



**VAST COMITÉ VAN TOEZICHT OP DE INLICHTINGEN EN
VEILIGHEIDSDIENSTEN**

Notitienummer 2020.281

Opvolging van het toezichtonderzoek PRISM (2013)

INHOUDSTAFEL

I.	INLEIDING	3
I.1.	TOEZICHTONDERZOEK PRISM (2013).....	3
I.2.	BEVOEGDHEID VAN HET VAST COMITÉ I	3
II.	OPVOLGING VAN DE AANBEVELINGEN VAN HET ONDERZOEK PRISM (2013).....	4
II.1.	EERSTE AANBEVELING : AANDACHT VOOR MASSALE DATA-CAPTATIE EN POLITIEKE EN ECONOMISCHE SPIONAGE	4
II.2.	TWEDE AANBEVELING : OMGAAN MET DE NOTIE “BEVRIENDE DIENSTEN”	6
II.3.	DERDE AANBEVELING: NAUWERE SAMENWERKING TUSSEN BEIDE INLICHTINGDIENSTEN	8
II.4.	VIERDE AANBEVELING : RICHTLIJNEN INZAKE DE SAMENWERKING MET BUITENLANDSE DIENSTEN	10
II.5.	VIJFDE AANBEVELING : DE NOOD AAN EEN POLITIEKE DEKKING VOOR SAMENWERKINGSVERBANDEN.....	12
II.6.	ZESDE AANBEVELING : DE NOOD AAN EEN POLITIEKE STURING DOOR HET MINISTERIEEL COMITÉ VOOR INLICHTING EN VEILIGHEID.....	14
II.7.	ZEVENDE AANBEVELING: INTERDEPARTEMENTALE SAMENWERKING INZAKE CYBERSECURITY, ICT-SECURITY EN CYBERINTELLIGENCE	15
II.8.	ACHTSTE AANBEVELING : DE NEGATIEVE GEVOLGEN VAN COMPARTIMENTERING EN GEHEIMHOUDING BINNEN DE ADIV	16
II.9.	NEGENDE AANBEVELING : HET TERRITORIAAL TOEPASSINGSGBIED VAN DE BIM-WET	17
II.10.	TIENDE AANBEVELING : EEN VERDUIDELIJING VAN DE INT-REGELING	20
II.11.	ELFDE AANBEVELING : EEN STRIKTE NALEVING VAN ARTIKEL 33 W.TOEZICHT	23

I. INLEIDING

I.1. TOEZICHTONDERZOEK PRISM (2013)

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

Het Vast Comité I besloot om bepaalde implementeringen van de aanbevelingen uit het onderzoek van 2013 tegen het licht te houden, en na te gaan op welke wijze de aanbevelingen werden opgevolgd.

I.2. BEVOEGDHEID VAN HET VAST COMITÉ I

Artikel 33 van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse (Wet Toezicht) stelt dat het Vast Comité I onderzoeken instelt naar de activiteiten en de werkwijze van de inlichtingendiensten.

II. OPVOLGING VAN DE AANBEVELINGEN VAN HET ONDERZOEK PRISM (2013)

Het toezichtonderzoek PRISM van 2013 bevatte 11 aanbevelingen. Huidig opvolgingsonderzoek gaat na op welke wijze elk van deze aanbevelingen werden opgevolgd.

II.1. EERSTE AANBEVELING : AANDACHT VOOR MASSALE DATA-CAPTATIE EN POLITIEKE EN ECONOMISCHE SPIONAGE

Aanbeveling - Toezichtonderzoek PRISM (2013)

Het Vast Comité I is van oordeel dat beide inlichtingendiensten aandacht moeten hebben voor de inherente risico's die nieuwe technologische mogelijkheden met zich mee kunnen brengen op vlak van massale datacaptatie en economische en politieke spionage, ook al gaan die uit van bevriende landen. Hierover zouden risicoanalyses moeten worden opgesteld, waarbinnen ook aandacht is voor de aanwezigheid van internationale instellingen op Belgisch grondgebied.

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

Wat betreft de VSSE is de aandacht voor massale data-captatie evident noodzakelijk omdat dit fenomeen een reële bedreiging vormt voor minstens twee wettelijk te beschermen belangen, te weten de fundamentele rechten en vrijheden en de soevereiniteit van de Staat. Veel informatie is bijvoorbeeld reeds terug te vinden in open bronnen of opvraagbaar bij de militaire inlichtingendienst. Op basis van die elementen kan reeds een globaal beeld gevormd worden van het fenomeen en van de risico's. Dit zou zijn neerslag kunnen vinden in een fenomeenanalyse¹ die op regelmatige tijdstippen naar de betrokken overheden wordt gezonden. Maar ook de burgers en de ondernemingen zouden nog meer dan nu moeten gesensibiliseerd worden voor de problematiek.

4

De aandacht voor massale datacaptatie en economische spionage door de VSSE en de ADIV is, naar het oordeel van het Vast Comité I, noodzakelijk. Beide diensten zijn immers verplicht om een goede informatiepositie op te bouwen om de mogelijkheden en de werkwijzen van andere buitenlandse diensten te kennen.

Dit is niet alleen nodig om, desgevallend, de Belgische overheden te kunnen inlichten of tegenmaatregelen te treffen, maar ook om zijn eigen collecte-technieken te evalueren.

¹ Het Vast Comité I wees reeds eerder op de troeven van wat de VSSE een 'fenomeenanalyse' noemt: '*L'analyse du phénomène expose un thème actuel qui relève des sphères d'intérêt et des missions dévolues à un service de renseignement et qui représente un défi politique et social majeur, tant aujourd'hui que pour les années à venir. Elle s'attache à décrire ce problème tant au niveau de ses origines historiques, qu'au plan de l'idéologie, de l'organisation, de la structure et des activités y relatives. Elle contextualise les défis et les risques, établit une « évaluation du risque » à destination de nos responsables politiques, des autorités administratives concernées et des autorités judiciaires qui sont également confrontées à cette problématique*', aldus de VSSE in haar eerste fenomeenanalyse. Mede omdat dergelijke analyses bedoeld zijn om een ruimere verspreiding te krijgen, lenen ze zich goed voor de problematiek van data-captatie.

