



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

Notitienummer: 2022.295

**Juridische analyse aangaande de wettelijke mogelijkheden waarover
de inlichtingendiensten beschikken met betrekking tot verstoring**

20 januari 2023

INHOUDSTAFEL

AANZET Error! Bookmark not defined.....	3
DEEL I. VERSTORING DOOR DE VSSE	3
I.1. GEBOORTE VAN DE DISRUPTIETHEORIE.....	3
I.2. OMSCHRIJVING EN SITUERING VAN HET BEGRIP DISRUPTIE.....	6
I.3. TOEPASSINGSVOORWAARDEN.....	16
I.4. PROCEDURES	18
I.5. POLITIEKE MANDATARISSEN	19
DEEL II. VERSTORING DOOR DE ADIV	22
II.1. ALGEMEEN.....	22
II.2. WETTELIJK KADER.....	24
II.3. CYBER.....	25
DEEL III. CONCLUSIES EN AANBEVELINGEN	26

Voorliggende nota bevat een juridische analyse over de disruptietheorie van de VSSE en formuleert terzake een aantal juridische georiënteerde aanbevelingen. Tevens wordt ingegaan op de wettelijke actiemogelijkheden van de ADIV in het kader van de verstoring van veiligheidsdreigingen, met bijzondere aandacht voor de offensieve cybercapaciteiten van de militaire inlichtingendienst. Er wordt op gewezen dat de verschillende termen die worden gebruikt om het verschijnsel te benoemen, namelijk "verstoring" en "disruptie", dezelfde betekenis hebben.

AANZET VAN HET ONDERZOEK

Voorliggend verslag bevat de door het Comité gemaakte juridische analyse aangaande de wettelijke mogelijkheden waarover de inlichtingendiensten beschikken met betrekking tot verstoring (ofwel disruptie). Het beoogt verduidelijking te brengen in een aangelegenheid die in stijgende mate aan bod komt in diverse door het Comité behandelde dossiers, waaronder het toezichtonderzoek naar de wijze waarop de Veiligheid van de Staat de opvolging heeft verzekerd van de imam Mohamed TOJGANI.¹ Ook binnen het door het Comité uitgeoefende toezicht in het kader van zijn opdracht als gegevensbeschermingsautoriteit (DPA) ten aanzien van de VSSE en de ADIV, in het bijzonder binnen de behandeling van DPA-klachtendossiers, komt deze aangelegenheid druppelgewijs op de voorgrond.

Tot slot vormt voorliggend verslag een uitwerking en uitdieping van de door het Comité gegeven aanbeveling rond disruptie in het toezichtonderzoek naar de opvolging van de in de parlementaire onderzoekscommissie Terroristische Aanslagen geformuleerde aanbevelingen met betrekking tot de inlichtingen- en veiligheidsdiensten.²

DEEL I. VERSTORING DOOR DE VSSE

1.1 GEBOORTE VAN DE DISRUPTIETHEORIE

De disruptietheorie binnen het Belgische 'intelligence'-domein kent zijn geboorte in de nota van 31 augustus 2016 van de administrateur-generaal van de Veiligheid van de Staat gericht aan de Voorzitter van de Parlementaire Onderzoekscommissie Terroristische aanslagen.³ Via deze nota wenste de VSSE de leden en experts van de onderzoekscommissie te informeren over diverse onderwerpen en aangelegenheden, waaronder haar visie inzake het verstoren van veiligheidsdreigingen.⁴ De inlichtingendienst stelt er: *"De VSSE is er zich van bewust dat in de huidige nationale en internationale situatie, waar de terreurdreiging nog nooit zo groot is geweest, de rol van de dienst niet beperkt kan blijven tot het louter informeren van de bevoegde autoriteiten. [De VSSE] is [...] vragende partij voor een duidelijkere definiëring van*

¹ VAST COMITÉ I, "Toezichtonderzoek naar de wijze waarop de Veiligheid van de Staat de opvolging heeft verzekerd van de imam Mohamed TOJGANI".

² VAST COMITÉ I, "Toezichtonderzoek naar de opvolging van de in de parlementaire onderzoekscommissie Terroristische Aanslagen geformuleerde aanbevelingen met betrekking tot de inlichtingen- en veiligheidsdiensten", pag. 13.

