoegdheid van de Cel Financiële Informatieverwerking wat betreft het extremisme, *Parl. St.* Senaat 2012-13, nrs. 5-1873/2 en 5-1873/3 en *Hand.* Senaat 2012-13, 16 mei 2013, nr. 5-102, 34

Benoeming van de leden van het Vast Comité van Toezicht op de inlichtingendiensten (Comité I), *Parl. St.* Senaat 2012-13, nr. 5-1956/1

Wetsvoorstel tot wijziging van diverse wetten tengevolge van de hervorming van de Senaat, *Parl. St.* Senaat 2012-13, nrs. 5-1991/1, 5-1991/3 en 5-1991/6 en *Hand.* Senaat 2013-14, 26 november 2013, nr. 5-125, 8

Voorstel van begroting voor het jaar 2013 van de Bestuurlijke commissie belast met de controle op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (Commissie BIM – C-BIM), *Parl. St.* Senaat 2012-13, nrs. 5-2014/1, 5-2014/2 en 5-2014/3 en *Hand.* Senaat 2012-13, 16 mei 2013, nr. 5-102, 39

Voorstel tot oprichting van een parlementaire onderzoekscommissie belast met het onderzoek naar de gevallen waarin de dienst Veiligheid van de Staat verkozen politici schaduwt, *Parl. St.* Senaat 2012-13, nr. 5-2034/1

Voorstel tot wijziging van artikel 86*bis* van het reglement van de Senaat, met betrekking tot de vaste commissie belast met de begeleiding van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, *Parl. St.* Senaat 2012-13, nr. 5-2040/1

Benoeming van de twee werkende leden, twee plaatsvervangende voorzitters en vier plaatsvervangende leden van het Vast Comité van Toezicht op de inlichtingendiensten (Comité I), *Hand*. Senaat 2012-13, 2 mei 2013, nr. 5-101, 42

Wetsvoorstel tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, met betrekking tot de samenstelling van de vaste commissie belast met de begeleiding van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, *Parl. St*. Senaat 2012-13, nr. 5-2157/1

Wetsontwerp houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van Strafvordering, *Hand*. Senaat 2012-13, 18 juli 2013, nr. 5-114, 39

Vast Comité van Toezicht op de inlichtingendiensten, jaarverslag voor 2012, *Hand*. Senaat 2013-14, 10 oktober 2013, nr. 5-118, 63

Voorstel van begroting voor het jaar 2014 van de Bestuurlijke commissie belast met de controle op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (Commissie BIM – C-BIM), *Parl. St*. Senaat 2013-14, nrs. 5-2312/2 en 5-2312/3

Kamer van Volksvertegenwoordigers

Onderzoek naar het taalevenwicht bij het leger, *Parl. St.* Kamer 2012-13, nr. 53K2631/001

Voorstel van resolutie over een verscherpte screening van de civiele en militaire (kandidaat-)leden van Defensie en over een uitbreiding van de middelen van de Algemene Dienst Inlichting en Veiligheid (ADIV), *Parl. St.* Kamer 2012-13, nr. 53K2641/001

Voorstel tot oprichting van een parlementaire onderzoekscommissie belast met het onderzoek naar de gevallen waarin de dienst Veiligheid van de Staat verkozen politici schaduwt, *Parl. St.* Kamer 2012-13, nr. 53K2652/001

Wetsvoorstel tot wijziging van de wet van 27 maart 2003 betreffende de werving van de militairen en het statuut van de militaire muzikanten en tot wijziging van verschillende wetten van toepassing op het personeel van Landsverdediging, *Parl. St.* Kamer 2012-13, nr. 53K2569/002

Hoorzittingen over de evaluatie van de wet van 19 juli 1991 tot regeling van het beroep van privédetective, *Parl. St.* Kamer 2012-13, nr. 53K2711/001

Wetsontwerp tot aanvulling van de wet van 11 januari 1993 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme, met het oog op de uitbreiding van de controlebevoegdheid van de Cel Financiële Informatieverwerking wat betreft het extremisme, *Parl. St.* Kamer 2012-13, nr. 53K2817/001

Wetsontwerp houdende dringende bepalingen inzake fraudebestrijding (2763/1-11), *Hand*. Kamer 2012-13, 29 mei 2013, CRIV53PLEN144, 19

Wetsvoorstel houdende strengere bestraffing van personen die oproepen tot haat of geweld met de bedoeling afbreuk te doen aan de door de Staat gewaarborgde rechten en vrijheden, *Parl. St.* Kamer 2012-13, nr. 53K2832/001

Wetsontwerp tot wijziging van de wet van 5 februari 2007 betreffende de maritieme beveiliging, *Parl. St.* Kamer 2012-13, nrs. 53K2897/001 en 53K2897/003

Voorstel van resolutie waarbij de oprichting wordt gevraagd van een Centrum voor cyberbeveiliging in België, *Parl. St.* Kamer 2012-13, nr. 53K2918/001

Wetsontwerp houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van Strafvordering, *Parl. St.* Kamer 2012-13, nrs. 53K2921/001, 53K2921/003, 53K2921/004, 53K2921/005 en 53K2921/006

Wetsontwerp houdende de Middelenbegroting voor het begrotingsjaar 2014, wetsontwerp houdende de algemene uitgavenbegroting voor het begrotingsjaar 2014, *Parl. St.* Kamer 2013-14, nr. 53K3070/007

Ontwerp van algemene uitgavenbegroting voor het begrotingsjaar 2014, *Parl. St.* Kamer 2013-14, nrs. 53K3071/001, 53-3071/008, 53K3071/021, 53K3071/024, 53K3071/027 en 53K3071/036

Verantwoording van de Algemene uitgavenbetroting voor het begrotingsjaar 2014, *Parl. St.* Kamer 2013-14, nrs. 53K3072/002, 53K3072/003 en 53K3072/008

Algemene beleidsnota, Binnenlandse Zaken, *Parl. St.* Kamer 2013-14, nr. 53K3096/010

Wetsontwerp tot wijziging van de wet op het politieambt, de wet van 8 december 1992 tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens en het wetboek van strafvordering, *Parl. St.* Kamer 2013-14, nrs. 53K3105/001 tot 53K3105/008 en *Hand*. Kamer 2013-14, 28 november 2013, CRIV53PLEN171, 43

Wetsontwerp tot wijziging van diverse wetten tengevolge van de hervorming van de Senaat, *Parl. St.* Kamer 2013-14, nrs. 53K3192/001 en 53K3192/004

Wetsontwerp tot wijziging van de wet van 10 april 1990 tot regeling van de private en bijzondere veiligheid, *Parl. St.* Kamer 2013-14, nr. 53K3224/001

Rekenhof, Grondwettelijk Hof, Hoge Raad voor de Justitie, Vaste Comités van toezicht op de politie- en inlichtingendiensten, Federale Ombudsmannen, Commissie voor de bescherming van de persoonlijke levenssfeer en Benoemingscommissies voor het notariaat – rekeningen van het begrotingsjaar 2012 – begrotingsaanpassingen 2013 – begrotingsvoorstellen voor het begrotingsjaar 2014, *Parl. St.* Kamer 2013-14, nrs. 53K3237/001 en 53K3237/002 en *Hand*. Kamer 2013-14, 17 december 2013, CRIV53PLEN175, 60 en *Hand*. Kamer 2013-14, 18 december 2013, CRIV53PLEN176, 11

Hoorzitting met de heer Jean-Claude Delepière, voorzitter van de Cel voor Financiële Informatieverwerking, *Parl. St.* Kamer 2013-14, nr. 53K3269/001

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 2013 TOT 31 DECEMBER 2013)

Senaat

Mondelinge vraag van A. Van dermeersch aan de minister van Binnenlandse Zaken over 'de mogelijke terreuraanslagen van de islamitische groep AQIM' (*Hand*. Senaat 2012-13, 17 januari 2013, nr. 5-88, 8, Vr. nr. 5-793)

Schriftelijke vraag van Y. Vastersavendts aan de minister van Binnenlandse Zaken over 'het OCAD – ondersteunende diensten – communicatie – veiligheidsincidenten' (Senaat 2012-13, 18 januari 2013, Vr. nr. 5-7802)

Schriftelijke vraag van Y. Vastersavendts aan de minister van Justitie over 'het Coördinatieorgaan voor de dreigingsanalyse (OCAD) – ondersteunende diensten – communicatie – veiligheidsincidenten' (Senaat 2012-13, 18 januari 2013, Vr. nr. 5-7803)

Schriftelijke vraag van Y. Vastersavendts aan de minister van Justitie over 'het Coördinatieorgaan voor de dreigingsanalyse (OCAD) – risicoanalyse – gebouw Europese Raad' (Senaat 2012-13, 18 januari 2013, Vr. nr. 5-7805)

Schriftelijke vraag van Y. Vastersavendts aan de staatssecretaris voor Staatshervorming over 'het Coördinatieorgaan voor de dreigingsanalyse (OCAD) – risicoanalyse – gebouw Europese Raad' (Senaat 2012-13, 18 januari 2013, Vr. nr. 5-7806)

Schriftelijke vraag van Y. Vastersavendts aan de minister van Justitie over 'de bestrijding van internetextremisme – "Clean IT Project" – meldingsplicht – klantgegevens – toezicht op sociale media – democratische inspraak in het project – privacybescherming – standpunt regering' (Senaat 2012-13, 21 januari 2013, Vr. nr. 5-7821)

Schriftelijke vraag van J. Ceder aan de minister van Justitie over de 'Baron Benoît de Bonvoisin – schadevergoeding – nota Staatsveiligheid – beroep' (Senaat 2012-13, 23 januari 2013, Vr. nr. 5-7917)

Mondelinge vraag van J. Ceder aan de minister van Justitie over 'de rapporten van de Staatsveiligheid over parlementsleden' (*Hand*. Senaat 2012-13, 7 februari 2013, nr. 5-91, 30, Vr. nr. 5-834)

Mondelinge vraag van F. Dewinter aan de minister van Justitie over 'het volgen van de activiteiten van politici door de Staatsveiligheid' (*Hand*. Senaat 2012-13, 7 februari 2013, nr. 5-91, 30, Vr. nr. 5-835)

Mondelinge vraag van R. Torfs aan de minister van Justitie over 'het onderzoek van de Staatsveiligheid naar schadelijke sektarische organisaties' (*Hand*. Senaat 2012-13, 7 februari 2013, nr. 5-91, 30, Vr. nr. 5-847)

Mondelinge vraag van B. Anciaux aan de minister van Justitie over 'de hulp van België aan de CIA bij de uitvoering van het detentieprogramma en harde ondervragingen' (*Hand*. Senaat 2012-13, 7 februari 2013, nr. 5-91, 47, Vr. nr. 5-839)

Schriftelijke vraag van K. Vanlouwe aan de staatssecretaris voor Ambtenarenzaken over het 'cyberdefensieproject – federale cyberstrategie – samenwerkingsverbanden – beveiligingsnormen – Disaster Recovery Plan – personeel – proactiviteit – Fedict – cyberaanvallen' (Senaat 2012-13, 19 februari 2013, Vr. nr. 5-8183)

Schriftelijke vraag van K. Vanlouwe aan de minister van Economie over het 'cyberdefensieproject – CERT (federale cyber emergency team) – beveiligingsnormen – Disaster Recovery Plan – samenwerkingsverbanden – personeel – proactiviteit –cyberaanvallen – industriële cyberspionage' (Senaat 2012-13, 19 februari 2013, Vr. nr. 5-8186)

Schriftelijke vraag van K. Vanlouwe aan de eerste minister over het 'cyberdefensieproject – federale coördinatie door de eerste minister – personeel – proactiviteit – cyberaanvallen – cyberspionage – actieplan voor cyberaanvallen van de Europese Unie – Disaster Recovery Plan' (Senaat 2012-13, 19 februari 2013, Vr. nr. 5- 8212)

Schriftelijke vraag van K. Vanlouwe aan de minister van Landsverdediging over het 'cyberdefensieproject – samenwerkingsverbanden – Disaster Recovery Plan – perso-

neel – proactiviteit – cyberaanvallen –CERT – NCIRC – Benelux' (Senaat 2012-13, 19 februari 2013, Vr. nr. 5- 8213)

Vraag om uitleg van B. Anciaux aan de minister van Binnenlandse Zaken over 'de brandstichting in een Koerdisch cultureel centrum in Genk' (*Hand*. Senaat 2012-13, 19 februari 2013, nr. 5-206, 13, Vr. nr. 5-2944)

Vraag om uitleg van G. Deprez aan de minister van Binnenlandse Zaken over 'de politie en sociale media' (*Hand*. Senaat 2012-13, 19 februari 2013, nr. 5-206, 14, Vr. nr. 5-2931)

Mondelinge vraag van F. Dewinter aan de minister van Justitie over 'het volgen van politici door de Staatsveiligheid en de controle op deze dienst' (*Hand*. Senaat 2012-13, 21 februari 2013, nr. 5-92, 16, Vr. nr. 5-850)

Mondelinge vraag van K. Vanlouwe aan de staatssecretaris voor Sociale Zaken over 'de MiniDuke-cyberaanval op overheidscomputers' (*Hand*. Senaat 2012-13, 28 februari 2013, nr. 5-93, 19, Vr. nr. 5-871)

Mondelinge vraag van A. De Decker aan de minister van Justitie over 'het personeelsbestand en de middelen van de Staatsveiligheid' (*Hand*. Senaat 2012-13, 7 maart 2013, nr. 5-94, 27, Vr. nr. 5-888)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over 'de Staatsveiligheid – informatiebewaring – databank – onjuiste informatie – gebruik – wettelijkheid' (Senaat 2012-13, 8 maart 2013, Vr. nr. 5-8421)

Schriftelijke vraag van M. Taelman aan de minister van Justitie over 'de haatpredikers – aantallen – lijst – vervolgingen en veroordelingen – jihad – Syrië' (Senaat 2012-13, 8 maart 2013, Vr. nr. 5-8436)

Schriftelijke vraag van K. Vanlouwe aan de minister van Justitie over 'de werking van het Computer Emergency Response Team' (Senaat 2012-13, 14 maart 2013, Vr. nr. 5-8500)

Mondelinge vraag van D. Pieters aan de minister van Justitie over 'de Staatsveiligheid en politici' (*Hand*. Senaat 2012-13, 14 maart 2013, nr. 5-95, 17, Vr. nr. 5-902)

Mondelinge vraag van J.-J. De Gucht aan de minister van Binnenlandse Zaken over 'het verhoogd terreuralarm' (*Hand*. Senaat 2012-13, 21 maart 2013, nr. 5-96, 27, Vr. nr. 5-919)

Mondelinge vraag van F. Dewinter aan de minister van Buitenlandse Zaken over 'de "Belgische" jihadi's die in Syrië strijden' (*Hand*. Senaat 2012-13, 21 maart 2013, nr. 5-96, 27, Vr. nr. 5-920)

Mondelinge vraag van B. Laeremans aan de minister van Justitie over 'het talmen van Justitie in het dossier van een Brusselse terrorist' (*Hand*. Senaat 2012-13, 28 maart 2013, nr. 5-97, 31, Vr. nr. 5-932)

Vraag om uitleg van R. Miller aan de minister van Binnenlandse Zaken over 'de Belgische onderdanen die in Syrië vechten en het Plan Radicalisme' (*Hand*. Senaat 2012-13, 16 april 2013, nr. 5-216, 22, Vr. nr.5-3344)

Vraag om uitleg van B. Anciaux aan de minister van Binnenlandse Zaken over 'de Belgische jongeren die in Syrië vechten en terugkeren' (*Hand*. Senaat 2012-13, 16 april 2013, nr. 5-216, 22, Vr. nr.5-3295)

Schriftelijke vraag van B. Anciaux aan de minister van Binnenlandse Zaken over 'de effecten van de cyberaanval MiniDuke op Belgische overheidscomputers' (Senaat 2012-13, 19 april 2013, Vr. nr. 5-8738)

Mondelinge vraag van B. Laeremans aan de minister van Justitie over 'de beveiliging van religieuze leiders en de vrijwaring van de vrije meningsuiting' (*Hand*. Senaat 2012-13, 25 april 2013, nr. 5-99, 23, Vr. nr.5-962)

Mondelinge vraag van K. Vanlouwe aan de staatssecretaris voor Ambtenarenzaken over 'de cyberstrategie en de rol van Fedict' (*Hand*. Senaat 2012-13, 25 april 2013, nr. 5-99, 37, Vr. nr.5-957)

Schriftelijke vraag van N. Lijnen aan de minister van Landsverdediging over de 'cyberoorlogen – Verenigde Naties – handboek – gebruik' (Senaat 2012-13, 7 mei 2013, Vr. nr. 5-8972)

Schriftelijke vraag van M.Taelman aan de minister van Binnenlandse Zaken 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. 5-9086)

Vraag om uitleg van B. Laeremans aan de minister van Justitie over 'de moeilijke strijd tegen cybercriminaliteit' (*Hand*. Senaat 2012-13, 29 mei 2013, nr. 5-227, 9, Vr. nr. 5-3508)

Mondelinge vraag van B. Laeremans aan de minister van Justitie over 'de radicalisering in Marokkaanse kringen en de toegenomen kans op aanslagen in België' (*Hand*. Senaat 2012-13, 30 mei 2013, nr. 5-105, voorlopig niet beschikbaar, Vr. nr. 5-1022)

Mondelinge vraag van H. Bousetta aan de minister van Justitie over 'het PRISM-programma en de bescherming van de privacy' (*Hand*. Senaat 2012-13, 13 juni 2013, nr. 5-107, 25, Vr. nr. 5-1042)

Mondelinge vraag van F. Piryns aan de minister van Justitie over 'het PRISM-programma van het Amerikaanse National Security Agency en privacy van de Belgische bevolking' (*Hand*. Senaat 2012-13, 13 juni 2013, nr. 5-107, 25, Vr. nr. 5-1049)

Mondelinge vraag van B. Hellings aan de minister van Binnenlandse Zaken over 'de nieuwe arrestatie van een Belgische activist' (*Hand*. Senaat 2012-13, 20 juni 2013, nr. 5-108, 12, Vr. nr. 5-1063)

Mondelinge vraag van G. Deprez aan de minister van Binnenlandse Zaken over 'de algemene nationale gegevensbank' (*Hand*. Senaat 2012-13, 20 juni 2013, nr. 5-108, 15, Vr. nr. 5-1066)

Vraag om uitleg van G. De Padt aan de minister van Binnenlandse Zaken over 'de hervorming van de algemene nationale gegevensbank' (*Hand*. Senaat 2012-13, 3 juli 2013, nr. 5-239, 11, Vr. nr. 5-3619)

Vraag om uitleg van K. Vanlouwe aan de minister van Justitie over 'het PRISM-project van de Amerikaanse veiligheidsdiensten en de digitale spionage van internetgebruikers' (*Hand*. Senaat 2012-13, 3 juli 2013, nr. 5-239, 11, Vr. nr. 5-3708)

Vraag om uitleg van K. Vanlouwe aan de minister van Buitenlandse Zaken over 'het PRISM-project van de Amerikaanse veiligheidsdiensten en de digitale spionage van internetgebruikers' (*Hand*. Senaat 2012-13, 3 juli 2013, nr. 5-239, 11, Vr. nr. 5-3711)

Schriftelijke vraag van K. Vanlouwe aan de staatssecretaris voor Ambtenarenzaken over 'de cyberveiligheid en cyberdefensie' (Senaat, 2012-2013, 10 juli 2013, Vr. nr. 5-9407)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over de 'terreur –Belgische lijst van verdachte personen en organisaties – procedure – openbaarheid – relatie tot andere lijsten – rechtsbescherming' (Senaat 2012-13, 10 juli 2013, Vr. nr. 5-9522)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over 'de rol van de Staatsveiligheid in het afluisterschandaal' (Senaat 2012-13, 19 juli 2013, Vr. nr. 5-9634)

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)

Mondelinge vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'de lijst van te volgen organisaties' (*Hand*. Senaat 2013-14, 24 oktober 2013, nr. 5-121, 24, Vr. nr. 5-1131)

Schriftelijke vraag van M. Taelman aan de minister van Buitenlandse Zaken over 'National Security Agency – bedrijfsspionage – afluisteren van bedrijfspersoneel – Staatsveiligheid – maatregelen' (Senaat 2013-14, 31 oktober 2013, Vr. nr. 5-10260)

Schriftelijke vraag van M. Taelman aan de eerste minister 'National Security Agency – Belgacom – Swift – afluisterenpraktrijken – hacking overzicht – onderzoek – maatregelen' (Senaat 2013-14, 31 oktober 2013, Vr. nr. 5-10284)

Vraag om uitleg van B. Hellings aan de minister van Binnenlandse Zaken over 'het toekomstige telecommunicatiesysteem van de veiligheidsdiensten' (*Hand*. Senaat 2013-14, 5 november 2013, nr. 5-254, 10, Vr. nr. 5-3895)

Mondelinge vraag van B. Hellings aan de minister van Landsverdediging over 'het potentiële gebruik van de bewakingsinstrumenten van de NSA door de Algemene Dienst inlichtingen en veiligheid in het kader van de opdrachten van het Belgisch leger in Afghanistan' (*Hand*. Senaat 2013-14, 14 november 2013, nr. 5-123, 11, Vr. nr. 5-1164)

Vraag om uitleg van R. Miller aan de minister van Justitie over 'de rechtspositie van gedetineerden' (*Hand*. Senaat 2013-14, 20 november 2013, nr. 5-159, 39, Vr. nr. 5-4222)

Mondelinge vraag van F. Dewinter aan de minister van Binnenlandse over 'de foto op het internet waarop de minister staat te poseren met een salafist, lid van Al Qaida' (*Hand*. Senaat 2013-14, 5 december 2013, nr. 5-129, 12, Vr. nr. 5-1209)

Kamer van Volksvertegenwoordigers

Vraag van M. Doomst aan de minister van Justitie over 'cybercriminaliteit' (*Hand*. Kamer, 2012-13, 10 januari 2013, CRIV53PLEN124, 57, Vr. nr. 1422)

Samengevoegde vragen van B. Schoofs en P. Luykx aan de minister van Binnenlandse over 'het geweld na een pro-Koerdische betoging in Genk' (*Hand*. Kamer, 2012-13, 24 januari 2013, CRIV53PLEN126, 44, Vr. nrs. 1471 en 1472)

Vraag van P. Dedecker aan de minister van Binnenlandse Zaken over 'cyberveiligheid' (*Vr. en Ant*. Kamer 2012-13, 28 januari 2013, QRVA 098, 46, Vr. nr. 714)

Vraag van B. Slegers aan de minister van Justitie over de 'Staatsveiligheid – beperkte budgettaire middelen' (*Vr. en Ant*. Kamer 2012-13, 28 januari 2013, QRVA 098, 60, Vr. nr. 770)

Vraag van P. Logghe aan de minister van Financiën over het 'witwassen van geld' (*Vr. en Ant*. Kamer 2012-13, 28 januari 2013, QRVA 098, 104, Vr. nr. 668)

Vraag van K. Grosemans aan de minister van Landsverdediging over 'de militaire achtergrond van de Special Forces' (*Vr. en Ant*. Kamer 2012-13, 28 januari 2013, QRVA 098, 268, Vr. nr. 363)

Vraag van N. Lanjri aan de minister van Justitie over 'de bevoegdheden en de toekomst van het Executief van de Moslims van België' (*Hand*. Kamer, 2012-13, 30 januari 2013, CRIV53COM 658, 6, Vr. nr. 15265)

Samengevoegde vragen van J. Galant en D. Ducarme aan de minister van Justitie over 'de controle van de islamitische scholen in België' (*Hand*. Kamer, 2012-13, 30 januari 2013, CRIV53COM 658, 35, Vr. nrs. 15448 en 15518)

Samengevoegde vragen van D. Ducarme, A. Ponthier en G. Dallemagne aan de minister van Landsverdediging over 'de aanwezigheid van extremisten in het leger' (*Hand*. Kamer, 2012-13, 17 februari 2013, CRIV53PLEN125, 26, Vr. nrs. 1442, 1443 en 1444)

Samengevoegde vragen van M. Doomst, P. Logghe, C. Van Cauter, G. Dallemagne, S. Van Hecke, B. Schoofs, K. Degroote en M. Jabour aan de minister van Justitie over 'de Staatsveiligheid' (*Hand*. Kamer, 2012-13, 7 februari 2013, CRIV53COM666, 1, Vr. nrs. 15667, 15671, 15693, 15705, 15706, 15730, 15739 en 15767)

Vraag van Z. Génot aan de minister van Justitie over 'de opvolging van de aanbevelingen van de Lumumbacommissie' (*Hand*. Kamer, 2012-13, 20 februari 2013, CRIV-53COM678, 35, Vr. nr. 15688)

Vraag van G. Dallemagne aan de eerste minister over 'het stelen van gegevens en saboteren van een Belgisch bedrijf door China' (*Hand*. Kamer, 2012-13, 21 februari 2013, CRIV53PLEN132, 19, Vr. nr. 1534)

Samengevoegde vragen van B. Schoofs, K. Degroote en M. Doomst aan de minister van Binnenlandse Zaken over 'de werking van de Veiligheid van de Staat' (*Hand*. Kamer, 2012-13, 21 februari 2013, CRIV53PLEN132, 27, Vr. nrs. 1535, 1536 en 1537)

Samengevoegde vragen van K. Degroote, M. Doomst, C. Van Cauter, S. Van Hecke, B. Weyts en B. Schoofs aan de minister van Justitie over 'de Staatsveiligheid' (*Hand*. Kamer, 2012-13, 26 februari 2013, CRIV53COM682, 1, Vr. nrs. 15873, 15876, 15882, 15896, 15934 en 15983)

Samengevoegde vragen van K. Lalieux, L. Van Biesen en T. Veys aan de staatssecretaris voor Leefmilieu over 'de veiligheid op Brussels Airport programma' (*Hand*. Kamer, 2012-13, 5 maart 2013, CRIV53COM689, 19, Vr. nrs. 16011, 16038 en 16355)

Vraag van K. Grosemans aan de minister van Landsverdediging over 'de deelname aan het MUSIS-programma' (*Hand*. Kamer, 2012-13, 6 maart 2013, CRIV53COM691, 4, Vr. nr. 16186)

Samengevoegde vragen van B. Valkeniers en D. Ducarme aan de minister van Justitie over ''Belgische' jongeren als huurlingen voor de radicale moslims in Syrië' (*Hand*. Kamer, 2012-13, 13 maart 2013, CRIV53COM698, 4, Vr. nrs. 16484, 16485 en 16587)

Samengevoegde vragen van B. Slegers, P. Logghe en S. Van Hecke aan de minister van Justitie over 'de databank van de Staatsveiligheid' (*Hand*. Kamer, 2012-13, 13 maart 2013, CRIV53COM698, 9, Vr. nrs. 16457, 16487 en 16524)

Vraag van P. Logghe aan de minister van Justitie over 'moslimterroristen en de Staatsveiligheid' (*Hand*. Kamer, 2012-13, 20 maart 2013, CRIV53COM703, 6, Vr. nr. 16711)

Vraag van J. Van Esbroeck aan de minister van Binnenlandse Zaken over de 'aanpassing van het dreigingsniveau' (*Vr. en Ant*. Kamer 2012-13, 25 maart 2013, QRVA 106, 146, Vr. nr. 711)

Samengevoegde vragen van O. Maingain en E. Thiébaut aan de minister van Binnenlandse Zaken en Gelijke Kansen over 'de zaak-Benladghem' (*Hand*. Kamer, 2012-13, 28 maart 2013, CRIV53PLEN137, 32, Vr. nrs. 1660 en 1661)

Vraag van T. Francken aan de minister van Landsverdediging over de 'topofficieren die geen functie vervullen' (*Vr. en Ant*. Kamer 2012-13, 2 april 2013, QRVA 107, 98, Vr. nr. 414)

Vraag van D. Thiéry aan de staatssecretaris voor Ambtenarenzaken over de 'maatregelen tegen cyberaanvallen' (*Vr. en Ant*. Kamer 2012-13, 2 april 2013, QRVA 107, 284, Vr. nr. 61)

Vraag van B. Valkeniers aan de minister van Buitenlandse Zaken over 'de monitoring van eurokritische meningen' (*Vr. en Ant*. Kamer 2012-13, 12 april 2013, QRVA 108, 422, Vr. nr. 424)

Vraag van P. Dedecker aan de minister van Binnenlandse Zaken over de 'cyberveiligheid' (*Vr. en Ant*. Kamer 2012-13, 12 april 2013, QRVA 108, 503, Vr. nr. 714)

Samengevoegde vragen van P. Logghe en W.-F. Schiltz aan de minister van Binnenlandse Zaken over 'de diamantroof op de luchthaven van Zaventem' (*Hand*. Kamer, 2012-13, 16 april 2013, CRIV53COM713, 24, Vr. nrs. 160534 en 16535)

Samengevoegde vraag van Ch. Lacroix en K. Grosemans aan de minister van Landsverdediging over 'de ambities van het Belgische leger op het stuk van satellietbeeldverwerking' (*Hand*. Kamer, 2012-13, 16 april 2013, CRIV53COM714, 6, Vr. nrs. 16482 en 85)

Vraag van K. Grosemans aan de minister van Landsverdediging over 'het lek tijdens een hoorzitting achter gesloten deuren' (*Hand*. Kamer, 2012-13, 16 april 2013, CRIV-53COM714, 21, Vr. nr. 16826)

Samengevoegde vragen van D. Ducarme, B. Somers en B. Schoofs aan de minister van Justitie over 'het uitblijven van wettelijke sancties tegen Belgen die geronseld worden voor de strijd of individueel gaan vechten in Syrië' (*Hand*. Kamer, 2012-13, 17 april 2013, CRIV53COM718, 6, Vr. nrs. 16917, 17256 en 17279)

Samengevoegde vragen B. Clerfayt, F. De Man, H. Bonte, L. Devin, B. Slegers, B. Weyts et J. M. Dedecker aan de eerste minister over 'de jonge Belgen die in Syrië gaan vechten' (*Hand*. Kamer, 2012-13, 18 april 2013, CRIV53PLEN138, 22, Vr. nrs. 1679 tot 1685)

Vraag van B. Slegers aan de minister van Justitie over de 'Staatsveiligheid – beperkte budgettaire middelen' (*Vr. en Ant*. Kamer 2012-13, 19 april 2013, QRVA 109, 203, Vr. nr. 770)

Vraag van K. Grosemans aan de minister van Landsverdediging over 'het standpunt van Defensie inzake het MUSIS-programma' (*Hand*. Kamer, 2012-13, 24 april 2013, CRIV-53COM723, 15, Vr. nr. 17386)

Vraag van S. Van Hecke aan de minister van Justitie over 'de werkomstandigheden bij de Staatsveiligheid' (*Hand*. Kamer, 2012-13, 24 april 2013, CRIV53COM725, 2, Vr. nr. 17123)

Vraag van S. De Wit aan de minister van Binnenlandse Zaken over 'de talenkennis bij de ondersteunende diensten van de politie' (*Vr. en Ant*. Kamer 2012-13, 26 april 2013, QRVA 110, 131, Vr. nr. 21)

Samengevoegde vragen van T. Francken aan de minister van Justitie over 'het inzagerecht van de koning in geheime documenten van de Staatsveiligheid' (*Hand*. Kamer, 2012-13, 30 april 2013, CRIV53COM732, 17, Vr. nrs. 17559 en 17577)

Samengevoegde vragen van D. Ducarme aan de minister van Justitie over 'Sharia4Belgium, de terugkeer van Belgische Syriëstrijders en de communicatie van gegevens van justitie aan het departement Buitenlandse Zaken' (*Hand*. Kamer, 2012-13, 30 april 2013, CRIV53COM732, 19, Vr. nrs. 17586 en 17587)

Vraag van K. Grosemans aan de minister van Landsverdediging over de 'Malware detecties in de computersystemen van Defensie' (*Vr. en Ant*. Kamer 2012-13, 6 mei 2013, QRVA 111, 64, Vr. nr. 441)

Samengevoegde vragen van T. Francken, W. De Vriendt, D. Van der Maelen en Ph. Blanchart aan de minister van Landsverdediging over 'de wapenleveringsdeal van Defensie' (*Hand*. Kamer, 2012-13, 8 mei 2013, CRIV53PLEN141, 2, Vr. nr. 1738, 1739, 1740 en 1741)

Vraag van D. Ducarme aan de minister van Justitie over 'het gebrek aan middelen van de Veiligheid van de Staat' (*Hand*. Kamer, 2012-13, 8 mei 2013, CRIV53PLEN141, 15, Vr. nr. 1747)

Vraag van B. Pas aan de minister van Buitenlandse Zaken over 'de dreigementen van Sharia4UK' (*Hand*. Kamer, 2012-13, 16 mei 2013, CRIV53PLEN142, 20, Vr. nr. 1768)

Samengevoegde vragen van D. Ducarme, W. De Vriendt, D. Geerts en A. Ponthier aan de minister van Landsverdediging over 'het noodzakelijke toezicht door Defensie en onze regering op de doorverkoop van militair materieel' (*Hand*. Kamer, 2012-13, 21 mei 2013, CRIV53COM750, 17, Vr. nrs. 17801, 17873, 17898 en 18001)

Vraag van G. Dallemagne aan de minister van Landsverdediging over 'cyberaanvallen' (*Hand*. Kamer, 2012-13, 21 mei 2013, CRIV53COM750, 24, Vr. nr. 17925)

Samengevoegde vragen van D. Ducarme en P. Logghe aan de minister van Binnenlandse Zaken over 'de terugkeer van Belgische gewezen jihadisten uit Syrië' (*Hand*. Kamer, 2012-13, 23 mei 2013, CRIV53PLEN143, 13, Vr. nrs. 1784 en 1785)

Vraag van B. Weyts aan de minister van Binnenlandse Zaken over de 'radicale islamisten in Syrië' (*Vr. en Ant*. Kamer 2012-13, 27 mei 2013, QRVA 114, 48, Vr. nr. 860)

Vraag van P. Dedecker aan de staatssecretaris voor Ambtenarenzaken over de 'cyberveiligheid' (*Vr. en Ant*. Kamer 2012-13, 27 mei 2013, QRVA 114, 325, Vr. nr. 125)

Samengevoegde vragen van K. Grosemans en A. Ponthier aan de minister van Landsverdediging over 'de kritiek van het Comité I op het gebrek aan controle op ISTAR' (*Hand*. Kamer, 2012-13, 29 mei 2013, CRIV53COM760, 8, Vr. nrs. 18156 en18164)

Samengevoegde vragen van L. Van Biesen, B. Slegers en P. Logghe aan de minister van Binnenlandse Zaken over 'het dreigement van Sharia4UK' (*Hand*. Kamer, 2012-13, 29 mei 2013, CRIV53COM761, 35, Vr. nrs. 17926, 17933, 18007, en 18050)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over de 'radicalisering van jongeren – invloed/tips uit Saoedi-Arabië, Tsjetsjenië en Quatar' (*Vr. en Ant*. Kamer 2012-13, 3 juni 2013, QRVA 115, 60, Vr. nr. 891)

Vraag van D. Ducarme aan de minister van Justitie over 'de gerechtelijke opvolging van Syriëstrijders na hun terugkeer naar België' (*Hand*. Kamer, 2012-13, 11 juni 2013, CRIV53COM773, 14, Vr. nr. 18227)

Vraag van D. Ducarme aan de minister van Justitie over 'de dreiging met terreur van Sharia4UK aan het adres van België' (*Hand*. Kamer, 2012-13, 11 juni 2013, CRIV53COM773, 15, Vr. nr. 18382)

Samengevoegde vragen van J. Van Esbroeck en P. Logghe aan de minister van Binnenlandse Zaken over 'terugkerende Syriëstrijders' (*Hand*. Kamer, 2012-13, 13 juni 2013, CRIV53PLEN148, 21, Vr. nrs. 1857 en 1858)

Vraag van I. Emmery aan de minister van Buitenlandse Zaken, Buitenlandse Handel over 'het PRISM-programma van de Amerikaanse geheime dienst' (*Hand*. Kamer, 2012-13, 13 juni 2013, CRIV53PLEN148, 54, Vr. nr. 1861)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over de 'Moslimstrijders in Syrië en berichtgeving' (*Vr. en Ant*. Kamer 2012-13, 17 juni 2013, QRVA 117, 70, Vr. nr. 929)

Vraag van K. Grosemans aan de minister van Landsverdediging over de 'aanbevelingen van het Comité I inzake de werking van de ADIV' (*Vr. en Ant*. Kamer 2012-13, 17 juni 2013, QRVA 117, 161, Vr. nr. 474)

Vraag van F. De Man aan de minister van Binnenlandse Zaken over 'de discretie met betrekking tot de dossiers van jihadi's die naar Syrië zijn vertrokken' (*Hand*. Kamer, 2012-13, 20 juni 2013, CRIV53PLEN150, 10, Vr. nr. 1880)

Vraag van G. Dallemagne aan de minister van Justitie over 'het PRISM-programma' (*Hand*. Kamer, 2012-13, 20 juni 2013, CRIV53PLEN150, 27, Vr. nr. 1887)

Vraag van B.Weyts aan de minister van Binnenlandse Zaken over 'het crisiscentrum – behandeling van dossiers van bedreigde personen' (*Vr. en Ant*. Kamer 2012-13, 24 juni 2013, QRVA 118, 172, Vr. nr. 824)