Wat de VSSE betreft

De VSSE is van oordeel dat aandacht voor massale data-captatie manifest noodzakelijk is omdat dit fenomeen een reële bedreiging vormt voor minstens twee wettelijk te beschermen belangen, te weten (1) de fundamentele rechten en vrijheden en (2) de soevereiniteit van de Staat.

Volgens de VSSE zou het globaal beeld dat we ons vormen over massale datacaptatie zijn neerslag kunnen vinden in een fenomeenanalyse² die op regelmatige tijdstippen naar de betrokken overheden wordt gezonden. Maar ook de burgers en de ondernemingen zouden, nog meer dan nu, moeten gesensibiliseerd worden voor de problematiek.

Wat de ADIV betreft

De ADIV erkent het bestaan van de dreiging, maar ziet niet direct veel heil in het opstellen van een analyse hieromtrent. De ADIV kampt klaarblijkelijk met een tekort aan personeel om ten volle massale datacaptatie van buitenlandse diensten maximaal op te volgen.

EVALUATIE VAN HET VAST COMITÉ I

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

Het Vast Comité I stelt vast dat beide diensten verklaren dat zij niet over de middelen beschikken om het fenomeen van massale datacaptatie naar behoren aan te pakken. Het Comité is echter van mening dat de diensten moeten blijven investeren in de bescherming tegen dergelijke massale afluisterpraktijken.

Vanaf 19 oktober 2022 zal het Belgische *Cyber Commando* van Defensie, dat nauw zal samenwerken met ADIV, officieel operationeel zijn. Het zal verantwoordelijk zijn voor de uitvoering van de strategie op het vlak van *Cyber Security* en voor het zich voorzien van de passende middelen om de daarin vervatte doelstellingen te bereiken.

² Het Vast Comité I wees reeds eerder op de troeven van wat de VSSE een 'fenomeenanalyse' noemt: *'L'analyse du phénomène expose un thème actuel qui relève des sphères d'intérêt et des missions dévolues à un service de renseignement et qui représente un défi politique et social majeur, tant aujourd'hui que pour les années à venir. Elle s'attache à décrire ce problème tant au niveau de ses origines historiques, qu'au plan de l'idéologie, de l'organisation, de la structure et des activités y relatives. Elle contextualise les défis et les risques, établit une « évaluation du risque » à destination de nos responsables politiques, des autorités administratives concernées et des autorités judiciaires qui sont également confrontées à cette problématique'*, aldus de VSSE in haar eerste fenomeenanalyse. Mede omdat dergelijke analyses bedoeld zijn om een ruimere verspreiding te krijgen, lenen ze zich goed voor de problematiek van data-captatie.

II.2. TWEEDE AANBEVELING : OMGAAN MET DE NOTIE “BEVRIENDE DIENSTEN”

Aanbeveling - Toezichtonderzoek PRISM (2013)

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

Op 26 september 2016 werd door de Nationale Veiligheidsraad in deze kwestie een richtlijn uitgevaardigd. Het betreft de *“Richtlijn aangaande de relaties van de Belgische inlichtingendiensten met buitenlandse inlichtingendiensten”*.³ Deze richtlijn bepaalt het mechanisme dat door de VSSE en de ADIV dient te worden toegepast.

De bedoeling is om op een gestructureerde wijze de keuze van hun internationale partners te objectiveren, om de mate en aard van de samenwerking met deze partners te bepalen en om deze samenwerking op regelmatige basis te evalueren. De richtlijn geeft ook sturing op het vlak van het verstrekken van persoonsgegevens aan buitenlandse diensten.

Het mechanisme dat in de richtlijn beschreven is, bevat een aantal beoordelingscriteria. Deze criteria dienen te worden gehanteerd en hebben enerzijds betrekking op eventuele belemmeringen voor een samenwerking met een buitenlandse partner, en anderzijds voor eventuele kansen of opportuniteiten voor samenwerking met deze partners. Op basis van deze beoordelingscriteria voorziet de richtlijn in een tweejaarlijkse evaluatie van de samenwerking van elke buitenlandse dienst waarmee wordt samengewerkt. Er dient over elke buitenlandse partnerdienst een synthesefiche te worden opgesteld. Ook worden deze partnerdiensten ondergebracht in categorieën, die bepalen wat de samenwerkingswijze is.

6

In het kader van dit onderzoek werd de vraag gesteld aan beide diensten in hoeverre deze richtlijn door hen systematisch wordt toegepast, en in welke mate, bij de evaluatie van de samenwerking met een buitenlandse dienst, wordt rekening gehouden met mogelijke datacaptatie door deze dienst.

Wat de VSSE betreft

De VSSE verklaarde dat getracht wordt om het evaluatiemechanisme voor buitenlandse inlichtingendiensten steeds meer in de dagelijkse werking van de dienst te integreren.

³ Voor wat betreft het verkrijgen van een overzicht van de voorgeschiedenis van deze richtlijn, en de terzake door het Vast Comité I gedane aanbevelingen, zie VAST COMITÉ I, « Toezichtonderzoek met betrekking tot het Memorandum of Understanding (MoU) dat in oktober werd afgesloten door de ADIV en de Rwandese inlichtingendiensten », 30 juni 2020, p. 4-6.

Wat de ADIV betreft

De ADIV gaf enkel te kennen dat de richtlijn volgens haar diende te worden herzien. De ADIV verduidelijkt niet in welke richting deze herziening zou moeten gaan.⁴

EVALUATIE VAN HET VAST COMITÉ I

Het Vast Comité I is van mening dat de dreiging die uitgaat van het gebruik maken van massacaptatiesystemen door een strategische partner moet worden betrokken in de evaluatie die de inlichtingendienst houdt betreffende haar relatie met een partnerdienst.

Het Vast Comité I is van oordeel dat de inlichtingendiensten zich moeten uitrusten met alle mogelijke menselijke en technische middelen om dergelijke dreigingen op te sporen, eventueel via tussenkomst van het Belgische *Cyber Commando* van Defensie. Volgens het Vast Comité I moeten de inlichtingendiensten blijvend aandacht besteden aan de mogelijkheid van massale datacaptatie door "bevriende" diensten of strategische partners.

⁴ Nota 21.50057672 dd. 23 maart 2021, ADIV, p.3.