³ Deze VSSE-nota van 31 augustus 2016 is eveneens gericht aan de Minister van Justitie, de Minister van Binnenlandse Zaken en de Voorzitter van het Vast Comité I.

⁴ Voor het onderdeel handelend over de disruptieleer, zie: pag. 24 tot 26.

de eigen rol en verantwoordelijkheid op het vlak van de strijd tegen radicalisering en terrorisme. De dienst is ook vragende partij om meer verantwoordelijkheid op te nemen in deze, met name wat betreft disruptie van extremistische en terroristische activiteiten.”. Tijdens de hoorzitting van de administrateur-generaal op 5 oktober 2016 voor de Parlementaire Onderzoekscommissie herhaalde het VSSE-hoofd in grote lijnen hetgeen reeds meegedeeld in vernoemde nota.⁵

In haar Derde Tussentijds Verslag van 15 juni 2017 (m.n. handelend over het onderdeel “veiligheidsarchitectuur”) sluit de onderzoekscommissie zich aan bij de VSSE. Ze verwoordt dit als volgt: *“In België wordt traditioneel uitgegaan van de opvatting dat inlichtingendiensten in wezen een informerende rol hebben, die tot uiting komt in het overmaken van intelligence aan andere overheidsdiensten. De onderzoekscommissie acht het aangewezen om aan de VSSE een meer uitgebreide verantwoordelijkheid toe te kennen op het vlak van de bestrijding van radicalisering, extremisme en terrorisme. De onderzoekscommissie sluit zich op dit punt aan bij de door de administrateur-generaal van de VSSE voorgestelde disruptietheorie en meent dat aan de VSSE inderdaad de mogelijkheid moet worden geboden om bepaalde schadelijke activiteiten dermate te verstoren dat zij niet langer plaatsvinden of dat minstens de schadelijkheid ervan wordt gereduceerd.”.*⁶

Een volgende stap in de ontstaansgeschiedenis situeert zich in 2018. Daar waar de VSSE in 2016 nog “vragende partij” is om meer verantwoordelijkheden op te nemen wat betreft disruptie van extremistische en terroristische activiteiten, neemt de inlichtingendienst in 2018 hiertoe zelf het initiatief. In november 2018 wordt namelijk binnen de VSSE een (geclassificeerde) dienstnota verspreid die de disruptieprocedures binnen de inlichtingendienst inricht en nader uitwerkt.⁷ Hierin wordt aandacht besteed aan aspecten zoals wanneer de VSSE aan disruptie doet alsook hoe het verstoren van dreigingen – procedureel gezien – geïntegreerd dient te worden in het inlichtingenwerk. In 2020 worden deze procedures geactualiseerd⁸, rekening houdende met de digitale hervormingen binnen de VSSE alsook indachtig de lopende hervormingen rond het in te richten onderzoeksmodel binnen het inlichtingenwerk (het zgn. het investigative model).

Naast de Parlementaire Onderzoekscommissie Terroristische aanslagen, vraagt en eist ook de Nationale Veiligheidsraad meer aandacht voor het verstoren van gevaren voor de veiligheid van de Staat. In haar (eerste) Nationale Veiligheidsstrategie d.d. 1 december 2021 stelt ze: *“België is als gastland van verschillende Europese instellingen en het NAVO-hoofdkwartier een aantrekkingspool voor spionage en inmenging. Om deze dreiging te bestrijden, zetten de inlichtingendiensten in de eerste plaats in op het creëren van een ‘hostile operating*

⁵ Bijlage nr. 1 bij het Derde Tussentijds Verslag over het onderdeel “veiligheidsarchitectuur” namens de Parlementaire onderzoekscommissie (...) – Integrale verslagen van de openbare vergaderingen, , *Parl. St.*, Kamer, 2015-2016, nr. 54-1752/008, pag. 102-137.

⁶ Derde Tussentijds Verslag over het onderdeel “veiligheidsarchitectuur” namens de Parlementaire onderzoekscommissie belast met het onderzoek naar de omstandigheden die hebben geleid tot de terroristische aanslagen van 22 maart 2016 in de luchthaven Brussel-Nationaal en in het metrostation Maalbeek te Brussel, met inbegrip van de evolutie en de aanpak van de strijd tegen het radicalisme en de terroristische dreiging, *Parl. St.*, Kamer, 2015-2016, nr. 54-1752/008, pag. 308-309.