Vraag van A. Frédéric aan de minister van Sociale Zaken over de 'Frans rapport over therapeutische sekten' (*Vr. en Ant*. Kamer 2012-13, 1 juli 2013, QRVA 119, 161, Vr. nr. 1005)

Samengevoegde vragen van H. De Croo, T. Francken, J. Fernandez Fernandez en S. Van Hecke aan de minister van Buitenlandse Zaken over 'het PRISM-programma' (*Hand*. Kamer, 2012-13, 3 juli 2013, CRIV53COM795, 2, Vr. nrs. 18510, 18525, 18693, 19037, 19071 en 19075)

Samengevoegde vragen van T. Francken aan de minister van Justitie over 'het gerechtelijk onderzoek naar mogelijke terroristische feiten door mensen uit het Brusselse anarchistische milieu' (*Hand*. Kamer, 2012-13, 3 juli 2013, CRIV53COM795, 38, Vr. nrs. 18734 en 18735)

Samengevoegde vragen van P. Logghe aan de minister van Binnenlandse Zaken over 'de internationale financiële stromen van het terrorisme' (*Hand*. Kamer, 2012-13, 3 juli 2013, CRIV53COM795, 42, Vr. nrs. 18756 en 18918)

Samengevoegde vragen van B. Schoofs aan de minister van Justitie over 'de adviezen van de Raad van Theologen van de Moslimexecutieve' (*Hand*. Kamer, 2012-13, 3 juli 2013, CRIV53COM795, 45, Vr. nrs. 18760 en 18785)

Samengevoegde vragen van O. Henry, H. De Croo en D. Van der Maelen aan de minister van Buitenlandse Zaken over 'het PRISM-programma' (*Hand*. Kamer, 2012-13, 4 juli 2013, CRIV53PLEN154, 8, Vr. nrs. 1925, 1935 en 1926)

Samengevoegde vragen van P. Logghe en J. Van Esbroeck aan de minister van Binnenlandse Zaken over 'het aantal radicale moslims in ons land' (*Hand*. Kamer, 2012-13, 9 juli 2013, CRIV53COM800, 25, Vr. nrs. 18161 en 18215)

Samengevoegde vragen van J. Van Esbroeck, B. Slegers, P. Logghe en D. Ducarme aan de minister van Binnenlandse Zaken over 'het gebrek aan eensgezindheid in de Syrië-

taskforce' (*Hand*. Kamer, 2012-13, 9 juli 2013, CRIV53COM800, 44, Vr. nrs. 18699, 18942, 19030, en 19073)

Samengevoegde vragen van K. Grosemans, Ch. Lacroix en T. Francken aan de minister van Landsverdediging over 'het PRISM-programma' (*Hand*. Kamer, 2012-13, 9 juli 2013, CRIV53COM801, 16, Vr. nrs. 18527, 18588 en 19070)

Interpellatie van de heer Filip De Man aan de minister van Landsverdediging over 'het bericht dat een fundamentalistische moslim, opgeleid door het Belgisch leger, sneuvelde in Syrië' (*Hand*. Kamer, 2012-13, 9 juli 2013, CRIV53COM801, 31, Vr. nr. 99)

Vraag van de P. Dedecker aan de staatssecretaris voor Ambtenarenzaken over 'de spionage door de Amerikaanse autoriteiten bij IT-bedrijven' (*Vr. en Ant.* Kamer 2012-13, 22 juli 2013, QRVA 122, 228, Vr. nr. 159)

Vraag van B. Schoofs aan de minister van Justitie over 'de werkzaamheden van de Staatsveiligheid' (*Vr. en Ant.* Kamer 2012-13, 29 juli 2013, QRVA 123, 182, Vr. nr. 841)

Vraag van G. Dallemagne aan de eerste minister over 'Chinese cyberaanvallen' (*Vr. en Ant.* Kamer 2012-13, 19 augustus 2013, QRVA 124, 389, Vr. nr. 95)

Vraag van S. Van Hecke aan de minister van Justitie over 'de cyberveiligheid' (*Hand*. Kamer, 2012-13, 29 september 2013, CRIV53COM816, 6, Vr. nr. 19749)

Vraag van S. Van Hecke aan de minister van Justitie over 'de opvolging van PRISM' (*Hand*. Kamer, 2012-13, 29 september 2013, CRIV53COM817, 47, Vr. nr. 19643)

Samengevoegde vragen van O. Maingain en M. Senecaut aan de minister van Justitie over 'de klacht die Belgacom heeft ingediend nadat zijn intern computersysteem werd gehackt' (*Hand*. Kamer, 2012-13, 2 oktober 2013, CRIV53COM824, 11, Vr. nrs. 19703 en 19716)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over de 'Belgische jihadstrijders' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 309, Vr. nr. 684)

Vraag van J. Galant aan de minister van Binnenlandse Zaken over de 'dodelijke schietpartij op de A8-autosnelweg – ontdekking van een wapenarsenaal in de woning van de neergeschoten gangster – terreurdreigingsniveau' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 317, Vr. nr. 889)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over de 'radicalisering van jongeren – invloed/tips uit Saoedi-Arabië, Tsjetsjenië en Quatar' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 322, Vr. nr. 891)

Vraag van B. Slegers aan de minister van Binnenlandse Zaken over de 'terrorismeaanpak – gesprekken met de Amerikaanse autoriteiten' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 345, Vr. nr. 973)

Vraag van Ph. Blanchart aan de minister van Binnenlandse Zaken over de 'inlichtingendienst van de Europese Unie (SitCen)' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 351, Vr. nr. 1118)

Vraag van D. Bacquelaine aan de minister van Justitie over de 'sluiting van provincieposten van de Veiligheid van de Staat – gebrek aan financiële en personele middelen' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 382, Vr. nr. 1047)

Vraag van I. De Meulenmeester aan de minister van Overheidsbedrijven over 'het bezoek van minister Labille aan Rwanda in juni 2013' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 464, Vr. nr. 584)

Vraag van J. Van den Bergh aan de staatssecretaris voor Leefmilieu over 'prioritaire voertuigen' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 582, Vr. nr. 150)

Vraag van K. Calvo aan de staatssecretaris voor Leefmilieu over 'de controle eindgebruiker na intra-EU nucleaire export' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 588, Vr. nr. 158)

Vraag van K. Grosemans aan de minister van Landsverdediging over 'het toezicht op het ISTAR-bataljon' (*Hand*. Kamer, 2013-14, 9 oktober 2013, CRIV53COM826, 7, Vr. nr. 19436)

Samengevoegde vragen van K. Grosemans en Ch. Lacroix aan de minister van Landsverdediging over 'de waarschuwingen per e-mail voor dreigende aanslagen op militairen' (*Hand*. Kamer, 2013-14, 9 oktober 2013, CRIV53COM826, 9, Vr. nrs. 19449 en 19595)

Samengevoegde vragen van J. Galant, J. Van Esbroeck en B. Slegers aan de minister van Binnenlandse Zaken over 'de verscherpte veiligheidsmaatregelen en het verslag van het Comité P waarin brandhout wordt gemaakt van het gegevensbeheer op het stuk van terrorisme, radicalisme en extremisme' (*Hand*. Kamer, 2013-14, 9 oktober 2013, CRIV53COM830, 7, Vr. nrs. 19452, 19473 en 19763)

Samengevoegde vragen van P. Dedecker, S. Van Hecke, R. Deseyn S. Lahaye-Battheu en T. Veys aan de minister van Overheidsbedrijven over 'de spionage bij Belgacom' (*Hand*. Kamer, 2013-14, 9 oktober 2013, CRIV53COM831, 29, Vr. nrs. 19670, 105, 108, 20082, 20083, 20084, 20142 en 20154)

Vraag van A. Frédéric aan de minister van Binnenlandse Zaken over 'het vertrouwelijke verslag van de Veiligheid van de Staat over de pogingen van de Scientologykerk om onze politici te benaderen' (*Hand*. Kamer, 2013-14, 23 oktober 2013, CRIV53COM839, 4, Vr. nr. 19591)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over 'de bevoegdheden voor privébewakingsfirma's' (*Hand*. Kamer, 2013-14, 23 oktober 2013, CRIV53COM839, 10, Vr. nr. 19679)

Samengevoegde vragen van D. Ducarme, B. Somers en P. Logghe aan de minister van Binnenlandse Zaken over 'de trainingskampen voor jihadstrijders in de Ardennen' (*Hand*. Kamer, 2013-14, 24 october 2013, CRIV53PLEN165, 2, Vr. nrs. 2000, 2001 en 2002)

Samengevoegde vragen van H. De Croo, G. Dallemagne, R. Deseyn, P. Dedecker en P. Logghe aan de minister van Binnenlandse Zaken over 'afluisterpraktijken' (*Hand*. Kamer, 2013-14, 24 october 2013, CRIV53PLEN165, 17, Vr. nrs. 2010, 2011, 2012, 2013 en 2014)

Vraag van de J. Van Esbroeck aan de minister van Binnenlandse Zaken over 'de kosten veroorzaakt door Sharia4Belgium' (*Vr. en Ant*. Kamer 2013-14, 4 november 2013, QRVA 134, 148, Vr. nr. 700)

Vraag van K. Grosemans aan de minister van Binnenlandse over de 'deelname van de ADIV aan het werkbezoek van de minister aan Turkije' (*Vr. en Ant*. Kamer 2013-14, 4 november 2013, QRVA 134, 155, Vr. nr. 974)

Vraag van R. Deseyn aan de minister van Binnenlandse Zaken over 'het PRISM-systeem' (*Vr. en Ant*. Kamer 2013-14, 4 november 2013, QRVA 134, 165, Vr. nr. 1012)

Vraag van H. Bonte aan de minister van Justitie over 'de risicovolle traagheid bij Justitie' (*Hand*. Kamer, 2013-14, 6 november 2013, CRIV53COM846, 24, Vr. nr. 20597)

Samengevoegde vragen van J. De Potter, D. Bacquelaine, P. Logghe en J. Van Esbroeck aan de minister van Binnenlandse Zaken over 'de radicalisering van jongeren en de genomen maatregelen' (*Hand*. Kamer, 2013-14, 12 november 2013, CRIV53COM850, 46, Vr. nrs. 20399, 20410, 20412 en 20433)

Samengevoegde vragen van D. Thiéry, Ch. Lacroix et D. Ducarme aan de minister van Landsverdediging over 'de samenwerking mer Amerikaanse inlichtingendiensten in het kader van onze militaire cyberdefensie' (*Hand*. Kamer, 2013-14, 13 november 2013, CRIV53COM851, 1, Vr. nrs. 19438, 19875, 20643 en 20749)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over 'Belgische burgers bij Al-Shabaab' (*Vr. en Ant*. Kamer 2013-14, 18 november 2013, QRVA 136, 78, Vr. nr. 1186)

Vraag van G. D'haeseleer aan de minister van Justitie over 'de extra bezoldigingen of vergoedingen van vakbondsafgevaardigden in beheerscomités en andere raden/ commissies' (*Vr. en Ant*. Kamer 2013-14, 18 november 2013, QRVA 136, 112, Vr. nr. 1020)

Vraag van Ch. Brotcorne aan de minister van Justitie over 'proselietenmakerij in de gevangenis van Bergen – radicale islam' (*Vr. en Ant*. Kamer 2013-14, 18 november 2013, QRVA 136, 127, Vr. nr. 1059)

Samengevoegde vragen van P. Logghe en J. Van Esbroeck aan de minister van Justitie over 'de verklaringen van een salafistische predikant' (*Hand*. Kamer, 2013-14, 4 december 2013, CRIV53COM879, 1, Vr. nrs. 20784 en 20807)

Samengevoegde vragen van J. Van Esbroeck en P. Logghe aan de minister van Justitie over 'de terugkeer van minderjarige strijders uit Syrië' (*Hand*. Kamer, 2013-14, 4 december 2013, CRIV53COM879, 5, Vr. nrs. 20805, 20833 en 21065)

Vraag van R. Deseyn aan de minister van Landsverdediging over 'het PRISM-systeem' (*Vr. en Ant*. Kamer 2013-14, 9 december 2013, QRVA 139, 71, Vr. nr. 614)

Vraag van E. Brems aan de minister van Buitenlandse Zaken over 'de opvang van gedetineerden in Guantanamo' (*Vr. en Ant*. Kamer 2013-14, 9 december 2013, QRVA 139, 92, Vr. nr. 574)

Vraag van E. Brems aan de minister van Buitenlandse Zaken over 'de Belgisch-Iraanse spion' (*Vr. en Ant*. Kamer 2013-14, 9 december 2013, QRVA 139, 132, Vr. nr. 650)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over 'het vertrek van minderjarigen naar Syrië' (*Vr. en Ant*. Kamer 2013-14, 16 december 2013, QRVA 140, 146, Vr. nr. 930)

Vraag van P. Logghe aan de minister van Justitie over 'Radicalisering van jongeren – invloed/tips uit Saoedi-Arabië, Tsjetsjenië en Quatar' (*Vr. en Ant*. Kamer 2013-14, 16 december 2013, QRVA 140, 244, Vr. nr. 1114)

Vraag van T. Francken aan de minister van Justitie over '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, 16 december 2013, QRVA 140, 271, Vr. nr. 1175)

Vraag van T. Francken aan de minister van Landsverdediging over 'inzet van de militaire veiligheidsdienst ADIV voor de beveiliging van de Koning en zijn entourage' (*Vr. en Ant*. Kamer 2013-14, 16 december 2013, QRVA 141, 194, Vr. nr. 621)

BIJLAGE D.
EERSTE TUSSENTIJDSE VERSLAG VAN HET TOEZICHTSONDERZOEK NAAR DE INFORMATIEPOSITIE VAN DE BELGISCHE INLICHTINGENDIENSTEN TEN AANZIEN VAN DE MOGELIJKHEDEN VAN BEPAALDE STATEN TOT MASSALE DATA-CAPTATIE EN -MINING EN VAN DE WIJZE WAAROP DEZE STATEN AAN POLITIEKE SPIONAGE ZOUDEN DOEN VAN ZOGENAAMDE 'BEVRIENDE LANDEN' (PRISM)

I. INLEIDING

Op 6 juni 2013 publiceerden *The Guardian*[203] en *The Washington Post*[204] 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 met de regelmaat van de klok.

De berichten gaven een inkijk in uitermate geheime programma's van voornamelijk de NSA. Ze onthulden onder meer het bestaan van het zogenaamde PRISM-programma waarbij de NSA massaal (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) waarbij ook 'bevriende landen' werden geviseerd.

Deze onthullingen waren het startschot voor vele (parlementaire, gerechtelijke en inlichtingen-[205]) onderzoeken 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. 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, een 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.*'

---

203 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").

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

205 Zo bijvoorbeeld in het Europese Parlement, waar Senator en lid van de Begeleidingscommissie Armand De Decker, samen met voorzitter van het Vast Comité I Guy Rapaille, werd gehoord voor het *LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens* over 'The role of Parliamentary oversight of intelligence services at national level in an era of mass surveillance' (zie hierover: www.europarl.europa.eu/committees/en/libe/events.html) en binnen de schoot van de Verenigde Naties (J. KASTRENAKES, *The Verge*, 3 december 2013 ("United Nations Counterterrorism Official Launches Investigation into NSA Surveillance")).

Het Vast Comité I heeft daarop drie toezichtonderzoeken geopend die uiteraard nauw met elkaar verweven zijn. Dit geldt ook voor een vierde onderzoek 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 het eerste tussentijdse resultaat is, wil een antwoord bieden 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 gecollecteerd 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? Alhoewel dit aspect van de onthullingen (met name bepaalde operaties van inlichtingendiensten van zogenaamde 'bevriende landen' ten aanzien van internationale of supranationale instellingen waarin België vertegenwoordigd is of ten aanzien van Belgische belangen) niet expliciet in de vraagstelling van de Begeleidingscommissie was opgenomen, heeft het Vast Comité I beslist om ook hieraan aandacht te besteden, en dit gelet op het intrinsieke belang van deze vraag.

Het eerste toezichtonderzoek omvat drie luiken:

– Een door een externe expert (met name drs. Mathias Vermeulen, VUB en *European University Institute,* Firenze) aan de hand van open bronnen opgesteld overzicht van de soorten 'gegevens' die mogelijks betrekking hebben op of afkomstig zijn van in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) en die door overheidsdiensten of private firma's in opdracht van de Amerikaanse en Britse overheid op grote schaal worden gecapteerd en opgeslagen en dit met het oog op een (eventuele latere) exploitatie door hun inlichtingendiensten.[206]
– Een analyse van de informatie die actueel beschikbaar is op het Comité onder meer op basis van BIM-dossiers en afgesloten toezichtonderzoeken (zoals de onderzoeken naar Echelon, SWIFT, Echelon bis, de inlichtingenactiviteiten van de ADIV in het buitenland …). Daarnaast werden derden bevraagd die mogelijks over relevante informatie beschikten.
– Een evaluatie van de inlichtingenpositie van de Veiligheid van de Staat (VSSE) en de Algemene Dienst inlichting en veiligheid (ADIV): wat wisten ze (of wat hoorden ze te weten) en hoe zijn ze met die informatie en kennis omgesprongen? Wat dit luik betreft, werden beide inlichtingendiensten reeds tweemaal grondig bevraagd. De analyse van alle antwoorden noopte het Vast Comité I tot een derde vragenronde.

---

206 Het ontwerpverslag van drs. Vermeulen werd aan een kritische lezing onderworpen door een werkgroep binnen het Vast Comité I. Op aangeven van de werkgroep werden verduidelijkingen aangebracht en elementen toegevoegd. Tevens werd aan de expert, onder de vorm van een bijkomende opdracht, gevraagd om het verslag te *updaten*, om een glossarium op te stellen en om (mogelijke) 'linken' met België op te lijsten.

Het **tweede toezichtonderzoek**[207] behandelt de in België geldende rechtsregels 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 (of die enige link hebben met België) te onderscheppen en te exploiteren. Qua internationale regels zal er uiteraard aandacht zijn voor artikel 8 EVRM (waarbij zowel de 'horizontale werking' van deze bepalingen en de eventuele 'positieve verplichtingen' die eruit voortvloeien voor een Staat, belicht worden), artikel 17 van het Verdrag inzake burgerrechten en politieke rechter (BUPO-verdrag), Richtlijn 95/46/EC van 24 oktober 1995 (met aandacht voor de uitzondering inzake data met betrekking tot de nationale veiligheid en voor de recente onderhandelingen om de Richtlijn te verscherpen), Verdrag nr. 108 van 28 januari 1981 van de Raad van Europa en de artikelen 7 en 8 van het Handvest van de Grondrechten van de Europese Unie. Maar ook meer specifieke regels zullen aan bod komen: de regels inzake Passenger Name Record, Swift, Safe Harbour … Ten slotte zullen de interne rechtsregels die betrekking hebben op de privacybescherming en dataprotectie, belicht worden: artikel 10 van de Grondwet, de Wet Verwerking Persoonsgegevens en haar uitvoeringsbesluit en de bepalingen die specifiek zijn voor de werking van inlichtingendiensten (bijvoorbeeld de grenzen gesteld aan de internationale uitwisseling van gegevens).

Daarnaast moet dit tweede toezichtonderzoek ook een overzicht bieden van de juridische mogelijkheden waarover Staten, burgers of bedrijven beschikken om actie te ondernemen tegen (mogelijke) inbreuken op (grond)rechten. In dit luik zal onder meer aandacht besteed worden aan de 'bruikbaarheid' van informatie die in het buitenland rechtmatig is verkregen maar in België nooit (op die wijze) had kunnen verkregen worden.

Ook voor dit tweede toezichtonderzoek werd een extern expert aangezocht. Het betreft Prof Annemie Schaus. Tevens werden de VSSE en de ADIV bevraagd omtrent bovenstaande regels en juridische mogelijkheden voor Staten, burgers en bedrijven. Ten slotte wordt informatie uitgewisseld met de Belgische Privacycommissie.

Het **derde toezichtonderzoek**[208] behandelt de mogelijke implicaties van datamining 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;
- 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.

---

207 Toezichtonderzoek naar 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.

208 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.

II. WOORD VOORAF BIJ HET EXPERTVERSLAG

Sinds de eerste gelekte NSA-slides en de opening van het toezichtonderzoek zijn onophoudelijk nieuwe (uitermate gevoelige) gegevens aan het licht gekomen die wijzen op massale datacaptatie én politieke en economische spionage van en bij bevriende landen. Daarbij gaat het al lang niet meer over PRISM, TEMPURA of de spionage van de G20 alleen. Dat zal ook overduidelijk worden bij het doornemen van het expertverslag.

Uiteraard dient het verslag met de nodige reserves te worden gelezen. Het is *quasi* uitsluitend gebaseerd op open bronnen. Wel ging de expert zeer kritisch te werk en werden al te speculatieve denkpistes of theorieën niet weergegeven. Toch wil het Comité hier reeds benadrukken dat het nog geen onderbouwde indicaties vond waaruit blijkt dat de Snowden-slides niet authentiek zouden zijn. Integendeel, uit de reeds verrichte onderzoeken meent het Comité te kunnen afleiden dat de onthullingen, zeker wat betreft de 'grote lijnen', waarheidsgetrouw zijn.[209] Dat daarbij – mede gelet op het fragmentarische karakter van de onthullingen[210] – geen zekerheid bestaat omtrent de waarachtigheid van *elk* (technisch) aspect van de zaak, doet geen afbreuk aan deze vaststelling. Hierbij moet ook rekening worden gehouden met het feit dat het expertverslag werd afgesloten op 23 oktober 2013. Nieuw vrijgegeven informatie of de contestatie vanuit officiële hoek van eerder becommentarieerde gegevens (zoals met betrekking tot – zie II.4) sluit een andere lezing van bepaalde aspecten van de zaak, niet uit.

Vooraf wil het Vast Comité I kort nog een aantal elementen toelichten. Ze moeten enerzijds een vlottere lezing van het uitgebreide en technische expertverslag toelaten en anderzijds de noodzakelijke context bieden waarbinnen dit verslag moet begrepen worden.

II.1. NIET ALLEEN DE NSA EN HET GCHQ

Het verslag bespreekt alleen de massale datacaptatie door het Amerikaanse *National Security Agency* en het Britse *Government Communications Headquarters* (GCHQ). Wellicht 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 tewerk gaan.

In de marge van de Snowden-onthullingen zijn bijvoorbeeld ook de activiteiten van de Franse[211], Duitse[212] en Zweedse[213] inlichtingendiensten aangekaart. En natuurlijk zijn er

---

209 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.

210 *The Guardian* zou vooralsnog 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")).

211 *Le Monde* stelde bijvoorbeeld dat de Franse DGSE op een systematische manier de metadata van telefoon, fax en internetcommunicaties tussen een Frans en een buitenlands nummer '*voor jaren*' bewaart in haar hoofdkwartier. Zes andere diensten hebben toegang tot deze database (J. FOLLOROU en F. JOHANNES, *Le Monde*, 4 juillet 2013 ("Révélations sur le Big Brother français")).

212 A. REIβMANN, *Der Spiegel*, 13 november 2013 ("Uberwachung: BND soll weitgehenden Zugriff auf Internetverkehr in Deutschland haben").

213 T.T., *The Local*, 6 september 2013 ("Sweden 'a close partner' in NSA surveillance"). Zie ook: "Snowden papers unmask close technical cooperation and loose alliance between British, Ger-

ook de mogelijkheden die ontplooid kunnen worden door pakweg Rusland[214] en China.[215] Maar minstens even belangrijk in dit kader zijn de samenwerkingsverbanden inzake *Signal Intelligence* (SIGINT) die (zouden) bestaan tussen bepaalde landen. Het meest gekend is de zogenaamde FIVE EYES die naast de Amerika en Groot-Brittannië ook Canada, Australië en Nieuw-Zeeland tellen. Deze landen werken sinds decennia zeer nauw samen en gecapteerde datacommunicatie 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 behoort.[216]

Ten slotte is massale data-captatie en -exploitatie geen monopolie 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 opgenomen in de toezichtonderzoeken van het Comité: ze ligt buiten zijn bevoegdheidssfeer.

II.2. NIET ALLEEN PRISM EN TEMPURA

De eerste onthullingen hadden vooral betrekking op – wat betreft de Amerikanen – het PRISM-programma en – wat betreft de Britten – TEMPURA. Deze twee inlichtingenprogramma's blijken een zeer belangrijke bron van informatie maar ze zijn zeker niet de enigen. Enigszins schematiserend zou men vijf[217] vormen of technieken van massale datacaptatie of 'ongerichte interceptie' van (tele)communicatie kunnen onderscheiden (II.2.1). Daarnaast zijn er de diverse mogelijkheden om deze bulk aan gegevens te bewaren en te exploiteren (II.2.2).

II.2.1. Vijf vormen van massale data-captatie

Het toezichtonderzoek van het Comité beperkt zich in essentie tot inlichtingenprogramma's of -technieken waarbij in essentie 'ongericht' gecapteerd wordt (ook '*phishing expedition*' genoemd) waarbij 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.

Het betreft 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 internati-

man, French, Spanish and Swedish spy agencies", in: J. BOGER, *The Guardian*, 1 november 2013 ("GCHQ and European Spy Agencies Worked together on Mass Surveillance").

214 Zie in dat kader de beweringen over 'SORM': S. WALKER, *The Guardian*, 6 oktober 2013 ("Russia to monitor 'all communications' at Winter Olympics in Sochi").

215 X., *www.sophos.com*, 7 mei 2008 ("Belgium accuses Chinese government of cyber-espionage").

216 "*Beyond that, the NSA has other coalitions, although intelligence-sharing is more restricted for the additional partners: the 9-Eyes, which adds Denmark, France, The Netherlands and Norway; the 14-Eyes, including Germany, Belgium, Italy, Spain and Sweden […].*" (E. MACASKILL en J. BALL, *The Observer*, 2 november 2013 ("Portrait of the NSA: no detail too small in quest for total surveillance").

217 Uiteraard zijn andere voorstellingen, waarbij eventueel meer of minder vormen van massale datacaptatie worden onderscheiden, even waardevol.

onale internetkabel passeert om vervolgens op digitale wijze zoekingen te verrichten (datamining). Een ander voorbeeld is het capteren van alle gsm-signalen in een bepaalde regio.

Uit het expertverslag blijkt dat bij het capteren van bijvoorbeeld glasvezelkabels, meestal gewerkt wordt met zogenaamde '*selectors*': 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 op basis van die vooraf ingegeven parameters, 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 kunnen we er niet omheen dat er op ongerichte wijze wordt gecollecteerd. Alhoewel hierover (vooralsnog) geen volledige duidelijkheid bestaat, zijn de aanwijzingen dat er zeker ook ongericht, massaal gecapteerd wordt, overtuigend.

Vooraf willen we nog opmerken dat onderstaande 'technieken' zowel elkaar zowel kunnen 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).

II.2.1.1. Upstream-collectie

Upstream-collectie[218] is de naam die gegeven wordt aan 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. Dit kan – zoals bij de meeste technieken – met of zonder medeweten van de operator/uitbater van de kabel.

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

Omdat er door dergelijke kabels massaal veel gegevens passeren, worden naar alle waarschijnlijkheid 'filters' of 'selectoren' geplaatst (zie II.2.1) zodat alleen mogelijks relevante informatie moet worden opgeslagen en verwerkt.

---

218 *Upstream* of stroomopwaarts ten aanzien van de bestemmeling van de communicatie. Een voorbeeld: wanneer een persoon webmail gebruikt (dit wil zeggen vanaf zijn PC inlogt bij een dienstenverstrekker van webmail, zoals bijvoorbeeld de *outlook* van Microsoft) dan is hij in feite aan het werk op de server van deze dienstenverstrekker. Zijn mailbox staat niet op zijn eigen PC maar wel op een server op een andere locatie (zeer dikwijls in de USA). Het bericht dat wordt verzonden, kan dus worden onderschept tussen de betrokken persoon en de server.

II.2.1.2. Downstream-collectie

Een andere mogelijkheid om op massale wijze data te capteren is deze ophalen of – al dan niet onder dwang – opvragen bij telecomoperatoren zelf. Deze vorm van dataverwerving is gekend onder de naam downstream-collectie.[219] Het meest gekende 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. Alhoewel PRISM ook werkt op basis van 'selectors' (zie II.2.1), blijkt uit het expertverslag dat op basis van dit programma massaal veel gegevens naar de NSA doorstroomden.

II.2.1.3. Draadloze communicatie onderscheppen

Heel wat (internationale) communicatie verloopt (ten dele) via elektromagnetische stralen: van klassieke radiosignalen tot meer moderne gsm-technologie dat via zendmasten en satellieten (kan) verlopen.

Het ongemerkt en massaal onderscheppen van deze signalen is technisch perfect mogelijk en laat toe in *real time* gesprekken te beluisteren. 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 (F6 SITES), zou onder deze noemer kunnen geplaatst worden.

II.2.1.4. Hacken van IT-systemen

Een andere mogelijkheid om *en masse* interessant geachte gegevens te verzamelen, is het binnendringen in het IT-systeem van bijvoorbeeld een operator om ongezien alle nuttige informatie weg te sluizen. 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[220] (*sic*) 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. Maar BICS is hoogst waarschijnlijk niet de enige die zich in dit geval bevindt. Recente onthullingen spreken over tienduizenden computersystemen wereldwijd die zouden besmet zijn met *malware* van de NSA.[221]

---

219 *Downstream* of stroomafwaarts ten aanzien van de bestemmeling van de communicatie. Hier wordt de informatie betrokken uit de server van de dienstverstrekker zelf door bijvoorbeeld toegang te nemen tot de mailbox op die server of door de informatie te vragen.

220 X., *Der Spiegel*, 20 september 2013 ("Belgacom Attack: Britain's GCQH tracked Belgian Telecoms Firm").

221 S. DERIX en H. MODDERKOLK, *NRC Handelsblad*, 23 november 2013 ("De hackers van de NSA dringen overal binnen").

II.2.1.5. Samenwerking en uitwisseling van gegevens

Een laatste 'methode' is het in bulk uitwisselen van informatie tussen partnerdiensten. Soms gebeurt die 'spontaan', soms binnen het kader van een samenwerkingsverband waarbij dan iedere betrokken dienst de *monitoring* van een bepaald aspect van de (tele) communicatie voor zijn rekening neemt en de verzamelde gegevens vervolgens doorgeeft. Het hoeft geen betoog dat – zoals overigens blijkt uit de open bronnen – hierbij het gevaar bestaat dat dienst A doet wat dienst B niet mag volgens zijn nationale wetgeving en omgekeerd en waarbij men de gegevens met elkaar deelt zodat de wettelijke beperkingen *de facto* worden omzeild.[222]

Het meest gekende samenwerkingsverband is de FIVE EYES. De landen die er deel van uitmaken, delen bijvoorbeeld de informatie die zij elk afzonderlijk uit de glasvezelkabel halen die op hun grondgebied passeren. Maar ook andere landen geven massaal vergaarde data in bulk door. Zo zouden bijvoorbeeld de Noren, de Fransen en de Nederlanders op een periode van een maand tijd verschillende miljoenen gegevens hebben doorgespeeld.[223]

II.2.2. Bewaren en exploiteren van bulkinformatie

Het is natuurlijk zinloos om massaal veel data te capteren – volgens *The Washington Post* onderschept de NSA elke dag 1,7 miljard e-mailberichten en andere vormen van communicatie –wanneer die niet kunnen bewaard en geëxploiteerd worden. Gelet op de enorme hoeveelheden data die de diverse programma's samen genereren, is niet alleen gigantische *hardware* nodig om gegevens te stockeren maar ook performante *software* die toelaat de spreekwoordelijke speld in de hooiberg te vinden.

XKEYSCORE stelt 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. Maar het is ook mogelijk bulkgegevens aan partnerlanden of –diensten te geven voor verdere analyse.

II.3. WELK SOORT GEGEVENS WORDEN GECAPTEERD VIA DE AMERIKAANSE EN BRITSE SIGINT?

Alhoewel hierover in het begin geen zekerheid bestond, is snel duidelijk geworden dat de diverse programma's niet alleen metadata capteren (zoals bijvoorbeeld het adres van afzender en bestemmeling, de connectie-identificatie, het tijdstip en duur, het gebruikte

---

222 "*De Amerikaanse inlichtingendienst bespioneerde volgens The Gardian sinds 2007 in ruime mate de gegevens van Britse burgers – en dat met gedoging van Londen.*" (X, De Morgen, 22 november 2013 ("Britse burgers massaal bespioneerd").

223 Dit werd publiekelijk toegegeven onder meer door de Noorse inlichtingendienst en door NSA-officials die zich verplicht voelden om een vermeende verkeerde lezing van bepaalde Snowden-slides door journalisten recht te zetten. De journalisten waren immers van mening dat het in elk van die landen om door de NSA afgetapte communicaties ging (VHN, *De Standaard*, 27 november 2013 ("Noorse inlichtingendienst betwist claims over NSA-spionage")).

technische middel, de grootte van een bestand …) maar ook de pure 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, werden onderschept. Maar ook hier hebben de open bronnen op overtuigende wijze aangetoond dat de interesse en de bevoegdheidssfeer van bijvoorbeeld de NSA vele malen ruimer is: ook economische en politieke informatie blijkt een target.

II.4. WAT MET PERSOONS-, ECONOMISCHE – OF POLITIEKE GEGEVENS VAN EN OVER BELGEN EN BELGIË?

De onophoudelijke onthullingen doen verwerkingscapaciteiten vermoeden van meerdere peta-bytes per dag of van miljarden metadata over langere periodes. Dat het virtuele net dat grote inlichtingendiensten over de digitale wereld hebben gespannen, een nooit geziene captatie toelaat, lijkt dan ook aangetoond.

Maar het Vast Comité I is vanzelfsprekend 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). Vooralsnog is hierover weinig specifieks bekend.

Het zou echter naïef zijn te besluiten dat wij als een van de enige Europese landen buiten schot zijn gebleven, zeker gelet op de aanwezigheid van belangrijke internationale organisaties op ons grondgebied. Mogelijks brengen nieuwe onthullingen hierover meer klaarheid.

Los daarvan zijn er in het expertverslag heel wat elementen aanwezig die doen besluiten dat 'Belgische data' noodzakelijkerwijs op grote schaal werden onderschept.

Alleen al de wijze waarop de NSA bepaalde gebruikersdata verkrijgt bijvoorbeeld, impliceert per definitie dat ook gegevens van Belgen kunnen gecapteerd worden. Immers talrijke landgenoten maken dagelijks gebruik van de diensten van een van de negen Amerikaanse bedrijven die opgenomen zijn in het PRISM-programma (Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL en Apple).

Maar ook voor *upstream*-collecte zijn Belgische data niet immuun. E-mails of chats kunnen bepaalde 'selectors' triggeren wanneer zij bijvoorbeeld – wat veelal het geval is – passeren via een kabel die over het Amerikaanse grondgebied loopt.

Daarbij is het van belang te weten dat een (deel van een) elektronische boodschap die vanuit België naar een ander land verstrekt veelal via Amerika reist. De route die een bericht (of een deel van een bericht) neemt, hangt af van de verkeersdensiteit of de kost op een bepaald moment op een bepaald traject, en dus niet van wat de geografisch kortste weg is. Heel veel informatie op het internet reist via de USA omdat zich daar de grootste vervoerscapaciteit van en naar de andere landen van de wereld bevindt, zelfs al moeten de berichten daarvoor een 'omweg' van duizenden kilometers maken. En wat de Amerikaanse diensten is ontgaan, hebben de Britse mogelijks onderschept via hun mogelijkheden om glasvezelkabels te tappen. In dezelfde context kan melding worden gemaakt van het feit dat de GCHQ data zou aftappen van de interne glasvezelverbindingen tussen Google's data centers. Daarbij moet opgemerkt dat een van de belangrijkste datacenters van Google in België ligt.

Verder worden metadata van 'Belgische gesprekken' verzameld indien Belgen rechtstreeks communiceren met een Amerikaan die door de NSA als *target* wordt beschouwd, maar ook indien ze communiceren met een 'contact van een contact' van die persoon.

Een totaal ander voorbeeld vormt de onthulling dat de NSA-divisie die instaat voor 'internationale veiligheid', onder meer focust op 'de buitenlandse politiek en handelsrelaties van België'.[224]

Ten slotte is er uiteraard de *hacking* van BICS/Belgacom. Alhoewel hier naar alle waarschijnlijkheid weinig 'puur' Belgische data zijn verzameld, kunnen we er natuurlijk niet om heen dat dit overheidsbedrijf deel uitmaakt van de Belgische kritieke infrastructuur.

III. TER AFRONDING

Dat bepaalde grootmachten – zoals de Verenigde Staten – al geruime tijd over verregaande middelen en programma's beschikten om aan massale data-captatie te doen, is algemeen geweten. Bij wijze van voorbeeld kunnen we hier verwijzen naar de onthullingen inzake het Echelon-netwerk en de Swift-zaak.[225]

Maar vandaag worden we geconfronteerd met twee 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 gebeurd is vanuit een inlichtingencontext is niet eens zo verwonderlijk. Bijvoorbeeld biedt de internettechnologie, inclusief alle communicatievormen die zich via het internet voordoen, een gedroomde bron van gedetailleerde gegevens die voordien onbereikbaar waren. Met de digitalisering opende zich een nieuwe dimensie voor de inlichtingenwereld, waarvan iedereen zich bewust moet zijn.