II.3. DERDE AANBEVELING: NAUWERE SAMENWERKING TUSSEN BEIDE INLICHTINGEDIENSTEN

Aanbeveling - Toezichtonderzoek PRISM (2013)

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

Het samenwerkingsprotocol van 2004 voorziet in de mogelijkheid om een ad hoc-samenwerkingsplatform op te richten met betrekking tot datacaptatie inzake economische spionage. Het Vast Comité I stelde vast dat er na het toezichtonderzoek van 2013, noch door de VSSE noch door en de ADIV, hiervan gebruik werd gemaakt.

Ongeveer 10 jaar later werden wel andere coördinatieplatforms opgericht. Eén van de platforms kreeg als opdracht aandacht te besteden aan de vrijwaring van het WEP, onder voorzitterschap van de VSSE. In 2018 werd daarop door de VSSE en de ADIV een voorstel tot Nationaal Strategisch Inlichtingenplan (NSIP) voorgesteld. Het betreft een document waarin onder andere een overzicht wordt gegeven van de reeds bestaande samenwerkingen en synergiën tussen de beide inlichtingendiensten, en van toekomstige samenwerkingsvoorstellen.

Het is van belang om op te merken dat in dit NSIP de diensten de aandacht vestigen op het feit dat de inlichtingenarchitectuur in België beperkt is in vergelijking met onze buurlanden. De inlichtingenactiviteit wordt immers gewoonlijk onder (minstens) 4 diensten verdeeld, waaronder een strategische en externe inlichtingendienst, en een dienst voor het onderscheppen van communicaties of technische dienst. In België is er geen echte externe inlichtingendienst die specifiek gewijd is aan de veiligheid, of aan de vitale en essentiële belangen van de federale staat ter ondersteuning van het economisch beleid van het land. Standaard vervult de ADIV deze rol gedeeltelijk, maar enkel binnen het domein van de veiligheid in ruime zin van het woord.

In december 2020 werd ook het Centrum voor Cybersecurity België (CCB) voor de eerste maal uitgenodigd voor de virtuele, plenaire bijeenkomst van het WEP-platform.

EVALUATIE VAN HET VAST COMITÉ I

Het Vast Comité I stelt vast dat de kwestie van de bescherming van het WEP niet vooraan op de prioriteitenlijst van de inlichtingendiensten staat. De initiatieven die op dit gebied worden ontplooid, worden steeds gecounterd door de actualiteit. Sinds 2014 zijn de diensten achtereenvolgens geconfronteerd met de "Syrische filière", de aanslagen in Parijs en Brussel, de opkomst van het extremisme en ten slotte een forse en opvallende terugkeer van de Koude Oorlog. Deze verschillende bedreigingen hebben de diensten ertoe gedwongen zich voortdurend te heroriënteren, wat zorgde voor een sterk verminderde aandacht voor het WEP. Volgens het Vast Comité I moeten de extra beloofde middelen qua personeel en materieel ook - op een permanente manier - aangewend worden voor de bescherming van het WEP. Het Vast Comité I is ook van mening dat de bescherming van het WEP zou kunnen worden opgevolgd via een gemeenschappelijk platform tussen de twee inlichtingendiensten.

II.4. VIERDE AANBEVELING : RICHTLIJNEN INZAKE DE SAMENWERKING MET BUITENLANDSE DIENSTEN

Aanbeveling - Toezichtonderzoek PRISM (2013)

De VSSE stelde in 2012 een gedetailleerde 'instructie voor de bilaterale samenwerking met de correspondenten' op. Het Vast Comité I beschouwde deze richtlijn als bijzonder waardevol. Wel wees het erop dat bepaalde door de VSSE genomen opties, gedragen moeten worden door de politieke verantwoordelijken, te weten de leden van het Ministerieel Comité voor inlichting en veiligheid. Tevens werd een van de belangrijkste aspecten van die samenwerking - welke inlichtingen mogen meegedeeld worden aan buitenlandse diensten? - in de instructie slechts summier aangeraakt. Het Vast Comité I herhaalt zijn aanbeveling aan de VSSE om haar richtlijn - aangevuld met meer precieze regels over informatie-uitwisseling - onverwijld over te zenden naar het Ministerieel Comité.⁵

Eenzelfde aanbeveling geldt voor de ADIV, zeker nu het Vast Comité I in voorliggend onderzoek heeft kunnen vaststellen dat er nauw wordt samengewerkt met buitenlandse SIGINT-afdelingen. De ADIV bereidt in navolging van de VSSE een soortgelijke nota voor met 'aantoetsbare criteria' in het kader van de samenwerking met buitenlandse inlichtingendiensten (in ruime zin). Deze nota zou in de loop van 2014 gefinaliseerd worden. Het Comité benadrukt het belang van dergelijke richtlijn voor de ADIV omdat ze - eveneens na goedkeuring door het Ministerieel Comité - een gelegitimeerd kader kan bieden voor samenwerkingsverbanden die de militaire inlichtingendienst vandaag reeds aangaat.

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

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

Tevens beveelt het Comité aan dat de evaluatie van de samenwerking aan de hand van de vooropgestelde criteria ook effectief én op geregelde tijdstippen plaatsvindt. De recente onthullingen tonen deze noodzaak aan.

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

10

Voor wat betreft de wijze waarop gevolg werd gegeven aan deze aanbeveling kan eenvoudigweg verwezen worden naar hetgeen gesteld wordt in het kader van de tweede aanbeveling ("het omgaan met bevriende diensten").

EVALUATIE VAN HET VAST COMITÉ I

Sinds 2012 heeft de VSSE het initiatief genomen om een richtlijn op te stellen voor de evaluatie van zijn bilaterale betrekkingen met strategische partners. Ook de toenmalige minister van Defensie ondertekende de richtlijn, waardoor deze ook van toepassing werd op de ADIV.

⁵ VAST COMITÉ I, *Activiteitenverslag 2012*, 95.

Tijdens het onderzoek van het Vast Comité I naar het *Memorandum of Understanding* (MoU) tussen de ADIV en de Rwandese inlichtingendienst, *National Intelligence and Security Services* (NISS) heeft het Comité het memorandum geëvalueerd en heeft een reeks aanbevelingen geformuleerd om deze doeltreffender te maken. Sindsdien zijn de diensten verplicht gezamenlijke evaluaties uit te voeren over hun gemeenschappelijke strategische partners. Zij zijn ook verplicht deze relaties om de twee jaar te evalueren.