⁷ Dienstnota n° 18-50 van 5 november 2018 van de administrateur-generaal van de VSSE inzake procedures betreffende primaire en secundaire verstoring.

⁸ Dienstnota n° 20-29 van 11 juni 2020 van de administrateur-generaal van de VSSE inzake actualisering procedures betreffende primaire en secundaire disruptie (niet-classificeerd, beperkte verspreiding).

environment' voor buitenlandse inlichtingenagenten. Politieke en diplomatieke vertegenwoordigers moeten terdege bewust gemaakt worden van het gevaar en vervolgens gewapend worden tegen deze dreiging. Op die manier wordt op nationaal niveau een veiligheidscultuur gecreëerd die de nodige weerbaarheid tegen de dreiging van spionage en inmenging verzekert.”⁹

Het Vast Comité I stelt vast dat er door diverse politieke overheden ten aanzien van de VSSE strategische doelstellingen worden geformuleerd en verwachtingen werden gecreëerd op vlak van het verstoren van nationale veiligheidsdreigingen. Tot op heden vond evenwel nog geen interventie van de wetgever plaats binnen de implementatie van de disruptietheorie. Vermeldenswaardig hierbij is dat de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (hierna: Inlichtingenwet of W.I&V) sinds de hoorzitting van de administrateur-generaal van de VSSE voor de Onderzoekscommissie intussen reeds tweemaal omstandig werd gewijzigd. Noch de Wet van 30 maart 2017¹⁰ noch de Wet van 14 juli 2022¹¹ hebben echter wijzigingen aan de Inlichtingenwet aangebracht die raken aan de disruptietheorie. De Onderzoekscommissie had nochtans aanbevolen dat “[g]ezien de impact van het disruptief optreden op de rechten van de geviseerde personen of entiteiten [...] de onderzoekscommissie het essentieel [acht] dat de noodzakelijke juridische waarborgen worden voorzien. Dergelijk optreden moet aldus steunen op een te creëren wettelijke basis, waarin niet alleen de toepassingsvoorwaarden worden geschetst, maar ook de vereiste controlemechanismen worden voorzien.”¹² De Onderzoekscommissie achtte het zodoende noodzakelijk om – tot tweemaal toe – te benadrukken dat de VSSE meer bevoegdheden dient te verkrijgen op vlak van het verstoren van dreigingen doch dat dit gepaard moet gaan met de “noodzakelijke juridische waarborgen” vastgelegd in een formele wet. De nadere uitwerking van de disruptietheorie moet met andere woorden volgens de Parlementaire Onderzoekscommissie voorafgegaan worden door een parlementair debat.

In voorliggend verslag gaat het Comité, in een eerste deel, na op welke wijze de VSSE haar disruptietheorie intern nader organiseert. Hierbij wordt aandacht besteedt aan het interne regelgevend kader, en wordt nagegaan of dit afdoende is in het licht van het op de VSSE van toepassing zijnde wettelijk en verdragsrechtelijk kader. Er werd niet nagegaan hoe de burgerlijke inlichtingendienst haar disruptietheorie in de praktijk (reeds) uitvoert. Hoewel de disruptietheorie afkomstig is van de VSSE wordt, in een tweede deel, onderzocht op welke wijze de Algemene Dienst Inlichting en Veiligheid (ADIV) veiligheidsdreigingen mag bestrijden en verstoren.

⁹ Nationale Veiligheidsstrategie d.d. 1 december 2021, pag. 38 (www.premier.be).

¹⁰ 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).

¹¹ Wet van 14 juli 2022 tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst en van artikel 259bis van het Strafwetboek (BS 5 augustus 2022).

¹² *Parl. St.*, Kamer, 2015-2016, nr. 54-1752/008, pag. 56 en 308.