Tweede 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.

---

224 X., *De Tijd*, 4 september 2013 ("Staatsveiligheid onderzoekt spionage door NSA").

225 Minder gekend is het feit dat er vóór Snowden reeds andere klokkenluiders bepaalde praktijken van de NSA hebben aangeklaagd. Zo bijvoorbeeld brachten voormalig NSA-medewerkers William Binney, Thomas Andrew Drake en Thomas Tamm in het begin van de jaren 2000 bepaalde collecte-programma's in de openbaarheid.

DE SNOWDEN-REVELATIES, MASSALE DATA-CAPTATIE EN POLITIEKE SPIONAGE

Open bronnenonderzoek[226]

INLEIDING

1. Dit verslag biedt een overzicht – aan de hand van open bronnen[227] – van de soorten gegevens die mogelijks betrekking hebben op (of afkomstig zijn van) in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) en die door het Amerikaanse National Security Agency (NSA) het Britse Government Communications Headquarters (GCHQ), of private firma's in opdracht van deze diensten, op grote schaal worden gecapteerd en opgeslagen en dit met het oog op een (eventuele latere) exploitatie door hun inlichtingendiensten. Tevens werd een overzicht geboden van gevallen waaruit blijkt dat onder meer deze diensten de afgelopen decennia operaties hebben opgezet die gericht waren op politiek spionage ten aanzien van zogenaamde 'bevriende landen'. De open bronnen die voor dit verslag geconsulteerd werden zijn van wisselende kwaliteit. Waar mogelijk werd zoveel mogelijk gebruikt gemaakt van primaire bronnen (*slideshows*, officiële documenten) die in de laatste maanden gepubliceerd werden door onderzoeksjournalisten. De kritische interpretatie van deze (onvolledige) stukken informatie werd geholpen door de consultatie van andere experten. Te speculatieve persanalyses waarbij geen extra informatie gevonden werd ter ondersteuning van een denkpiste werden niet weerhouden. Als bijlage bij dit verslag werd een verklarende afkortingenlijst opgenomen.

2. Om de specifieke collectiemechanismen die onthuld werden sinds juni 2013 beter te begrijpen, is het vooreerst evenwel nodig om summier de wettelijke context te beschrijven waarin respectievelijk de NSA en GCHQ actief zijn, om vervolgens inzicht te krijgen in het mandaat en de voorzorgsmaatregelen die al dan niet van toepassing zijn in de uitvoering van dat mandaat. Ook werd getracht om telkens een inzicht te krijgen in de grootteorde van de gegevensverzameling en de tijdsspanne waarin deze collectiemechanismen actief zijn.

---

226 Dit open bronnenonderzoek werd in opdracht van het Vast Comité I uitgevoerd door drs. Mathias Vermeulen, Research Fellow aan het European University Institute in Firenze en het Centre for Law, Science and Technology Studies aan de VU Brussel. Werkte van 2008 tot 2011 als onderzoeker voor de toenmalige United Nations Special Rapporteur on the promotion and protection of human rights while countering terrorism, en deed onderzoek voor het Europese Parlement over 'Parliamentary oversight of security and intelligence agencies in the European Union'. Zie:www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf).

227 De expert ging zeer kritisch te werk en werden al te speculatieve denkpistes of theorieën niet weergegeven. Nieuw vrijgegeven informatie of de contestatie vanuit officiële hoek van eerder becommentarieerde gegevens sluit een andere lezing van bepaalde aspecten van de zaak, niet uit.

3. De ervaring met de Snowden-documenten tot nu toe leert dat vooralsnog ongepubliceerde, vertrouwelijke documenten die mogelijks in de toekomst gepubliceerd zullen worden, een impact zullen hebben op de interpretatie van eerdere gepubliceerde documenten en berichtgeving over de revelaties. Deze nota is dus onvermijdelijk een tijdsopname, die een stand van zaken weergeeft tot en met 23 oktober 2013.

I. HET AMERIKAANSE NATIONAL SECURITY AGENCY (NSA)

4. De NSA is een militaire inlichtingendienst die geleid wordt door Generaal Keith B. Alexander. Alexander rapporteert aan de Under Secretary of Defense for Intelligence, Michael G. Vickers, de voornaamste intelligence-adviseur van de Amerikaanse Minister van Defensie, Chuck Hagel. De NSA is ook een onderdeel van de US 'Intelligence Community', die geleid wordt door James Clapper. Volgens EO 12333 heeft de directeur van de NSA (DIRNSA) onder meer de taak om *signals intelligence* (SIGINT[228]) te verzamelen (inclusief via clandestiene middelen), verwerken, analyseren, produceren en te verspreiden voor *foreign intelligence* en *counterintelligence* doelen[229] en om militaire operaties te ondersteunen.[230] De NSA's SIGINT-verzameling is geregeld door twee belangrijke documenten: Executive Order 12333 (EO 12333)[231] en de Foreign Intelligence Surveillance Act (FISA).

I.1. HET WETTELIJKE KADER VOOR HET INZAMELEN VAN INFORMATIE OVER BUITENLANDSE DOELWITTEN

I.1.1. Executive Order 12333

5. *Foreign intelligence*' wordt in EO 12333 gedefinieerd als alle informatie die gerelateerd is aan de capaciteiten, intenties of activiteiten van buitenlandse machten, organisaties of personen.[232] Het verzamelen van SIGINT kan gebaseerd worden louter en alleen op basis

---

228 SIGINT is *intelligence* die gecreëerd wordt door elektronische signalen en systemen, zoals communicatiesystemen, radars, satellieten of wapensystemen. Zie hierover bijvoorbeeld www.nsa.gov/sigint/.

229 Executive Order 12333 – United States intelligence activities, 4 December 1981, sectie 1.7(c)(1). EO 12333 werd geamendeerd door de Executive Orders 13284 (2003), 13355 (2004) en 13470 (2008). De geconsolideerde versie van EO 12333 is consulteerbaar op https://www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf. Er moet opgemerkt worden dat EO 12333 de activiteiten van alle leden van de US Intelligence Community regelt, en dus niet alleen van de NSA.

230 *Idem*, sectie 1.7(c)(3) en (5).

231 Voor EO 12333 was er al EO 12139 (Exercise of Certain Authority Respecting Electronic Surveillance), die werd geamendeerd door EO 12333, EO 13383 en EO 13475.

232 *Idem*, sectie 3.5(e). EO 12333 maakt ook duidelijk dat *foreign intelligence* niet alleen via SIGINT kan verzameld worden, maar ook door andere elementen van de *intelligence community* kan gebeuren via fysieke surveillance (zie bijv. sectie 2.4(d) "*Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means*".

van deze *executive order*, zonder dat daarbij de uitgebreidere FISA-procedures moeten gevolgd worden.[233] EO 12333 vormt bijvoorbeeld de wettelijke basis voor het verwerven van enorme hoeveelheden metadata buiten Amerikaans grondgebied[234], alsook voor het verzamelen van contactlijsten of adresboeken van e-mail- en chatprogramma's.[235] Dat soort informatie valt immers niet onder de definitie van *electronic surveillance* zoals FISA die gebruikt.[236] EO 12333 lijkt ook de wettelijke basis te vormen voor de meest controversiële activiteiten van de NSA, en dan vooral van subdivisies zoals het Office of Tailored Access Operations (TAO) en de Special Collection Service (SCS), zoals het omzeilen van commerciële encryptiebeveiligingen[237], het hacken van buitenlandse computers[238] of het bespioneren van buitenlandse leiders vanuit Amerikaanse ambassades.[239] Er is weinig tot geen toezicht over deze activiteiten door het US Senate Intelligence Committee.[240]

I.1.2. Foreign Intelligence Surveillance Act

6. Een groot deel van de 'elektronische surveillance' wordt geregeld door de Foreign Intelligence Surveillance Act (FISA) uit 1978. FISA werd gecodificeerd in 50 U.S.C. § 1801 *et seq.*, en werd daarna onder meer significant aangevuld met nieuwe provisies uit de Patriot Act[241], die onder meer de installatie en het gebruik van 'pen registers'[242] en '*trap*

---

233 N.S.A., The National Security Agency: Missions, Authorities, Oversight and partnerships. 9 Augustus 2013 (www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf, 2).

234 Foreign Intelligence Surveillance Court, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13 – 109, 29 August 2013 op pag. 10, n.10. ("*The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders*".) Zie ook paragraaf 15.

235 Zie paragrafen 25-27.

236 US Code Title 50 – War and National Defence, 50 USC 1801(f).

237 Zie paragrafen 45-48.

238 Zie bijvoorbeeld paragrafen 29, 47 en 48.

239 Zie bijvoorbeeld paragraaf 19.

240 Een staflid van het Committee hierover: "*In general, the committee is far less aware of operations conducted under 12333 (…). I believe the NSA would answer questions if we asked them, and if we knew to ask them, but it would not routinely report these things, and, in general, they would not fall within the focus of the committee.*" www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story_1.html.

241 Zie 50 U.S.C. § 1841 *et seq.*

242 Een '*pen register*' wordt gedefinieerd in 18 U.S.C. § 3127(3) als "*a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business*".

and trace devices'[243] en het produceren van 'tastbare dingen' regelen.[244] FISA werd het meest recent geamendeerd in 2008 door de FISA Amendments Act (FAA).[245] In december 2012 verlengde de Amerikaanse Senaat de werking van de FISA Amendments Act tot en met 31 december 2017. Volgens de NSA is de belangrijkste toepassing van FAA het verzamelen van de communicaties van buitenlandse personen die Amerikaanse aanbieders van communicatiediensten gebruiken.[246] Momenteel liggen er verschillende wetgevende voorstellen op tafel die de binnenlandse collectie van informatie door de VS zou moeten beperken[247], maar tot nu toe zijn er geen gelijkaardige initiatieven om de collectie van informatie van 'buitenlanders' in te perken.[248] In dit verslag zal alleen verder ingegaan worden op de recentste FISA-Amendments Act, die op zich een aanvulling vormen op 50 USC § 1802. Onder 50 U.S.C. § 1802 kan de Amerikaanse Procureur-Generaal (*Attorney-General*) elektronische surveillance machtigen voor een periode van één jaar als die surveillance exclusief gericht is op (1) het verwerven van de inhoud van de communicaties die uitgezonden worden communicatiemiddelen die alleen door of tussen 'buitenlandse machten'[249] gebruikt worden of (2) het verwerven van *technical intelligence* van plaatsen die onder de openlijke en exclusieve controle van een 'buitenlandse macht' staan.

7. De FISA Amendments Act geeft de AG en de DNI de bevoegdheid om voor een periode van één jaar elektronische surveillance te machtigen van personen waarvan redelijkerwijs kan aangenomen kan worden dat die zich buiten de Verenigde Staten bevinden, met als specifiek doel om 'buitenlandse inlichtingen' te verzamelen.[250] 'Buitenlandse inlichtingen' worden zeer breed gedefinieerd als:

---

243 Een '*trap and trace device*' wordt gedefinieerd in 18 U.S.C. § 3127(4) als "*a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication*".

244 Zie 50 U.S.C. § 1861. Dit is bijvoorbeeld de wettelijke basis voor de MAINWAY database, zie para. 37.

245 Zie H.R. 6404, FISA Amendments Act of 2008' (zie www.gpo.gov/fdsys/pkg/BILLS-110hr6304enr/pdf/BILLS-110hr6304enr.pdf. De vaak aangehaalde 'Section 702. Procedures for targeting certain persons outside the United States other than United States persons' werd geconsolideerd in de U.S Code als 50 USC § 1881a, (www.law.cornell.edu/uscode/text/50/chapter-36). Eerder werd FISA ingrijpend geamendeerd door de Patriot Act in 2001.

246 N.S.A., "The National Security Agency: Missions, Authorities, Oversight and partnerships", 9 Augustus 2013. zie www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf, 4.

247 Voor een overzicht van de twee belangrijkste initiatieven, zie J. GRANICK, "A tale of two surveillance reform bills. Centre for Internet and Society", 29 October 2013, zie https://cyberlaw.stanford.edu/blog/2013/10/tale-two-surveillance-reform-bills.

248 Zie bijvoorbeeld D. POKEMPNER, "Dispatchers: Taming the NSA – Reform bills fall short. Human Rights Watch", 30 October 2013, zie www.hrw.org/news/2013/10/30/dispatches-taming-nsa-reform-bills-fall-short.

249 Zie definitie in para. 8.

250 Het moet opgemerkt worden dat *acquire* niet hetzelfde betekent als *collect*. Zie bijvoorbeeld Department of Defense, DoD 5240 1-R, Procedures governing the activities of DoD intelligence components that affect United States persons. December 1982, 15. *"Data acquired by electronic means is "collected" only when it has been processed into intelligible form"*. De titel van sectie 1881a heet voluit: *"Procedures for targeting certain persons outside the United States other than United States persons."* De betekenis van *targeting* wordt echter niet gedefinieerd in 50 USC

"(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against–
(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to–
(A) the national defense or the security of the United States; or
(B) the conduct of the foreign affairs of the United States."[251]

8. Vooral die laatste categorie staat een in principe ongelimiteerde inzameling van informatie toe. Dat is nog meer het geval aangezien de definitie van een 'buitenlandse macht' ook uitgebreid gedefinieerd wordt. De term houdt niet alleen buitenlandse regeringen, parlementsleden of internationale organisaties in, maar ook bijvoorbeeld "*een politieke organisatie in het buitenland, die niet substantieel bestaat uit Amerikaanse burgers*"[252] en "*een entiteit die gestuurd en gecontroleerd wordt door een buitenlandse overheid*".[253] Beide categorieën zouden in theorie bijvoorbeeld respectievelijk NGO's die anti-Amerikaanse betogingen organiseren of staatsbedrijven kunnen inhouden.

9. De Foreign Intelligence Surveillance Court (FISC) gaat na of de machtiging van de AG en DNI (zie para. 7) aan een aantal procedurele voorwaarden voldoet. De AG en DNI voegen een geschreven certificaat toe aan de machtiging die aantoont hoe men aan die procedurele voorwaarden voldoet. Die voorwaarden hebben voornamelijk als doel dat zo weinig mogelijk gegevens van Amerikaanse burgers intentioneel wordt verzameld.[254] Er zijn nergens in de Amerikaanse wetgeving gelijkaardige 'minimizatie procedures' voorzien die moeten voorkomen dat 'onschuldige' buitenlandse gegevens verzameld en bewaard kunnen worden. Het certificaat moet ook nergens vermelden welke specifieke faciliteiten, plaatsen of eigendommen precies het doelwit zijn van de SIGINT-verzameling.[255] De Amerikaanse overheid declassificeerde een document van 31 oktober 2011 dat de 'minimizatie procedures' beschreef die de NSA hanteerde om '*foreign intelligence* informatie' te verzamelen. Daaruit bleek dat communicaties van of over Amerikaanse

---

§ 1881. 50 USC § 1801 definieert *electronic surveillance* als *"the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes*". Een interpretatie zou dus kunnen zijn de gegevens van informatie pas gezien wordt als *targeting*, als het de *bedoeling* was om bepaalde informatie te verzamelen. Incidenteel verzamelde informatie wordt dan niet gezien als *targeting*.

251 50 USC § 1801(e).

252 50 USC § 1801(a)(5).

253 50 USC § 1801(a)(6).

254 50 USC § 1801(g).

255 50 USC § 1801(g)(2)(4).

burgers die niet met opzet werden verzameld tot vijf jaar bewaard mochten worden[256] en gedeeld mochten worden met buitenlandse overheden.[257]

10. Als de FISC zijn goedkeuring geeft, dan kunnen de AG en DNI op basis van een dergelijk breed certificaat, '*identifiers*' (bijvoorbeeld e-mailadressen of telefoonnummers)[258] doorgeven aan een Amerikaans bedrijf dat dan verplicht is om onmiddellijk alle "*informatie, faciliteiten of andere assistentie*" te geven om die SIGINT-verzameling te doen slagen.[259] Die bedrijven worden daarvoor financieel gecompenseerd, en kunnen in "*geen enkele rechtbank*" aansprakelijk worden gesteld voor het leveren van dergelijke informatie.[260] Een bedrijf kan in beroep gaan tegen een dergelijke vraag (bijvoorbeeld omdat de vraag te breed is)[261], waarna de FISC de vraag kan verwerpen of een finaal bevel tot medewerking kan uitspreken.[262]

I.1.3. Safe Harbour

11. Amerikaanse bedrijven kunnen dus verplicht worden om gegevens over te dragen aan de NSA, inclusief gegevens van en over Belgische klanten. Die eis naar Amerikaans recht kan botsen met de principes van het EU-US Safe Harbour akkoord uit 2000, waarbij Amerikaanse bedrijven vrijwillig de principes in dat akkoord kunnen onderschrijven. Bedrijven worden daar bijvoorbeeld geacht om aan hun klanten te kennen geven dat hun persoonlijke data aan een derde partij werd doorgegeven.[263] De Federal Trade Commission (FTC) ziet toe op de handhaving van het akkoord. Van deze principes mag afgeweken worden in naam van nationale veiligheid of omdat rechtshandhaving het vereist. De grote schaal waarop persoonlijke gegevens van Europese gebruikers van Amerikaanse bedrijven naar de NSA werden verstuurd binnen het PRISM-programma (zie para's 32-38), leidde er echter toe dat de Europese Commissie momenteel onderzoekt of het Safe Harbour akkoord niet herzien moet worden.[264]

---

256 Exhibit B, Minimization Procedures used by the National Security Agency in connection with acquisitions of foreign intelligence information pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%207 02.pdf), s.3(b)(1).

257 *Idem*, (s.8(a)).

258 N.S.A., "The National Security Agency: Missions, Authorities, Oversight and partnerships", 9 Augustus 2013, 4.

259 50 USC § 1802, (a)(4); 50 USC § 1881a(1) en (2).

260 50 USC § 1881a (h)(3).

261 In 2007 kreeg Yahoo een dergelijke *order* om data te geven. Yahoo vocht deze aan bij het Foreign Intelligence Surveillance Court of Review. De rechtbank verwierp echter Yahoo's tegenwerpingen. Die beslissing werd recent pas vrijgegeven. Zie https://www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf.

262 50 USC § 1881a (h)(4).

263 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.) Zie ook http://export.gov/safeharbor/eu/eg_main_018493.asp.

264 Commisaris Reding: "*The Safe Harbor agreement may not be so safe after all (.) It could be a loophole for data transfers because it allows data transfers from EU to U.S. companies-although*

12. Op 22 oktober 2013 stemde het Europese Parlement voor het toevoegen van een zogenaamde 'anti-FISA clausule', die bedrijven niet zou toestaan om zonder toelating van een *supervisory authority* persoonlijke data van Europese inwoners door te sturen naar een derde land op vraag van een rechtbank of een andere autoriteit in dat land. Die *supervisory authority* moet eerst nagaan of de transfer noodzakelijk is en in conformiteit met de nieuwe Europese databeschermingswetgeving. Het valt af te wachten of dit artikel de onderhandelingen met de Raad zal overleven.[265]

I.2. AARD EN SCHAAL VAN SIGINT-VERZAMELING DOOR DE NSA

13. Het is moeilijk om de totaliteit van de SIGINT-verzameling van de NSA in kaart te brengen. Enkele cijfers geven alvast een idee over de grootteorde. *The Guardian* citeert een NSA-rapport uit 2007 dat schat dat er op dat moment ongeveer 850 miljard ongedefinieerde *call events* in verschillende NSA-databases te vinden zijn, en ongeveer 150 miljard ongedefinieerde *internet records*. Volgens het document worden er elke dag één tot twee miljard *records* toegevoegd.[266] Een artikel uit *The Washington Post* stelde in 2010 dat de NSA per dag de inhoud en metadata van 1,7 miljard e-mails, telefoongesprekken en andere vormen van communicatie bewaarde, en dat een fractie daarvan in ongeveer 70 aparte databases werd bewaard.[267]

14. Die capaciteit is sindsdien exponentieel toegenomen. Slides van de NSA's interne Boundless Informant programma[268] die gepubliceerd werden door *The Guardian* tonen dat in de periode van een maand (maart 2013) de NSA's Global Access Operations divisie (GAO)[269] 97 miljard metadata van internet communicaties (e-mails, chats …) verzamelde en bijna 125 miljard metadata van telefoongesprekken die afkomstig waren uit meer dan 504 SIGINT Activity Designator (SIGADS).[270] Uit de slide blijkt dat België één van de

---

U.S. data protection standards are lower than our European ones. (…) I have informed ministers that the commission is working on a solid assessment of the Safe Harbor Agreement, which we will present before the end of the year" European Commission, Memo/13/710, 19/07/2013, http://europa.eu/rapid/press-release_MEMO-13-710_en.htm.

265 Zie artikel 43a van de "Unofficial consolidated version of the European Data Protection Regulation after the LIBE Committee vote provided by the rapporteur", 22 October 2013, beschikbaar op www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf Zie ook C., "The US surveillance programmes and their impact on EU citizens' fundamental rights", European Parliament, Directorate General for Internal Policies, 2013, 28.

266 www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu.

267 D. PRIEST, W. M. ARKIN, *The Washington Post* ("Secret America: A Hidden World, Growing Beyond Control"), http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/3/.

268 Meer informatie zie: NSA, Boundless Informant – Frequently Asked Questions (09-06-2012), zie www.theguardian.com/world/interactive/2013/jun/08/boundless-informant-nsa-full-text.

269 Dit houdt dus niet de metadata collectie in van andere NSA-divisies zoals TAO of SSO.

270 *Signals activity/address designators* – kunnen verwijzen naar een specifiek fysiek collectieplatform (zoals bijvoorbeeld een Amerikaanse legerbasis in het buitenland, een ambassade, een schip …), een virtueel dataverwerkingsplatform (PRISM staat bijvoorbeeld bekend als SIGAD US-984XN) of een ruimtesatelliet.

landen was van waaruit in absolute getallen het minst metadata werden verzameld.[271] De slide verraadt niet over hoeveel metadata het gaat, maar aan de hand van de kleurcode die België daar heeft, lijkt het dat er alvast op dat er minder metadata vanuit België wordt verzameld in vergelijking met bijvoorbeeld Nederland.

15. *Der Spiegel* publiceerde extra slides uit het programma in augustus 2013 die duidelijk maakten dat in december 2012 vanuit Nederland er ongeveer 1,8 miljoen metadata van telefoongesprekken verzameld werden.[272] In diezelfde periode werd er vanuit Frankrijk 70 miljoen metadata van telefoongesprekken verzameld[273], uit Spanje 60 miljoen en uit Italië 47 miljoen.[274]

16. Vanuit Duitsland werd er in dezelfde periode meer dan 500 miljoen metadata verzameld. Dat aantal is veel groter omdat het ook over internet-metadata gaat. Uit een document blijkt dat meer dan 471 miljoen metadata uit SIGAD US-987LA komen.[275] Volgens *Der Spiegel* gelooft de Bundesnachrichtendienst (BND) dat hiermee verwezen wordt naar de Bad Aibling site, een site die tot 2004 gerund werd door de NSA, maar daarna werd overgenomen door de BND. Vanuit die site verzamelt de BND buitenlandse SIGINT, vooral uit Afghanistan en het Midden Oosten. Die data wordt dan doorgespeeld naar de NSA.[276]

17. Volgens de NSA vervoert het internet iedere dag 1,826 petabytes aan informatie. Daarvan 'raakt' de NSA 1,6% 'aan', ongeveer 29 miljoen gigabyte per dag.[277] Van die 1,6%

---

271 www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining#.

272 Www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-6.html.

273 Www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-6.html *Le Monde* publiceerde in oktober 2013 meer details waaruit het lijkt dat onder de codenaam DRTBOX 62,5 miljoen metadata werd verzameld van mobiele telefoongespreken en onder de codenaam WHITEBOX de metadata van 7,8 miljoen gesprekken van het openbare telefoonnet (*Public switched telephone network (PSTN)*). Doelwitten waren zowel mensen die geassocieerd werden met terroristische activiteiten alsook mensen uit de zakenwereld, de Franse politiek of de Franse zakenwereld. www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-crosshair-phone-networks-under-surveillance_3499741_651865.html Verschillende media berichtten dat er 70 miljoen Franse telefoongesprekken afgeluisterd werden. Dat is zeker een foute interpretatie van de Snowden-documenten. Zie hierover ook "DNI Statement on Inaccurate and Misleading Information in Recent Le Monde Article", 22 oktober 2013 (http://icontherecord.tumblr.com): "*The allegation that the National Security Agency collected more than 70 million "recordings of French citizens' telephone data" is false. (…) While we are not going to discuss the details of our activities, we have repeatedly made it clear that the United States gathers intelligence of the type gathered by all nations*."

274 Www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-5.html.

275 Www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-4.html.

276 Volgens *Der Spiegel* worden er vanuit Bad Aibling alleen al 62.000 e-mails per dag onderschept. www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html.

277 '*Touch*' is geen term die wettelijk gedefinieerd is, maar impliceert informatie waar de NSA effectief naar kijkt (in tegenstelling tot de loutere verzameling van informatie). *The Wall Street Journal* hierover: "*One U.S. official says the agency doesn't itself "access" all the traffic within the*

wordt 0,025% geselecteerd om geëvalueerd te worden. Volgens de NSA "bekijkt het dus amper 0,00004% van alle internetverkeer per dag".[278] Een gewone berekening zou suggereren dat dat aantal 10 keer zo hoog ligt, waardoor de NSA dus 0,0004% van alle internetverkeer berekent, maar volgens de NSA is het originele cijfer correct.[279]Dat lijkt weinig, maar dat is nog een enorme hoeveelheid wetende dat bijvoorbeeld slechts 2,9% van alle webtraffiek in de VS bestaat uit communicaties.[280]

18. *The Guardian* beschreef een document van 26 december 2012 waarin de 'Special Source Operations' (SSO) divisie aankondigde dat het een nieuwe capaciteit (codenaam EVILOLIVE) zou verwerven om nog meer metadata te verzamelen van communicaties waarvan een partij niet-Amerikaans is (One-End Foreign (1EF) solution). De NSA zou nu meer dan de helft van alle metadata informatie die het verzamelt via haar SIGADS in haar eigen databases kunnen opslaan.[281] Een ander, niet vrijgegeven document spreekt over een ander metadata-verwervings-capaciteit genaamd SHELLTRUMPET, waarvan op 31 december 2012 een SSO-official zei dat dit programma net haar triljoenste metadata-record had verwerkt. De helft van die verwerkingen vond in 2012 plaats. Nog twee andere metadata-programma's (MOONLIGHTPAD en SPINNERET) werden verwacht operationeel te worden tegen september 2013.[282]

19. Een recent vrijgegeven uitspraak van de FISC uit 2011 suggereert dat 91% van de internetdata die de NSA verzamelt uit het PRISM programma komt.[283] De rest komt van zogenaamde '*upstream*' dataverwerking, en clandestiene missies uit het zogenaamde 'Specialized Reconnaissance Program' (SRP) die uitgevoerd kunnen worden samen met de CIA. *The Washington Post* gaf het budget van de 'US intelligence community' in 2013 vrij, en daaruit blijkt dat 2% van het totale budget gereserveerd werd voor twee gezamenlijke

---

surveillance system. The agency defines access as "things we actually touch," this person says, pointing out that the telecom companies do the first stage of filtering. http://online.wsj.com/article_email/SB10001424127887324108204579022874091732470-lMyQjAxMTAzMDIwMDEyNDAyWj.html.

278 N.S.A., "The National Security Agency: Missions, Authorities, Oversight and partnerships", 9 Augustus 2013, 6.

279 NSA woordvoerder V. VINES:"*Our figure is valid; the classified information that goes into the number is more complicated than what's in your calculation*". Zie www.thewire.com/politics/2013/08/nsa-better-data-collection-math/68490/.

280 In de VS bijvoorbeeld is '*real time entertainment*' (*streaming* sites zoals Netflix bijvoorbeeld) verantwoordelijk voor 62% van alle webtraffiek en *peer-to-peer file-sharing* (via sites zoals Bittorrent bijvoorbeeld) voor 10,5%. Zie J. JARVIS, *Buzzmachine*, 10 Augustus 2013 ("NSA by the numbers"), http://buzzmachine.com/2013/08/10/nsa-by-the-numbers/.

281 www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection "*This new system, SSO stated in December, enables vastly increased collection by the NSA of internet traffic. (…) The 1EF solution is allowing more than 75% of the traffic to pass through the filter," the SSO December document reads. "This milestone not only opened the aperture of the access but allowed the possibility for more traffic to be identified, selected and forwarded to NSA repositories.*"

282 www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.

283 Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates), 3 October 2011, 71. Zie www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa – deel 8.

CIA-NSA programma's. Het eerste programma heet CLANSIG ('*clandestine signals collection*'), dat een variëteit aan *black bag jobs* of *off-net* operaties dekt. Dat zijn zeer risicovolle clandestiene operaties waarbij toegang gezocht wordt tot bijvoorbeeld radiofrequenties en cruciale telecominfrastructuur van een land, maar ook de specifieke toegang tot de e-mails en computers van *high interest* doelwitten zoals buitenlandse overheden, militaire communicatiesystemen en grote multinationals. Het laatste decennium zijn er meer dan honderd van dergelijke *black bag jobs* uitgevoerd. In deze operaties wordt bijvoorbeeld *spyware* geïnstalleerd op computers of worden beveiligde telefoonlijnen, routers, glasvezelkabels, data switch centra en andere systemen 'afluisterbaar' gemaakt de CIA, waardoor de NSA toegang krijgt tot die gegevens. Dergelijke operaties hebben vooral plaatsgevonden in het Midden Oosten en Azië, vooral in China.[284] Het tweede gezamenlijke initiatief van de NSA en de CIA is de Special Collection Service (SCS), die officiële VS-gebouwen zoals ambassades en consulaten als uitvalsbasis gebruikt om in het geheim communicaties te onderscheppen, onder meer van (geëncrypteerd) diplomatiek verkeer in het land waar de ambassade of het consulaat gevestigd is.[285] SCS-personeel bezit diplomatieke status.[286] Hun operaties verlopen vaak vanuit een Secure Compartmented Intelligence Facility (SCIF) op de bovenste verdieping van een ambassade. De meeste diplomaten van een ambassade lijken niet te weten wat er in deze *staterooms* gebeurt.[287] Volgens *Der Spiegel* is de SCS actief in 80 landen, waaronder 19 Europese.[288] Tot nu toe vrijgegeven documenten en slides lijken te suggereren dat de SCS niet actief lijkt te zijn in België.[289] Het is de SCS die verdacht wordt van het afluisteren van de mobiele telefoon van Angela Merkel.[290]

I.3. 'UPSTREAM'-VERZAMELING IN DE VS

20. Via glasvezelkabels passeert meer dan 80% van het wereldwijde telefoon- en internetverkeer cruciale punten in de VS die uitgebaat worden door de drie grootste Ameri-

---

284 Bijvoorbeeld: "*In another more recent case, CIA case officers broke into a home in Western Europe and surreptitiously loaded Agency-developed spyware into the personal computer of a man suspected of being a major recruiter for individuals wishing to fight with the militant group al-Nusra Front in Syria, allowing CIA operatives to read all of his email traffic and monitor his Skype calls on his computer*": www.foreignpolicy.com/articles/2013/07/16/the_cias_new_black_bag_is_digital_nsa_cooperation.

285 US Intelligence 2013 budget http://apps.washingtonpost.com/g/page/national/inside-the-2013-us-intelligence-black-budget/420/#document/p13/a117314 Foreign Policy: "*For example, virtually every U.S. embassy in the Middle East now hosts a SCS SIGINT station that monitors, twenty-four hours a day, the complete spectrum of electronic communications traffic within a one hundred mile radius of the embassy site.* www.foreignpolicy.com/articles/2013/07/16/the_cias_new_black_bag_is_digital_nsa_cooperation?page=0,1).

286 Zie noot 99.

287 www.spiegel.de/fotostrecke/photo-gallery-spies-in-the-embassy-fotostrecke-103079-6.html.

288 www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.

289 http://cpunks.files.wordpress.com/2013/10/20131027-191221.jpg?w=545 Oorsprong van de slide is geverifieerd door de auteur.

290 www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205-2.html.

kaanse telecom-operatoren (AT&T, Verizon en Sprint). Daar zit per definitie communicatieverkeer bij met een Belgische oorsprong of bestemming. De NSA's 'Special Source Operations' divisie controleert apparatuur die op deze punten wordt geplaatst, waardoor alle data die langs deze punten passeren, gekopieerd en gefilterd kunnen worden op basis van door de NSA ingestelde parameters.[291] De belangrijkste daarvan is een 'wettelijke' filter: alleen communicaties waarvan op zijn minst een deelnemer geen Amerikaan is, of zich niet in de VS bevindt, mogen in theorie doorgestuurd worden naar de NSA. Andere filters moeten ervoor zorgen dat alleen data met een *foreign intelligence*-waarde worden doorgestuurd naar de NSA. Programma's zoals XKEYSCORE stellen NSA-analisten in staat om deze *upstream data* te doorzoeken op basis van *strong selectors* (bijvoorbeeld een telefoonnummer, of een e-mailadres of een groep IP-adressen die toehoren aan een organisatie waarin de NSA geïnteresseerd is), *soft selectors* (zoals trefwoorden), of selectors die een bepaald type van geëncrypteerd trafiek detecteren (zoals Tor[292] of Virtual Private Network (VPN)-gebruik[293]).[294] Om deze beslissing te maken kan de NSA dus zowel naar de inhoud als naar de metadata van een communicatie kijken.[295] Informatie uit XKEYSCORE wordt dan naar tal van andere databases gestuurd. XKEYSCORE wordt in detail in paragrafen 28-31 behandeld.

21. Een gelekt document gepubliceerd door *The Washington Post* meldt dat FAIRVIEW (US-990), STORMBREW (US-983), ORANGEBLOSSOM (US-3251), en SILVERZEPHYR (US-3273) allemaal *special source operations* zijn die data verwerven van dataverkeer dat pas-

---

291 *The Wall Street Journal*: "*There are two common methods used, according to people familiar with the system. In one, a fiber-optic line is split at a junction, and traffic is copied to a processing system that interacts with the NSA's systems, sifting through information based on NSA parameters. In another, companies program their routers to do initial filtering based on metadata from Internet "packets" and send copied data along. This data flow goes to a processing system that uses NSA parameters to narrow down the data further*". http://online.wsj.com/article/SB10001424127887324108204579025222244858490.html.
En verder: "*According to a U.S. official, lawyers at telecom companies serve as checks on what the NSA receives. "The providers are independently deciding what would be responsive," the official says. Lawyers for at least one major provider have taken the view that they will provide access only to "clearly foreign" streams of data–for example, ones involving connections to ISPs in, say, Mexico, according to the person familiar with the legal process. The complexities of Internet routing mean it isn't always easy to isolate foreign traffic, but the goal is "to prevent traffic from Kansas City to San Francisco from ending up" with the NSA, the person says",* in S. GORMAN en J. VALENTINO-DEVRIES, *The Wall Street Journal*, 20 Augustus 2013 ("New Details Show Broader NSA Surveillance Reach"). Een deel van het bestaan van dit soort activiteiten werd al bekend in 2006 door AT&T klokkenluider Mark Klein (Declaration of Mark Klein in support of plaintiffs' motion for preliminary injunction. United States District Court, Northern District of California. 8 June 2006).

292 Tor is een netwerk van servers die gebruikers toelaten om anoniem te surfen. Zie hierover https://www.torproject.org/.

293 Vaak gebruikt door bedrijven om werknemers van thuis uit toegang te verschaffen – via een geëncrypteerde 'tunnel' tot het bedrijfsnetwerk.

294 www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 2.

295 Voor een technische analyse van XKeyscore zie http://arstechnica.com/information-technology/2013/08/building-a-panopticon-the-evolution-of-the-nsas-xkeyscore/.

seert door de VS, maar waarvan beide kanten niet-Amerikaans zijn.[296] Een andere gelekte slide spreekt over FAIRVIEW, STORMBREW, BLARNEY en OAKSTAR als *upstream* SIGADS.[297] Volgens *The Wall Street Journal* valt ook LITHIUM onder deze cluster.[298]

22. BLARNEY (US-984) is de SIGAD die initieel verwees naar *upstream data* die de NSA verkreeg via AT&T[299] maar lijkt later uitgebreid te zijn naar meerdere bedrijven.[300] Volgens *The Washington Post* wordt er nog altijd data uit BLARNEY verwerkt.[301] Een slide van een NSA-presentatie die te zien was in het Braziliaanse TV-programma Fantastico suggereerde dat BLARNEY zorgt voor "*collection against DNR and DNI FISA Court Order authorized communications*". DNR staat voor Dial Number Recognition, terwijl DNI staat voor Digital Network Intelligence. De slide vermeldt verder dat de hoofddoelen van BLARNEY "*diplomatic establishment, counterterrorism, counter proliferation, foreign government, economic, military en political/intention of nations*" zijn.[302] Volgens een andere slide startte BLARNEY al in 1978 om toegang te krijgen tot de communicaties van "*foreign establishments, agents of foreign powers and terrorists*".[303] *Der Spiegel* meldde eerder dat NSA-technici die voor het BLARNEY-programma werkten erin geslaagd waren om de VN's interne video teleconferentie systeem (VTC) te exploiteren.[304] Informatie uit BLARNEY werd volgens dezelfde slide verstuurd naar 'externe klanten' zoals het US Department of State, de CIA, de US UN Mission, the Joint Chiefs of Staff, Department of Homeland Security, DNI, 2nd parties to Five eyes, National Counterterorrism Center, White House, Defense Intelligence Agency, NATO, Office of Secretary of Defense en military commands (Army, EUCOM).[305] Het programma heeft veel weg van het NSA-programma dat beschreven wordt in de rechtszaak Jewel v. NSA.[306]

---

296 http://apps.washingtonpost.com/g/page/national/nsa-report-on-privacy-violations-in-the-first-quarter-of-2012/395/#document/p2/a114809.