II.5. VIJFDE AANBEVELING : DE NOOD AAN EEN POLITIEKE DEKKING VOOR SAMENWERKINGSVERBANDEN

Aanbeveling - Toezichtonderzoek PRISM (2013)

Het Comité is van oordeel dat er vanuit de diensten een grotere openheid moet zijn over bestaande bi- of multilaterale samenwerkingsverbanden en dit in de eerste plaats ten aanzien van de bevoegde ministers. In dergelijke samenwerkingsverbanden kunnen immers engagementen worden genomen of keuzes gemaakt die het beslissingsniveau van een inlichtingendienst overstijgen en die een politieke aftoetsing en dekking behoeven. Anders gezegd, dienen de bevoegde ministers afdoende worden geïnformeerd zodat zij steeds in de mogelijkheid zijn om hun politieke verantwoordelijkheid op te nemen. Wat 'politiek relevant' is, kan echter evolueren in de tijd.

De "Richtlijn aangaande de relaties van de Belgische inlichtingendiensten met buitenlandse inlichtingendiensten" (zie hoger - tweede aanbeveling) voorziet in de mogelijkheid om een formele of informele overeenkomst voor samenwerking met een buitenlandse diensten te sluiten.

Deze richtlijn bepaalt niet eenduidig of de VSSE en de ADIV al dan niet een voorafgaande ministeriële toestemming of de toestemming van een andere instantie moeten verkrijgen. Dergelijke toestemming lijkt voor het Vast Comité I essentieel, nu elke overeenkomst tot samenwerking politiek dient gedekt te zijn.⁶

Op te merken valt dat er naast deze aanbeveling uit 2013, in 2017 een nieuwe aanbeveling door het Vast Comité I werd geformuleerd. Deze nieuwe aanbeveling was een herbevestiging van de aanbeveling van 2013: *"In het kader van de internationale samenwerkingsverbanden die door de ADIV (maar ook door de VSSE) worden aangegaan, kunnen engagementen worden genomen of keuzes worden gemaakt die een politieke afsplitsing en dekking behoeven. Bij wijze van algemeen principe beval het Comité vroeger reeds aan dat de bevoegde ministers afdoende zouden worden geïnformeerd opdat zij in de mogelijkheid zouden zijn om ten aanzien van het parlement hun politieke verantwoordelijkheden op te nemen"*.

De aanbeveling van 2013 werd in 2017 zelfs nog ietwat verfijnd: *"Het Comité herhaalt deze aanbeveling en maakt deze concreter, door elementen mee te geven die criteria kunnen vormen om al dan niet te kunnen beoordelen of en wanneer de minister door de dienst moet worden geïnformeerd. Daarbij horen onder andere de vragen welk bureau de operatie uitvoert; waar een operatie zich voordoet (een conflictgebied of niet, Belgisch militair operatiegebied of niet); hoe groot de strategisch-beleidsmatige risico's (die op een structurele en formele manier zijn opgelijst) zijn; de internationale context; de vraag of er al dan niet een verband is met een gerechtelijk onderzoek; het gevaar op compromittering van de operatie... Deze opsomming is niet limitatief. Het komt de dienst en de minister toe om deze criteria zo nodig aan te vullen en verder uit te werken."*⁷

⁶ Zie in die zin: Wetsvoorstel tot wijziging van de wet van 30 november 1998 houdende regeling van inlichtingen- en veiligheidsdiensten met het oog op het invoeren van wegingsnotities voor de samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten, Parl. St. Kamer 2019-20, nr. 55- 956/001 (23 januari 2020).

⁷ VAST COMITÉ I, Activiteitenverslag 2017, 107 ('XII. Politieke dekking voor samenwerkingsverbanden').

EVALUATIE VAN HET VAST COMITÉ I

Het Vast Comité I heeft naar aanleiding van het onderzoek "MoU Rwanda" (zie hoger - vierde aanbeveling) de verplichting ingevoerd dat bilaterale overeenkomsten tussen de diensten en hun strategische partners door de bevoegde minister moeten worden goedgekeurd of gedekt.

Op heden verwijst het Vast Comité I naar haar aanbeveling genomen in 2017 wat betreft de samenwerking met een buitenlandse partner. Er bestaat volgens het Vast Comité I immers nog steeds de noodzaak van de politieke toestemming voorafgaand aan het sluiten van bilaterale of internationale overeenkomsten.

II.6. ZESDE AANBEVELING : DE NOOD AAN EEN POLITIEKE STURING DOOR HET MINISTERIEEL COMITÉ VOOR INLICHTING EN VEILIGHEID

Aanbeveling - Toezichtonderzoek PRISM (2013)

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

Het Comité acht het wenselijk dat het Ministerieel Comité zijn sturende rol - mede op aangeven van de twee inlichtingendiensten die tevens deel uitmaken van het College voor inlichting en veiligheid - zou opnemen ten aanzien van de fenomenen van massale data-captatie en politieke en economische spionage. Het Comité is van oordeel dat België daardoor minstens ten dele zou tegemoetkomen aan zijn positieve verplichting uit artikel 8 EVRM om de privacy van haar burgers te beschermen.⁸

Daarnaast wijst het Comité op het ontbreken van de formele goedkeuring door het Ministerieel Comité van de eind 2012 opgestelde lijst met bedrijven waarvan de ADIV het WEP moet beschermen.

Het Ministerieel Comité voor Inlichting en Veiligheid werd ondertussen omgevormd tot de Nationale Veiligheidsraad (NVR).

Voor zover het Vast Comité I kon nagaan is vanuit de NVR, na het PRISM-onderzoek van 2013, geen specifieke aandacht uitgegaan aan het fenomeen van massale datacaptatie.

EVALUATIE VAN HET VAST COMITE I

Het Comité is van mening dat het aan de NVR toekomt om het algemene inlichtingenbeleid en de daaruit voortvloeiende prioriteiten te bepalen. Het Vast Comité I suggereert daarenboven een actievere betrokkenheid van de NVR terzake.