1.2 OMSCHRIJVING EN SITUERING VAN HET BEGRIP DISRUPTIE

1.2.1 Aard en finaliteit van disruptie

De VSSE omschrijft 'disruptie' als *"het dermate hinderen van dreigingen dat deze niet langer plaatsvinden of dat de schadelijkheid ervan aanzienlijk wordt teruggebracht"*.¹³ Er wordt een onderscheid gemaakt tussen primaire disruptie (ofwel eerstelijnsdisruptie) en secundaire disruptie (ofwel tweedelijnsdisruptie). Primaire disruptie bestaat uit *"de maatregelen waarbij de VSSE executief optreedt (zonder medewerking van externe partners) om een dreiging te verstoren"*. Secundaire disruptie is *"het resultaat van de verstrekking van gegevens of inlichtingen door de VSSE aan (overheids)instanties die binnen de eigen bevoegdheden maatregelen nemen die een dreiging verstoren"*.¹⁴

De door de VSSE bepaalde finaliteit van disruptiemaatregelen wordt als volgt omschreven: *"[v]erstoring vormt – samen met voorkomen en adviseren – een antwoord op de wens van de directie om inlichtingen te activeren enerzijds en de (inter)actievere rol die de 'klanten' van de VSSE verlangen anderzijds. Verder is verstoring een [conditio]¹⁵ sine qua non voor meer projectmatig werken volgens het investigatieve model. Het meer consequent realiseren van de visie 'Voorkomen – Adviseren – Verstoren', in de verschillende opdrachten van de VSSE, moet het de VSSE immers mogelijk maken om met beperkte middelen toch een antwoord te bieden op de dreiging"*.¹⁶ De VSSE verduidelijkt nog dat *"[a]l het werk dat de VSSE doet [...] een verstorend effect [kan] hebben"*, maar dat onder disruptie wordt verstaan *"die acties die worden ondernomen met de intentie om te verstoren en waarbij verstoren de finaliteit is"*.¹⁷

In haar nota van 31 augustus 2016 gericht aan de Onderzoekscommissie preciseert de VSSE dat *"[d]isruptie [...] zowel gericht [kan] zijn op personen die schadelijke activiteiten ontwikkelen, als op andere entiteiten die aan de basis liggen van schadelijke activiteiten of er zich mee inlaten, zoals radicale boekhandels of extremistische onderwijsinstellingen. Op macro-niveau kan het zelfs derde landen betreffen die op enigerlei wijze betrokken zijn bij de disseminatie van extremisme (of – meer hypothetisch – terrorisme) op ons grondgebied."*

Deze (interne) omschrijving maakt duidelijk dat disruptie zich situeert binnen het doelgericht gebruik van de door de VSSE ingewonnen en verwerkte inlichtingen. Bij secundaire disruptie gaat het hierbij om het gebruik van inlichtingen door de (overheids)instanties aan wie de dienst haar inlichtingen heeft overgemaakt. De VSSE gaat haar inlichtingen verstrekken aan derde instanties en personen met het specifieke doel dat laatstgenoemden vanuit hun eigen taakstelling en actiemogelijkheden maatregelen nemen die een door de VSSE vastgestelde dreiging beogen te verstoren. De VSSE gaat m.a.w. derde instanties niet enkel waarschuwen voor veiligheidsdreigingen, maar hen ook voorstellen om welbepaalde maatregelen te nemen die deze dreigingen beogen te neutraliseren of te frustreren. Typevoorbeelden van dergelijke tegenmaatregelen zijn het intrekken door de Dienst Vreemdelingenzaken van de verblijfstitel

¹³ Deze definitie vindt men terug in de dienstnota's n° 18-50 en n° 20-29. Ze werd evenwel voor de eerste maal vastgelegd in de VSSE-nota van 31 augustus 2016 gericht aan de Parlementaire Onderzoekscommissie.

¹⁴ Dienstnota n° 20-29, pag. 1.

¹⁵ Dit woord ontbreekt in de Nederlandstalige versie van betrokken definitie.

¹⁶ Dienstnota n° 18-50, pag. 1-2.

¹⁷ *Ibid.*

van een vreemdeling die op Belgisch grondgebied optreedt als agent van een buitenlandse inlichtingendienst, de *persona non grata*-verklaring tegenover een spionerende buitenlandse diplomaat, het nemen van een orde- of tuchtmaatregel tegenover een spionerende Belgische ambtenaar, en het vervolgen en berechten van een terrorist of extremist a.h.v. het bestaande straffenarsenaal.