297 www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html?wprss=rss_national *The Washington Post* had eerder de namen 'STORMBREW' en 'OAKSTAR' gecensureerd.

298 http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html.

299 S. GORMAN en J. VALENTINO-DEVRIES, *The Wall Street Journal*, 20 Augustus 2013 ("New Details Show Broader NSA Surveillance Reach").

300 Zie *The Washington Post*: "*BLARNEY's top-secret program summary describes it as "an ongoing collection program that leverages IC [intelligence community] and commercial partnerships to gain access and exploit foreign intelligence obtained from global networks*." www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_print.html.

301 *Idem*.

302 http://leaksource.files.wordpress.com/2013/09/blarney.jpg. *Der Spiegel* meldde eerder dat "*NSA technicians working for the Blarney program have managed to decrypt the UN's internal video teleconferencing (VTC) system*".

303 *Screengrab* van een segment dat werd getoond op http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html; https://pbs.twimg.com/media/BTxAU7ZIYAA3OW_.png:large.

304 www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html.

305 *Screengrab* van segment getoond op http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html; https://pbs.twimg.com/media/BTxAU7ZIYAA3OW_.png:large.

306 Zie https://www.eff.org/files/filenode/jewel/jewel.complaint.pdf Volgens ex-NSA werknemer Thomas Drake is BLARNEY "*a key access program facilitated by these commercial arrange-*

I.4. 'UPSTREAM'-VERZAMELING BUITEN DE VS

23. Informatie uit glasvezelkabels die het grondgebied van een van de secundaire partners van de VS passeren (UK, Canada, Australië en Nieuw-Zeeland) worden ook met de VS gedeeld.[307] Volgens Duncan Campbell, deelt ook het Zweedse SIGINT-agentschap 'Försvarets radioanstalt' (FRA) upstream data die het verwerft via glasvezelkabels met Five Eyes. De data die zo verkregen zou worden zou bekend staan onder de codenaam SARDINE.[308] Campbell claimt dat ook de Deense *Forsvarets Efterretningstjeneste* (Danish Defence Intelligence Service) op deze manier informatie deelt met de NSA. De data die zo verkregen zou worden, zou bekend staan onder de codenaam DYNAMO.[309] De NSA heeft ook gelijkaardige samenwerkingsverbanden met buitenlandse telecombedrijven "*vooral in Europa en het Midden Oosten*" volgens een anonieme bron in *The Wall Street Journal*.[310] Volgens Glenn Greenwald sluit de NSA geen rechtstreekse samenwerkingsverbanden af met buitenlandse bedrijven, maar gebruikt het de toegang van een groot – tot nu toe onbekend – Amerikaans telecombedrijf dat samenwerkt met dergelijke buitenlandse bedrijven. Het Amerikaanse bedrijf in kwestie heeft direct toegang tot de telecominfrastructuur van haar partner, dat daarmee – onbewust – ook toegang geeft tot de NSA. Deze info komt dan in het FAIRVIEW programma, aldus Greenwald.[311] Andere glasvezelkabels zijn voor de VS legitieme doelwitten om clandestien internet- en telefoonverkeer te onderscheppen op basis van EO 12333.

24. Via het *upstream* programma werden e-mails van Franse telecombedrijven als Alcatel – Lucent automatisch onderschept. Het is niet duidelijk of de inhoud van alle e-mails van die adressen automatisch werd bijgehouden, enkel e-mails die bepaalde trefwoorden bevatten, en/of de metadata van dat e-mailverkeer.[312] Op basis van de functies en operaties die beide bedrijven uitvoeren, lijkt het niet onmogelijk dat gelijkaardige e-mails van werknemers van BICS, Belgacom of Tecteo op eenzelfde manier onderschept werden.[313]

---

ments that exploits the Internet data at these junctions. (…) BLARNEY is to the international Internet space as PRISM is to the domestic". www.dailydot.com/news/fairview-prism-blarney-nsa-internet-spying-projects/.

307 http://apps.washingtonpost.com/g/page/world/how-the-nsa-tried-to-collect-less/518/.

308 Duncan Campbell testimony: www.youtube.com/watch?v=ZX1tmizZLpc. Dit is geen verrassing in het licht van de 'FRA-wet' die Zweden in 2008 aannam, zie http://news.bbc.co.uk/2/hi/europe/7463333.stm.

309 Duncan Campbell testimony to the Council of Europe, 1 October 2013, zie www.duncancampbell.org/PDF/CoECultureCommittee1Oct2013.pdf, 19.

310 S. GORMAN en J. VALENTINO-DEVRIES, *The Wall Street Journal*, 20 Augustus 2013 ("New Details Show Broader NSA Surveillance Reach").

311 www.theguardian.com/commentisfree/2013/jul/07/nsa-brazilians-globo-spying. Eerder noemde ex-NSA werknemer Thomas DRAKE FAIRVIEW, een *umbrella programma* waaronder veel andere programma's resorteren. www.dailydot.com/news/fairview-prism-blarney-nsa-internet-spying-projects/.

312 www.lemonde.fr/technologies/article/2013/10/21/les-services-secrets-americains-tres-interesses-par-wanadoo-et-alcatel-lucent_3499762_651865.html).

313 Alcatel Lucent levert bijvoorbeeld cruciale infrastructuur voor onderwater glasvezelkabels. Zie hierover: www.alcatel-lucent.com/solutions/submarine-networks).

25. Een van de data die de SSO-divisie van de NSA collecteert via dergelijke 'upstream verzameling' zijn miljoenen contactlijsten of adresboeken van e-mail- en chatprogramma's alsook *screenshots* van een volledige e-mail-inbox. Contactlijsten van chatprogramma's kunnen soms de inhoud van een bepaald bericht bijhouden, en in de e-mail inbox van een persoon is ook vaak de eerste lijn van het bericht te zien.[314] Een PowerPoint presentatie van de NSA stelt dat op 10 januari 2012 op één dag 444.743 adresboeken van Yahoo werden verzameld, 105.068 van Hotmail, 82857 van Facebook, 33.697 van Gmail en 22.881 van andere providers. De Amerikaanse bedrijven in kwestie hebben – naar zij zeggen – ook geen weet van de collectie van dergelijke informatie.[315] Op jaarbasis zou dit neerkomen op het verzamelen van meer dan 250 miljoen adreslijsten per jaar.

26. De NSA geeft toe dat de veel van deze adresboeken geen '*foreign intelligence value*' hebben – zeker omdat men in 22% van de gevallen niet weet wie de eigenaar is van de adreslijst.[316] Maar een analyse van die data stelt de NSA in staat om 'geheime connecties' en relaties te zien van een veel kleinere groep van '*foreign intelligence*' doelwitten. Die lijsten worden dan in verschillende NSA-databases opgeslagen zoals MARINA, MAINWAY, PINWALE en CLOUDs. Volgens een *intelligence* bron van *The Washington Post* mag een NSA-analist deze databases niet doorzoeken, of informatie hieruit niet verspreiden tenzij hij/zij kan aantonen dat er zich in deze gegevens een *valid foreign intelligence* doelwit bevindt.[317]

27. Metadata die op basis van Executive Order 12333 wordt verzameld, mag sinds november 2010 gebruikt worden om aan '*contact chaining*' te doen om relaties tussen *foreign intelligence targets* en inwoners van de Five Eyes in kaart te brengen.[318] De data mag verder aangevuld worden met *enrichment data,* data uit voornamelijk publieke en commerciële bronnen zoals passagierslijsten, Facebook profielen, bank codes, kiesregistratie lijsten, GPS data van TomTom en Amerikaanse belastingdata.[319] Aangezien het hier

---

314 http://apps.washingtonpost.com/g/page/world/the-nsas-overcollection-problem/517/.

315 Het hoge aantal Yahoo-adresboeken kan verklaard worden doordat Yahoo niet automatisch data encrypteert via *secure socket layer* (SSL) – in dit in tegenstelling tot de andere providers. Deels als antwoord op de onthullingen heeft Yahoo aangekondigd om vanaf januari 2014 ook 'SSL by default' aan te bieden. www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story_2.html.

316 http://apps.washingtonpost.com/g/page/world/an-excerpt-from-intellipedia/519/).

317 Www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story_1.html.

318 www.nytimes.com/interactive/2013/09/29/us/documents-on-nsa-efforts-to-diagram-social-networks-of-us-citizens.html.

319 *"A top-secret document titled "Better Person Centric Analysis" describes how the agency looks for 94 "entity types," including phone numbers, e-mail addresses and IP addresses. In addition, the N.S.A. correlates 164 "relationship types" to build social networks and what the agency calls "community of interest" profiles, using queries like "travelsWith, hasFather, sentForumMessage, employs. (…) A 2009 PowerPoint presentation provided more examples of data sources available in the "enrichment" process, including location-based services like GPS and TomTom, online social networks, billing records and bank codes for transactions in the United States and overseas.*" In: www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=all.

volgens de NSA louter om metadata en open bronnen gaat, is er geen toezicht van de FISC nodig om dergelijke profielen te maken.[320]

I.5. (UPSTREAM) DATA ORDENEN EN DOORZOEKEN MET XKEYSCORE

28. Een gelekte presentatie uit februari 2008 beschrijft XKEYSCORE (ook gekend als CrossKeyScore of XKS) als een *DNI exploitation system/analytic Framework*.[321] XKEYSCORE houdt gedurende drie tot vijf dagen[322] ongefilterde internet data bij ('*full take*'), en gedurende 30 dagen metadata, bij die verzameld worden van 150 SIGADS overal ter wereld.[323] Dat houdt niet alleen het verzamelen van *upstream* informatie via bijvoorbeeld onderwaterkabels in, maar ook informatie vanuit satellieten (Fornsat[324]) en vanuit diplomatieke en consulaire missies van de VS overal ter wereld (F6 sites).[325] In 2012 bevatte XKEYSCORE gedurende een periode van 30 dagen gemiddeld 41 miljard records[326] Volgens de slide laat een dergelijke *full-take* een analist onder meer toe om via metadata doelwitten te vinden die daarvoor niet gekend waren.[327] Een analist moet eerst aantonen dat hij voor 51% zeker is dat zijn zoekopdracht gaat over een buitenlands doelwit. Analisten kunnen XKEYSCORE dan doorzoeken *in real time*[328], en data doorsturen naar andere

320 *Idem*.

321 www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 2.

322 Soms kan dit soort data maar één dag bijgehouden worden: "*One document explains: "At some sites, the amount of data we receive per day (20+ terabytes) can only be stored for as little as 24 hours."* In: www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu.

323 www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 6. Volgens NSA-expert Marc AMBINDER, die al voor de Snowden documenten over XKeyscore schreef, is Xkeyscore "*not a thing that DOES collecting; it's a series of user interfaces, backend databases, servers and software that selects certain types of metadata that the NSA has ALREADY collected using other methods*." In: http://theweek.com/article/index/247684/whats-xkeyscore.

324 Volgens Duncan CAMPBELL, de man die het bestaan van GCHQ onthulde in 1976, is dit de opvolger van Echelon. Het programma bestaat nog steeds, maar boette aan belang in aangezien veel telefoondata zich nu ook verplaatsen via glasvezelkabels. Voor Duncan CAMPBELL getuigenis in het Europese Parlement, zie www.youtube.com/watch?v=ZX1tmizZLpc.

325 Xkeyscore presentatie, gelekt op www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 5. Volgens AMBINDER verwijst 'F6' technisch gezien naar het hoofdkwartier van de Special Collection Service (SCS) in Beltsville, Maryland, die informatie verzamelt uit minstens 75 F6-sites die zich vooral bevinden in landen waar het onmogelijk is om informatie naar de NSA te sturen via gewone telefoonkabels of glasvezelkabels omdat de V.S. technisch gezien niet verondersteld wordt om daar aanwezig te zijn. De NSA erkent het bestaan van de SCS niet omdat de meeste personeelsleden als State Department officials werken. Zie http://theweek.com/article/index/247684/whats-xkeyscore en http://theweek.com/article/index/247761/5-nsa-terms-you-must-know.

326 ???

327 Xkeyscore presentatie, gelekt op www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 2.

328 *Idem*. Voor meer details over dit proces (inclusief andere originele slides) zie www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu.

databases zoals PINWALE, MARINA of TRAFFICTHIEF.[329] Daar wordt die ruwe informatie gedurende een langere periode opgeslagen.

29. De voorbeelden die in de slides aangehaald worden, tonen aan dat een analist via XKEYSCORE zeer veel data kan analyseren. XKEYSCORE kan de inhoud van elke http-activiteit lezen: dus elke e-mail en elke attachment en chatconversatie[330], alle metadata van een internetcommunicatie, alle surfgeschiedenis en alle *online* zoekopdrachten die een persoon uitvoert.[331] Verder kan het ook het gebruik van een bepaalde encryptie- of VPN-technologie detecteren[332] of nagaan welke taal iemand *online* gebruikt.[333] XKEYSCORE kan ook de IP-adressen nagaan van elke persoon die een door de analist gespecificeerde website bezoekt.[334] Met XKEYSCORE kan ook nagegaan worden wie de auteur is van een document dat *online* verstuurd werd.[335] Aan de hand van 'kwetsbaarheidprofielen' die geleverd worden door de NSA's Tailored Access Operations (TAO), kan XKEYSCORE ook gebruikt worden om 'exploiteerbare machines' in een bepaald land te vinden.[336] De inhoud van opgeslagen e-mails en Facebook-chats of privéberichten kan ook binnen XKEYSCORE gelezen worden door een analist die het programma DNI PRESENTER gebruikt.[337]

30. De slides, die uit 2008 dateren, laten zien dat XKEYSCORE op dat moment nog geen Voice over Internet Protocol (VoIP)[338] kon onderscheppen, maar het verwachtte in de toekomst ook meer metadata te onderscheppen zoals *exif tags*.[339]

---

329 *Idem.*

330 Xkeyscore kan dingen opzoeken zoals "*toon me elke Excel-spreadsheet uit Irak waarin Media Access Control Addresses te vinden zijn*" (23) of, "*toon me elk word-document dat de IAEA of Osama Bin Laden vermeldt*" (26), www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation,.

331 Xkeyscore houdt alle zoekopdrachten bij, of het gebruik van bijv. Google Maps. www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 20.

332 Met XKeyscore is het bijvoorbeeld mogelijk om "*alle geëncrypteerde word-documenten uit Iran, of elk PGP-gebruik in Iran*" te tonen. www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation (16). Een analyst kan ook aan Xkeyscore vragen om het gebruik van bepaalde technologieën te detecteren, bijv. door te vragen: "*toon me alle VPN start-ups in land X, en geef me de data zodat ik de gebruikers van die service kan identificeren*". Zie: www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation (17).

333 Xkeyscore kan ook gebruikt worden om aan *language tracking* te doen, via Xkeyscore's 'http activity plugin' die html language tags bijhoudt. www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation (19).

334 *Idem.* Bijvoorbeeld: elke Belg die extremistische website X bezoekt.

335 www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 21.

336 Voor een technische analyse zie http://arstechnica.com/tech-policy/2013/08/nsas-internet-taps-can-find-systems-to-hack-track-vpns-and-word-docs/.

337 www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu.

338 Verwijst naar services zoals Skype en Apple's Facetime.

339 Xkeyscore presentatie, gelekt op www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 32. Een *exchangeable image file format* (exif) is een technische standaard die metadata van digitale camera's bijhoudt, zoals bijvoorbeeld de datum en tijd wanneer een digitale foto werd genomen.

31. De NSA erkende het bestaan van XKEYSCORE als een onderdeel van de NSA's *lawful foreign signals intelligence collection system*, maar benadrukte dat toegang tot XKEYSCORE gelimiteerd is en dat elke zoekopdracht door een analist *fully auditable* is. De NSA benadrukt dat meer dan 300 terroristen werden gevat op basis van intelligence die uit XKEYSCORE komt.[340]

I.6. PRISM: DOWNSTREAM VERZAMELING VAN SIGINT

32. Deels omdat steeds meer buitenlanders de diensten van Amerikaanse bedrijven begonnen te gebruiken, en deels omdat die bedrijven hun communicaties begonnen te encrypteren via SSL[341], besloot de NSA om met de belangrijkste van deze bedrijven een samenwerkingsverband te sluiten om gebruikersdata op een efficiënte en gestroomlijnde manier door te sturen naar de NSA.[342] Het resultaat van deze onderhandelingen was het PRISM-programma. Via PRISM kreeg de NSA – in vergelijking met de *upstream* collectie – op een gestructureerde manier *downstream* data van negen grote technologiebedrijven binnen: Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL en Apple.[343]

33. Alle PRISM-providers hebben een code gekregen. P1: Microsoft[344], P2: Yahoo, P3: Google[345], P4: Facebook, P5: PalTalk, P6: YouTube, P7: Skype[346], P8: AOL, PA: Apple.[347]

---

340 www.nsa.gov/public_info/press_room/2013/30_July_2013.shtml.

341 Een encryptieprotocol om communicatie op het internet te beveiligen.

342 C.C. MILLER, *The New York Times*, 7 june 2013 ("Tech companies concede to surveillance programme").

343 De meest volledige slideshow van PRISM werd in oktober gepubliceerd door *Le Monde*. www.lemonde.fr/technologies/article/2013/10/21/espionnage-de-la-nsa-tous-les-documents-publies-par-le-monde_3499986_651865.html.

344 *The Guardian* beschreef verder SSO documenten die aantoonden dat Microsoft en de FBI ervoor zorgden dat de NSA makkelijk de encryptie van outlook.com chats kon omzeilen. Een ander document toont aan dat de NSA toegang heeft tot e-mails van Hotmail, Windows Live en Outlook.com vooraleer die geëncrypteerd worden. www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

345 De NSA heeft hiermee toegang tot Gmail, Google voice and video chat, Google Drive files, Google's fotodienst Picasa Web, en (real time) surveillance van zoektermen die door een persoon worden ingetypt in Google. www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_3.html.

346 "*According to a separate "User's Guide for PRISM Skype Collection," that service can be monitored for audio when one end of the call is a conventional telephone and for any combination of "audio, video, chat, and file transfers" when Skype users connect by computer alone*". Zie: www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_3.html
Een ander document stelde dat "*Prism monitoring of Skype video production has roughly tripled since a new capability was added on 14 July 2012. (…) The audio portions of these sessions have been processed correctly all along, but without the accompanying video. Now, analysts will have the complete 'picture' it says.*" www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

347 De providers startten hun deelname in PRISM op verschillende tijdstippen. Microsoft: 11/09/2007, Yahoo: 12/3/2008, Google: 14/01/2009, Facebook: 3/6/2009, PalTalk: 7/12/2009,

34. Er zijn negen grote types aan content die via PRISM worden verzameld, die ook weer een codeletter hebben gekregen. A= opgeslagen communicaties (zoals privéberichten op een sociale netwerksites, chat-geschiedenis, e-mails etc.), B: Instant Messaging (chat), C: RTN-EDC (notificatie in *real time* van een login op een account of een verstuurd bericht), D: RTN-IM (notificatie in *real time* voor een chat login of logout), E: E-mail, F: VoIP (services zoals Skype, inclusief videoconferencing), G: Full (Webforum), H: OSN (Online Social Networking information – foto's, *wallposts*, activiteiten op sociale media sites …) I: OSN informatie die geleverd wordt wanneer men zich inschrijft voor een OSN-dienst. J: video's.[348]

35. Het systeem lijkt als volgt te werken: een NSA-analist kan zelf de *selectors* (e-mailadres, telefoonnummer, naam, maar ook zoektermen) invoeren in een *Unified Targeting Tool*.[349] Die *selectors* worden bekeken door een overste, die nagaat of er 51% kans is dat het om een buitenlands doelwit gaat.[350] Als de NSA opgeslagen data (bijv. e-mails in een inbox) wil consulteren, dan moet de FBI een extra check doen om te zien of er geen Amerikanen bespioneerd worden. Als de NSA in '*real-time*' surveillance wil doen, dan is die extra check niet nodig. In beide gevallen gebruikt de FBI's Data Intercept Technology Unit (DITU) materiaal (*government equipment*) om informatie over die doelwitten te verkrijgen van een van de bedrijven die meedoen aan PRISM. De FBI stuurt dat materiaal dan door naar de CIA of de NSA.[351]

36. Als er informatie over een doelwit wordt verzameld, dan betekent dat ook dat informatie kan verzameld worden over iedereen waarmee het doelwit tot in de tweede graad mee gecommuniceerd heeft. Een eenvoudig hypothetisch voorbeeld toont aan dat informatie inwinnen over een doelwit in de praktijk betekent dat data van een enorm aantal mensen potentieel kan verzameld worden. Als een doelwit gecommuniceerd heeft met 700

Youtube: 24/9/2010, Skype: 6/2/2011, AOL: 31/3/2011, Apple: oktober 2012. PRISM startte dus maar na de aanname van de Protect America Act in 2007. www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1# In April 2013 heette het dat de toevoeging van Dropbox nakende was. www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_2.html.

348 www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1#.

349 "*In another classified report obtained by The Post, the arrangement is described as allowing "collection managers [to send] content tasking instructions directly to equipment installed at company-controlled locations," rather than directly to company servers.*" Zie: www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html.

350 Merk op dat de FISC alleen de certificaten jaarlijks onderzoekt (zie para. 9), niet de individuele zoektermen.

351 "*The information the NSA collects from Prism is routinely shared with both the FBI and CIA. A 3 August 2012 newsletter describes how the NSA has recently expanded sharing with the other two agencies. The NSA, the entry reveals, has even automated the sharing of aspects of Prism, using software that "enables our partners to see which selectors [search terms] the National Security Agency has tasked to Prism". The document continues: "The FBI and CIA then can request a copy of Prism collection of any selector …*". Zie: www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

mensen via Facebook of e-mail, en die mensen hebben op hun beurt ook elk gecommuniceerd met 700 mensen, dan kan de NSA gegevens verzamelen over 490.000 mensen.[352]

37. De NSA sorteert op haar beurt de verkregen data op basis van datatype, en haalt de ze nog eens door een filter om na te gaan of geen Amerikaanse gegevens worden bekeken. DNI content[353] en video worden doorgestuurd naar de PINWALE database.[354] Metadata van '*internet records*' worden verstuurd naar MARINA[355] en metadata van telefoongesprekken naar MAINWAY.[356] Een intern NSA bulletin gaf aan dat MAINWAY in 2011 per dag metadata binnen kreeg van 700 miljoen telefoongesprekken. Vanaf augustus 2011 kwamen daar nog eens 1,1 miljard metadata van telefoongesprekken extra bij per dag.[357]

38. Op 5 april 2013 waren er 117.675 actieve surveillance doelwitten in PRISM's *counterterrorism database*.[358] Volgens de vrijgegeven slides is PRISM de SIGAD waaruit de meeste ruwe informatie komt voor alle NSA-rapporten.[359] In 2012 verscheen PRISM-data

---

352 www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1#
The Washington Post merkt verder op: "*it is true that the PRISM program is not a dragnet, exactly. From inside a company's data stream the NSA is capable of pulling out anything it likes, but under current rules the agency does not try to collect it all.*" www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_2.html
Verder: "*To collect on a suspected spy or foreign terrorist means, at minimum, that everyone in the suspect's inbox or outbox is swept in. Intelligence analysts are typically taught to chain through contacts two "hops" out from their target, which increases "incidental collection" exponentially.*" Zie: www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_3.html.

353 Zoals forum posts, chats, e-mails … of simpel gezegd: "internet content".

354 Pinwale houdt de inhoud van communicaties bij voor een periode van vijf jaar. Die informatie lijkt te komen op basis van op voorhand ingestelde *dictionary tasked terms* die het onder andere krijgt uit Xkeyscore en PRISM. www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu.

355 Marina wordt in een Xkeyscore slide beschreven als "*user activity meta-data with front end full take feeds and back-end selected feeds*". Hierover: www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu *The Guardian* quote uit een document waarin Marina verder wordt beschreven. "*The Marina metadata application tracks a user's browser experience, gathers contact information/content and develops summaries of target," the analysts' guide explains. "This tool offers the ability to export the data in a variety of formats, as well as create various charts to assist in pattern-of-life development." (…) "Of the more distinguishing features, Marina has the ability to look back on the last 365 days' worth of DNI metadata seen by the Sigint collection system, regardless whether or not it was tasked for collection.*" In: www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents.

356 www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1#.

357 www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=all.

358 Ter vergelijking: de Terrorist Identities Datamart Environment (TIDE) van de Amerikaanse overheid telde in december 2011 740.000 'records', waarbij eenzelfde persoon een aantal keer kan voorkomen wegens een foute spelling van zijn/haar naam. www.dni.gov/files/Tide_Fact_Sheet.pdf.

359 Dat wordt ook bevestigt door de FISC, zie para.19. "*According to the slides and other supporting materials obtained by The Post, "NSA reporting increasingly relies on PRISM" as its leading*

in 1.477 items van de Amerikaanse President's Daily Intelligence Brief.[360] DNI-director Clapper bevestigde het bestaan van PRISM (zonder het programma bij naam te noemen), en noemde het "*een van de belangrijkste bronnen*" van de NSA.[361]

I.7. FINANCIËLE DATA

39. Volgens documenten die *Der Spiegel* kon inzien, heeft de NSA een '*Follow the money*'-tak die internationale geldstromen – vooral in Afrika en het Midden Oosten – in de gaten houdt. Die informatie komt terecht in een database, genaamd TRACFIN, die in 2011 al 180 miljoen datasets had over banktransfers, kredietkaarttransacties en geldtransfers. Volgens *Der Spiegel* houdt de NSA dit soort data gedurende vijf jaar bij.[362]

40. Nog steeds volgens *Der Spiegel* heeft de NSA een grondige kennis van de interne processen van maatschappijen zoals Visa en Mastercard (zoals '*payment authorisation processes*' en interne geëncrypteerde communicaties[363]), en houdt het ook alternatieve betaalmethodes zoals Bitcoin in het oog. Volgens *Der Spiegel* verzamelt de NSA via het DISHFIRE-programma informatie over transacties die met kredietkaarten worden uitgevoerd van meer dan 70 banken wereldwijd – vooral in 'crisisgebieden', inclusief in landen als Italië, Spanje en Griekenland. DISHFIRE is actief sinds de lente van 2009. De transacties van Visa-klanten in Europa, het Midden Oosten en Afrika werden ook geanalyseerd om financiële associaties bloot te kunnen leggen.[364] Door deze kennis werden verschillende Arabische banken op de *blacklist* van de US Treasury geplaatst.[365]

---

source of raw material, accounting for nearly 1 in 7 intelligence reports." In: www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html.

360 www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html.

361 www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa.

362 www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html.

363 "*According to the presentation, the NSA was previously only able to decrypt payment transactions by bank customers, but now they have access to the internal encrypted communication of the company's branch offices. This "provides a new stream of financial data and potentially encrypted internal communications" from the financial service provider, the analysts concluded with satisfaction. This bank data comes from countries that are of "high interest." It's interesting to note that the targeted company is also one of the many SWIFT service partners*." In: www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430-2.html.

364 "*Furthermore, the author concluded, thanks to network analyses and the use of the XKeyscore spying program, NSA analysts had stumbled across the encrypted traffic of a large financial network operator in the Middle East*." In: www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430-2.html.

365 *"In one case, the NSA provided proof that a bank was involved in illegal arms trading -- in another case, a financial institution was providing support to an authoritarian African regime"*. In: www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html.

41. Andere documenten tonen aan dat de NSA's Tailored Access Operations (TAO) divisie sinds 2006 clandestien toegang heeft verworven tot de interne data trafiek van de Society for Worldwide Interbank Financial Telecommunication (SWIFT).[366] Dat is opmerkelijk, aangezien de VS een akkoord heeft met de EU om SWIFT-data te delen – maar dat akkoord laat niet het versturen van *bulk data* toe.[367] Na deze onthullingen stemde het Europese Parlement op 23 oktober 2013 in met de opschorting van het Terrorist Finance Tracking Program (TFTP Agreement).[368] In een statement liet Commissaris Malmström weten dat het TFTP-akkoord niet zal opgeschort worden.[369]

I.8. METADATA VAN AMERIKAANSE TELEFOONGESPREKKEN

42. In Amerika spitst het NSA-debat zich vooral toe op het verzamelen van Amerikaanse telefoondata door de NSA, onder meer op basis van de *business records* sectie 215 die door de Patriot Act geïntroduceerd werd in FISA.[370] Op basis van deze sectie kon de VS de grootste Amerikaanse telecom-operatoren verplichten om alle metadata van telefoongesprekken met een Amerikaans begin- of eindpunt ter beschikking te stellen van de NSA. Volgens de NSA kunnen deze data enkel geconsulteerd worden voor anti-terreurdoeleinden. Een consultatie kan enkele beginnen met een telefoonnummer dat eerder geassocieerd werd met een buitenlandse terroristische organisatie (*a seed*).[371]

I.9. SMARTPHONE DATA

43. Volgens *Der Spiegel* heeft de NSA de capaciteit om een grote waaier aan smartphonedata te verkrijgen van *high interest targets*.[372] De NSA had toegang tot de contactlijsten, call logs, sms-trafiek, drafts van sms'en en locatie-informatie van de mobiele platformen van Apple (IOS), Google (Android) en Blackberry.[373] De NSA heeft bijvoorbeeld toegang

---

366 www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html "*Since then, it has been possible to read the "SWIFT printer traffic from numerous banks.*"

367 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:195:0005:0014:EN:PDF.

368 European Parliament resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance (2013/2831(RSP)), zie: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0449+0+DOC+XML+V0//EN.

369 European Commission, Memo, 23 October, zie: http://europa.eu/rapid/press-release_MEMO-13-928_en.htm.

370 Zie para 6.

371 N.S.A., The National Security Agency: Missions, Authorities, Oversight and partnerships, 9 Augustus 2013, 5.

372 Zie ook para. 19.

373 "*The presentation notes that the acquisition of encrypted BES (Blackberry Services) communications requires a "sustained" operation by the NSA's Tailored Access Operation department in order to "fully prosecute your target. (.) The alleged telecommunications surveillance has been a targeted activity that was performed without the smartphone makers' knowledge.*" In: M. ROSENBACH, L. POITRAS en H. STARK, *Der Spiegel*, 9 September 2013 ("iSpy: How the NSA Accesses Smartphone Data").

tot 38 iPhone applicaties zoals het gebruik van de ingebouwde kaartfunctie, voicemail en foto's, Google Earth, Yahoo en Facebook Messenger.[374]

I.10. PNR-DATA

44. Via het Passenger Name Records (PNR) akkoord uit 2012 verkrijgt het US Department of Homeland Security (DHS) PNR-data van passagiers die van de EU naar de VS vliegen. Die data bestaat uit informatie die een passagier gegeven heeft aan de luchtvaartmaatschappij zoals de naam van de passagier en zijn eventuele medepassagiers, hun adressen en telefoonnummers, reisdata, eindbestemming, ticket informatie, de manier van betalen, credit card nummer, bagage informatie enz. De volledige lijst kan teruggevonden worden in de annex bij het akkoord.[375] DHS mag die data delen met binnenlandse diensten[376] en derde landen.[377] De data worden gebruikt ter preventie, opsporing en berechting van terroristische misdrijven en ernstige grensoverschrijdende misdaden.[378] Na zes maanden worden alle persoonlijke data gemaskeerd, en na vijf jaar worden de data in een 'slapende' database gestoken. De data mogen gedurende tien jaar gebruikt worden ter preventie van grensoverschrijdende misdaad, en vijftien jaar voor terrorisme.[379]

I.11. NSA-INSPANNINGEN TEGEN ENCRYPTIE

45. *The New York Times* publiceerde een *briefing sheet* van de NSA aan het GCHQ uit 2010 over een programma genaamd BULLRUN, waarin de NSA suggereert dat de meest gebruikte encryptie-protocollen die verantwoordelijk zijn voor de beveiliging van de wereldwijde handel, banksystemen, medische data en internet surfgedrag (zoals het zenden van e-mails, online opzoekingen, chats en online telefoongesprekken) door de NSA gekraakt of omzeild konden worden. Het gaat over TLS/SSL[380], https[381], SSH[382], VPNs[383] en geëncrypteerde chats[384] en VOIP communicaties.[385] De specifieke technische details

374 *Idem*.
375 http://register.consilium.europa.eu/pdf/en/11/st17/st17434.en11.pdf, 36.
376 *Idem*, artikel 16.
377 *Idem*, artikel 17.
378 *Idem*, artikel 4.
379 *Idem*, artikel 8.
380 Transport Layer Security/Secure sockets layer. De meest gebruikte manier om informatie te verzenden over het internet en interne servers. HTTPS is beveiligd door TLS/SSL toe te passen op een website.
381 Hypertext transfer protocol secure. Manier om financiële informatie en paswoorden veilig te versturen van een computer naar een netwerk. Sites zoals Facebook, Twitter en Gmail gebruiken vaak https 'by default'. Herkenbaar aan het slotje voor de https in de web-browser.
382 Secure Shell. De manier voor Linux en Max gebruikers om toegang te krijgen tot een computer vanop afstand.
383 Virtual Private Network. Vaak gebruikt door bedrijven om werknemers van thuis uit toegang te verschaffen – via een gencrypteerde 'tunnel' tot het bedrijfsnetwerk.
384 Een voorbeeld is het Adium programma, waarmee 'end to end' encryptie mogelijk is, waarbij de data niet kan gedecrypteerd worden op enig punt gedurende de transfer.
385 Verwijst naar services zoals Skype en Apple's Facetime.

over wat er precies werd gekraakt werden tot nu toe niet vrijgegeven.[386, 387] Het bestaan van deze decryptiemogelijkheden én het gebruik van alle geëxploiteerde data (zowel *plaintext* als metadata) die uit deze mogelijkheden voortkwamen, werden geclassificeerd als Exceptionally Controlled Information (ECI), een *level* hoger dan 'Top Secret'.[388]

46. Een budgetaanvraag uit 2012 onthulde verder het bestaan van het Sigint Enabling Project dat erop gericht is om in het geheim Amerikaanse en buitenlandse internetbedrijven te beïnvloeden het design van hun producten aan te passen zodat deze kunnen geëxploiteerd worden. Het programma omvat een hele reeks activiteiten: (1) Samenwerking met bedrijven om 'achterpoortjes' te installeren in commerciële encryptie systemen, IT-systemen, netwerken en *endpoint communication devices* die gebruikt worden door 'doelwitten'.[389] Die samenwerking kan vrijwillig zijn[390], of afgedwongen worden door FISA-dwangbevelen.[391] (2) Het beïnvloeden van technische standaarden en specificaties voor commerciële *public key technologies*, inclusief de standaard uit 2006 van het National Institute of Standards and Technology.[392] (3) Het voortzetten van de samenwerking met grote *telecommunications carriers*.[393] De meest controversiële manier is echter het clandestien stelen van encryptie-sleutels. NSA-documenten tonen aan dat de NSA een interne database heeft (de Key Provisioning Service), die de encryptiesleutels bevat van specifieke commerciële producten. Als een bepaalde sleutel niet aanwezig is, dan gaat een aanvraag naar de Key Recovery Service, waarvan beweerd wordt dat die sleutels verkrijgt door in te breken in de servers van de bedrijven die de sleutel gemaakt hebben. Om deze methode geheim te houden, zou de NSA alleen gedecrypteerde boodschappen met andere diensten delen als de sleutels verkregen werden door legale middelen.[394]

---

386 www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us Experts hebben opgemerkt dat de documenten niet tonen welke geëncrypteerde systemen de NSA gekraakt heeft door pure wiskunde, en welke door hacking of samenwerking van ontwikkelaars. Een systeem als Pretty Good Privacy (PGP) zou nog altijd werken. Voor meer info zie (de links) hierin: www.washingtonmonthly.com/political-animal-a/2013_09/the_nsa_is_mostly_not_breaking046760.php of www.newyorker.com/online/blogs/elements/2013/09/the-nsa-versus-encryption.html.

387 www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us.

388 www.theguardian.com/world/interactive/2013/sep/05/nsa-classification-guide-cryptanalysis.

389 www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=1&hp&&pagewanted=all.

390 "*In one case, after the government learned that a foreign intelligence target had ordered new computer hardware, the American manufacturer agreed to insert a back door into the product before it was shipped, someone familiar with the request told The Times*." In: www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=1&hp&&pagewanted=all.

391 www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=1&hp&&pagewanted=all.

392 *Idem*.

393 www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us.

394 www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=1&hp&&pagewanted=all.