⁸ Zie in dezelfde zin de aanbeveling van het LIBE-Committee: "roept de lidstaten onmiddellijk op te voldoen aan hun positieve verplichting uit hoofde van het EVRM om hun burgers te beschermen tegen door derde landen uitgeoefend toezicht dat in strijd is met de vereisten daarvan, ook wanneer het doel ervan de waarborging van de nationale veiligheid is, en te garanderen dat de rechtsstaat niet is verzwakt als gevolg van extraterritoriale toepassing van een wet van een derde land", in: EUROPEES PARLEMENT, Commissie burgerlijke vrijheden, justitie en binnenlandse zaken, Ontwerpverslag over het surveillanceprogramma van de NSA in de VS, toezichthoudende instantie in verschillende lidstaten en gevolgen voor de grondrechten van EU-burgers en voor de trans-Atlantische samenwerking op het gebied van justitie en binnenlandse zaken, (2013/2188(INI), PR/1014703NL.doc, PES26.085v02-00, 8 januari 2014).

II.7. ZEVENDE AANBEVELING: INTERDEPARTEMENTALE SAMENWERKING INZAKE CYBERSECURITY, ICT-SECURITY EN CYBERINTELLIGENCE

Aanbeveling - Toezichtonderzoek PRISM (2013)

Bepaalde aspecten van de E. Snowden-onthullingen wezen op zwaktes in de beveiligingssystemen van IT-netwerken van zowel private actoren als publieke instellingen.

Het Comité herhaalt dan ook met klem dat er meer aandacht moet uitgaan naar cyber- en ICT-Security (INFOSEC) en dat deze problematieken - die niet alleen tot het takenpakket van de inlichtingendiensten behoren - een interdepartementale samenwerking vereisen. Zo bijvoorbeeld is in deze een cruciale rol weggelegd voor de Nationale Veiligheidsoverheid.

Het Comité verwijst in dit verband eveneens naar de goedkeuring van een ontwerpbesluit door de Ministerraad op 19 december 2013 dat moet leiden tot de oprichting van een Centrum voor Cybersecurity België bij de Kanselarij van de Eerste minister. Ook werden bijkomende middelen toegewezen om de cybersecurity-strategie zoals die eind 2012 was goedgekeurd, uit te voeren. Een deel van deze middelen zou bestemd zijn voor de ADIV⁹ wat deze dienst moet toelaten zijn capaciteit te verhogen en meer aandacht te besteden aan *cyberintelligence*. Het Vast Comité I is echter overtuigd dat *cybersecurity* en *-intelligence* de komende decennia blijvende investeringen zullen vereisen.

Het Vast Comité I stelt vast dat op 10 oktober 2014 het CCB werd opgericht. Dit CCB neemt sinds december 2020 deel aan de plenaire beraadslagingen van het Platform WEP, dat onder voorzitterschap staat van de VSSE.

Het CCB neemt echter niet systematisch deel aan de bijeenkomsten van het Strategisch Comité voor Inlichtingen en Veiligheid en het Coördinatiecomité voor Inlichting en Veiligheid, noch van de NVR.

Het CCB heeft ook niet de opdracht om cyberdreigingen op te sporen, en heeft ook geen directe verantwoordelijkheid voor de vrijwaring van het WEP.

EVALUATIE VAN HET VAST COMITE I

Sinds het bekend worden van de Snowden-affaire zijn er - en het Vast Comité I kan dit alleen maar toejuichen - belangrijke ontwikkelingen geweest in het Belgische veiligheidslandschap. Zo wordt momenteel gewerkt aan de toekomstige structuur van de Nationale Veiligheidsoverheid (NVO), en zal het Belgische *Cyber Command* van Defensie het huidige inlichtingen-en veiligheidslandschap drastisch veranderen. Het Vast Comité I is van mening dat deze twee nieuwe entiteiten onder collegiaal toezicht van de NVR zullen moeten werken aan de bescherming van de Belgische vitale belangen. Er zal een grotere inspanning moeten worden geleverd op het gebied van de homologatie van computersystemen en bij de ontwikkeling van eigen cryptografie. Niettemin acht het Comité I het noodzakelijk om, naast de materiële investeringen, eraan te herinneren dat de zwakste schakel in dit verband de 'menselijke factor' is. Er moet een inspanning worden gedaan om het personeel regelmatig bewust te maken van de bedreigingen die uitgaan van massa-captatietechnologieën.

⁹ Vijf personen aan te werven in 2014 en nog eens vijf in 2016.

II.8. ACHTSTE AANBEVELING : DE NEGATIEVE GEVOLGEN VAN COMPARTIMENTERING EN GEHEIMHOUDING BINNEN DE ADIV

Aanbeveling - Toezichtonderzoek PRISM (2013)

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

Hieromtrent heel specifiek bevraagd liet ADIV weten dat de situatie op heden nauwelijks is geëvolueerd.

EVALUATIE VAN HET VAST COMITÉ I

Gelet op de vaststellingen gedaan naar aanleiding van een onderzoek naar het PRISM-toezichtonderzoek van 2013¹⁰ en gelet op de informatie verstrekt in juni 2022 is het Vast Comité I van oordeel dat, wat betreft deze aanbeveling, onvoldoende vooruitgang werd geboekt, en is er nog steeds sprake van ontoelaatbare compartimentering binnen de ADIV. De reden is - onder meer - nog steeds de afwezigheid van één allesomvattend informaticasysteem binnen de ADIV.

Het Vast Comité I is van mening dat de ADIV de beschikbaarheid van informatie nog verder dient te maximaliseren. Om dit te bereiken moet worden geïnvesteerd in adequate gebouwen en in performante informatica-infrastructuur. Het Comité is van mening dat de ADIV bijzondere inspanningen moet leveren om de politieke besluitvormers te bewegen tot de nodige investeringen.

¹⁰ Zie in hoofdzaak het "toezichtonderzoek naar het opsporen en het opvolgen - door de twee inlichtingendiensten - van de radicalisering van een militair werkzaam bij Defensie, en anderzijds naar hun samenwerking met hun partnerdiensten, waaronder Defensie, onder meer wat betreft hun informatie-uitwisseling".