Bij primaire disruptie daarentegen gaat het om het gebruik door de VSSE zelf van de door haar geproduceerde inlichtingen (*intelligence*). Hier gaat de VSSE zich niet langer gedragen als inlichtingendienst belast met het detecteren en opvolgen van dreigingen, maar eerder als actiedienst belast met het daadwerkelijk bestrijden van dreigingen. De VSSE neemt m.a.w. zelf de volgens haar noodzakelijke tegenmaatregelen.

Vermeldenswaardig binnen een omschrijving van de aard en finaliteit van disruptie is de eerder door de regering omschreven doelstelling van het inlichtingenwerk: *“de finaliteit van de inlichtingenopdracht bestaat uit het identificeren en beheersen van fenomenen, groeperingen en personen die een bepaalde veiligheidsdreiging betekenen of zouden kunnen betekenen. Het gaat met andere woorden zowel over het detecteren, opvolgen en beheersen van potentiële dreigingen (of risico’s), alsook over het opvolgen en beheersen van reeds gedetecteerde dreigingen (of gevaren).”*¹⁸ Dit beheersen van reeds gedetecteerde dreigingen komt duidelijk overeen met het nemen van verstoringsmaatregelen. De centrale vraag hierbij is onder welke vorm, in welke gevallen en onder welke voorwaarden een dergelijke activiteit dient plaats te vinden, alsook onder welke beperkingen en verbodsbepalingen. Zoals we hiernavolgend verduidelijken, moet bij de formulering van een antwoord hierop niet enkel gekeken worden naar het op de VSSE en, bij uitbreiding, de ADIV van toepassing zijnde wettelijke kader (bv. Inlichtingenwet¹⁹, Gegevensbeschermingswet²⁰, Classificatiewet²¹), maar eveneens naar het op beide inlichtingendiensten toepasselijke verdragsrechtelijke kader (bv. EVRM²²).

Tot slot moet de aandacht gevestigd worden op het feit dat de VSSE disruptie omschrijft als een noodzakelijke voorwaarde voor een meer projectmatig werken volgens het Investigative model. Overeenkomstig haar Strategisch Plan 2021-2024 werkt de VSSE momenteel aan een nieuw ‘onderzoeksmodel’ – het Investigative model genaamd – dat vanaf maart 2023 in gebruik zal worden genomen voor alle dreigingen waarvoor de VSSE bevoegd is. Dit model gaat uit van een onmiddellijke verwerking van de nieuwe leads²³ in een REDDbox (*Read-Evaluate-Develop-Decide* box). *“De ‘lead’ wordt onmiddellijk geëvalueerd op basis van bepaalde criteria en zo deze evaluatie een hoge score oplevert, wordt de betrokken ‘lead’*

¹⁸ Memorie van Toelichting bij de Wet van 30 maart 2017, *Parl. St.* Kamer 2015-2016, nr. 54-2043/001, 59.

¹⁹ Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (BS 18 december 1998 – afgekort: Inlichtingenwet of W.I&V).

²⁰ Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (BS 5 september 2018).

²¹ Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (BS 7 mei 1999).

²² Verdrag van 4 november 1950 tot bescherming van de rechten van de mens en de fundamentele vrijheden, ondertekend te Rome en goedgekeurd bij wet van 13 mei 1955 (BS 19 augustus 1955, *err. B.S.* 29 juni 1961).

²³ Met een *lead* wordt informatie bedoeld met betrekking tot een dreiging.