47. Op 4 oktober 2013 onthulden *The Guardian* en *The Washington Post* hoe de NSA sinds 2006 probeerde om gebruikers van het Tor-netwerk te identificeren en te bespioneren.[395] Tor is een netwerk van servers die gebruikers toelaten om anoniem te surfen.[396] Gebruikers kunnen dat netwerk via speciale, complexe software gebruiken, maar een alternatieve, gemakkelijkere manier om Tor te gebruiken is het downloaden van de Tor Browser Bundle (TBB) – een versie van Firefox die automatisch data verzendt over het Tor-netwerk. Uit de documenten blijkt dat de NSA in 2007 TBB-gebruikers kon onderscheiden van gewone Firefox gebruikers[397], maar dat het er in 2007 nog niet in geslaagd was om het Tor-netwerk zelf te hacken. Een NSA-presentatie uit juni 2012 stelt dat de NSA nooit in staat zal zijn om alle Tor-gebruikers tegelijkertijd te de-anonimiseren, en dat de NSA ook geen technieken heeft die toestaan om een specifieke gebruiker op verzoek te de-anonimiseren. Door manuele analyse is het echter mogelijk om een 'zeer kleine fractie' van Tor gebruikers te de-anonimiseren.[398] Slides van de NSA's Tailored Access Operations (TAO) beschrijven hoe de NSA Javascript-kwetsbaarheden in Firefox exploiteerde via de programma's EGOTISTICALGOAT en EGOTISTICALGIRAFFE.[399] Deze kwetsbaarheden zouden verdwenen zijn met de meest recente *update* van Firefox in januari 2013[400], maar het is onduidelijk of de NSA dit intussen al omzeild heeft.[401]

48. Onder de codenaam Quantum plaatste de NSA geheime Quantum-servers op belangrijke plaatsen van de infrastructuur van het internet, waardoor de NSA een *man in the middle* aanval kon uitvoeren op Tor-gebruikers.[402] Dit betekent dat deze servers sneller kunnen reageren dan andere websites, waardoor ze de gebruiker naar een geïnfecteerde imitatie van de gevraagde website kunnen sturen die op een FoxAcid-server staat. De servers in dit FoxAcid-systeem worden gerund door TAO, en kunnen op verschillende manieren computers voor lange periodes besmetten.[403] Het bezoek van de homepage van

---

395 *The Washington Post* plaatste een document uit 2006 van 49 pagina's online dat beschrijft welke methodes potentieel de grootschalige de-anonymisatie van Tor gebruikers zouden toelaten. In: http://apps.washingtonpost.com/g/page/world/nsa-research-report-on-the-tor-encryption-program/501/. James Clapper statement op de onthullingen: http://icontherecord.tumblr.com/post/63103784923/dni-statement-why-the-intelligence-community.

396 www.washingtonpost.com/blogs/the-switch/wp/2013/10/04/everything-you-need-to-know-about-the-nsa-and-tor-in-one-faq/.

397 http://apps.washingtonpost.com/g/page/world/nsa-slideshow-on-the-tor-problem/499/#document/p5/a124608.

398 www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document?utm_source=hootsuite&utm_campaign=hootsuite.

399 www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document.

400 www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.

401 "*In anticipation of a new release of Firefox, one agency official wrote in January that a new exploit was under development: "I'm confident we can have it ready when they release something new, or very soon after:)."*
In: www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story_2.html.

402 B. SCHNEIER: "*More specifically, they are examples of "man-on-the-side" attacks*". www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.

403 *"After identifying an individual Tor user on the internet, the NSA uses its network of secret internet servers to redirect those users to another set of secret internet servers, with the codename FoxAcid, to infect the user's computer. FoxAcid is an NSA system designed to act as a matchma-*

een FoxAcid-server zou niet direct tot besmetting leiden; daarvoor is een door TAO gecreeerde specifieke URL voor nodig. Die URL zou de FoxAcid server in staat stellen om precies te weten welk doelwit de FoxAcid server bezoekt.[404] FoxAcid is een algemeen CNE-systeem dat gebruikt wordt voor verschillende digitale aanvalsvormen. Het wordt dus voor veel meer gebruikt dan om Tor-gebruikers te identificeren. Documenten uit *Der Spiegel* suggereren bijvoorbeeld dat de Belgacom-aanval (deels) via Quantumservers zou uitgevoerd zijn.[405]

II. HET BRITSE GOVERNMENT COMMUNICATIONS HEADQUARTERS (GQHQ)

II.1. HET BRITSE WETTELIJKE KADER VOOR HET INZAMELEN VAN INFORMATIE OVER BUITENLANDSE

Doelwitten

49. De Intelligence Services Act uit 1994 zette voor het eerst de functies uit van het Government Communications Headquarters (GCHQ). Het Britse SIGINT-agentschap heeft onder meer als mandaat om "*elektromagnetische, akoestische en andere emissies, alsook ieder toestel dat zulke emissies produceert*" te monitoren of te storen.[406] Het agentschap moet informatie over die emissies doorsturen naar het Britse leger, de regering en andere diensten[407] als dat nodig is voor de nationale veiligheid van de UK (waarbij specifiek verwezen wordt naar de defensie- en buitenlandse politiek van de UK), het economische welzijn van de UK (met betrekking tot de handelingen en intenties van personen buiten de Britse eilanden) en ter ondersteuning van de preventie en het opsporen van ernstige misdaden.[408]

50. De UK heeft geen specifieke wetgeving die exclusief het gebruik van *foreign intelligence* reguleert, maar de Regulation of Investigatory Powers Act (RIPA) maakt een onderscheid tussen 'interne' en 'externe' surveillance, waarbij die laatste categorie refereert naar surveillance van communicaties waarvan op zijn minst een uiteinde buiten de UK ligt.[409] In deze gevallen moet GCHQ geen bevelschrift aanvragen op naam van een specifieke

---

ker between potential targets and attacks developed by the NSA, giving the agency opportunity to launch prepared attacks against their systems. Once the computer is successfully attacked, it secretly calls back to a FoxAcid server, which then performs additional attacks on the target computer to ensure that it remains compromised long-term, and continues to provide eavesdropping information back to the NSA". In: www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.

404 *Idem.*

405 *Idem.*

406 Intelligence Services Act 1994, Chapter 13, s3, (1)(a).

407 Intelligence Services Act 1994, Chapter 13, s3, (1)(b).

408 Intelligence Services Act 1994, Chapter 13, s3, (2).

409 RIPA, s20.

persoon of een specifieke locatie[410], maar kan het een bevelschrift vragen om bijvoorbeeld data van een externe communicatielink te onderscheppen, zoals bijvoorbeeld een specifieke glasvezelkabel die tussen de UK en het Europese vasteland loopt.[411] Ter illustratie, alle glasvezelkabels die aan land komen in België zijn verbonden met een landingspunt in de UK. De Tangerine-kabel verbindt Broadstairs met Oostende; Concerto verbindt Zeebrugge met Sizewell en Thorpeness en de Pan-European Crossing verbindt Bredene met Dumpton Gap. De grote SeaMeWe-3 kabel, waarvan Belgacom deels eigenaar is, verbindt Oostende met Goonhilly Downs in de UK, maar heeft ook landingspunten in Saudi Arabië, Maleisië en China.

51. Een dergelijk breed bevelschrift wordt dan uitgevaardigd door de Secretary of State, die in een 'certificaat' beschrijft welk materiaal precies noodzakelijk is om onderzocht te worden[412] in het belang van de UK's nationale veiligheid, om ernstige misdaden te voorkomen of op te sporen of om het economische welzijn van de UK veilig te stellen.[413] De inhoud van de certificaten is geheim, maar volgens documenten die *The Guardian* heeft ingezien, zijn deze heel breed geformuleerd, en laten deze toe om materiaal te onderscheppen over wijde thema's zoals de politieke intenties van buitenlandse overheden, de militaire toestand van andere landen, terrorisme, internationale drugshandel en fraude. Volgens *The Guardian* zijn er minstens tien van die certificaten.[414] Volgens RIPA is zo'n bevelschrift initieel drie maanden geldig[415], maar het bevelschrift kan elke zes maand hernieuwd worden.[416] Telecombedrijven kunnen verplicht worden om mee te werken met de interceptie van deze communicaties.[417]

---

410 RIPA, s.8.4. Interceptie wordt als volgt gedefinieerd in s.2.2: "*A person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he- (a) so modifies or interferes with the system, or its operation, (b) so monitors transmissions made by means of the system, or (c) monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system, as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.*"

411 "*Lawyers at GCHQ speak of having 10 basic certificates, including a "global" one that covers the agency's support station at Bude in Cornwall, Menwith Hill in North Yorkshire, and Cyprus. Other certificates have been used for "special source accesses" – a reference, perhaps, to the cables carrying web traffic. All certificates have to be renewed by the foreign secretary every six months.*" In: www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world.

412 RIPA, s8.4(b).

413 RIPA s.5(3)a-c. *The Guardian* quote een GCHQ document als volgt: "*The certificate is issued with the warrant and signed by the secretary of state and sets out [the] class of work we can do under it … cannot list numbers or individuals as this would be an infinite list which we couldn't manage.*" In: www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world.

414 *The Guardian* quote een interne GCHQ memo uit oktober 2011: *"[Our] targets boil down to diplomatic/military/commercial targets/terrorists/organised criminals and e-crime/cyber actors*". In: www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet.

415 RIPA, s9.6.c.

416 RIPA s9.6.b. Voor meer informatie over s(8)4 warrants, zie: UK Home Office, Interception of Communications Code of Practice. TSO, London, 22-27, op https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97956/interception-comms-code-practice.pdf.

417 RIPA, s.12.

52. Het moet opgemerkt worden dat het niet duidelijk is wat er precies in het bevelschrift en het certificaat moet staan. Onder meer hierover is de wet onduidelijk. Het Intelligence Security Committee (ISC), dat toezicht houdt over GCHQ, heeft aangekondigd dat "*meer gedetailleerde beleidslijnen en procedures in het leven zijn geroepen zodat GCHQ de Human Rigts Act van 1998 naleeft*". De ISC gaat nu onderzoek doen naar de 'complexe interactie tussen de ISA, de Human Rights Act en RIPA en de procedures die dit regelen.[418]

53. De wet staat GCHQ ook toe om vanop afstand in te breken in computersystemen om op die manier data te verkrijgen.[419] Op basis van sectie 7 ISA is iedere actie van GCHQ buiten de UK vrijgesteld van burgerlijke of strafrechtelijke aansprakelijkheid indien deze gebeurt op basis van een machtiging van de Secretary of State.

II.2. AARD EN SCHAAL VAN DE BRITSE GEGEVENS-INZAMELING

54. Volgens *The Guardian* startte GCHQ begin 2007 met de voorbereidingen voor het Mastering the Internet (MTI) project in de basis in Bude.[420] Het doel was om buitenlandse *upstream* data te verzamelen door *deep packet inspection* materiaal te plaatsen op de onderwaterkabels wanneer die de Britse kust raakte.[421] In mei 2009 berichtten *The Register* en *The Sunday Times* dat de financiering van MTI was goedgekeurd in oktober 2007. Meer dan één miljard pond zou de komende drie jaar uitgetrokken worden om die *upstream* collectie mogelijk te maken.[422] GCHQ erkende het bestaan van MTI, maar benadrukte dat het geen technologie aan ontwikkelen was die het mogelijk zou maken om al het Internet- en telefoongebruik *in de UK* te monitoren.[423]

55. Op een onbekend moment tussen 2010 en 2011 slaagde GCHQ in haar opzet, en begon het de uitbaters van de commerciële glasvezelkabels via een bevelschrift te verplichten om mee te werken als *intercept partners*. Dit afgedwongen samenwerkingsproces wordt '*special source exploitation*' genoemd, en de '*intercept partners*' worden vergoed

---

418 Intelligence and Security Committee of Parliament, Statement on GCHQ's alleged interception of communications under the US PRISM Programme. 17 juli 2013, zie: http://isc.independent.gov.uk/news-archive/17july2013.

419 Zie Computer Misuse Act 1990, s.10; RIPA, s32 en ISA, s.5.

420 Naast MTI is er ook een programma dat Global Telecoms Exploitation heet, maar het is niet duidelijk wat daarmee bedoeld wordt. Zie: www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

421 www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet. Een eerste experimenteel project om dat te bereiken stond bekend als het Cheltenham Processing Centre (CPC). Vanaf maart 2010 werd naar dit project als een gezamenlijk GCHQ/NSA-initiatief verwezen genaamd TINT.

422 Volgens die berichten zouden Lockheed Martin en Detica meehelpen om MTI te ontwikkelen. Sinds 2008 werden inderdaad jobadvertenties aangeboden die te maken hadden met het MTI-contract www.theregister.co.uk/2009/05/03/gchq_mti/; www.timesonline.co.uk/tol/news/politics/article6211101.ece.

423 (Eigen nadruk) www.telegraph.co.uk/technology/news/5271796/Government-not-planning-to-monitor-all-web-use.html.

voor de kosten die dit meebrengt.[424] De namen van de samenwerkende bedrijven werden later bekend gemaakt door de *Suddeütsche Zeitung*. Ze stonden alle zeven bekend onder een andere codenaam: BT (Remedy), Verizon Business (Dacron), Vodafone Cable (Gerontic), Global Crossing (Pinnage), Level 3 (Little), Viatel (Vitreous) en Interoute (Streetcar).[425] De glasvezelkabel die aankomen in België (zie para. 50) worden allen uitgebaat door een van deze bedrijven.

56. Die *upstream* informatie wordt via het TEMPORA-programma eerst gefilterd om internet trafiek dat veel volume inneemt (zoals downloads van films of muziek) uit te sluiten, waardoor het volume met ongeveer 30% daalt.[426] De overblijvende *upstream*-informatie wordt gefilterd op basis van 'harde selectors' (zoals telefoonnummers en e-mailadressen) en 'zachte selectors' (zoals zoektermen). Volgens *The Guardian* werden 40.000 van deze selectors gekozen door GCHQ en 31.000 door de NSA.[427] Die baseren zich op de brede certificaten om die *selectors* zelf te kiezen. De ongefilterde data wordt weggesmeten, en de metadata die overblijft wordt bijgehouden gedurende dertig dagen en inhoud gedurende drie dagen.[428] Een bron van *The Guardian* lijkt te suggereren dat alle 'gefilterde' data gelogd worden en ingezien kan worden door de UK's Interception Commissioner, maar het is onduidelijk of dit gaat over alle informatie die wordt opgeslagen na de *selector*-filtering, of alleen die data die effectief gebruikt wordt.[429] Deze data kan dan – onder andere – retroactief onderzocht worden op zoek naar verdachten die nog niet bekend waren bij de Britse of Amerikaanse inlichtingendiensten.[430]

57. Voor het overige kan alle *upstream*-informatie verzameld worden die ook door de NSA verzameld wordt via haar *upstream*collectie (zie para 29): inhoud van e-mails, browsergeschiedenis, Facebook-berichten, documenten die als attachment werden toegevoegd etc. Hier moet opgemerkt worden dat analisten ook kunnen beslissen om alle metadata en inhoud van de contacten van een doelwit te verzamelen als zij dat proportioneel achten.[431] Minstens 300 GCHQ-analisten en 250 NSA-analisten hebben directe toegang tot de data van TEMPORA.[432] Veel metadata wordt ook opgeslagen door de NSA.[433] In februari 2011 meldde de NSA in een document dat GCHQ nu "*meer metadata verwerkte*" dan de NSA.[434] In 2012 kon GCHQ 600 miljoen 'telefoon events' per dag verwerken, tapte het 200 glasvezelkabels af en was het in staat om van 46 van die kabels tegelijkertijd data te verwerken. *The Guardian* schatte dat GCHQ daarmee in theorie toegang heeft tot 21,6 petabytes per

---

424 www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
425 www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq.
426 www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
427 *Idem*.
428 www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work Het is interessant dat GCHQ in bepaalde gevallen zelfs paswoorden als metadata beschouwd.
429 www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
430 www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work.
431 "*If analysts believe it is proportional, they can look at all the traffic – content and metadata – relating to all of the target's contact.*" In: www.theguardian.com/uk/2013/jun/23/mi5-feared-gchq-went-too-far.
432 www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet.
433 www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.
434 www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet.

dag – 192 keer de inhoud van alle boeken de zich in de British Library of Congress bevinden.[435]

II.3. DE MALWARE BIJ BELGACOM

58. Op 21 juni 2013 vindt Belgacom *malware* op haar intern computersysteem. Nadat hulp van onder meer toeleveranciers Microsoft en HP geen soelaas brachten, wordt op 25 juni de Nederlandse firma Fox-IT ingehuurd om naar de malware te kijken.[436] Na verder onderzoek van Fox-IT dient Belgacom vervolgens op 19 juli 2013 een klacht in tegen onbekenden bij het federale parket wegens frauduleuze toegang tot zijn interne computersystemen. Dat onderzoek wordt geleid door de gerechtelijke politie van Brussel (Regional Computer Crime Unit) met de (technische) steun van de Federal Computer Crime Unit (FCCU) en Algemene Dienst inlichting en veiligheid (ADIV).[437] De voorzitter van de Privacycommissie besluit in september om in samenwerking met Belgacom en het Belgisch Instituut voor Postdiensten en Telecommunicatie (BIPT), een apart onderzoek in te stellen naar wat er precies is gebeurd. Belgacom communiceert in een persbericht op 16 september 2013 dat in het weekend van 14 en 15 september "*een onbekend virus*" verwijderd werd. Volgens Belgacoms is er "*tot dusver geen enkele aanwijzing van impact op de klanten of hun gegevens*".[438] De kostprijs van de schoonmaakoperatie wordt tot dan op vijf miljoen euro geschat.[439]

59. Volgens een persbericht van het parket wijst de aanval, gezien "*de inzet van belangrijke financiële en logistieke middelen door de inbreker*" en "*de technische complexiteit ervan*" in de richting van "*state-sponsored cyberspionage gericht op het verzamelen van strategische informatie*".[440] Later bevestigt Belgacom dat 124 van de 26.600 apparaten[441]

---

435 www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa?CMP=twt_fd *The Guardian* meldt verder: "*The system seems to operate by allowing GCHQ to survey internet traffic flowing through different cables at regular intervals, and then automatically detecting which are most interesting, and harvesting the information from those. The documents suggest GCHQ was able to survey about 1,500 of the 1,600 or so high-capacity cables in and out of the UK at any one time, and aspired to harvest information from 400 or so at once – a quarter of all traffic. As of last year, the agency had gone halfway, attaching probes to 200 fibre-optic cables, each with a capacity of 10 gigabits per second. In theory, that gave GCHQ access to a flow of 21.6 petabytes in a day, equivalent to 192 times the British Library's entire book collection*". In: www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work.

436 Belgacom GCHQ Affair – EP/LIBE hearing on surveillance 3 October 2013. Zie: www.youtube.com/watch?v=ayR6CAuNE4w.

437 M. EECKHAUT en P. DE LOBEL, *De Standaard*, 17 September 2013 ("Natuurlijk zat de NSA hier achter").

438 Belgacom, Belgacom onderneemt actie in het kader van haar IT-beveiliging. 16 september 2013. Zie www.belgacom.com/be-nl/newsdetail/ND_20130916_Belgacom.page.

439 P. DE LOBEL en N. VANHECKE, *De Standaard*, 21 September 2013 ("Op het randje van de catastrofe").

440 M. EECKHAUT en P. DE LOBEL, *De Standaard*, 17 September 2013 ("Natuurlijk zat de NSA hier achter").

441 Belgacom GCHQ Affair – EP/LIBE hearing on surveillance 3 October 2013. Zie: www.youtube.com/watch?v=ayR6CAuNE4w.

die aangesloten zijn op het interne Windows-systeem van Belgacom werden gecompromitteerd[442] door wat experts een *advanced persistent threat* noemen.[443] De omschrijving van de symptomen van de *malware*, valt onder het geheim van het gerechtelijk onderzoek, maar de FCCU heeft de *malware* in de mate van het mogelijke vrijgeven zodat andere (Belgische en Europese) instellingen na kunnen gaan of ze zijn besmet. Informatie is onder meer gedeeld met het permanente Computer Emergency Response Team (CERT-EU) van de EU.

60. *De Standaard* meldt op basis van "*bronnen dicht bij het dossier*" en "*in kringen van de veiligheidsdiensten*" dat de NSA achter de aanval zit, en dat de NSA het in het bijzonder gemunt had op de activiteiten van Belgacom International Carrier Services (BICS), een dochteronderneming van Belgacom.[444] Belgacom heeft 57,6% van BICS in handen, Swisscom 22,4% en het Zuid-Afrikaanse MTN 20%. BICS levert diensten aan verschillende telecomoperatoren in verschillende landen, en baat onder meer – samen met een groep andere bedrijven – de TAT-14, SEA-ME-WE3 en SEA-ME-WE4 onderwater-glasvezelkabels uit (zie ook para. 50). Op die manier zou bijv. telefoon- en internetverkeer vanuit Syrië, Yemen en Afghanistan onderschept kunnen worden. Dat was een van de redenen achter de aanval die door *De Standaard* werd aangehaald in haar eerste berichtgeving.[445] In een mededeling zegt BICS op 16 september 2013 dat er geen enkele aanwijzing is "*dat ons telecomnetwerk, langs waar ons communicatieverkeer loopt, door spionageoperaties werd getroffen. Het is ons intern informaticasysteem dat geïntegreerd is met dat van Belgacom dat gehackt werd*".[446]

61. Op 20 september 2013 publiceerde *Der Spiegel* ongedateerde slides uit de Snowden-documenten waarin GCHQ's 'Network Analyses Centre' vertelt over de successen die behaald werden in 'Operation Socialist'. Belgacom stond in de operatie bekend onder de naam Merion Zeta. In deze operatie lijkt het erop dat werknemers die sleutelposities bezetten bij BICS via door de NSA-gecontroleerde Quantum-servers naar een andere NSA-gecontroleerde server werden geleid (Fox Acid server), waarbij die laatste op hun beurt een kwetsbaarheid in de browser van het doelwit gebruikte om *malware* op de computer van het slachtoffer te installeren. (zie ook para 48). Het ultieme doel van 'Operation Socialist' was volgens de slides van *Der Spiegel* om Belgacom's core GRX router te exploiteren om van daar *man in the middle* aanvallen te kunnen uitvoeren op doelwitten die met hun smartphone aan het *roamen* zijn.[447] Volgens de slides was GCHQ erg dicht bij dit

442 X., *De Standaard*, 16 september 2013 ("Bellens: 'Geen aanwijzing dat Belgacomklanten zijn getroffen'").

443 DOD, *De Standaard*, 17 september 2013 ("Zeg nooit 'virus' tegen advanced persistent attack"). www.standaard.be/cnt/dmf20130916_00745157. Voor meer informatie, zie bijvoorbeeld https://www.damballa.com/knowledge/advanced-persistent-threats.php.

444 M. EECKHAUT, P. DE LOBEL, N. VANHECKE, *De Standaard*, 16 september 2013 ("NSA verdacht van hacken Belgacom").

445 M. EECKHAUT en P. DE LOBEL, *De Standaard*, 17 September 2013 ("Natuurlijk zat de NSA hier achter").

446 G. QUOISTIAUX, *Trends*, 16 september 2013 ("BICS, succesvolle dochter van Belgacom en doelwit NSA").

447 www.spiegel.de/fotostrecke/photo-gallery-operation-socialist-fotostrecke-101663.html. Voor een meer technische achtergrond; zie https://www.troopers.de/wp-content/uploads/2011/10/TR12_TelcoSecDay_Langlois_Attacking_GRX.pdf.

doel.[448] BICS heeft wereldfaam in het aanbieden van 3GRX-diensten, die een lokale telefoonoperator onder meer moet toelaten aan haar klanten om te *roamen* in meer dan 190 landen.[449] De VPN-verbindingen van BICS en MyBICS, de online toepassing waarlangs het contact met klanten verloopt, werden ook als interessante doelwitten gezien.

62. Na de onthullingen in *Der Spiegel* citeerde *De Standaard* bronnen dicht bij het gerechtelijk onderzoek die op basis van "*de handtekening van de malware*" en "*vooral de plaats waar de sporen heen leiden*" nog steeds overtuigd zijn dat de aanval uit de VS komt. Volgens de speurders is Amerika de belangrijkste bestemming, en leiden er slechts "*in zeer beperkte mate*" sporen naar het Verenigd Koninkrijk.[450] Op vraag van Premier Di Rupo heeft de Belgische Veiligheid van de Staat nu officieel haar Britse tegenhanger om uitleg gevraagd.[451]

63. Op basis van 'verschillende bronnen' meldt de Nederlandse zender NOS op 3 oktober dat eind 2011 "*een team van GCHQ (…) het hart van Belgacom aan heeft gevallen*" via *named pipes*, een geavanceerde manier om vrijwel onzichtbaar communicatie te versturen over een netwerk. Volgens de NOS "*bevestigen loggegevens dat het om Engeland gaat: tijdens Engelse feestdagen en lunchtijd is er duidelijk minder spionageactiviteit*".[452] De NOS beweert dat "*nadat het netwerk gekraakt werd*", de Britten "*bijna onbeperkte toegang hadden tot het Belgacom netwerk*".[453] Eerder vertelde een andere bron aan *De Standaard* dat degene die dit deed, alles kon "*wat de hoogst geplaatste netwerkbeheerder bij Belgacom kon* (…) *Het had alle sleutels, alle paswoorden en de volledige controle*".[454] De NOS beweert ook dat "*een ander team*" vervolgens op zoek ging naar "*specifieke informatie*". De informatie werd vervolgens gedeeld met de NSA.[455] Volgens "*bronnen bij het onderzoek*" hebben de verantwoordelijken "*een beetje overal zitten rondkijken en gepakt wat ze konden*".[456] Volgens *De Standaard* levert BICS diensten waar tal van belangrijke klanten gebruik van maken: Swift, Electrabel, bpost, Belgocontrol, de Navo in Evere, de Europese Commissie en het Europese Parlement in Brussel en Straatsburg, het Supreme Headquarters Allied Powers Europe (SHAPE) in Bergen, maar ook bijvoorbeeld het hoofdkwartier van de Allied Air Command van de Navo in Ramstein.[457] Tijdens een hoorzitting in het Europees Parlement ontkenden twee topmannen van Belgacom dat de Britse geheime dienst toegang zou hebben gehad tot telefoonnetwerken van Europese instellingen. Volgens Bel-

---

448 www.spiegel.de/fotostrecke/photo-gallery-operation-socialist-fotostrecke-101663-3.html.

449 www.bics.com/sites/default/files/mosaic/3GRX_web.pdf.

450 N. VANHECKE, *De Standaard*, 21 september 2013 ("Operatie socialist: succes!").

451 K. VAN DE PERRE, *De Morgen*, 4 oktober 2013 ("België vraag uitleg aan Britten over Belgacom-hacking").

452 http://nos.nl/artikel/558286-hoe-belgacom-werd-gekraakt.html.

453 NOS Journaal, 3 oktober 2013, 20u CET. Zie http://nos.nl/uitzendingen/12720-nos-journaal-3-oktober-2013-2000u.html.

454 P. DE LOBEL en N. VANHECKE, *De Standaard*, 21 September 2013 ("Op het randje van de catastrofe").

455 NOS Journaal, 3 oktober 2013, 20u CET, zie http://nos.nl/uitzendingen/12720-nos-journaal-3-oktober-2013-2000u.html.

456 P. DE LOBEL en N. VANHECKE, *De Standaard*, 21 September 2013 ("Op het randje van de catastrofe").

457 *Idem*.

gacom is er via hun systeem "*geen overflow geweest naar systemen van klanten. Dus ook niet naar systemen van de Europese instanties*".[458]

64. Het is echter op dit moment onmogelijk om met zekerheid te zeggen welke data er precies onderschept werden. Zowel Belgacom[459], de FCCU[460], als Frank Robben[461], co-rapporteur van het Belgacom-rapport van de Privacycommissie, hebben verklaard dat het virus zelf encryptietechnieken gebruikte om te verhullen welke gegevens er precies gecompromitteerd werden. Volgens de NOS is het "*niet meer te achterhalen wie er precies is afgeluisterd en welke informatie er precies is verkregen. Om daar achter te komen, was meer tijd nodig geweest. Maar dat kon niet, omdat Belgacom het netwerk zo snel mogelijk weer operationeel wilde hebben*".[462] Het is ook onduidelijk hoe lang het virus al aanwezig was. Op een persconferentie van 16 september 2013 zegt het hoofd van Belgacom dat "*hij geen enkel idee heeft*" van wanneer het virus zich op Belgacoms netwerk bevindt. Volgens *Der Spiegel* blijkt uit een (tot nu toe ongepubliceerd) document dat toegang mogelijk was sinds 2010.[463] Volgens *De Standaard* en de *NOS* was het virus al aanwezig sinds 2011.[464]

65. Op 18 oktober 2013 meldt Belgacom dat doorgedreven controles nieuwe onregelmatigheden aan het licht brachten op een router bij BICS. "*Het eerste onderzoek wijst erop dat er wijzigingen zijn aangebracht in de software van de router, wat gebeurd kan zijn tijdens de recente digitale inbraak*".[465] Belgacom sloot niet meer uit dat gegevens van klanten zijn gehackt. "*Het lopende onderzoek zal moeten uitwijzen of er impact is geweest op de gegevens van klanten*", aldus Belgacom in *Le Soir*.[466] Op 23 oktober bericht Belga dat ook Tecteo het slachtoffer is geworden van een cyberaanval die gelijkaardig lijkt te zijn aan die op telecomoperatoren Belgacom, France-Telecom en Wanadoo. Dat zegt het bedrijf. Het is momenteel nog te vroeg om te zeggen of er informatie is gehackt bij de groep of bij de filialen VOO of RESA.[467]

II.4. BRITSE INSPANNINGEN TEGEN ENCRYPTIE

66. De Britse tegenhanger van het BULLRUN-programma (zie para 45) werd EDGEHILL genoemd. Documenten die *The Guardian* kon inkijken suggereren dat de UK nog niet zo ver staat als de VS en slechts op een *case-by-case* basis informatie kon decrypteren.

---

458 http://nos.nl/artikel/558285-spionage-belgacom-omvangrijker.html.

459 Belgacom GCHQ Affair – EP/LIBE hearing on surveillance 3 October 2013. Zie www.youtube.com/watch?v=ayR6CAuNE4w.

460 N. VANHECKE, *De Standaard*, 20 september 2013 ("Info over malware Belgacom verspreid").

461 Belgacom GCHQ Affair – EP/LIBE hearing on surveillance 3 October 2013, verkrijgbaar op www.youtube.com/watch?v=ayR6CAuNE4w.

462 http://nos.nl/artikel/558286-hoe-belgacom-werd-gekraakt.html.

463 www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html.

464 M. EECKHAUT, P. DE LOBEL, N. VANHECKE, *De Standaard*, 16 september 2013 ("NSA verdacht van hacken Belgacom").

465 www.belgacom.com/be-nl/newsdetail/ND_20131017_Belgacom.page.

466 X., Belga, 19 oktober 2013 ("Belgacom sluit hacking gegevens klanten niet meer uit").

467 X., *Belga*, 23 oktober 2013 ("Ook Tecteo slachtoffer van spionage").

Het oorspronkelijke doel van EDGEHILL was om de geëncrypteerde internettrafiek van drie grote internetbedrijven te ontcijferen en 30 VPN-types. Tegen 2015 hoopte GCHQ de geëncrypteerde internettraffiek van 15 grote internetbedrijven ontcijferd te hebben, en 300 VPN-types.[468] Een ander programma, genaamd CHEESY NAME, was erop gericht om bepaalde encryptiesleutels (bekend als *certificates*) te kraken met behulp van GCHQ 'supercomputers'.[469] GCHQ richtte ook een *Humint Operations Team* (HOT) op dat verantwoordelijk is voor het identificeren, rekruteren en runnen van informanten (*covert agents*) in the globale telecom industrie, onder andere om zo toegang te krijgen tot bepaalde sleutels.[470]

67. Documenten die in een programma van Fantastico werden getoond, suggereren dat GCHQ's *network exploitation unit* programma's gebruikten (FLYING PIG en HUSH PUPPY) die TLS/SSL netwerken konden monitoren. De programma's lijken te zijn opgestart omdat steeds meer e-mailproviders zoals Yahoo, Google of Hotmail, SSL-encryptie gebruikten waardoor die berichten niet meer leesbaar waren via de directe *upstream* collectie. Minstens één document toont dat zowel de NSA als GCHQ hun toevlucht zochten tot *man in the middle attacks* om de encryptie te omzeilen.[471] FLYING PIG lijkt ook informatie te kunnen tonen over het gebruik van Tor (Tor Events).[472]

68. Een document van 10 oktober 2012 beschrijft hoe GCHQ in operatie MULLENIZE erin geslaagd is via *user agent staining* individuele gebruikers te herkennen op een IP-adres dat simultaan gebruikt wordt door veel gebruikers. Dat is bijvoorbeeld het geval in een internet café, maar ook in bepaalde regio's gebruiken duizenden gebruikers ook één IP-adres. De techniek staat ook toe om individuele Tor-gebruikers te herkennen. In een periode van twee maanden slaagde GCHQ er in om op deze manier ongeveer 200 computers te besmetten met unieke *stains*.[473]

---

468 "*GCHQ's phrasing of beating "30" then "300" VPNs suggest it's done on a case-by-case basis, rather than a blanket capability. It's also worth noting that just because the NSA can, say, beat SSL in some (or many, or most) cases, it doesn't mean they can do it all the time, especially as they often seem to circumvent rather than directly beat security.*" In: www.theguardian.com/commentisfree/2013/sep/06/nsa-surveillance-revelations-encryption-expert-chat. *The Guardian* meldt ook het volgende: "*Analysts on the Edgehill project were working on ways into the networks of major webmail providers as part of the decryption project. A quarterly update from 2012 notes the project's team "continue to work on understanding" the big four communication providers, named in the document as Hotmail, Google, Yahoo and Facebook, adding "work has predominantly been focused this quarter on Google due to new access opportunities being developed*". www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

469 *Idem*.

470 *Idem*.

471 "*The document illustrates with a diagram how one of the agencies appears to have hacked into a target's Internet router and covertly redirected targeted Google traffic using a fake security certificate so it could intercept the information in unencrypted format*". www.slate.com/blogs/future_tense/2013/09/09/shifting_shadow_stormbrew_flying_pig_new_snowden_documents_show_nsa_deemed.html.

472 *Idem*.

473 Http://apps.washingtonpost.com/g/page/world/gchq-report-on-mullenize-program-to-stain-anonymous-electronic-traffic/502/.

III. OPSOMMING VAN DE IN OPEN BRONNEN VERSCHENEN CASUSSEN VAN SPIONAGEACTIVITEITEN TEN AANZIEN VAN POLITIEKE ACTIVITEITEN VAN ZOGENAAMDE 'BEVRIENDE LANDEN'

III.1. (VERMEENDE) SPIONAGEACTIVITEITEN LOS VAN DE SNOWDEN-CASE

69. In deze lijst wordt gefocust op het bespioneren van bevriende landen door de VS of de UK Het bespioneren van Europese landen die deel uitmaakten van het Warschau Pact tijdens de Koude Oorlog worden niet meegeteld. De historische voorbeelden zijn illustratief.

70. De Britse historicus Richard Aldrich heeft beschreven hoe de voorloper van GCHQ sinds 1940 de diplomatieke communicaties afluisterde van haar geallieerde partners, onder andere de Vrije Fransen onder leiding van De Gaulle, Turkije, Spanje en een twintigtal andere landen.[474] Op *adhoc* basis werd diplomatieke informatie uit Italië, Frankrijk, Spanje, Portugal, Japan en West-Duitsland met de VS gedeeld.[475]

71. Op 21 februari 1967 onthulde de Britse krant de *Daily Express* hoe bedrijven zoals Western Union en Cable & Wireless alle internationale telegrammen en telexen, inclusief materiaal van buitenlandse ambassades, naar de Britse overheid bracht, waarop deze gekopieerd werden. Volgens Aldrich ging deze traditie terug tot WO I – en had het VK dus voor een periode van meer dan vijftig jaar toegang tot alle diplomatieke verkeer van alle ambassades vanop haar grondgebied.[476]

72. Volgens Aldrich onderschepte de Nederlandse dienst diplomatieke communicaties van België en Duitsland in de jaren 1980.[477]

73. In 2006 kwam het 'top secret' jaarrapport van 1985-1986 boven water van het Government Communications Security Bureau (GCSB), Nieuw Zeeland's sigint agentschap. Het rapport vermeldde de landen en agentschappen die Nieuw Zeeland dat jaar bespioneerd had, inclusief diplomatieke communicaties van de VN, Egypte, Japan, de Filippijnen, verschillende eilanden in de Stille Oceaan, Frankrijk, Vietnam, de Sovjet Unie, Noord Korea, Oost Duitsland, Laos en Zuid Afrika.[478] De Franse geheime dienst had in 1985 de 'Rainbow Warrior' van Greenpeace doen zinken, en de GCSB schakelde dat jaar de hulp in van de NSA en GCHQ om bronnen in Frankrijk te bespioneren.[479]

---

474 R. ALDRICH, *GCHQ. The uncensored story of Britain's most secret intelligence agency*, Harper Press, London, 2010, 28; 52-53.
475 R. ALDRICH, *o.c.*, 44.
476 R. ALDRICH, *o.c.*, 238-240.
477 R. ALDRICH, *o.c.*, 604.
478 H. BAIN, *Sunday Star*, 15 januari 2006 ("Lange's secret papers reveal USA's bully tactics").
479 R. ALDRICH, *o.c.*, 446.