II.9. NEGENDE AANBEVELING : HET TERRITORIAAL TOEPASSINGSGBIED VAN DE BIM-WET

Aanbeveling - Toezichtonderzoek PRISM (2013)

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

De Wet van 30 maart 2017 tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst en van artikel 259bis van het Strafwetboek (BS 28 april 2017; hierna de BIM-actualisatiewet) bracht belangrijke wijzigingen aan het territoriaal toepassingsgebied van de specifieke en uitzonderlijke methoden (samen de BIM-methoden genoemd). De wetwijziging heeft een weerslag op de geografische werking van de binnen dit toezichtonderzoek onderzochte BIM-methoden, zijnde het onderscheppen van (tele)communicaties (cf. art. 18/17 van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst (W.I&V) en het binnendringen in informaticasystemen (cf. art. 18/16 W.I&V).

Wat betreft de VSSE

Vóór de vernoemde wetwijziging kon een BIM-methode slechts “op het grondgebied van het Rijk” worden aangewend. De wet stelt op heden dat de inlichtingendienst de BIM-methoden “op of vanaf het grondgebied van het Rijk” uitoefent (cf. art. 18/1, 1° W.I&V).

De memorie van toelichting¹¹ van de BIM-actualisatiewet verduidelijkt hierbij dat de VSSE voortaan de BIM-methoden ‘op’ het Belgisch grondgebied moet ‘aanwenden’, wat betekent dat de VSSE-agenten zich niet fysiek naar het buitenland mogen begeven om bijvoorbeeld een woning te doorzoeken, een micro of camera te installeren of een telefoon uit te lezen. De memorie van toelichting stelt dat het verzamelen van informatie zelf wel in het buitenland mag gebeuren.¹²

Wat betreft de ADIV

Ook voor de ADIV bracht de BIM-actualisatiewet wijzigingen in het territoriaal toepassingsgebied van de BIM-methoden. De wetgever ging hierbij nog een grote stap verder door voor de ADIV niet langer enige territoriale beperkingen te koppelen aan de uitoefening van BIM-methoden (cf. art. 18/1, 2° W.I&V).

De memorie van toelichting¹³ van de BIM-actualisatiewet stelt hierover dat deze wijziging is gerechtvaardigd door het feit dat de meerderheid van de opdrachten van de ADIV worden

¹¹ MVT, *Parl. St.*, Kamer 2015-16, nr. 54-2043/001, 46-47.

¹² Ter verduidelijking hiervan worden volgende voorbeelden gegeven, die eveneens van onmiddellijk belang zijn voor dit toezichtonderzoek: (1) het binnendringen in een informaticasysteem vanuit België, maar die op een grensoverschrijdend netwerk wordt uitgevoerd, en (2) een doelwit dat afgeluisterd wordt die een buitenlandse oproep ontvangt.

¹³ MVT, *Parl. St.* Kamer 2015-16, nr. 54-2043/001, 47-50.

uitgevoerd in het buitenland, zoals bijvoorbeeld de bescherming van de opdrachten van de Krijgsmacht, of de bescherming van Belgische onderdanen in het buitenland. Verder wordt gesteld dat in het kader van de operaties met een door de Veiligheidsraad van de Verenigde Naties toegekend mandaat vaak van de inlichtingendiensten van de coalitie wordt verwacht dat ze inlichtingenonderzoeken voeren waarvoor specifieke en uitzonderlijke methoden moeten worden aangewend en dat de beperking van het territoriale toepassingsgebied de ADIV verhindert zijn deel van de samenwerking na te komen.¹⁴

De memorie van toelichting stelt eveneens dat het verbod om specifieke en uitzonderlijke methoden door de ADIV aan te wenden in het buitenland op dit moment ernstige problemen veroorzaakt.

De volgende voorbeelden zijn betekenisvol in het kader van voorliggend toezichtonderzoek:

- *“Wanneer bijvoorbeeld tijdens een militaire operatie in het buitenland de gsm van een kamikaze gevonden wordt, mag de ADIV de gegevens die hierop staan en die cruciale informatie kunnen leveren over eventuele nieuwe dreigingen, niet verzamelen. Het betreft immers een uitzonderlijke methode van intrusie in een informaticasysteem (artikel 18/16 W.I&V) die enkel op het grondgebied van het Rijk is toegestaan.”. Verder wordt verduidelijkt “dat de intrusie in een informaticasysteem op grond van artikel 44/1 (zie infra), niet kan plaatsvinden indien de kamikaze niet toebehoort tot een organisatie of instelling opgenomen in de jaarlijkse intrusieplan. Bijvoorbeeld indien “een Belgische militair radicaliseert in het buitenland dan is het gebruik van de uitzonderlijke methode bedoeld in artikel 18/16 onontbeerlijk is aangezien het vanzelfsprekend is dat het Belgisch leger nooit zal worden opgenomen op de lijst met de te volgen instellingen en organisaties opgenomen in het jaarlijkse intrusieplan”;*
- *“Art. W.I&V. 18/7: het gebruik van een IMSI-catcher laat toe om een gevaarlijk persoon waarvan men het telefoonnummer kent te lokaliseren. Deze locatie zou, bijvoorbeeld, noodzakelijk kunnen zijn als de ADIV ontdekt dat een gestoorde Belgische militair, tijdens een operatie, een wraakactie plant tegen zijn collega’s”;*
- *“Art 18/8 W.I&V: om de filières van mensensmokkelaars (bijvoorbeeld van migranten) in kaart te brengen vereist het inlichtingenwerk dat er kennis wordt genomen van bestaande contacten tussen het doelwit in het buitenland en andere individuen. De legale mogelijkheid om zich, dankzij een technisch middel, te verbinden met een antenne om oproepgegevens van de target waarvan de organisatie zich niet in het luisterplan bevindt te verzamelen, zou het werk veel efficiënter maken”;*
- *“Art. 18/16 W.I&V: de ADIV identificeert een individu die er van verdacht wordt een cyberdreiging te vormen tegen een militair belang: dit individu bevindt zich in het buitenland en maakt geen deel uit van een organisatie of instelling die zijn opgenomen in het jaarlijkse intrusieplan bedoeld in artikel 44/3. De ADIV moet kunnen overgaan tot een intrusie, in het buitenland, in het informaticasysteem van dit individu om gegevens te verzamelen om een aanval te kunnen verhinderen, om het geheel van gevaarlijke individuen te identificeren, ...”;*

¹⁴ MvT, Parl. St. Kamer 2015-16, nr. 54-2043/001, p. 6.