74. Alastair Campbell, Director of Communications and Strategy voor Tony Blair tussen 1997 en 2003 beschreef in zijn memoires hoe Britse veiligheidsagenten twee 'bugs' ontdekten in de hotelkamer die bedoeld was voor Tony Blair tijdens zijn bezoek aan New Delhi in oktober 2001.De bugs werden toegeschreven aan de Indische geheime dienst.[480]

75. In 1999 verschenen er verschillende rapporten in de Amerikaanse pers die stelden dat zowel de NSA als GCHQ de UNSCOM-missie met wapeninspecteurs van de VN hadden geïnfiltreerd om gevoelige sigint-operaties te ondernemen in Irak. Niet alle informatie die op deze manier gevonden werd, werd gedeeld met UNSCOM.[481] Volgens VN-hoofdinspecteur Hans Blix, was dergelijke informatie uiterst valabel voor een potentiële latere inval.[482]

76. In 2003 publiceerde *The Observer* een volledige memo van de NSA aan GCHQ waarin het die laatste om hulp vroeg om de toenmalige niet-permanente leden van de VN-Veiligheidsraad (Angola, Kameroen, Chili, Bulgarije en Guinea) af te luisteren om inzicht te krijgen in de houding van die landen tegenover een potentiële resolutie van de Veiligheidsraad om een militaire interventie tegen Irak goed te keuren.[483]

77. Rond hetzelfde tijdstip, in februari 2003, werd er in het Justus Lipsius gebouw van de Europese Raad afluisterapparatuur gevonden in die delen van het gebouw die gebruikt werden door de Britse, Franse, Duitse en Spaanse delegaties. Onderzoek suggereerde dat de apparatuur al in het gebouw was geplaatst sinds haar constructie in 1993. Hoewel nooit onomstotelijk bewezen, wezen een aantal indicatoren in de richting van Israël als de verantwoordelijke voor de spionage.[484]

78. In 2004 verklaarde voormalig Brits minister Clare Short op BBC Radio 4's Today programma dat ze regelmatig sigint had gehoord waarop conversaties van VN Secretaris Generaal Kofi Annan in zijn privé-kantoor in het VN-hoofdkwartier in New York te horen waren net voor de oorlog in Irak begon in 2003.[485]

79. In 2004 werd er afluisterapparatuur gevonden in het 'Salon Francais' in het Palais des Nations van de VN in Geneve. Het salon was een van de kamers die in september 2003 gebruikt werden om private onderhandelingen te voeren over de kwestie Irak. Er werd nooit een verantwoordelijke gevonden.[486]

---

480 A. CAMPBELL, *The Blair Years: The Alastair Campbell diaries,* Knopf Doubleday Publishing Group, 2011, 577.

481 C. LYNCH, *Boston Globe*, 6 januari 1999 ("US used UN to spy on Iraq, aides say"); B. GELLMAN, *The Washington Post*, 6 January 1999 ("Annan suspicious of UNSCOM probe").

482 H. BLIX, *Disarming Iraq: The search for weapons of mass destruction,* Bloomsbury, 2005, 36-37.

483 De memo stelde verder: "*We have a lot of special UN-related diplomatic coverage (various UN delegations) from countries not sitting on the UNSC right now that could contribute related perspectives/insights/whatever.*" X., *The Observer*, 2 maart 2003 ("US plan to bug Security Council: the text"). Zie ook www.theguardian.com/world/2003/mar/02/iraq.unitednations1.

484 Zie onder meer VAST COMITÉ I, *Activiteitenverslag 2010,* Intersentia, Antwerpen, 2010, 6-14.

485 C. SHORT, *An honourable deception? New Labour, Iraq and the misuse of power,* Free Press, 2005, 242-243.

486 B. WHITAKER, *The Guardian*, 18 december 2004 ("Bugging device found at UN offices").

80. In december 2004 werd er gesuggereerd dat de NSA tientallen telefoongesprekken van Mohamed ElBaradei, het hoofd van het Internationale Atoomagentschap (IAEA), met Iraanse diplomaten had afgeluisterd. De *Washington Post* suggereerde dat er naar materiaal werd gezocht om ElBaradei af te zetten als hoofd van het IAEA.[487]

III.2. ONTHULLINGEN UIT DE SNOWDEN-DOCUMENTEN

81. Volgens *Der Spiegel* wordt er vanuit 80 Amerikaanse ambassades en consulaten clandestien sigint onderschept door de Special Collection Service.[488] Dit team is ook verantwoordelijk voor top-secret surveillance-operaties in andere ambassades en consulaten die bij de NSA gekend zijn onder de naam STATEROOM.[489]

82. *Der Spiegel* beschreef in wat voor soort informatie de NSA geïnteresseerd is inzake de EU. EU informatie die gerelateerd is aan de economische stabiliteit en handelspolitiek kreeg een '3' op een prioriteitenschaal van 1 (hoogste interesse) tot 5 (laagste interesse). Informatie die gerelateerd was aan energy security, voedselproducten en technologische innovatie kreeg een 5.[490] Der Spiegel gaf details vrij over hoe de NSA de 'ambassador's room' bespioneerde op de 31ste verdieping van de EU's delegatie aan de VN in New York, die bij de NSA gekend is onder de codenaam 'Apalachee'. De NSA had toegang tot de bouwplannen van het gebouw, en infiltreerde het interne VPN-netwerk tussen de EU-missie aan de VN in New York en Washington. Die laatste stond gekend onder de codenaam MAGOTHY. Zowel de EU-missies in Washington en New York werden afgeluisterd. In de EU-missie in New York werden ook harde schijven gekopieerd, en in Washington werd het interne computernetwerk geïnfiltreerd.[491]

83. De NSA is bij de VN vooral geïnteresseerd in alles wat te maken heeft met wapencontrole in de IAEA (prioriteit 1), buitenlandse politiek (prioriteit 2) en mensenrechten, oorlogsmisdaden, milieuzaken en ruwe materialen (allen prioriteit 3). De NSA heeft een eigen team in de VN die onder cover van diplomaat werken. Ze worden versterkt door een team uit Washington voor iedere sessie van de Algemene Vergadering. De NSA luisterde ook mee naar de videoconferenties van VN-diplomaten.[492]

---

487 D. LINZER, *The Washington Post*, 12 december 2004 ("IAEA Leader's phone tapped"). El Baradei had de Amerikaanse intelligence inzake Irak ernstig betwijfeld, en nam in die periode ook een zeer voorzichtige houding aan ten opzichte van Iran.

488 Zie paragraaf 19.

489 www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html.

490 "*Of particular note, the data systems of the EU embassies in America are maintained by technicians in Brussels; Washington and New York are connected to the larger EU network. Whether the NSA has been able to penetrate as far as Brussels remains unclear. What is certain, though, is that they had a great deal of inside knowledge from Brussels*." www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html.

491 www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html.

492 www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html.

84. Der Spiegel onthulde ook het ontstaan van het RAMPART-T programma waaronder de NSA sinds 1991 de communicaties van staatshoofden en hun directe omgeving uit meer dan twintig landen onderschept om de President en zijn national security adviseurs beter te kunnen informeren. Der Spiegel meldde dat niet alleen doelwitten in China en Rusland geviseerd werden, maar ook in Oost-Europese staten.[493]

85. The Guardian meldde dat de 38 ambassades en missies als doelwitten beschouwd werden in een NSA-document van september 2010. Daar zijn geen West-Europese gebouwen bij, maar wel de eerder genoemde EU-missies, en de ambassades van de Frankrijk, Italië en Griekenland, alsook de ambassades van Japan, Mexico, Zuid Korea, India[494] en Turkije. Ook de Franse en Griekse missie bij de VN werden bespioneerd.[495] Le Monde gaf op 18 Oktober een document vrij dat aangaf dat 'close access' collectie op Amerikaans grondgebied tegen buitenlandse diplomatieke doelwitten bekend stond als SIGAD US-3136. Een suffix van twee letters daarnaast duidt op de specifieke locatie en missie. Het document van 10 September 2010 beschrijft een 15-tal manieren waarop informatie kon worden verkregen.[496] 'Close acces' collectie van diplomatie bronnen buiten de VS staat bekend als SIGAD US-3137 met een suffix van twee letters.

86. *Der Spiegel* beschreef verder hoe de NSA informatie uit de Franse diplomatie exploiteert. Een intern NSA-document uit juni 2010 beschreef hoe de NSA succesvol toegang had verkregen tot het VPN-netwerk van het Franse Ministerie van Buitenlandse Zaken, dat alle Franse ambassades en consulaten verbind met Parijs, en (interne) sub-domeinen van de 'diplomatie.gouv.fr' URL. NSA-agenten installeerden *bugs* in de Franse ambassade in Washington en in de Franse missie in New York. Nog steeds volgens *Der Spiegel*, is de

---

493 www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html.

494 Voor meer info zie S. SAXENA, *The Hindu,* 25 September 2013 ("NSA planted bugs at Indian missions in D.C., U.N.").

495 "*The US intelligence service codename for the bugging operation targeting the EU mission at the United Nations is "Perdido". The operation against the French mission to the UN had the covername "Blackfoot" and the one against its embassy in Washington was "Wabash". The Italian embassy in Washington was known to the NSA as both "Bruneau" and "Hemlock".The eavesdropping of the Greek UN mission was known as "Powell" and the operation against its embassy was referred to as "Klondyke".*" www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies.

496 HIGLANDS: collection from implants, VAGRANT: collection of computer Screens, MAGNETIC: sensor collection of magnetic emanations, MINERALIZE: collection from LAN implant, OCEAN: optical collection system for raster-based computer screens, LIFESAVER: imaging of the hard drive, GENIE: multi-stage operatoins; jumping the airgap etc.; BLACKHEART: collection from an FBI implant, PBX: Public Branch Exchange Switch, CRYPTO ENABLED: collection derived from AO's efforts to enable crypto, DROPMIRE (1) passive collection of emanations using an antenna (2) laser printer collection, purely proximal access, DEWSWEEPER: USB hardware host tap that provides covert link over USB link into a target network. Operates w/RF delay sybsytem to provide wireless bridge into target network. RADON: bi-directional host tap that can inject Ethernet packets onto the same target. Allows bi-direction exploitation of denied networks using standard on-net tools. Tegen de Franse missies werden bijvoorbeeld de HIGHLAND, VAGRANT en PBX technieken gebruikt. https://www.documentcloud.org/documents/807030-ambassade.html#document/p1.

NSA is vooral geïnteresseerd in Frankrijks buitenlandse politiek, vooral wapenhandel, en Frankrijks economische politiek.[497]

87. Een document van 17 mei 2006 dat gepost werd op de website van Globo meldde dat de International Security Issues (ISI) missie binnen de NSA verantwoordelijk is voor dertien individuele staten in drie continenten. Die dertien landen hebben met elkaar gemeen dat ze belangrijk zijn voor de VS inzake economie, handel en buitenlandse politiek. De 'Western Europe and Strategic Partnerships division' binnen die missie focust zich voornamelijk "*op de buitenlandse politiek en handelsactiviteiten van België, Frankrijk, Duitsland, Italië, Spanje als ook Brazilië, Japan en Mexico*". Deze divisie geeft ook *key intelligence* over 'militaire en intelligence activiteiten in enkele van deze landen'. De 'Aegean and Ukraine division' houdt zich bezig met alle aspecten van Turkije – 'governmental/leadership, military and intelligence'. ISI werkt samen met F6 en *second and third party* buitenlandse partners die zowel 'waardevolle analytische inzichten als technische capaciteiten' bevatten.[498] Volgens *Le Monde* verwijzen nummers die beginnen met US-98 (zoals US-985D (Frankrijk), US-987 (Duitsland)) naar SIGADS op het territorium van *third party* partners van de NSA. Die bestaan volgens *Der Spiegel* onder meer uit Frankrijk, Duitsland, Oostenrijk, Polen en België.[499] Hetzelfde document maakte melding van het feit dat de 'ISI' actief samenwerkt met de "*Combating Proliferation (CP, S2G) and Counterterrorism (CT, S2I) product lines to incorporate financial intelligence analysis into their mission build-out plans*".[500]

88. Een document van augustus 2010 bevestigt dat de NSA de communicaties onderschepte van acht leden van de VN Veiligheidsraad. Alleen Frankrijk, Japan, Mexico en Brazilië werden expliciet genoemd. Doel was om de US missie aan de VN (en andere Amerikaanse diensten) van de meest *up-to-date* informatie te voorzien over hun stemintenties en onderhandelingsposities over een VN-resolutie over sancties tegen Iran.[501]

89. Een bericht in *Globo* bevestigde hoe de NSA Latijns-Amerikaanse landen als Mexico, Venezuela, Argentinië, Colombia, Ecuador, Panama, Costa Rica, Nicaragua, Honduras, Chili, El Salvador en Peru bespioneerde. De NSA was geïnteresseerd in de olie-politiek van Venezuela, de energie- en drugspolitiek van Mexico en de Colombiaanse positie tegenover

---

497 X., *Der Spiegel*, 1 september 2013 ("'Success Story': NSA targeted French Foreign Ministry").

498 http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html.

499 www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-3.html.

500 "*The idea is to integrate financial analysis with traditional target efforts as opposed to working the target from two separate perspectives, as is done in NSA Washington. ISI's long-term goal is to introduce financial analysis a part of the Intelligence Analysis curriculum so any target can be enriched with the use of financial intelligence*." In: http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html In die zin is het misschien interessant om op te merken dat volgens sommige bronnen van *De Standaard* er problemen zouden zijn vastgesteld bij de FOD Financiën, waarbij onderzocht werd of het om dezelfde malware als bij Belgacom gaat. Topman Hans D'Hondt van Financiën sprak echter formeel tegen dat zijn diensten gehackt of besmet zouden zijn. In: N. VANHECKE, P. DE LOBEL, *De Standaard*, 4 oktober 2013 ("Vrees voor massale besmetting").

501 http://epoca.globo.com/tempo/noticia/2013/07/spies-bdigital-ageb.html.

de FARC. Door het gebruik van XKEYSCORE kon een 'buitenlander' opgespoord worden door de taal die hij gebruikte om te communiceren.[502]

90. Een top-secret document uit November 2010, gepubliceerd door *Der Spiegel*, toont dat de NSA's TAO-divisie geslaagd was in operatie FLATLIQUID om toegang te krijgen tot de publieke e-mail account van de toenmalig Mexicaanse president Felipe Calderon om "*inzicht te krijgen in Mexico's politieke systeem en interne stabiliteit*". De account werd ook gebruikt door leden van Calderon's kabinet.[503] Gedurende een periode van twee weken in de vroege zomer van 2012 lanceerde de NSA ook een intensieve 'structurele surveillance' campagne tegen huidig president Enrique Pena Nieto. Op basis van zijn communicatiepatronen werd bepaald wie negen van zijn dichtste adviseurs waren. De gegevens van deze personen werden in de DISHIRE database gestoken, waarna ook hun communicaties onderschept werden. Op die manier werden bijvoorbeeld 85.489 sms'en onderschept. Doel van de operatie was om te bepalen of Mexico een nieuwe strategie zou aannemen vis-a-vis de drugskartels.[504] De NSA is vooral geïnteresseerd in de drughandel (niveau 1), de leiders van Mexico, Mexico's economische stabiliteit, militaire capaciteiten, mensenrechten en internationale handelsrelaties (niveau 3) en contraspionage (niveau 4). Om die doelen te bereiken voerde TAO in augustus 2009 'Operatie Whitetamale', waarmee het toegang kreeg tot de e-mails van verschillende hoge ambtenaren in Mexico's 'Public Security Secretariat' dat zich onder andere bezighoudt met drugshandel en mensenhandel. Via operatie EVENINGEASEL tapte de SCS divisie van de NSA vanuit de ambassade in Mexico stad telefoonconversaties af en las het sms'en die verstuurd werden via Mexico's mobiele telefoonnetwerk.[505]

91. Het Braziliaanse nieuwsprogramma Fantastico op de zender *Globo* toonde een slideshow waarin de communicatiepatronen tussen Braziliaans president Dilma Roussef, haar voornaamste adviseurs en derden werden getoond.[506] Volgens Glenn Greenwald had het desbetreffende NSA programma toegang tot het volledige communicatienetwerk van de Braziliaanse presidente en haar staff in kaart te brengen, inclusief telefoonconversaties, e-mails en uitwisselingen op sociale netwerk sites.[507]

92. DNI Clapper reageerde door te zeggen dat het 'geen geheim is dat de Intelligence community informatie verzamelt over economische en financiële zaken, en de financie-

---

502 http://oglobo.globo.com/mundo/espionagem-dos-eua-se-espalhou-pela-america-latina-8966619.

503 www.spiegel.de/fotostrecke/photo-gallery-nsa-hacked-into-mexican-president-s-email-account-fotostrecke-102797-2.html.

504 www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html.

505 www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html.

506 http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html.

507 Y. MARULL, *AFP*, 2 september 2013 ("Brazil, Mexico summon US envoys over spy claims"). Een vertegenwoordiger van het State Department zei: "*while we are not going to comment publicly on every specific alleged intelligence activity, as a matter of policy we have made clear that the United States gathers foreign intelligence of the type gathered by all nations*".

ring van terrorisme'. Volgens Clapper verzamelt de VS dit soort informatie onder meer om de VS en haar partners *early warnings* te geven over internationale financiële crisissen die een negatief effect zouden kunnen hebben op de wereldeconomie.[508]

93. Een dag later melde Fantastico dat de NSA ook het interne computernetwerk van de Braziliaanse oliemaatschappij Petrobras als een spionagedoelwit zag. Een presentatie uit mei 2012 die als doel had om nieuwe NSA-agenten op te leiden in manieren om toegang te verkrijgen tot private computernetwerken, vermeldde de maatschappij als doelwit. Het is niet duidelijk welke informatie precies werd gezocht of verkregen, maar *Globo* suggereert dat dit over informatie kon gaan zoals details over de meest waardevolle ongeëxploiteerde olievelden die binnenkort door Petrobras zouden aangeboden worden in een veiling, of over informatie over *state-of-the art ocean-floor exploration* technologie. De presentatie werd (nog) niet online gezet.[509] Dezelfde presentatie melde ook dat Google, Franse diplomaten die toegang hadden tot het privé netwerk van het ministerie van Buitenlandse Zaken van Frankrijk[510] en SWIFT gezien werden als doelwitten.

94. Een GCHQ-slideshow toont hoe GCHQ data verzamelde van de smartphones, inclusief Blackberries, van verschillende diplomatieke delegaties op de G20 meeting in Londen in 2009.[511] Die data kon bijna in 'real time' doorgestuurd worden naar analisten, die briefings konden maken voor Britse ministers, inclusief Gordon Brown.[512] Op basis van deze informatie werden ook twintig nieuwe 'e-mail selectors' gevonden.[513] GCHQ ging heel ver om dergelijke diplomatieke informatie in te winnen. Zo werd een vals internetcafé opgezet waar *key-loggers* alles konden zien wat een délégué intypte op een computer. Een ander document toonde aan dat GCHQ succesvol het netwerk van het Zuid-Afrikaanse Ministerie van Buitenlandse Zaken had gekraakt, waardoor onder meer briefings onderschept konden worden voor délégués op de G20 en G8 meetings. Ook wordt melding gemaakt van GCHQ-pogingen om geëncrypteerde telefoongesprekken van Medvedev en andere Russische délégués te onderscheppen wanneer deze zich in Londen bevonden. GCHQ bespioneerde ook de Turkse Minister van Financiën op de meeting, alsook vijftien

508 Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage, 8 september 2013, zie: http://icontherecord.tumblr.com/post/60712026846/statement-by-director-of-national-intelligence. "*What we do not do, as we have said many times, is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of – or give intelligence we collect to – US companies to enhance their international competitiveness or increase their bottom line.*"

509 www.reuters.com/article/2013/09/09/us-usa-security-snowden-petrobras-idUSBRE98817N20130909.

510 www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies.

511 "*The document refers to a tactic which was "used a lot in recent UK conference, eg G20" (…) the tactic is defined in an internal glossary as "active collection against an email account that acquires mail messages without removing them from the remote server". A PowerPoint slide explains that this means "reading people's email before/as they do*". In: www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits.

512 Gordon Brown zat de G20 voor en wou vooruitgang boeken op twee fronten: de coordinatie van de globale economisch heropleving om een nieuwe recessie te voorkomen en een overeenkomst om *global economic governance* te versterken en internationale financiële institutions te hervormen.

513 www.theguardian.com/uk/interactive/2013/jun/16/gchq-surveillance-the-documents.

andere leden van zijn delegatie. GCHQ probeerde ook een nieuwe techniek uit op de meeting die het telefoonverkeer van alle deelnemers in kaart bracht.[514]

95. De UK plande een operatie om verschillende delegaties op de Commonwealth 'Heads of Government' meeting te bespioneren in Trinidad in 2009 om de UK extra diplomatieke informatie te geven. Een document beschrijft bijvoorbeeld hoe sigint moest verzameld worden over Zuid Afrika's opinie over Zimbabwe vooraleer Prime Minister Brown een ontmoeting had met Zuma. Het is niet duidelijk of er effectief sigint verzameld werd.[515]

BIJLAGE: AFKORTINGEN EN BEGRIPPEN

1EF solution	One-End Foreign solution
ADIV	Algemene Dienst inlichting en veiligheid
AG	Attorney General
BICS	Belgacom International Carrier Services
BIPT	Belgisch Instituut voor Postdiensten en Telecommunicatie
BND	Bundesnachrichtendienst (DE)
CERT-EU	Computer Emergency Response Team
CLANSIG	clandestine signals collection
CIA	Central Intelligence Agency
CNE	Computer Network Exploitation
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DITU	Data Intercept Technology Unit van de FBI
DNI	(1) Director of National Intelligence in de V.S. (James Clapper), (2) Digital Network Intelligence
DNR	Dialed Number Recognition
ECI	Exceptionally Controlled Information
EO 12333	Executive Order 12333
ECI	Exceptionally Controlled Information
EXIF	Exchangeable image file format
FAA	FISA Amendments Act
FBI	Federal Bureau of Investigation
FCCU	Federal Computer Crime Unit
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
Five eyes	De SIGINT-agentschappen van de V.S., de U.K, Australië, Canada en Nieuw Zeeland
Fornsat	Informatie afkomstig van satellieten
FTC	Federal Trade Commission
FRA	Försvarets radioanstalt (Zweeds SIGINT-agentschap)

514 www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits.
515 www.theguardian.com/world/2013/jun/16/uk-intelligence-agencies-spy-commonwealth-delegates.

F6-sites	Diplomatieke en consulaire missies van de VS
GAO	Global Access Operations-divisie (NSA)
GCHQ	Government Communications Headquarters (UK)
HOT	Humint Operations Team
IM	Instant Messaging
ISA	Intelligence Services Act (UK)
ISC	Intelligence Security Committee
Metadata	Metadata – soms ook 'communications data' of 'traffic data' genoemd, is de informatie die gecreëerd wordt wanneer data verzonden wordt. De precieze inhoud is afhankelijk van het type data dat verzonden wordt en hangt ook soms af van de lokale wetgeving. – Voor *vaste telefoonlijnen*: nummers die gebeld werden via dat toestel, alsook de datum en de tijd waarop een nummer gebeld en opgebeld werd. Soms ook de naam en het adres van de persoon die het contract van de vaste lijn heeft afgesloten. – *Mobiele telefoons*: (1) nummers die gebeld of ge-sms't werden via dat toestel, (2) de datum en de tijd waarop een nummer gebeld of opgebeld werd of een sms stuurde of ontving, (3) de locatie van waar er gebeld of ge-sms't werd, en waar die communicatie ontvangen werd. (4) Soms ook de naam en het adres van de persoon die het contract van de vaste lijn heeft afgesloten. (5) Soms ook het International Mobile Subscriber Identity (IMSI) nummer en (6) het International Mobile station Equipment Identity (IMEI) nummer. (6) Soms ook de nummer van de telefoonkaart die gebruikt werd. – *Voice over Internet Protocol (VoIP), e-mail, chat, Facebookberichten*: (1) online gebruikersnaam, login naam of accountnaam waarmee iemand belt, gesprekken ontvangt, e-mails verzendt, chatberichten verstuurd (2) het IP adres van de computers die gebruikt werden, (3) de tijd en datum van de communicatie. Sommige landen lijken ook de onderwerp-lijn van e-mails als metadata te zien. – *Internet surfgedrag:* (1) IP adres van het toestel waarmee iemand online gaat (2) de tijd en datum van het in- en uitloggen, en een lijst van webdomeinen die bezocht werden.
NCtC	National Counterterorrism Center
MTI	Mastering the Internet
NSA	National Security Agency
OSN	Online Social Networking
PNR	Passenger Name Records
PSTN	Public switched telephone network
RIPA	Regulation of Investigatory Powers Act (UK)
SCIF	Secure Compartmented Intelligence Facility
SCS	Special Collection Service
SHAPE	Supreme Headquarters Allied Powers Europe
SIGAD	Signals activity/address designators – kunnen verwijzen naar een specifiek fysiek collectieplatform (zoals bijvoorbeeld een Amerikaanse

	legerbasis in het buitenland, een ambassade, een schip.), een virtueel dataverwerkingsplatform (PRISM staat bijvoorbeeld bekend als SIGAD US-984XN) of een ruimtesatelliet.
SIGINT	Signals Intelligence
SRP	Specialized Reconnaissance Program
SSL	Secure Sockets Layer
SSO	Special Source Operations
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAO	Tailored Access Operations
TBB	Tor Browser Bundle
TFTP	Terrorist Finance Tracking Program
TIDE	Terrorist Identities Datamart Environment
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTC	Video teleconferencing systeem
XKS	Xkeyscore

BIJLAGE E.
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

Annemie Schaus
Gewoon hooglerares
Vice-rector academisch beleid
Université libre de Bruxelles

I. KORTE BESCHRIJVING VAN DE BEKENDE CONTEXT VAN DE MASSALE ONDERSCHEPPING VAN PERSOONSGEGEVENS[516]

Enorme hoeveelheden persoonsgegevens werden onderschept door het programma *PRISM*, dat inlichtingen verzamelt op een nooit geziene schaal en niveau en waarvan het doel veel verder reikt dan het bestrijden van terrorisme of economische spionage.

Hoewel er onduidelijkheid blijft bestaan over de precieze feiten en vooral de rol van bepaalde betrokkenen, lijkt iedereen het eens over de omvang van de onderschepping, monitoring en exploitatie van persoonsgegevens. Na de eerste onthullingen over *PRISM* bevestigde de directeur van het *NSA* namelijk dat de dienst zowel binnen als buiten de Verenigde Staten metagegevens over communicatie verzamelt bij alle grote operatoren en deze metagegevens gedurende vijf jaar opslaat in een database.[517]

Het is ook bewezen dat het *GCHQ* hetzelfde type intercepties heeft verricht en dat grote operatoren van communicatienetwerken of sociale netwerken[518] grote hoeveelheden persoonsgegevens hebben bezorgd aan het *NSA*.

---

516 Zie het verslag van Mathias Vermeulen, "De Snowden-revelaties, massale datacaptatie en politieke spionage. Open bronnenonderzoek", 25 november 2013.

517 *Le programme de surveillance des Etats-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE,* Nota van het Directoraat-generaal intern beleid, Beleidsondersteunende afdeling C: Rechten van de burger en constitutionele zaken, IPOL-LIBE_NT(2013)474405_FR; zie ook het verslag van Mathias Vermeulen.

518 Onder andere *Facebook, Twitter, Microsoft, Google, Yahoo!, PalTalk, YouTube, Skype, AOL* en*Apple;* zie het verslag van Mathias Vermeulen.

II. TOEPASSELIJKE WETGEVING

Eerst en vooral moet er op worden gewezen dat er niet wordt getwijfeld aan de verenigbaarheid van het bestaan van de inlichtingendiensten met het Europees Verdrag tot bescherming van de rechten van de mens.[519] Zoals het Europees Hof voor de Rechten van de Mens benadrukte, kan de bescherming van de mensenrechten het bestaan van inlichtingendiensten vereisen, op voorwaarde dat hun methodes de fundamentele beginselen inzake de bescherming van de mensenrechten in acht nemen:"*Quel que soit le système de surveillance retenu, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus. Cette appréciation ne revêt qu'un caractère relatif: elle dépend de toutes les circonstances de la cause, par exemple la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne*".[520, 521]

Het Hof benadrukt dat de bewegingsruimte van de Verdragsluitende Staten niet onbeperkt is om personen binnen hun jurisdictie te onderwerpen aan maatregelen van geheime monitoring. In het besef dat de democratie dreigt te worden miskend of zelfs vernietigd in een poging haar te beschermen, wijst het Hof erop dat de Staten niet om het even welke maatregelen mogen nemen die ze geschikt achten in naam van de strijd tegen spionage en terrorisme.

Ter zake moeten de beginselen van legaliteit, finaliteit en proportionaliteit in acht worden genomen zodra het legitiem doel is vastgesteld.[522] Dit betekent dat het juridisch arsenaal om de privacy en de persoonsgegevens te beschermen in acht moet worden genomen (A), maar ook de soevereiniteit van de Staat op het grondgebied waarvan de persoonsgegevens worden verzameld, opgeslagen en verwerkt (B). Voor zover de feiten die ons zijn voorgelegd dat mogelijk maken, zullen we analyseren in hoeverre de regels toepasselijk zijn op het massaal verzamelen van persoonsgegevens waarvan wij kennis hebben gekregen. Tot slot geven we een overzicht van de eventuele rechtsmiddelen (C).

A. NALEVING VAN HET RECHT OP EERBIEDIGING VAN HET PRIVÉLEVEN EN BESCHERMING VAN PERSOONSGEGEVENS

In deze zaak kunnen verschillende wetsbepalingen ter bescherming van het recht op eerbiediging van het privéleven van toepassing zijn; die bepalingen *vullen elkaar aan*. We

519 Hierna EVRM.

520 EHRM, *Klass en anderen tegen Duitsland* van 6 september 1978; EHRM, *Vereniging weekblad Bluf! tegen Nederland* van 9 februari 1995 (vrije vertaling).

521 "Welk monitoringsysteem er ook wordt gebruikt, het Hof moet zich vergewissen van het bestaan van passende en voldoende garanties tegen misbruiken. Deze beoordeling is slechts van relatieve aard: ze is afhankelijk van alle omstandigheden van de zaak, zoals de aard, de omvang en de duur van eventuele maatregelen, de vereiste redenen om daartoe het bevel te geven, de bevoegde overheden om toelating te geven voor die maatregelen, ze uit te voeren en te controleren, het type verhaal krachtens het intern recht" (vrije vertaling).

522 Terwijl de bestrijding van terrorisme een geldig doel kan vormen, geldt dat niet noodzakelijk voor de economische profilering van individuen.

zullen die bepalingen beknopt toelichten, gaande van de bepaling met de meest algemene draagwijdte tot de bepaling met een specifieker doel, i.e. artikel 17 van het Verdrag inzake burgerrechten en politieke rechten (1); artikel 8 van het EVRM (2); Verdrag nr. 108 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (3) en het recht van de Europese Unie: artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie (4), Richtlijn 95/46/EG van het Europees Parlement en de Raad 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 [523] (zoals aangevuld door Richtlijn 2002/58/EG van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie) (5) en Richtlijn 2006/24/EG betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG [524] (6). Tot slot moet verwezen worden naar het territoriaal toepassingsgebied van de Belgische wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens [525, 526]; het is niet duidelijk of die voorwaarden in casu vervuld zijn. In het kader van deze studie kunnen we deze wetgeving dus niet specifiek analyseren. Voor zover ze aansluit bij de bepalingen van internationaal recht en het ter zake toepasselijk Europees recht uitvoert, zijn de onderstaande analyses ook van toepassing op de bewuste wetgeving.

Vervolgens bekijken we hoe de eerbiediging van de normen inzake de bescherming van persoonsgegevens het voorwerp is geweest van het *Safe Harbor*-akkoord tussen de EU en de Verenigde Staten (7).

Op het vlak van de doorgifte, de monitoring, de controle en de bewaring van persoonsgegevens door middel van nieuwe technologieën moet – zoals Cécile de Terwangne en Jean-Noël Colin benadrukken [527] – privacy niet worden geïnterpreteerd in de klassieke betekenis, namelijk in die van bescherming van de persoonlijke, intieme, familiale of vertrouwelijke levenssfeer. Overeenkomstig de evolutie van het recht en de technologieën moet privacy worden begrepen als de mogelijkheid tot zelfbeschikking en autonomie en het vermogen van het individu om existentiële of informatieve keuzes te maken.[528] In overeenstemming met het Handvest van de grondrechten van de Europese Unie[529] gaat het om informatieve zelfbeschikking, i.e. het recht van het individu om kennis te hebben

523 Hierna "Richtlijn 95/46".

524 Hierna "Richtlijn 2006/24".

525 Hierna "WBPL".

526 De WBPL is van toepassing op de verwerking van persoonsgegevens wanneer de verwerking wordt verricht in het kader van de effectieve en daadwerkelijke activiteiten van een vaste vestiging van de verantwoordelijke voor de verwerking op het Belgisch grondgebied, zoals aangegeven door artikel 3*bis*, 1°.

527 *Défis pour la vie privée et la protection des données posés par la technologie,* Verslag, Namen FNDP, februari 2011.

528 Voor de expliciete erkenning van een recht op zelfbeschikking of persoonlijke autonomie zoals vervat in het recht op eerbiediging van het privéleven van artikel 8 EVRM, zie EHRM, *Evans tegen Verenigd Koninkrijk,* arrest van 7 maart 2006 (bevestigd door de Grote Kamer in zijn arrest van 10 april 2007); *Tysiac tegen Polen*, arrest van 20 maart 2007; *Daroczy tegen Hongarije*, arrest van 1 juli 2008.

529 Zie *infra* en de volgende voetnoot.

van de gegevens die op hem betrekking hebben en die worden bijgehouden, de kanalen te beheersen via dewelke die gegevens worden gecommuniceerd en het ongepast of bedrieglijk gebruik ervan te beletten. Op dit gebied is persoonlijke levenssfeer dus niet beperkt tot een zoeken naar privacy, maar gaat het om de beheersing door elk individu van zijn 'informatiebeeld'.[530] Dit gezegd zijnde en zoals het EHRM benadrukt, *"la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention"*.[531, 532] Het is in deze betekenis dat persoonlijke levenssfeer hier moet worden begrepen.

1. Artikel 17 van het Internationaal verdrag inzake burgerrechten en politieke rechten[533]

Artikel 17 van het IVBPR is de enige internationale bepaling met universele draagwijdte die het recht op eerbiediging van het privéleven garandeert. Net als de zusterbepalingen van dit artikel 17, die van dezelfde periode dateren, verwijst dit artikel nergens naar persoonsgegevens als onderdeel van het recht op eerbiediging van het privéleven. Echter wordt die privacy, die beschermd wordt door Artikel 17, op de proef gesteld door nieuwe inmengingen die mogelijk gemaakt worden door nieuwe technologieën. Daarom spoort de 35ste internationale conferentie van commissarissen voor privacy en gegevensbescherming de Staten ertoe aan algemene opmerking nr. 16 van het IVBPR van 1988 aan te nemen, om zo de bescherming van het privéleven te versterken.[534] Die opmerking stimuleert de creatie van een wereldwijd rechtskader voor de bescherming van persoonsgegevens en van de persoonlijke levenssfeer. De Verenigde Staten hebben deze opmerking niet aangenomen en dat is de reden waarom tal van voorstellen tot doel hebben om artikel 17 van het IVBPR zelf aan te passen aan het digitale tijdperk[535], aangezien de Verenigde Staten dat Verdrag hebben getekend. Anderen stellen voor om een bijkomend protocol aan te nemen op basis van Algemene Opmerking nr. 16 zoals goedgekeurd door de Algemene Vergadering van de Verenigde Naties in 1996.[536]

Onlangs heeft de derde Commissie van de Algemene Vergadering van de Verenigde Naties een tekst aangenomen over het recht op eerbiediging van het privéleven in het digi-

---

530 Paul De Hert, Katja de Vries en Serge Gutwirth, Observatienota over het arrest van het Duits federaal Grondwettelijk Hof van 27 februari 2008, *Revue du droit des technologies et de l'information,* 2009, p. 87. In dit arrest kent het Hof op basis van het algemeen recht van persoonlijkheid een volkomen nieuw fundamenteel recht toe op de bescherming van "de vertrouwelijkheid en de integriteit van de technologische informatiesystemen". Dit nieuw fundamenteel recht inzake informatietechnologie moet lacunes in de bestaande fundamentele rechten aanvullen.

531 EHRM, *S. en Marper tegen Verenigd Koninkrijk* van 4 december 2008.

532 "speelt de bescherming van persoonsgegevens een fundamentele rol voor de uitoefening van het recht op eerbiediging van het privéleven en het familie- en gezinsleven zoals bekrachtigd door artikel 8 van het Verdrag" (vrije vertaling).