- *“Art. 18/17 W.I&V: de ADIV moet een individu kunnen af luisteren die een Belgisch schip in internationale wateren gijzelt, zelfs wanneer deze geen deel uitmaakt van het luisterplan bedoeld in artikel 44/3 W.I&V”.*

Vermeldenswaardig tot slot is dat de memorie van toelichting stelt dat de toepassing van specifieke en uitzonderlijke methoden bij operaties in het buitenland niet altijd toepasbaar is.¹⁵

EVALUATIE VAN HET VAST COMITÉ I

Volgens het Vast Comité I is in het kader van de wijziging van de wet op de inlichtingen -en veiligheidsdiensten, doorgevoerd in 2017, de territoriale toepassing van de BIM-wet verduidelijkt.

Deze wijziging maakt het voor de ADIV ook mogelijk om in het buitenland stilstaande of bewegende beelden te maken en in te breken in een computersysteem in het kader van artikel 44 W.I&V van de wet op de inlichtingen -en veiligheidsdiensten. Als gevolg hiervan vallen deze methoden, die gelijkwaardig zijn aan methoden voorzien door de artikelen 16/4 en 18/16 W.I&V, niet langer onder de goedkeuring van de BIM-Commissie, maar vallen deze rechtstreeks onder het toezicht van het Vast Comité I.

Enigszins verrassend heeft het Vast Comité I naar aanleiding van haar uitgevoerde controle op de BIM's, moeten vaststellen dat de ADIV tot op heden nog nooit een BIM in het buitenland heeft ingezet.

¹⁵ MvT, *Parl. St. Kamer* 2015-16, nr. 54-2043/001, 7, p. 84 en 86.

II.10. TIENDE AANBEVELING : EEN VERDUIDELIJING VAN DE INT-REGELING

Aanbeveling - Toezichtonderzoek PRISM (2013)

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

De ADIV beschikt over een bijzondere bevoegdheid tot het intercepteren van buitenlandse communicatie.

Deze "SIGINT"-bevoegdheid (m.n. *Signals Intelligence*) werd ingesteld via de Inlichtingenwet van 30 november 1998, en gewijzigd en uitgebreid door de wet van 3 april 2003. De wetswijziging van 2003 zorgde ervoor dat de ADIV niet langer uitsluitend bevoegd was voor het onderscheppen van militaire radiocommunicaties maar van elk type van communicatie uitgezonden in het buitenland.¹⁶

Een beperkt aantal, vooral legistische wijzigingen werden doorgevoerd via de wetten van 4 februari 2010¹⁷ en 5 mei 2014.

Een (vooralsnog¹⁸) laatste en inhoudelijk verregaande wijziging vond plaats via de BIM-actualisatiewet van 30 maart 2017. De BIM-actualisatiewet voerde ter zake volgende wijzigingen door:

1. De interceptiemogelijkheden van de ADIV hebben niet enkel betrekking op elke communicatie "uitgezonden in het buitenland". De mogelijkheden worden uitgebreid in die zin dat ook communicaties "ontvangen in het buitenland" voortaan onder het toepassingsgebied vallen. Hierdoor werd de ADIV bevoegd om elke communicatievorm in het buitenland te intercepteren, ongeacht wie aan de basis van de oproep ligt en waar degene die aan de basis van de oproep ligt zich bevindt, voor zover een deel van de communicatie in het buitenland verloopt;
2. Er werd in het kader van de uitvoering van de interceptiebevoegdheid in hoofde van de telecomoperatoren en -providers een wettelijke medewerkingsplicht gecreëerd. De memorie van toelichting verduidelijkt dat "(d)e doelmatigste en snelste manier om aan cable tapping te doen, (erin) bestaat (...) een beroep te doen op de medewerking van de netwerkoperatoren en verstrekkers van telecommunicatiediensten. De

¹⁶ MvT, *Parl. St.* Kamer 2002-2003, nr. 50-2059/001, 4-6.

¹⁷ Via de BIM-wet van 4 februari 2010 werd in de SIGINT-regeling – toendertijd vastgelegd in o.m. artikel 259bis, §5 Sw. – toegevoegd dat de ADIV, naast het onderscheppen, het afluisteren, het kennismaken en het opnemen van buitenlandse communicatie, bevoegd wordt voor het opsporen van dergelijke communicatie.

¹⁸ De memorie van toelichting bij de BIM-actualisatiewet stelt dat er binnen de vijf jaar na de inwerkingtreding van de wet een evaluatie moet plaatsvinden.

medewerking van bepaalde actoren die actief zijn in België, welke transmissiediensten via kabel naar en van het buitenland aanbieden, zou het immers eenvoudiger maken om communicatie- en gegevensstromen uitgezonden in het buitenland te intercepteren. Deze stromen zullen door de ADIV gefilterd worden op basis van het af luisterplan, teneinde daaruit enkel de in het buitenland uitgezonden communicaties en gegevens te halen, welke door dit plan en in verband met de opdrachten van de ADIV zijn toegestaan.”¹⁹

Cable tapping, die reeds sinds de wet van 3 april 2003 (*supra*) tot de wettelijke mogelijkheden van de ADIV behoorde, wordt hierdoor meer uitvoerbaar;

3. De SIGINT-regeling, zijnde de interceptie van buitenlandse communicatie (*cf.* art. 44 W.I&V), werd uitgebreid naar een CYBER-reglementering, m.n. inzake de intrusie van buitenlandse informaticasystemen (*cf.* art. 44/1 W.I&V) en een reglementering voor de opname van beelden in het buitenland (*cf.* art. 44/2 W.I&V). Net zoals er een jaarlijks, door de minister van Defensie goedgekeurd af luisterplan is dat een lijst bevat van de organisaties en instellingen die het voorwerp zullen zijn van de betrokken intercepties, wordt een jaarlijks intrusieplan en een jaarlijks beeldopnameplan vereist. Ook in laatstgenoemde plannen wordt een oplistijng gemaakt van de te volgen organisaties en instellingen;
4. Er wordt verduidelijkt dat de ADIV deze SIGINT-, CYBER- en beeldopnamebevoegdheid kan inzetten bij al haar wettelijke inlichtingen- en veiligheidsopdrachten van de inlichtingendienst, met uitzondering van het uitvoeren van veiligheidsonderzoeken en veiligheidsverificaties;
5. Betekenisvol in dit kader is dat de inlichtingenopdracht van de ADIV in belangrijke mate werd uitgebreid. Vanaf nu behoort ook tot de inlichtingenopdracht van de ADIV: *“het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de factoren die de nationale en internationale veiligheid beïnvloeden of kunnen beïnvloeden in die mate dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties, en er de bevoegde ministers onverwijld over in te lichten”* (*cf.* art. 11, §1, 1° in *limine* W.I&V). Dit onderdeel van de inlichtingenopdracht wordt aangeduid als de ‘inlichtingensteun aan militaire operaties’. Deze uitbreiding van het toepassingsgebied creëert logischerwijs eveneens een ruimer toepassingsgebied bij de interceptiebevoegdheid bedoeld in artikel 44 W.I&V;
6. Het toezicht werd versterkt met name door een meer ontwikkelde motivering van de jaarlijkse lijst en door de maandelijkse overzending aan het Comité van een gemotiveerde lijst met landen of organisaties en instellingen die het voorwerp zijn geweest van een af luistering intrusie of beeldopnames. Zo wordt het Comité op regelmatige wijze op de hoogte gehouden van de uitgevoerde af luisteringen, intrusies en beeldopnames;

¹⁹ MvT, *Parl. St.* Kamer 2002-2003, nr. 50-2059/001, 89.

7. Tot slot werd een verplichte evaluatie in het vooruitzicht geplaatst. De memorie van toelichting bij de BIM-actualisatiewet stelt onder andere dat binnen de vijf jaar na de inwerkingtreding van de wet de situatie opnieuw wordt geëvalueerd om na te gaan of de voorrechten van de ADIV in het buitenland uitvoerbaar zijn.

EVALUATIE VAN HET VAST COMITE I

In dit opzicht is het Vast Comité I van mening dat de huidige wetgeving volstaat.

II.11. ELFDE AANBEVELING : EEN STRIKTE NALEVING VAN ARTIKEL 33 W.TOEZICHT

Aanbeveling - Toezichtonderzoek PRISM (2013)

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

Met het oog op zijn toezichtrol wees het Vast Comité I in het verleden herhaaldelijk²⁰ op de verplichting *ex artikel 33 W.Toezicht* om 'uit eigen beweging aan het Vast Comité I de interne reglementen en richtlijnen over, alsook alle documenten die de handelwijze van de leden van die diensten regelen' over te zenden.

Nog in 2020²¹ werd in het bijzonder de ADIV aanbevolen tot een strikte naleving van dit artikel. Deze verplichting geldt ook voor afspraken, MoU's (en de bijhorende ministeriële toestemming evenals de ministeriële goedkeuringen in het geval van informele samenwerking) of akkoorden gesloten op internationaal vlak, weze het bi- of multilateraal.

Wat de VSSE betreft

De VSSE is de enige dienst die uit eigen beweging tweemaal per jaar diverse documenten/nota's meedeelt aan het Comité. Telkenmale worden tussen de 20 en 40 documenten toegestuurd. Slechts een aantal documenten zijn van belang voor de toezichts- en andere opdrachten van het Comité. De andere documenten hebben voornamelijk betrekking op administratieve en logistieke kwesties.²²

Wel interessant zijn de interne oproepen tot kandidaturen, de personeelsbewegingen, de dienstnota's en omzendbrieven (bijv. de dienstnota over de politieke mandatarissen, de omzendbrief over de erkenningsprocedure van geloofsgemeenschappen, de recente dienstnota over de reorganisatie van de Directie van de Operaties), nieuwsbrieven (bijv. deze over het nieuw ingevoerde onderzoeksmodel), de mededelingen van het directiecomité (waarin vaak toelichting wordt gegeven bij strategische keuzes). Ook verslagen van vergaderingen en rapporten van vergaderingen van het Directiecomité kunnen in die zin relevant zijn.

²⁰ Hierover werd eerder reeds onderzoek uitgevoerd: VAST COMITÉ I, *Activiteitenverslag 1996*, 28-32 (Verslag over de toepassing door de inlichtingendiensten van artikel 33 alinea 2 W.Toezicht); *Activiteitenverslag 2001*, 218-220 (De noodzakelijke inlichtingen waarover het Vast Comité I meent te moeten beschikken met het oog op de doeltreffende uitvoering van zijn opdracht); *Activiteitenverslag 2002*, 27 (Het ambtshalve toezenden van bepaalde documenten van de inlichtingendiensten aan het Vast Comité I); *Activiteitenverslag 2006*, 12; *Activiteitenverslag 2013*, 116; *Activiteitenverslag 2014*, 120.

²¹ VAST COMITÉ I, *Activiteitenverslag 2020*, 174.

²² Een aantal doorgestuurde documenten hebben geen eigenlijk nut voor het Comité; het betreft de 'delegaties van handtekening', aankondigingen van recepties, Kerstpermanenties....

Toch kon het Comité, maar dan eerder uitzonderlijk, vaststellen dat niet alle richtlijnen, protocollen,... worden toegezonden (bijv. protocol BELPIU, internationale MoU's...).

Wat de ADIV betreft

Alle richtlijnen worden verzameld in (niet steeds geactualiseerde) *Standing Operating Procedures* (SOP's). Het *updaten* van deze bundel behoort al jaren tot één van de prioriteiten uit de diverse actieplannen van de militaire inlichtingendienst.²³

EVALUATIE VAN HET VAST COMITE I

Het Vast Comité I dient vaak de verplichting voortvloeiend uit artikel 33 van de wet tot regeling van het toezicht op de politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse aan de beide inlichtingendiensten in herinnering te brengen. Het doorgeven van richtlijnen, SOP's en andere voorschriften gebeurt nog steeds niet automatisch en systematisch. Het Comité I dringt bij de diensten aan om over te gaan tot een systematische toezending van deze documenten.

Volgens het Vast Comité I blijft de naleving van art. 33 van de wet tot regeling van het toezicht op de politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse een werkpunt, zij het veel meer voor de ADIV dan voor de VSSE.

²³ J5-DOC blijkt belast met dit proces: gecentraliseerd beheer van SOP's, MoU's, NAVO STANAG's enz.