533 Hierna "IVBPR".

534 www.unhchr.ch/tbs/doc.nsf/0/7dc7e7821c5da97680256523004a423d?Opendocument.

535 www.franceonu.org/IMG/pdf/Vie_privee_FR.pdf.

536 Http://droitdu.net/2013/10/35eme-conference-internationale-des-commissaires-a-la-protection-des-donnees-et-de-la-vie-privee-une-volonte-duniformiser-la-protection-des-donnees-personnelles/.

tale tijdperk.[537] Ze beveelt de bescherming van de persoonlijke levenssfeer aan van personen, zowel offline als online, en vraagt alle Lidstaten om "het recht op eerbiediging van het privéleven in acht te nemen en te beschermen, meer bepaald in de context van de digitale communicatie".[538] De interpretatie die vandaag aan artikel 17 van het IVBPR kan worden gegeven, is dat de bescherming van dit artikel betrekking heeft op persoonsgegevens.

2. Artikel 8 van het EVRM

Artikel 8 van het EVRM verzekert aan eenieder het recht op eerbiediging van het privéleven. Het Europees Hof voor de Rechten van de Mens heeft de draagwijdte van het concept 'privéleven' uitdrukkelijk uitgebreid tot de bescherming van persoonsgegevens. Voor het Hof speelt de bescherming van persoonsgegevens een fundamentele rol voor de uitoefening van het recht op eerbiediging van het privéleven zoals bekrachtigd door artikel 8.[539] Het Hof oordeelt dat *"la protection offerte par l'article 8 serait affaiblie de manière inacceptable si l'usage des techniques scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part."*[540, 541]

Volgens het Hof brengt artikel 8 de verplichting mee dat het intern recht voorziet in passende garanties om elk ongepast en onrechtmatig gebruik van persoonsgegevens te voorkomen. De nationale wetgeving moet ook verzekeren dat de gegevens relevant en niet excessief zijn ten opzichte van de doeleinden waarvoor ze zijn opgeslagen en dat ze slechts worden bewaard gedurende de periode die vereist is voor de doeleinden waarvoor ze zijn opgeslagen, in een vorm die de identificatie van personen mogelijk maakt.

Het Hof wijst erop dat *"dans ce contexte comme dans celui des écoutes téléphoniques, de la surveillance secrète et de la collecte secrète de renseignements, il est essentiel de fixer des règles claires et détaillées régissant la portée et l'application des mesures et imposant un minimum d'exigences concernant, notamment, la durée, le stockage, l'utilisation, l'accès des tiers, les procédures destinées à préserver l'intégrité et la confidentialité des données et les procédures de destruction de celles-ci, de manière à ce que les justiciables disposent de garanties suffisantes contre les risques d'abus et d'arbitraire […]"*[542]

---

537 www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1&Lang=F.

538 Artikel 4 van de tekst van de derde Commissie van de Algemene Vergadering van de Verenigde Naties.

539 Zie document "Case law of the European Court of Human Rights concerning the protection of personal data", DP(2013)CASE LAW, 30 januari 2013 [niet beschikbaar in het Nederlands], www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/DP%202013%20Case%20 Law_Eng%20%28final%29.pdf.

540 EHRM, *S. en Marper tegen Verenigd Koninkrijk* van 4 december 2008.

541 "de bescherming geboden door artikel 8 op onaanvaardbare wijze zou worden verzwakt indien het gebruik van moderne wetenschappelijke technieken in het systeem van het strafrecht zou worden toegelaten tegen gelijk welke prijs en zonder nauwgezette afweging van enerzijds de voordelen die kunnen voortvloeien uit een grootschalig gebruik van die technieken en anderzijds de essentiële belangen van de bescherming van het privéleven" (vrije vertaling).

542 "het in deze context, net als in die van het afluisteren van telefoongesprekken, het geheim toezicht en de geheime inzameling van inlichtingen, van wezenlijk belang is om duidelijke en gedetailleerde regels vast te leggen die de draagwijdte en de toepassing van de maatregelen vastleggen en een minimum aan vereisten opleggen betreffende meer bepaald de duur, de

Aldus oordeelde het Hof dat de opslag door een overheidsinstantie van gegevens over de persoonlijke levenssfeer van een individu een inmenging vormde in het recht op eerbiediging van zijn privéleven zoals gewaarborgd door artikel 8, lid 1 van het EVRM, en verduidelijkte dat het gebruik van die gegevens er weinig toe doet, meer bepaald in de volgende bewoordingen:

> "De opslag door een overheidsinstantie van gegevens over de persoonlijke levenssfeer van een individu vormt een inmenging in de betekenis van artikel 8. Het later gebruik van de opgeslagen informatie is van weinig tel." (vrije vertaling).[543]

De inzameling en de bewaring van gegevens moeten dus de garanties inhouden die noodzakelijk zijn om het recht op eerbiediging van het privéleven van de individuen te beschermen.[544]

Op 1 juli 2008 veroordeelde het Hof (in een zaak met gelijkaardige feiten) het Verenigd Koninkrijk wegens inbreuk op artikel 8 voor het illegaal onderscheppen van communicatie te land door de inlichtingendienst *GCHQ,* van 1990 tot 1998. Het *GCHQ* onderschepte alle communicatie te land (fax, e-mail, telex en informatica) vanuit en naar de Ierse Republiek via de toren van *Capenhurst,* die binnen een kerncentrale ligt en 24 uur per dag operationeel is. De toren van *Capenhurst* diende niet alleen om informatie over terrorisme te verzamelen, maar werd ook gebruikt in het kader van economische spionage en voor het onderscheppen van diplomatieke communicatie van Ierland en persoonlijke communicatie van vooraanstaande Ieren, met behulp van specifieke lijsten van telefoonnummers of systemen van stemherkenning.[545]

Het EHRM is ook van mening dat de Staten verplicht zijn om een doeltreffende procedure in te voeren die het de belanghebbenden mogelijk maakt toegang te hebben tot de documenten die de veiligheidsdiensten over hen verzamelen.[546]

De grootschaligheid van de interceptie, waarbij zonder onderscheid te werk wordt gegaan, de monitoring, het gebruik en de bewaring van persoonsgegevens waarvan in deze zaak sprake is, zijn in alle opzichten duidelijk strijdig met artikel 8; de gelaakte maatregelen hebben op onbepaalde wijze betrekking op private of publieke natuurlijke of rechtspersonen; de slachtoffers zijn meestal niet-identificeerbaar; deze maatregelen steunen op geen enkele geldige wettelijke basis en miskennen integendeel het recht dat van toepassing is op de doorgifte van persoonsgegevens; ze staan kennelijk niet in verhouding tot de beoogde doelstellingen, die zelf ook niet gedefinieerd zijn.

Omdat sommige actoren die aan dit systeem zouden hebben deelgenomen privépersonen zouden kunnen zijn, past het te benadrukken dat artikel 8 van het EVRM een horizontaal effect kan hebben.

---

opslag, het gebruik, de toegang door derden, de procedures met het oog op het beschermen van de integriteit en de vertrouwelijkheid van de gegevens en de procedures tot vernietiging van die gegevens, zodat de rechtsonderhorigen voldoende garanties genieten tegen de risico's van misbruik en willekeur […]" (vrije vertaling).

543 EHRM, *Leander tegen Zweden* van 26 maart 1987; *Kopp tegen Zwitserland* van 25 maart 1998; *Amann tegen Zwitserland* van 16 februari 2000; *Association '21 Décembre 1989' en anderen tegen Roemenië* van 24 mei 2011.

544 EHRM, *Rotaru tegen Roemenië* van 4 mei 2000.

545 EHRM, *Liberty en andere ngo's tegen het Verenigd Koninkrijk* van 1 juli 2008.

546 EHRM, *Joanna Szulc tegen Polen* van 13 november 2012.

Al in 1979 benadrukte het Europees Hof voor de Rechten van de Mens immers het volgende:

> *"Si l'article 8 a essentiellement pour objet de prémunir l'individu contre les ingérences arbitraires des pouvoirs publics, il ne se contente pas de commander à l'État de s'abstenir de pareilles ingérences: à cet engagement plutôt négatif s'ajoutent des obligations positives inhérentes à un respect effectif de la vie privée ou familiale. Elles peuvent impliquer l'adoption de mesures visant au respect de la vie privée jusque dans les relations des individus entre eux".*[547, 548]

In het arrest *Soderman tegen Zweden* van 12 november 2013 wijst het Hof erop dat wanneer een bijzonder belangrijk aspect van het bestaan of de identiteit van een individu op het spel staat of de betrokken activiteiten betrekking hebben op een van de intiemste aspecten van het privéleven, de Staat nog minder bewegingsruimte heeft om de verplichting voor de particulieren te reglementeren.[549]

In hun activiteiten die afbreuk kunnen doen aan het recht op eerbiediging van het privéleven van individuen of publieke of private rechtspersonen vormt de eerbiediging van het privéleven duidelijk een verplichting voor providers van sociale netwerken, voor handelsondernemingen die actief zijn op het gebied van de nieuwe technologieën en voor andere verantwoordelijken voor de verwerking van persoonsgegevens, onder voorbehoud welteverstaan van een onderzoek in elk bijzonder geval van de territoriale werkingssfeer van de activiteit van die providers.[550]

3. Verdrag nr. 108 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens

Verdrag nr. 108 van de Raad van Europa tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens is het enige bindende specifieke rechtsinstrument voor alle Lidstaten van de Raad van Europa op dit gebied. De beginselen zijn de volgende:

- beginsel van eerlijkheid, rechtmatigheid en evenredigheid met het doel (gegevens opgeslagen voor expliciete en legitieme doeleinden die niet worden gebruikt op een manier die onverenigbaar is met die doeleinden);
- beginsel van kwaliteit van de gegevens (relevant, passend, actueel, bewaard voor beperkte duur);
- specifieke regeling voor gevoelige gegevens;
- vereiste inzake veiligheid;
- recht op toegang, rectificatie en beroep;
- mogelijkheid tot afwijking in naam van doorslaggevende publieke of private belangen.

---

547 EHRM, *Airey tegen Ierland* van 9 oktober 1979.

548 "Hoewel artikel 8 voornamelijk tot doel heeft het individu te beschermen tegen de willekeurige inmenging van het openbaar gezag, beperkt het zich er niet toe aan de Staat te bevelen zich te onthouden van dergelijke inmenging: deze veeleer negatieve verbintenis gaat gepaard met positieve verplichtingen die inherent zijn aan de daadwerkelijke eerbieding van het privé-, familie- en gezinsleven. Die verplichtingen kunnen impliceren dat er maatregelen worden getroffen met het oog op de eerbiediging van het privéleven tot in de onderlinge relaties tussen individuen" (vrije vertaling).

549 Zie ook o.a. EHRM, *I.B. tegen Griekenland* van 3 oktober 2013.

550 Voor Richtlijn 95/46, zie *infra*.

In 2001 werd het Verdrag aangevuld met een bijkomend protocol betreffende de toezichthoudende autoriteiten en de grensoverschrijdende gegevensstromen. Het Verdrag nr. 108 is een van de beste rechtsinstrumenten om individuen te beschermen tegen de risico's die gepaard gaan met elektronische monitoring. Het verleent namelijk uitgebreide rechten, zoals een recht van toegang, verbetering of schrapping van persoonsgegevens.

Momenteel wordt het Verdrag gemoderniseerd[551] teneinde de leemtes te vullen die het jammer genoeg nog bevat ten opzichte van de technologische uitdagingen, meer bepaald met betrekking tot de extraterritoriale toepassing.[552]

4. Artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie

Artikel 7 waarborgt het recht op eerbiediging van het privéleven in aansluiting op de overige instrumenten die de mensenrechten beschermen. Artikel 8 heeft een meer originele draagwijdte en bepaalt dat eenieder recht heeft op bescherming van de hem betreffende persoonsgegevens en dat deze gegevens eerlijk moeten worden verwerkt, voor bepaalde doeleinden en op basis van een gerechtvaardigde grondslag (toestemming of andere grondslag waarin de wet voorziet), alsook dat eenieder recht heeft op toegang tot en rectificatie van de over hem verzamelde gegevens. Artikel 7 bekrachtigt dus een autonoom recht op bescherming van persoonsgegevens.

Zoals advocaat-generaal Pedro Cruz Villalon onderstreept in zijn conclusies van 12 december ll.[553], bekrachtigt artikel 8 van het Handvest het recht op bescherming van persoonsgegevens als een recht dat zich onderscheidt van het recht op eerbiediging van het privéleven. Terwijl de bescherming van persoonsgegevens ertoe strekt de eerbiediging van het privéleven te waarborgen, is ze vooral onderworpen aan een autonome regeling die voornamelijk wordt gedefinieerd door Richtlijn 95/46, Richtlijn 2002/58, Verordening nr. 45/2001 en Richtlijn 2006/24, alsook, op het domein dat valt onder de politiële en justitiële samenwerking in strafzaken, door kaderbesluit 2008/977/JBZ.[554]

Omdat de 'privésfeer' de kern van de 'persoonlijke levenssfeer' vormt, valt omgekeerd niet uit te sluiten dat een regelgeving die het recht op bescherming van persoonsgegevens in overeenstemming met artikel 8 van het Handvest beperkt, niettemin kan worden geacht een buitensporige inbreuk op artikel 7 van het Handvest te vormen.[555]

Natuurlijk berust het recht op bescherming van persoonsgegevens op het fundamenteel recht op eerbiediging van het privéleven. Net als het HJEU kunnen we zeggen dat "*les*

---

551 Voorstel tot modernisering van het Raadgevend comité van het Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens, 18 december 2012, STE nr. 108 (T-PD); zie ontwerpaanbeveling www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/T-PD %282013%295rev_fr_Projet%20de%20Rec.%20emploi.pdf; Over de herziening van *Verdrag nr. 108* Staat van de werkzaamheden in uitvoering: www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_fr.asp.

552 *Rapport sur les lacunes de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques,* Cécile de Terwangne, Jean-Philippe Moiny, Yves Poullet en Jean-Marc Van Gyzeghem, November 2010, Bureau van het Raadgevend Comité van het Verdrag nr. 108.

553 Conclusies van advocaat-generaal Pedro Cruz Villalon van 12 december 2013 in de zaken C-293/12 en C-494/12 die hangende zijn voor het HJEU.

554 Zie *infra*.

555 Conclusies van advocaat-generaal Pedro Cruz Villalon, voornoemd.

articles 7 et 8 de la Charte sont étroitement liés, au point de pouvoir être considérés comme établissant un "droit à la vie privée à l'égard du traitement des données à caractère personnel"[556, 557]

5. Richtlijn 95/46/EG van 24 oktober 1995

Richtlijn 95/46 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, die in oktober 1998 in werking is getreden, is de basisnorm in het afgeleid communautair recht. Richtlijn 95/46 heeft tot doel aan de Lidstaten de verplichting op te leggen het recht op eerbiediging van de persoonlijke levenssfeer van natuurlijke personen ten aanzien van de verwerking van hun persoonsgegevens te waarborgen teneinde het vrije verkeer van die gegevens tussen de Lidstaten mogelijk te maken.

Bijgevolg legt ze de inachtneming op van regels die de voorwaarden van rechtmatigheid van de verwerking van persoonsgegevens bepalen, met vermelding van de rechten van personen wiens gegevens worden ingezameld en verwerkt (recht op informatie, recht op toegang en rectificatie of recht van verzet en recht op beroep, en recht op de vertrouwelijkheid en veiligheid van de verwerking).

Deze richtlijn werd aangevuld door Richtlijn 2002/58 van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, die de vertrouwelijkheid van elektronische communicatie waarborgt. De verplichting om deze vertrouwelijkheid te waarborgen ligt bij de aanbieders van voor het publiek toegankelijke elektronische-communicatiediensten. Ze brengt voor de Lidstaten ook de verplichting mee, behoudens uitzondering, om de vertrouwelijkheid te waarborgen van niet alleen de communicatie, maar ook de verkeersgegevens van abonnees en gebruikers van elektronische-communicatiediensten. Artikel 6 verplicht aanbieders van elektronische-communicatiediensten ertoe om verkeersgegevens met betrekking tot abonnees en gebruikers die worden verwerkt en opgeslagen, te wissen of anoniem te maken.

– *Beginselen*

Richtlijn 95/46 heeft tot doel de rechten en vrijheden van personen te beschermen ten opzichte van de verwerking van persoonsgegevens, door beginselen vast te stellen tot bepaling van de rechtmatigheid van die verwerkingen.

Die beginselen[558] hebben betrekking op:

– de kwaliteit van de gegevens: persoonsgegevens moeten meer bepaald eerlijk en rechtmatig worden verwerkt en moeten worden ingezameld om welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Bovendien moeten ze nauwkeurig zijn en zo nodig worden bijgewerkt;

---

556 Arresten C-92/09 en C-93/09 van 9 november 2010.

557 "artikelen 7 en 8 van het Handvest nauw met elkaar zijn verbonden, in die mate dat ze kunnen worden geacht een recht op eerbiediging van het privéleven ten aanzien van de verwerking van persoonsgegevens te vestigen" (vrije vertaling).

558 Zie synthese van de wetgeving op: http://europa.eu/legislation_summaries/information_society/data_protection/l14012_nl.htm (december 2013).

- de *toelaatbaarheid* van de gegevensverwerking: persoonsgegevens mogen alleen worden verwerkt indien de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend of wanneer de verwerking noodzakelijk is:
- voor de uitvoering van een overeenkomst waarbij de betrokkene partij is; of
- om een wettelijke verplichting na te komen waaraan de verantwoordelijke voor de verwerking onderworpen is; of
- ter vrijwaring van een vitaal belang van de betrokkene; of
- voor de vervulling van een taak van algemeen belang; of
- voor de behartiging van het gerechtvaardigd belang van de verantwoordelijke voor de verwerking;
- bijzondere categorieën van verwerking: verboden is de verwerking van persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, alsook de verwerking van gegevens die de gezondheid of het seksuele leven betreffen. Deze bepaling is onder voorbehoud voor bijvoorbeeld het geval waarin de verwerking noodzakelijk is met het oog op de verdediging van de vitale belangen van de betrokkene of voor de doeleinden van preventieve geneeskunde of medische diagnose;
- informatie van de personen die betrokken zijn bij de gegevensverwerking: bepaalde gegevens (identiteit van de verantwoordelijke voor de verwerking, doeleinden van de verwerking, ontvangers van de gegevens …*)* moeten door de verantwoordelijke voor de verwerking worden verstrekt aan de persoon bij wie hij gegevens betreffende die persoon verzamelt;
- het recht van toegang van die personen tot de gegevens: elke betrokkene moet het recht hebben om van de verantwoordelijke voor de verwerking de volgende zaken te verkrijgen:
- uitsluitsel omtrent het al dan niet bestaan van verwerkingen van gegevens betreffende hem en verstrekking van de gegevens die zijn verwerkt;
- de rectificatie, de uitwissing of de afscherming van de gegevens waarvan de verwerking niet overeenstemt met de bepalingen van deze richtlijn, met name op grond van het onvolledige of onjuiste karakter van de gegevens, net als kennisgeving van deze wijzigingen aan derden aan wie de gegevens zijn verstrekt;
- *uitzonderingen en beperkingen*: de reikwijdte van de beginselen betreffende de kwaliteit van de gegevens, de informatieverstrekking aan de betrokkene, het recht van toegang en de openbaarheid van de verwerkingen kan worden beperkt ter vrijwaring, onder meer, van de veiligheid van de Staat, de landsverdediging, de openbare veiligheid, het vervolgen van strafbare feiten, een belangrijk economisch en financieel belang van een Lidstaat of van de EU of de bescherming van de betrokkene;
- het recht van verzet tegen gegevensverwerking: de betrokkene moet het recht hebben zich om gerechtvaardigde redenen te verzetten tegen de verwerking van gegevens die op hem betrekking hebben. De betrokkene moet zich, op verzoek en kosteloos, ook kunnen verzetten tegen de verwerking van gegevens met het oog op direct marketing. Tot slot moet de betrokkene worden ingelicht voordat persoonsgegevens aan derden worden verstrekt voor direct marketing en moet hij het recht ter kennis gebracht krijgen zich tegen deze verstrekking te kunnen verzetten;• de vertrouwelijkheid en beveiliging van de verwerking: eenieder die handelt onder het gezag van de verantwoorde-

lijke voor de verwerking of van de verwerker alsmede de verwerker zelf, die toegang heeft tot persoonsgegevens, mag deze slechts in opdracht van de verantwoordelijke voor de verwerking verwerken. Voorts moet de verantwoordelijke voor de verwerking passende maatregelen nemen om persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang;

– aanmelding van de verwerking bij een toezichthoudende autoriteit: de verantwoordelijke voor de verwerking moet de nationale toezichthoudende autoriteit van tevoren kennis geven van de uitvoering van een verwerking. Na ontvangst van de kennisgeving voert de toezichthoudende autoriteit voorafgaande onderzoeken uit naar mogelijke risico's voor de rechten en vrijheden van de betrokkenen. De openbaarheid van de verwerkingen moet worden gewaarborgd en de toezichthoudende autoriteit moeten een register bijhouden van de aangemelde verwerkingen.

Eenieder kan zich tot de rechter wenden wanneer de rechten die hem worden gegarandeerd door het op de betrokken verwerking toepasselijke nationale recht geschonden worden. Bovendien hebben personen die schade hebben geleden ten gevolge van een onrechtmatige verwerking van hun persoonsgegevens het recht vergoeding van de geleden schade te verkrijgen.

– *Territoriale werkingssfeer*

Deze richtlijn brengt verplichtingen mee voor de aanbieders van internettoegang, zoekmachines, sociale netwerken en andere aanbieders van communicatiediensten die verantwoordelijk zijn voor de verwerking van persoonsgegevens. In ieder afzonderlijk geval kan de omvang van de aansprakelijkheid van de verantwoordelijke voor de gegevensverwerking worden geanalyseerd, meer bepaald ten aanzien van de territoriale werking van Richtlijn 95/46. Krachtens artikel 4 van de richtlijn moet een Staat zijn wetgeving inzake de bescherming van persoonsgegevens ter uitvoering van deze richtlijn toepassen indien de verantwoordelijke voor de verwerking vestiging heeft op zijn grondgebied of in functie van de plaats van de middelen voor de gegevensverwerking, dit wil zeggen indien de middelen voor gegevensverwerking op het grondgebied van deze Staat bevinden.
De werkgroep 'Artikel 29'[559] benadrukte in zijn advies 5/2009 over de bescherming van gegevens door online sociale netwerken[560] dat

> "De richtlijn gegevensbescherming is in de meeste gevallen van toepassing op aanbieders van sociale-netwerkdiensten, ook als hun hoofdkantoor buiten de EER is gevestigd."

Ook een van de voornaamste conclusies van advies 1/2008 over gegevensbescherming en zoekmachines bepaalt dat de richtlijn inzake gegevensbescherming algemeen van toepassing is op de verwerking van persoonsgegevens door zoekmachines, ook al staat hun hoofdkantoor buiten de EER, en dat het aan de betreffende zoekmachines toekomt duide-

559 Deze werkgroep werd opgericht krachtens artikel 29 van Richtlijn 95/46. Het is een Europees adviesorgaan, van wie de taken worden beschreven in artikel 30 van de Richtlijn en in artikel 15 van Richtlijn 2002/58.

560 Groep 29, WP 163 "Advies 5/2009 over online sociale netwerken" van 12 juni 2009.

lijk te maken welke rol zij spelen in de EER en hoe ver hun verantwoordelijkheden overeenkomstig de richtlijn reiken.[561]

De doorgifte van persoonsgegevens van een Lidstaat naar een derde land met een passend niveau van bescherming is toegelaten. Dergelijke doorgiftes zijn echter niet toegelaten wanneer ze bestemd zijn voor een derde land dat niet over een dergelijk niveau van bescherming beschikt, behoudens afwijkingen die op beperkende wijze worden opgesomd.

Bijgevolg past het om de verantwoordelijkheid van elke speler te bepalen in functie van precieze feiten.

– *Uitsluitingen van de materiële werkingssfeer*

Artikel 3, lid 2 van voornoemde richtlijn geeft een van de grenzen van de *materiële werkingssfeer* van de richtlijn aan en bepaalt:

> "De bepalingen van deze richtlijn zijn niet van toepassing op de verwerking van persoonsgegevens:
> – *die met het oog op de uitoefening van niet binnen de werkingssfeer van het Gemeenschapsrecht vallende activiteiten geschiedt zoals die bedoeld in de titels V en VI van het Verdrag betreffende de Europese Unie en in ieder geval verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de Staat (waaronder de economie van de Staat, wanneer deze verwerkingen in verband staan met vraagstukken van Staatsveiligheid), en de activiteiten van de Staat op strafrechtelijk gebied".*

De bescherming van persoonsgegevens in het kader van de openbare veiligheid en het strafrecht wordt dus geregeld in verschillende specifieke instrumenten. Het gaat met name om instrumenten waarbij gemeenschappelijke informatiesystemen op Europees niveau worden ingesteld, zoals de Schengenuitvoeringsovereenkomst met specifieke gegevensbeschermingsbepalingen die gelden voor het Schengeninformatiesysteem (SIS); de overeenkomst op grond van artikel K.3 van het Verdrag betreffende de Europese Unie tot oprichting van een Europese Politiedienst; het besluit van de Raad betreffende de oprichting van Eurojust en de beschikkingen van het interne reglement van Eurojust betreffende de verwerking en bescherming van persoonsgegevens; de Overeenkomst op grond van artikel K.3 van het Verdrag betreffende de Europese Unie inzake het gebruik van informatica op douanegebied, met de gegevensbeschermingsbepalingen die van toepassing zijn op het douane-informatiesysteem, en de Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de Lidstaten van de Europese Unie.[562] Op 27 november 2008 keurde de Raad kaderbesluit 2008/977/JBZ van de Raad goed over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en gerechtelijke samenwerking in strafzaken. Deze is echter alleen van toepassing op de doorgifte van gegevens tussen Lidstaten (artikelen 26 en 13).

---

561 Groep 29, WP 148 "Advies 1/2008 over gegevensbescherming en zoekmachines" van 4 april 2008.

562 HJEU, arresten C-317/04 en C-318/04 van 30 mei 2005, conclusies van advocaat-generaal LEGER, punt 41.

6. *Richtlijn 2006/24/EG betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van elektronische communicatiediensten*

Richtlijn 2006/24 is in deze belangrijk omdat ze wijzigingen aanbrengt aan richtlijnen 95/46 en 2002/58 door te bepalen dat de Lidstaten een verplichting moeten opleggen inzake het verzamelen en bewaren van verkeers- en lokalisatiegegevens, namelijk door aan de aanbieders van openbaar beschikbare elektronische communicatiediensten of openbare communicatienetwerken verplichtingen op te leggen inzake de bewaring van de verkeers- en lokalisatiegegevens die zij bepaalt, teneinde hun beschikbaarheid te waarborgen "voor het onderzoeken, opsporen en vervolgen van zware criminaliteit zoals gedefinieerd in de nationale wetgevingen van de Lidstaten". Aldus wijkt deze richtlijn af van de afwijkende regels zoals vastgesteld door artikel 15, lid 1 van Richtlijn 2002/58 die de mogelijkheid regelen, voor de Lidstaten, om de reikwijdte van het recht op bescherming van persoonsgegevens en, algemener, het recht op eerbiediging van het privéleven in het specifieke kader van de levering van elektronische communicatiediensten of openbare communicatienetwerken te beperken om de redenen zoals bepaald in artikel 13, lid 1 van Richtlijn 95/46.
Richtlijn 2006/24 heeft tot doel een harmonisatie tot stand te brengen van de regelgevingen van de Lidstaten betreffende de bewaring van verkeers- en lokalisatiegegevens inzake elektronische communicatie en legt bijgevolg aan de Lidstaten die niet over dergelijke regelgeving zouden beschikken, een verplichting op om de voornoemde gegevens te verzamelen en te bewaren.
Volgens advocaat-generaal Pedro Cruz Villalon (12 december 2013) is deze verplichting die de richtlijn aan de Lidstaten oplegt in strijd met het Handvest van de grondrechten.[563]
Het HJEU moet nog een arrest vellen.
Het is interessant om de motivering van de advocaat-generaal hier over te nemen[564]:

> "72. Dat neemt niet weg dat het verzamelen en vooral het bewaren, in gigantische databases, van de talloze gegevens die zijn gegenereerd of verwerkt in het kader van het grootste deel van de gebruikelijke elektronische communicatie van de burgers van de Unie, een duidelijke inmenging in hun privéleven vormt, ook al worden daarmee enkel de voorwaarden geschapen om achteraf hun persoonlijke alsook beroepsmatige activiteiten te kunnen controleren. Het verzamelen van deze gegevens creëert de voorwaarden voor een toezicht dat, ook al wordt dit slechts met terugwerkende kracht uitgevoerd bij de exploitatie van de gegevens, niettemin, zolang de gegevens worden bewaard, het recht van de burgers van de Unie op vertrouwelijkheid van hun persoonlijke levenssfeer permanent bedreigt. Het opgewekte vage gevoel van gecontroleerd worden leidt bijzonder acuut tot de vraag wat de bewaringstermijn van de gegevens is.
> *73. Dienaangaande moet ten eerste rekening worden gehouden met het feit dat de gevolgen van deze inmenging worden verveelvoudigd door de plaats die de elektronische communicatiemiddelen in de moderne samenleving hebben ingenomen, of het nu gaat om digitale mobiele netwerken dan wel om internet, en het massale en intensieve gebruik ervan door een zeer groot deel van de Europese burgers op alle terreinen van hun privé- of beroepsactiviteiten.*
> *74. De betrokken gegevens, zo wil ik nogmaals benadrukken, zijn geen persoonsgegevens in de klassieke zin des woords die verband houden met precieze informatie over de identiteit van perso-*

563 Conclusies in de zaken C-293/12 en C-494/12 die hangende zijn voor het HJEU.
564 De verwijzingen zijn weggelaten met het oog op de leesbaarheid; zie de verwijzing in de vorige voetnoot.

nen, maar in feite 'gekwalificeerde' persoonsgegevens, die, wanneer zij worden geëxploiteerd, een belangrijk deel van het gedrag van een persoon, dat strikt onder zijn privéleven valt, op getrouwe en uitputtende wijze in kaart kunnen brengen of zelfs een volledig en precies beeld kunnen schetsen van zijn privé-identiteit.
75. De intensiteit van deze inmenging wordt des te duidelijker door factoren die het risico vergroten dat de bewaarde gegevens, ondanks de verplichtingen die door richtlijn 2006/24 aan zowel de lidstaten zelf als de aanbieders van elektronische communicatiediensten worden opgelegd, worden gebruikt voor onrechtmatige doeleinden die potentieel inbreuk maken op het privéleven, of ruimer, voor frauduleuze of zelfs kwaadwillende doeleinden.
76. Deze gegevens worden namelijk niet bewaard door de autoriteiten zelf of zelfs maar onder hun directe toezicht, maar door de aanbieders van elektronische communicatiediensten, op wie het merendeel van de verplichtingen rust die als waarborg van de bescherming en de veiligheid van de gegevens moeten dienen."

En verder:

"102. De duidelijke inmenging in recht op eerbiediging van het privéleven die de lidstaten, als gevolg van de constitutieve werking van richtlijn 2006/24 geacht worden op te nemen in hun eigen rechtsorde, lijkt aldus buiten verhouding te staan tot enkel de noodzaak om de werking van de interne markt te waarborgen, ook al worden dit verzamelen en bewaren overigens als geschikte en zelfs noodzakelijke middelen beschouwd ter bereiking van de uiteindelijke doelstelling van de richtlijn, namelijk ervoor zorgen dat de gegevens beschikbaar zijn voor het opsporen en vervolgen van zware criminaliteit. Samenvattend zou richtlijn 2006/24 de evenredigheidstoets niet doorstaan op basis van de redenen die de keuze van haar rechtsgrondslag rechtvaardigden. Paradoxaal genoeg zouden de redenen die haar sauveerden vanuit het oogpunt van de rechtsgrondslag, de redenen zijn waarom zij geen stand houdt in het licht van de evenredigheid."

Alvorens te besluiten:

"131. Concluderend meen ik dat richtlijn 2006/24 in haar geheel onverenigbaar is met artikel 52, lid 1, van het Handvest, aangezien de beperkingen die zij aan de uitoefening van de grondrechten stelt door de opgelegde verplichting tot het bewaren van gegevens, niet gepaard gaan met de onmisbare beginselen die hebben te gelden voor de waarborgen waarmee de toegang tot deze gegevens en de exploitatie ervan behoren te zijn omkleed."

7. Safe Harbor-akkoord ('veilige haven') – Beschikking van de Commissie van 26 juli 2000[565]

De normen inzake bescherming van de persoonlijke levenssfeer in Europa enerzijds en de Verenigde Staten anderzijds verschillen duidelijk van elkaar en meer bepaald in de Ver-

565 Beschikking van de Commissie van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende vaak gestelde vragen, die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd document C(2000) 2441 (http://eur lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:NL:PDF).

enigde Staten biedt het recht op eerbiediging van het privéleven zoals hierboven omschreven nagenoeg geen bescherming voor wie niet in de VS verblijft.[566]

Het bleek dan ook noodzakelijk om een rechtskader te creëren dat geschikt is om de doorgifte van gegevens *voor commerciële doeleinden* van de Europese Economische Ruimte[567] naar de Verenigde Staten mogelijk te maken.

Dit rechtskader was des te noodzakelijker omdat, zoals we hebben gezien, de specifieke regels van Richtlijn 95/46 betreffende het uitwisselen van gegevens met derde Staten de doorgifte verbiedt van persoonsgegevens buiten Staten die geen lid zijn van de EER en die minder bescherming van persoonsgegevens zouden bieden dan de EER.

De Verenigde Staten beschikken over een systeem voor de bescherming van de gegevens van hun burgers dat niet voldoet aan dezelfde normen degene die binnen de EER zijn aangenomen. Zonder het *Safe Harbor*-systeem hadden de door Richtlijn 95/46 ingestelde vereisten een obstakel kunnen vormen voor de trans-Atlantische uitwisselingen en transacties, omdat het gebrek aan naleving van de Europese regels betreffende persoonsgegevens door een Amerikaanse onderneming de commerciële onderhandelingen had kunnen vertragen of opschorten of zelfs had kunnen leiden tot gerechtelijke vervolgingen in geval van schending van de toepasselijke regels.

Het rechtskader van de 'veilige haven' of *Safe Harbor* slaat de brug tussen beide visies op de eerbiediging van het privéleven door een gemeenschappelijke noemer in het leven te roepen die Amerikaanse ondernemingen en organisaties in acht moeten nemen en die de doorgifte van persoonsgegevens mogelijk maakt met inachtneming van het recht van de EER.

Het *Safe Harbor*-akkoord werd gesloten tussen de Amerikaanse *Federal Trade Commission* (*FTC*) en de Europese Commissie met als doel Amerikaanse ondernemingen in staat stellen te certificeren dat ze de EER-wetgeving in acht nemen om aldus de toelating te verkrijgen persoonsgegevens voor commerciële doeleinden door te geven van de EER naar de Verenigde Staten.

Bijlage I van de beschikking van 26 juli 2000 bepaalt dat "persoonsgegevens en persoonlijke informatie gegevens zijn over een specifieke of een identificeerbare persoon die binnen de werkingssfeer van de richtlijn vallen, vanuit de Europese Unie door een organisatie in de Verenigde Staten worden ontvangen en in de een of andere vorm zijn vastgelegd."

Indien een Amerikaanse onderneming schriftelijk verklaart de Veiligehavenbeginselen te onderschrijven, dan zou de Europese onderneming in principe persoonsgegevens naar die onderneming moeten kunnen uitvoeren.

– *Beginselen*

Het rechtskader van *Safe Harbor* berust op zeven beginselen die de onderneming die de certificering wenst te verkrijgen in acht moet nemen. Deze beginselen worden uitvoerig beschreven in Bijlage I van de Beschikking van de Commissie van 26 juli 2000 betreffende

566 Nota van het Directoraat-generaal intern beleid, Beleidsondersteunende afdeling C: Rechten van de burgers en constitutionele zaken, IPOL-LIBE_NT(2013)474405_FR.

567 Hierna "EER"; *Safe Harbor* werd opgenomen in het akkoord over de EER, zodat IJsland, Liechtenstein en Noorwegen niet worden beschouwd als derde Staten bij de toepassing van deze norm.

de gepastheid van de bescherming geboden door de Veiligehavenbeginselen en zijn grotendeels geïnspireerd op de beginselen van Richtlijn 95/46:
- Kennisgeving: in kennis stellen van personen,
- Keuze: de mogelijkheid voor de betrokkene om zich te verzetten tegen een doorgifte aan derden of tegen het gebruik van de gegevens om andere doeleinden, de expliciete toestemming van de personen voor het verzamelen van gevoelige informatie,
- Verdere doorgifte: de beginselen inzake kennisgeving en keuze zouden van toepassing moeten zijn op de doorgifte van gegevens aan derden,
- Beveiliging: maatregelen tot bescherming van de gegevens,
- Integriteit van de gegevens: kwaliteit en gepastheid van de gegevens,
- Toegang: het recht op toegang, correctie, verwijdering van gegevens,
- Rechtshandhaving: recht op verhaal, procedures van opvolging en sancties.[568]

Op te merken valt echter dat de beginselen worden omschreven in vage bewoordingen die open staan voor een interpretatie die bovendien onderworpen is aan het Amerikaans recht.

Het proces berust op een systeem van vrijwillige zelfcertificering door Amerikaanse ondernemingen en voorziet in een hernieuwing van de certificering om de twaalf maanden. De onderneming die een certificering wenst te verkrijgen, moet aan de *Federal Trade Commission* een jaarlijkse schriftelijke verklaring bezorgen waarin ze bevestigt de Veiligehavenbeginselen in acht te nemen. De *Federal Trade Commission* heeft de taak het certificeringsprogramma te beheren en te waken over de uitvoering ervan. Ze kan vorderingen in rechte instellen tegen een onderneming die in gebreke blijft of administratieve boetes opleggen aan ondernemingen die ondanks hun verklaring de Veiligehavenbeginselen *de facto* niet in acht nemen.

Eens de Amerikaanse onderneming een *Safe Harbor*-certificering heeft verkregen, wordt ze toegevoegd aan de lijst van geaccrediteerde ondernemingen die de *Federal Trade Commission* bijhoudt. De lijst telt 3.246 ondernemingen en kan worden geraadpleegd op de website van de Federal Trade Commission.[569]

Het *Safe Harbor*-systeem bepaalt ook dat de klachten van EER-burgers tegen een Amerikaanse onderneming of organisatie betreffende de bescherming van persoonsgegevens voor een Amerikaans rechtscollege moeten worden ingediend (behoudens enkele uitzonderingen).

In de praktijk gaat het er echter anders aan toe, zoals blijkt uit de recente studie in opdracht van het Europees Parlement over het *Safe Harbor-systeem:* "De Amerikaanse onderhandelaars van het ministerie van handel hebben nauw samengewerkt met de Amerikaanse commerciële lobby's om een lijst van 'vaak gestelde vragen' op te stellen die het voor Amerikaanse ondernemingen mogelijk maken het Veiligehavenakkoord op zodanige wijze te interpreteren dat de rechten van de EU inzake de bescherming van de persoonlijke levenssfeer worden beperkt en die aangeven hoe ze de regels inzake identificeerbare gegevens kunnen omzeilen, het recht op toegang kunnen weigeren en zich kunnen onttrekken aan elke plicht tot finaliteit of elk verzoek tot schrapping. De veilige haven is

---

568 Voor een gedetailleerde beschrijving van de 7 beginselen, zie Bijlage I van de beschikking van de Commissie van 26 juli 2000 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:NL:PDF).

569 http://export.gov/safeharbor/ (eind september 2013).

zo complex gebleken dat er jarenlang geen enkele EU-burger is geweest die alle stappen van het bureaucratisch proces om klacht in te dienen heeft doorlopen." (vrije vertaling).[570]

Richtlijn 95/46 en de *Veiligehavenbeginselen* hebben geen betrekking op persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken[571], wat alle politie-, gerechts- en inlichtingenbestanden omvat. Artikel 1 van de Beschikking van de Commissie van 26 juli 2000 betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen bepaalt immers dat de beschikking alleen van toepassing is op activiteiten die binnen de werkingssfeer van Richtlijn 95/46 vallen.

Voorts bepaalt Bijlage I lid 4 van voornoemde beschikking dat "de naleving van de beginselen kan worden beperkt: a) voor zover dit nodig is om aan de *eisen van de nationale veiligheid*, het algemeen belang en de rechtshandhaving van de Verenigde Staten te voldoen; b) door wettelijke of bestuursrechtelijke bepalingen of rechtspraak die tegenstrijdige verplichtingen of uitdrukkelijke machtigingen scheppen, mits een organisatie die van een dergelijke machtiging gebruikmaakt, kan aantonen dat de niet-naleving van de beginselen beperkt is tot de mate die nodig is om de met de machtiging beoogde hogere legitieme belangen te waarborgen; c) indien de richtlijn of de wetgeving van de betrokken lidstaat uitzonderingen of afwijkingen toestaat, mits deze ook in vergelijkbare contexten worden toegepast."

De uitwisseling van persoonsgegevens tussen de Europese Unie en de Verenigde Staten voor rechtshandhavingsdoeleinden, met inbegrip van het voorkomen en bestrijden van terrorisme en andere vormen van zware criminaliteit, is, althans in theorie, geregeld in een aantal overeenkomsten op EU-niveau. Het gaat om de overeenkomst inzake wederzijdse rechtshulp, de overeenkomst inzake het gebruik en de doorgifte van persoonsgegevens van passagiers (PNR), de overeenkomst inzake de verwerking en doorgifte van gegevens betreffende het financiële-berichtenverkeer ten behoeve van het programma voor het traceren van terrorismefinanciering (TFTP), evenals de overeenkomst tussen Europol en de Verenigde Staten.

– *Lacunes*

Als gevolg van de verschillende onthullingen die we hier analyseren met betrekking tot Amerikaanse programma's voor het verzamelen van inlichtingen op grote schaal is het vertrouwen dat vooral op grond van de Veiligehavenbeginselen was opgebouwd, ernstig aan het wankelen gebracht. Die onthullingen hebben het besef doen ontstaan dat de huidige bescherming van persoonsgegevens ontoereikend is en dat het noodzakelijk is om de bestaande regels, die *ernstige lacunes* vertonen, te herbekijken en te versterken.

Sinds de *FISA* werd geamendeerd en uitgebreid, meer bepaald in 2008, kunnen Amerikaanse ondernemingen er namelijk toe worden gedwongen om aan het NSA elektronische informatie over niet-Amerikanen te bezorgen. Artikel 702 van de FISA[572] vormt een algemene volmacht die het de Amerikaanse autoriteiten mogelijk maakt om gegevens te

---

570 Le programme de surveillance des Etats-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE, Nota van het Directoraat-generaal intern beleid, Beleidsondersteunende afdeling C: Rechten van de burger en constitutionele zaken, IPOL-LIBE_NT(2013)474405_FR. http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT%28 2013%29474405_FR.pdf.

571 Artikel 25 van Richtlijn 95/46.

572 Foreign Intelligence Surveillance Act van 1978 (beschrijft de procedures van fysieke en elektronische monitoring evenals het verzamelen van informatie bij vreemde mogendheden, hetzij

verzamelen en informatie te onderscheppen die betrekking heeft op de buitenlandse aangelegenheden van de Verenigde Staten, terwijl de persoonsgegevens van Amerikanen een betere bescherming genieten. De mogelijke omvang van een dergelijke bevoegdheidsoverdracht komt vandaag op duidelijke en onevenredige wijze naar voren in het licht van de onthullingen van Snowden en de technologische ontwikkelingen die de captatie van immense hoeveelheden gegevens op wereldniveau mogelijk maken.

Op 27 november 2013 publiceerde de Europese Commissie[573] het resultaat van haar overleg in (1) een strategiedocument (mededeling) over trans-Atlantische gegevensstromen waarin de problemen en risico's worden uiteengezet die voortvloeien uit de onthullingen over Amerikaanse programma's voor het verzamelen van inlichtingen, alsook de stappen die moeten worden ondernomen om deze problemen aan te pakken, (2) een analyse van de werking van 'Safe Harbor' (veilige haven) dat het doorgeven van gegevens voor commerciële doeleinden tussen de EU en de VS regelt, en (3) een verslag van over de bevindingen van de EU-VS-werkgroep (MEMO/13/1059) over gegevensbescherming, die in juli 2013 is opgericht.

Uit dit rapport blijkt ook dat grote bedrijven die actief zijn in de nieuwe technologieën en die aan de operatie *PRISM* hebben deelgenomen over een *Safe Harbor*-certificering beschikken, zodat we kunnen besluiten dat het *Safe Harbor*-systeem kan worden beschouwd als een belangrijk kanaal voor persoonsgegevens dat tot de grootschalige inzameling van gegevens door het NSA heeft geleid.

Hoewel deze praktijken door de Amerikaanse wet zijn toegelaten, zijn ze niet voorzien in het rechtskader van de *Safe Harbor*, zodat ze plaats hebben gevonden bij inbreuk op dit akkoord en op de beschikking van de Commissie die het akkoord formaliseert in het Europees rechtskader. Omdat de *Safe Harbor*-beginselen zijn vastgesteld om voor de Verenigde Staten een 'passend beschermingsniveau' te waarborgen dat borg staat voor een bescherming van persoonsgegevens op een niveau dat in de buurt komt van het beschermingsniveau binnen de EER, moeten we beschouwen dat de Verenigde Staten de geest van het akkoord in hun voordeel hebben omgebogen. Het *Safe Harbor*-systeem werd geenszins gecreëerd om de doorgifte mogelijk te maken van gegevens die vervolgens massaal aan de Amerikaanse veiligheidsautoriteiten kunnen worden bezorgd, terwijl de Europese veiligheidsautoriteiten niet op dezelfde wijze kunnen handelen.

Volgens de Europese Commissie kan de grootschalige onderschepping van persoonsgegevens door het NSA niet worden geacht te zijn gedekt door de beperking van de gegevensbescherming zoals bedoeld in het *Safe Harbor*-akkoord, met het oog op de nationale veiligheid. Als gevolg van de grootschaligheid en het feit dat er geen voorafgaande toestemming is verleend om gegevens op te slaan, kan dit proces immers niet worden beschouwd als noodzakelijk en in verhouding staand tot de belangen van de nationale veiligheid. Omdat er sprake is van een inbreuk op een fundamenteel mensenrecht, moet deze op restrictieve wijze worden beoordeeld, zoals bedoeld en beperkt door de wet.

Voorts stelt de Europese Commissie ook haar nieuwe onderzoek voor naar de bestaande akkoorden over passagiersgegevens (PNR) (MEMO/13/1054) en naar het programma voor het traceren van terrorismefinanciering (TFTP), die de uitwisseling van gegevens voor repressieve doeleinden in deze sectoren regelen.

---

rechtstreeks, hetzij door uitwisseling van informatie met andere vreemde mogendheden), zoals gewijzigd in 2008 door de FISA Amendments Act.

573 Newsroom van de Europese Commissie: http://europa.eu/rapid/press-release_MEMO-13-1059_nl.htm.

In deze mededeling geeft de Commissie meer bepaald blijk van haar wil om uiterlijk in het voorjaar van 2014 een hervorming van de gegevensbescherming in de EU goed te keuren om ervoor te zorgen dat persoonsgegevens effectief en volledig worden beschermd.

Met betrekking tot de trans-Atlantische relaties heeft de Commissie bovendien *13 aanbevelingen gedaan om de werking van de veiligehavenregeling te verbeteren*, nadat uit een op dezelfde dag bekendgemaakte analyse is gebleken dat de werking van de regeling op verscheidene punten tekortschiet. Het geheel van regels zou dus moeten worden herzien en verbeterd.

Op het vlak van de politiële en justitiële samenwerking in strafzaken zou de Commissie druk willen uitoefenen op de Amerikaanse regering opdat zij zich ertoe zou verbinden, als algemeen beginsel, gebruik te maken van een rechtskader zoals de sectorale overeenkomsten en de overeenkomsten inzake wederzijdse rechtshulp die tussen de EU en de Verenigde Staten zijn gesloten (bv. de overeenkomst over PNR en het programma voor het traceren van terrorismefinanciering) telkens wanneer de doorgifte van gegevens vereist is voor rechthandhavingsdoeleinden. Rechtstreekse verzoeken aan de ondernemingen mogen alleen mogelijk zijn in welbepaalde, uitzonderlijke en door de rechter toetsbare situaties.

Meer algemeen heeft de Europese Commissie verklaard te wensen dat de door de Amerikaanse president aangekondigde evaluatie van de activiteiten van de nationale veiligheidsautoriteiten voorziet in de bescherming van EU-burgers die hun verblijfplaats buiten de USA hebben. Die laatsten zouden dezelfde waarborgen moeten genieten als Amerikaanse burgers.

– *Globale hervorming van de regels inzake gegevensbescherming*

Zoals aangekondigd in januari 2012[574] werkt de Commissie aan een globale hervorming van de gegevensbescherming. De hervorming wil de beginselen van de gegevensbeschermingsrichtlijn van 1995 actualiseren en moderniseren om de privacyrechten te waarborgen in de toekomst. Deze hervorming omvat twee wetgevingsvoorstellen: een *verordening* tot vaststelling van het algemene EU-kader voor gegevensbescherming en een *richtlijn* inzake de bescherming van persoonsgegevens die worden verwerkt voor het voorkomen, opsporen, onderzoeken of vervolgen van strafbare feiten en aanverwante gerechtelijke activiteiten.

De hervorming beoogt meer bepaald de volgende voornaamste wijzigingen[575]:

– "*Eén stel regels inzake gegevensbescherming, geldend in de gehele EU*. Overbodige administratieve formaliteiten, zoals sommige verplichte meldingen door bedrijven, worden afgeschaft. Dit moet hen circa 2,3 miljard euro aan kosten per jaar besparen.
– Elk bedrijf is momenteel verplicht om alle maatregelen inzake gegevensbescherming aan de toezichthouders te melden, wat overbodige administratieve lasten meebrengt en bedrijven jaarlijks 130 miljoen euro kost. In plaats daarvan verplicht de verordening de verwerkers van persoonsgegevens meer verantwoording en rekenschap af te leggen.
– Zo moeten bedrijven en organisaties ernstige gegevenslekken zo snel mogelijk (zo mogelijk binnen 24 uur) aan de nationale toezichthouder melden.
– Organisaties krijgen te maken met slechts één nationale gegevensbeschermingsautoriteit, in de EU-lidstaat waar zij hun belangrijkste vestiging hebben. Insgelijks is de nationale gegevensbeschermingsautoriteit het aanspreekpunt voor burgers, ook als hun gegevens worden verwerkt door een bedrijf dat buiten de EU is gevestigd. Wanneer voor de verwerking van gegevens toestemming vereist is, moet deze uitdrukkelijk worden gegeven, en niet worden verondersteld stilzwijgend te zijn gegeven.

574 Persbericht: http://europa.eu/rapid/press-release_IP-12-46_nl.htm.
575 Persbericht: http://europa.eu/rapid/press-release_IP-12-46_nl.htm.

- Mensen zullen gemakkelijker toegang krijgen tot hun eigen gegevens en hun persoonsgegevens gemakkelijker van de ene dienstverstrekker naar de andere kunnen overdragen (recht op gegevensoverdraagbaarheid), wat de onderlinge concurrentie zal vergroten.
- Een 'recht om te worden vergeten' moet mensen in staat stellen om privacyrisico's op internet beter te beheren, d.w.z. hun gegevens te wissen als er geen gegronde redenen zijn om ze te bewaren.
- De EU-regels zijn van toepassing wanneer persoonsgegevens *buiten de EU worden verwerkt* door bedrijven die op de markt van de EU actief zijn en hun diensten aan EU-burgers aanbieden.
- Onafhankelijke nationale gegevensbeschermingsautoriteiten zullen meer bevoegdheden krijgen om de EU-regels op hun grondgebied te doen eerbiedigen, onder meer om boetes op te leggen aan bedrijven die die regels overtreden. Die boetes kunnen oplopen tot 1 miljoen euro of tot 2% van de totale jaarlijkse omzet van een bedrijf.
- In een nieuwe *richtlijn zullen grondbeginselen en algemene regels worden vastgesteld voor de bescherming van persoonsgegevens in het kader van de politiële en justitiële samenwerking in strafzaken*. De voorschriften zullen zowel op binnenlandse als grensoverschrijdende gegevensoverdrachten van toepassing zijn."

B. SOEVEREINITEIT VAN BELGIË

Het traceerprogramma waarvan sprake in deze studie steunt duidelijk op een internationale structuur waaraan zeker de Verenigde Staten (NSA) en het Verenigd Koninkrijk (*GCHQ)* deelnemen, maar wellicht nog andere Lidstaten van de Raad van Europa en de Europese Unie. Die laatste werden wellicht 'ingehaald' door de structuur waaraan ze hebben meegewerkt en zijn zelf het slachtoffer geworden van de grootschalige controleoperaties.

Laten we niet vergeten dat het UKUSA-akkoord betreffende inlichtingen inzake telecommunicatie, dat in 1947 werd gesloten door vijf Angelsaksische landen (Verenigde Staten, Verenigd Koninkrijk, Canada, Nieuw-Zeeland en Australië), het basisakkoord is voor de controle van communicatie in de ruime betekenis en al aan de basis stond van de ruggengraat van het controlesysteem Echelon, dat in de jaren 2000 voor schokgolven zorgde in Europa. De uitstekende studie van Dimitri Yernault over dit afluistersysteem is nog steeds brandend actueel en zou hier bijna volledig kunnen worden overgenomen.[576]

Een fundamentele vraag rond de grootschalige controle van elektronische communicatie zonder instemming van de Staat op wiens grondgebied de controle plaats heeft, zelfs vanaf een installatie op het grondgebied van een derde Staat, bestaat erin te weten of ze de soevereiniteit van die Staat schendt. Het antwoord is positief indien de Staat er niet mee heeft ingestemd, zelfs indien de afluisteroperaties conform zijn aan het recht van de Staat die ze uitvoert (rechtstreeks of via handelsondernemingen die er vrijwillig of gedwongen aan deelnemen): dit type afluisteroperaties schendt de soevereiniteit van de Staat op wiens grondgebied de communicaties worden onderschept.

---

576 Dimitri Yernault, De la fiction à la réalité: le programme d'espionnage électronique global "Echelon" et la responsabilité internationale des Etats au regard de la convention européenne des droits de l'homme, *RBDI,* 2000, p. 137 e.v.

Het onderscheppen van communicatie is namelijk per definitie een daad van dwang – clandestien of toegestaan door de wetgeving van de derde Staat – die wordt uitgeoefend op het grondgebied van een andere Staat en zijn soevereiniteit schendt.[577]

De Staat op wiens grondgebied de dwang wordt uitgeoefend, moet zijn voorafgaande toestemming geven.[578] Gebeurt dat niet, dan schenden de afluisteroperaties, de controle, de clandestiene onderschepping en *a fortiori* de operaties door *malware*systemen de soevereiniteit van die Staat. Aldus kan die dwang een diplomatieke reactie rechtvaardigen.

Hetzelfde geldt voor de clandestiene afluisteroperaties vanuit ambassades van derde Staten op het grondgebied van de Staat waar de afluister- en controleoperaties plaatsvinden. Ook die kunnen de goede diplomatieke relaties in gevaar brengen.

Ze vormen immers een inbreuk op het Verdrag van Wenen inzake diplomatiek verkeer van 18 april 1961, meer bepaald op artikel 3d, dat voor de diplomatieke zending [alleen] het volgende mogelijk maakt:

d) het met alle wettige middelen nagaan van de toestanden en ontwikkelingen in de ontvangende Staat en het uitbrengen van verslag daarvan aan de regering van de zendstaat;

Krachtens artikel 41.1 hebben diplomatieke zendingen de plicht "de wetten en regelingen van de ontvangende Staat te eerbiedigen. Ze hebben ook de plicht zich niet in te laten met de binnenlandse aangelegenheden van die Staat." Voor het overige mogen de gebouwen van de zending, overeenkomstig artikel 41.3, niet worden gebruikt op een wijze die onverenigbaar is met de functie van de zending, die, zoals we net hebben gezien, alleen inlichtingen mag inwinnen met behulp van wettige middelen (voornoemd artikel 3d).

Tot slot bepaalt artikel 27.1: "1. Door de ontvangende Staat wordt aan de zending toegestaan voor alle officiële doeleinden onbelemmerd verbindingen te onderhouden; deze verbindingen worden door de ontvangende Staat beschermd. Ten einde zich met de regering en met andere zendingen en consulaire posten – waar deze zich ook mogen bevinden – van de zendstaat in verbinding te stellen, mag de zending alle daarvoor in aanmerking komende middelen gebruiken, diplomatieke koeriers en codeberichten daarbij inbegrepen. De zending mag evenwel geen radiozender installeren en gebruiken zonder toestemming van de ontvangende Staat."

Het spreekt voor zich dat dit type clandestiene en ongecontroleerde onderschepping van communicatie op zich het recht op privacy schendt zoals het wordt beschermd door de voornoemde bepalingen en tot gevolg heeft dat de Staat internationaal aansprakelijk wordt, ongeacht of die Staat al dan niet lid is van de Raad van Europa of de Europese Unie. Is dat het geval, dan gaat de internationale aansprakelijkheid voor schending van de soevereiniteit van de Staat gepaard met de schending van de internationale verdragen die van toepassing zijn op het recht op eerbiediging van het privéleven.

C. OVERZICHT VAN DE ACTIEMIDDELEN TER BESCHIKKING VAN DE STAAT, BURGERS EN BEDRIJVEN

Natuurlijk is het onmogelijk, tenzij er precieze bewezen feiten aanhangig worden gemaakt die in specifieke gevallen worden aangeklaagd, om alle mogelijke rechtsmiddelen te bestu-

577 PHIJ, *Lotus case,* 7 september 1927, *Recueil,* Série A, nr. 9, p. 18.

578 Zie de werkzaamheden van het Institut de droit international, *Annuaire de droit international,* vol. 68-I, 1999; zie ook Dimitri Yernault, *op. cit.,* p. 180.

deren in een zaak met een dergelijke reikwijdte zoals die welke E. Snowden heeft aangeklaagd en waarin alle verantwoordelijken nog niet zijn aangewezen. Een van de te voeren acties zou erin kunnen bestaan te vragen dat er een parlementair onderzoek wordt gehouden om de feiten en de elementen van verantwoordelijkheid van de betrokkenen nauwkeurig vast te stellen. De Staat op wiens grondgebied structurele inbreuken op de mensenrechten worden begaan, is algemeen verplicht die te 'voorkomen' of te bestraffen.[579] Die Staat kan dus niet onverschillig blijven. In dit geval lijkt het duidelijk dat de grootschalige controle van persoonsgegevens door het NSA en/of andere spelers op het Belgisch grondgebied van structurele aard is.

In deze fase kunnen we hier alleen maar enkele pistes naar voren schuiven.

1. Internationaal Gerechtshof

De Staat kan het internationaal geschil, dit wil zeggen de internationale aansprakelijkheid van de vreemde Staat die de illegale afluisterpraktijken heeft begaan of die heeft toegestaan dat dergelijke afluisterpraktijken hebben plaatsgevonden, bijvoorbeeld door zijn grondgebied ter beschikking te stellen voor het onderscheppen en illegaal afluisteren, voor het Internationaal Gerechtshof brengen indien de zeer restrictieve voorwaarden betreffende de bevoegdheid van dit Hof vervuld zijn. De vraag betreffende de naleving van het Verdrag van Wenen inzake diplomatiek verkeer en consulaire betrekkingen kan bij hetzelfde Hof aanhangig worden gemaakt.

2. Europees Hof voor de Rechten van de Mens[580]

Indien de Staat die aansprakelijk is voor de controle of eraan heeft meegewerkt lid is van de Raad van Europa, dan is een transnationaal beroep voor het Europees Hof voor de Rechten van de Mens een rechtsmiddel om de schendingen te doen ophouden en schadevergoeding te verkrijgen. Een dergelijk beroep werd ernstig overwogen in de zogenaamde zaak 'Echelon'.[581] Indien in deze zaak het bewijs zou worden geleverd van interventies van de geheime diensten van het Verenigd Koninkrijk of andere Staten die het EVRM hebben ondertekend, dan zou het om een exemplarische actie gaan.

3. Belgische gerechten: hacking en strafbare feiten

– Belgische bedrijven die het slachtoffer zijn van illegale onderschepping van gegevens in hun bezit kunnen – naargelang de feiten – klacht indienen tegen de vreemde Staat voor de gerechten van de betrokken Staat, maar ook voor de Belgische gerechten indien bewezen is dat de feiten een verband hebben met België (onderschepping in België). Zo kan de malware die het informaticasysteem van Belgacom lijkt te hebben besmet, het voorwerp zijn van een rechtsvordering in België. Een nauwkeuriger uiteenzetting van de feiten is echter noodzakelijk om een juridische studie aan deze mogelijkheid te wijden.

---

579 Zie meer bepaald Dimitri Yernault, op. cit., p. 214.

580 Dit beroep lijkt efficiënter dan een beroep voor het Mensenrechtencomité, maar deze mogelijkheid mag niet worden uitgesloten.

581 Zie Dimitri Yernault, *op. cit.,* p. 154 e.v.

– In de mate waarin specifieke bepalingen betreffende de bescherming van persoonsgegevens daarin voorzien, kunnen ze natuurlijk van toepassing zijn op private personen zodra die verantwoordelijk zijn voor de verwerking van persoonsgegevens in de betekenis van de hierboven bestudeerde bepalingen. Dit is meer bepaald het geval met de richtlijnen die ook bestemd zijn voor de aanbieders van netwerken, telecommunicatiediensten enzovoort; dit moet natuurlijk verder worden uitgeklaard in elk afzonderlijk geval. Voor Facebook bijvoorbeeld werd er een grondige studie gevoerd.[582] Dit zou moeten gebeuren voor elke potentiële verantwoordelijke wiens rol zou kunnen worden bepaald in de zaak die ons bezighoudt.
– Volgens de vaststelling van de feiten, indien bewezen was dat private bedrijven buiten medeweten van de Staat hebben meegewerkt aan de uitvoering van de onderscheppingspraktijken (bv. op de optische kabel in Oostende of door vrijwillig persoonsgegevens door te geven aan een vreemde Staat (NSA of ander)), dan kunnen de Staat of particulieren of bedrijven die het slachtoffer zijn van deze hacking een strafrechtelijke klacht indienen krachtens de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, meer bepaald op grond van artikelen 550*bis* en 314*bis* van het Strafwetboek en van de artikelen 124 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie. Hacking wordt immers strafrechtelijk bestraft.[583]

Titel IXbis van het Belgisch Strafwetboek heeft als titel "Misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en van de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen". Artikelen 550*bis* en 550*ter* bestraffen diverse gedragingen met straffen die gaan van 3 maanden tot 5 jaar opsluiting. De Belgische strafwet verbiedt het feit "zich toegang te verschaffen tot een informaticasysteem" of "zich daarin te handhaven" (artikel 550*bis*, § 1, 1ste lid), maar ook "om enig gebruik te maken van een informaticasysteem van een derde" (artikel 550*bis*,§ 3, 2°) of "enige schade aan dit systeem te veroorzaken" (artikel 550*bis*, § 1, 3°). De wet bestraft "hij die opdracht geeft of aanzet tot het plegen van een van de misdrijven bedoeld in §§ 1 tot 5" (artikel 550*bis*, § 6) en "hij die, terwijl hij weet dat gegevens bekomen zijn door het plegen van een van de misdrijven bedoeld in §§ 1 tot 3, deze gegevens onder zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt" met gevangenisstraf van zes maanden tot drie jaar en/of met geldboete van 26 tot 100.000 euro (artikel 550*bis,* § 7).

Titel V van het Belgisch Strafwetboek ("Misdaden en wanbedrijven tegen de openbare orde door bijzondere personen gepleegd") bevat een hoofdstuk VII*bis* met als titel "Misdrijven betreffende het geheim van privé-communicatie en -telecommunicatie". Artikel 314*bis,* § 1 bestraft met gevangenisstraf van zes maanden tot één jaar en/of honderd tot tienduizend euro hij die "privé-communicatie", "waaraan hij niet deelneemt", "tijdens de overbrenging ervan", […], "er kennis van neemt", "opneemt", "zonder de toestemming van alle deelnemers aan die communicatie of telecommunicatie" of die daartoe "enig toestel opstelt of doet opstellen". Artikel 314*bis,* § 2 bestraft met gevangenisstraf van zes maanden

582 Jean-Philippe Moiny, Facebook au regard des règles européennes concernant la protection des données, *Rev. Eur.de droit de la consommation,* p. 235.

583 De Belgische wetgeving strekt in dit verband tot voorbeeld.

tot twee jaar en/of met geldboete van vijfhonderd tot twintigduizend euro hij die "een op die manier verkregen inlichting" "onthult, verspreidt of er wetens enig gebruik van maakt".

Personen en bedrijven die het slachtoffer van deze misdrijven zijn geweest, kunnen in België een strafrechtelijke klacht indienen bij de procureur des Konings of zich burgerlijke partij stellen. De vraag naar de territoriale bevoegdheid om een dergelijke klacht te kunnen indienen wordt opgelost in functie van de feiten van de zaak. Ofwel werd het misdrijf in België gepleegd (bv. onwettige toegang tot een informaticasysteem in België), ofwel hebben de gevolgen van de misdaad zich voorgedaan in België (indien jurisprudentie van het Hof van Cassatie ter gelegenheid van een zaak met betrekking tot een cheque die in Teheran werd uitgegeven en op een Belgische bank werd getrokken, op cybercrime wordt toegepast[584]).

Dit gezegd zijnde, in het Belgisch recht kunnen deze feiten van hacking wettelijk zijn indien ze, overeenkomstig de bepalingen van het Wetboek van Strafvordering betreffende de opslag van informaticagegevens, worden begaan met behulp van het procedé van de zoeking in een informaticasysteem en de uitbreiding van die zoeking, bevolen door de onderzoeksrechter bij gemotiveerde beschikking, "naar een informaticasysteem dat zich op een andere plaats bevindt" (artikel 88*ter* van het Wetboek van Strafvordering) en door het bevel dat dezelfde magistraat geeft aan een persoon die "bijzondere kennis" heeft om toegang te verkrijgen tot gegevens die zijn opgeslagen "in een verstaanbare vorm" (artikel *88quater* van het Wetboek van Strafvordering). Deze onderzoeksmaatregel kan ook onder strenge voorwaarden plaatsvinden als "uitzonderlijke methode voor het verzamelen van gegevens" door de Veiligheid van de Staat of de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht (artikel 18/16, §§ 1 tot 5 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst).

Hacking of het gebruik van gegevens die in België zijn verzameld of gebruikt, zonder wettelijke toelating, blijft een strafbaar feit. Het Belgisch Wetboek van Strafvordering bevat in artikel 29 voor elke ambtenaar die kennis krijgt van een misdrijf de verplichting om die te melden aan de procureur des Konings. Het gaat om een algemene verplichting die betrekking heeft op eender welk misdrijf.[585]

4. Gebruik van de informatie verkregen door een onwettig controlesysteem

De vraag stelt zich of een politie- of inlichtingendienst die dit soort informatie ontvangt, die informatie mag gebruiken in het kader van zijn opdrachten. *De wet betreffende de bijzondere methoden voor het verzamelen van gegevens bepaalt dat indien een uitzonderlijke maatregel* voor het verzamelen van gegevens, zoals hacking, op onwettige wijze heeft plaatsgevonden, de commissie die belast is met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens van de inlichtingen- en veiligheidsdiensten die gegevens bewaart en de inlichtingen- en veiligheidsdiensten verbiedt die gegevens te exploiteren (artikel 18/10, § 6, lid 4 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst). Op te merken valt dat geen enkele bepaling de gevolgen reglementeert

---

584 Correctionele rechtbank, Dendermonde, 29 september 2008, *Tijdschrift voor Strafrecht,* 2009/2, 111-114.

585 Alain Winants, De Veiligheid van de Staat en de BIM-Wet, in Wauter Van Laethem, Dirk Van Daele en Bart Vangeebergen(Eds), *De Wet op de bijzondere inlichtingenmethoden,* Intersentia, Antwerpen Oxford, p. 141.

die moeten worden gegeven in het geval waarin deze onwettigheid door een buitenlandse dienst werd begaan. Een mogelijke oplossing kan worden gevonden in de besprekingen die zijn voorafgegaan aan de goedkeuring van de wet van 4 februari 2010 betreffende de bijzondere methoden voor het verzamelen van inlichtingen. De wet van 1998 betreffende de inlichtingendiensten verwijst in artikel 20, § 1 immers naar de samenwerking met buitenlandse diensten. De voorzitter van het Vast Comité I heeft echter aangegeven dat "het Comité geen toezicht kan uitoefenen op de buitenlandse inlichtingendiensten. Het zou aangewezen zijn om de wet op dit punt aan te vullen zodat de wettelijkheid van de operaties van bevriende buitenlandse inlichtingendiensten, die op ons grondgebied worden toegelaten, eveneens kan worden gecontroleerd door de Veiligheid van de Staat."[586] De heer Winants heeft bij deze gelegenheid verklaard: "Indien een buitenlandse inlichtingendienst zijn bevoegdheden te buiten gaat, dan geniet de Veiligheid van de Staat de mogelijkheid om tussen te komen op grond van voornoemd artikel 20 van de wet van 1998)."[587] De heer Hellemans, directeur van de ADIV, verklaarde van zijn kant: "De ADIV gaat uit van het principe dat het stelselmatig door de buitenlandse diensten op de hoogte wordt gebracht wanneer die diensten een doel nastreven in België. De dienst onderhoudt goede contacten met de bevriende landen en maakt gebruik van een systeem voor gegevensuitwisseling. Natuurlijk blijft de dienst aansprakelijk voor de gegevens die op het Belgisch grondgebied worden verzameld."[588]

Uit dit alles blijkt ten eerste dat het aanwenden door een buitenlandse dienst van een uitzonderlijke methode voor het verzamelen van gegevens in België, zoals hacking, niet gereglementeerd is, ten tweede dat deze methode om inlichtingen te verzamelen een strafbaar feit vormt en ten derde dat het voor de Belgische diensten verboden is om op onwettige wijze verkregen inlichtingen te gebruiken, zo niet zouden de Belgische diensten zich eveneens schuldig maken aan het plegen van een misdrijf als ze dit wetens en willens doen.

De problematiek van de samenwerking met buitenlandse diensten en de manier om daarop toezicht uit te oefenen is een van de prioriteiten van het Vast Comité I. Al in het activiteitenverslag van 2008 bracht het Comité verslag uit over verschillende bijdragen in het buitenland teneinde een doeltreffende democratische controle op de inlichtingendiensten te bevorderen en deze initiatieven krijgen de steun van Martin Scheinin, Speciaal Rapporteur van de Verenigde Naties voor bevordering en bescherming van de mensenrechten en de fundamentele vrijheden in de strijd tegen het terrorisme.[589] De uitwisseling van informatie met 'bevriende' diensten is momenteel slechts onderworpen aan ethische beginselen. Deze lacune in de wetten betreffende het toezicht op de inlichtingendiensten werd bekritiseerd en er werd voorgesteld dat nieuwe regelgeving dit juridisch vacuüm zou opvullen.[590]

De kwestie betreffende het gerechtelijk gebruik van dit soort informatie krijgt een andere oplossing. Het Belgisch strafprocesrecht voorziet immers in een regel die onwettig verkregen bewijselementen uitsluit. Deze uitsluiting is echter niet absoluut. De wet van

---

586 *Parl. st.,* Kamer, 52ste zittingsperiode, 2009-2010, DOC 52 / 2128/000, p. 41.

587 *Ibid.*

588 *O.c.,* p. 46.

589 Vast Comité I, Activiteitenverslag 2008, p. 87.

590 Oor een grondige studie hierover, zie o.a. Elizabeth Sepper, Democracy, Human Rights and Intelligence Sharing, *Texas International Law Journal,* Vol. 46: 151, 2010, pp. 153-206; Europees parlement, Comité burgerlijke vrijheden, justitie en binnenlandse zaken, *Working Document 5 on Democratic oversight of Member State intelligence services and of EU intelligence bodies,* 11 november 2013, DT\1009342EN.doc.

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-'Antigone' van 14 oktober 2003 van het Belgisch Hof van Cassatie .[591] 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 90*ter* 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. In een belangrijk boek[592] heeft de voorzitter van de strafkamer van het Belgische Hof van Cassatie echter verklaard dat er, naast de nietigheden waarin een wettekst specifiek voorziet of die welke de betrouwbaarheid van het bewijsmateriaal aantasten of waarvan het gebruik het recht op een eerlijk proces schendt, ook nietigheden bestaan als gevolg van onrechtmatig verkregen bewijs, dit wil zeggen het geval waarin het bewijsmateriaal is aangetast door het plegen van een misdrijf.[593] Ter gelegenheid van een studie naar de rechtspraak in deze materie maakt deze eminente magistraat, met betrekking tot misdrijven gepleegd door onderzoeksorganen, een onderscheid tussen enerzijds de situatie van een misdrijf dat wordt begaan om een bewijs te verkrijgen en anderzijds de situatie van een misdrijf dat al is gepleegd op het ogenblik waarop de vaststelling wordt gemaakt van een door een delinquent gepleegd misdrijf.[594] In het eerste geval, bijvoorbeeld onwettige hacking, is het bewijs niet ontvankelijk. In het tweede geval, bijvoorbeeld de deelname aan de handel in verdovende middelen teneinde de daders aan te houden, "zou het bewijs ontvankelijk zijn wanneer het misdadig voornemen duidelijk voorafgaat aan de interventie van de politie en de verbaliserende overheid slechts onregelmatigheden begaat die extern zijn aan de beslagleggingen, zoekingen, observaties en verhoren" (vrije vertaling).[595]

---

591 AR P.03.0762.N.
592 Jean de CODT, *Des nullités de l'instruction et du jugement,* Brussel, Larcier, 2006, 233 pp.
593 *O.c.,* p. 16.
594 *O.c.,* p. 103-104.
595 *O.c.,* p. 105.