sneller en grondiger verwerkt^{24, 25} Een van de centrale doelstellingen van het in te voeren Investigative model is dat de VSSE meer doelgericht wenst te werken, en dit niet enkel bij het initiëren en uitvoeren van een inlichtingenonderzoek, doch eveneens bij het navolgend gebruik van de behaalde onderzoeksresultaten. Of zoals de VSSE het zelf verwoordde in haar communicatie naar de Parlementaire Onderzoekscommissie Terroristische aanslagen: *“De VSSE is er zich van bewust dat in de huidige nationale en internationale situatie, waar de terreurdreiging nog nooit zo groot is geweest, de rol van de dienst niet beperkt kan blijven tot het louter informeren van de bevoegde autoriteiten.”*²⁶ En verder: *“Als wij tot nu toe onze rol vaak beperkten tot het louter informeren van de autoriteiten, dan denk ik dat wij nu actiever moeten proberen te communiceren inzake de inlichtingen die door onze dienst kunnen worden verstrekt. Eventueel kunnen die vergezeld gaan van een soort van beleidsadvies, waarbij wij bepaalde zaken aanraden om te doen.”*²⁷ De interne dienstnota ‘disruptie’ van 2018 – en de actualisatie ervan in 2020 – veruitwendigen de wijze waarop de VSSE een actievere rol wenst op te nemen, en dit niet enkel binnen de externe communicatie naar de partners van de inlichtingendienst (cf. de secundaire disruptie) doch eveneens binnen het eigenmachtig executief optreden (cf. de primaire disruptie).

1.2.2 Wettelijke omschrijving

Het begrip ‘disruptie’ is een beleidsmatig en operationeel concept die juridische vertaling behoeft opdat nagegaan zou kunnen worden welke gebods- en verbodsbepalingen deze activiteiten sturen alsook welke regelgeving desgevallend ontbreekt.

SECUNDAIRE DISRUPTIE

Vanuit juridisch oogpunt is een secundaire disruptiemaatregel een doorgifte door de VSSE van inlichtingen aan derde instanties en personen overeenkomstig de toepasselijke wettelijke regeling. Een inlichtingenverstrekking kan zowel gericht zijn aan een Belgische (overheids)instantie (via een NA-nota), waarbij de Dienst Vreemdelingenzaken, de Diplomatie en het Openbaar Ministerie een bijzondere positie innemen, alsook aan een buitenlandse inlichtingen- en veiligheidsdienst (via een NE-nota).

In hoofddeorde wordt de inlichtingenverstrekking van de VSSE geregeld door artikel 19, eerste lid W.I&V.²⁸ Deze bepaling stelt: *“(d)e inlichtingen- en veiligheidsdiensten delen de*

²⁴ Overzichtsrapport "Stand van zaken Aanbevelingen Justitie, Parlementaire onderzoekscommissie aanslagen van 22 maart 2016", door de minister van Justitie toegezonden aan de Commissie voor Justitie op 18 maart 2022, Aanbeveling 43 voor de VSSE.

²⁵ VAST COMITÉ I, "Toezichtonderzoek naar de opvolging van de in de parlementaire onderzoekscommissie Terroristische Aanslagen geformuleerde aanbevelingen met betrekking tot de inlichtingen- en veiligheidsdiensten", pag. 13.

²⁶ Nota van 31 augustus 2016 van de administrateur-generaal van de VSSE gericht aan de Voorzitter van de Parlementaire Onderzoekscommissie Terroristische aanslagen, aan de Ministers van Justitie en van Binnenlandse Zaken en aan de Voorzitter van het Vast Comité I, pag. 24 (m.b.t. het disruptie-project).

²⁷ Hoorzitting op 5 oktober 2016 van de administrateur-generaal van de VSSE in de Parlementaire Onderzoekscommissie Terroristische aanslagen, Bijlage nr. 1 bij het Derde Tussentijds Verslag over het onderdeel "veiligheidsarchitectuur" namens de Parlementaire onderzoekscommissie (...) – Integrale verslagen van de openbare vergaderingen, , *Parl. St.*, Kamer, 2015-2016, nr. 54-1752/008, pag. 102-137 (118).

²⁸ Andere wetsbepalingen die het verstrekken van inlichtingen en persoonsgegevens aan derde instanties regelen, betreffen bijv. : art. 29 Wetboek van Strafvordering, art. 19/1 W.I&V, art. 6 Wet OCAD, art. 21, §5

inlichtingen bedoeld in artikel 13, tweede lid,” – m.a.w. de verwerkte informatie (‘inlichtingen’ of ‘intelligence’) die verband houden met veiligheidsdreigingen die binnen de materiële bevoegdheid van de VSSE vallen – *“slechts mee aan de betrokken ministers en de betrokken gerechtelijke en administratieve overheden, aan de politiediensten en aan alle bevoegde instanties en personen overeenkomstig de doelstellingen van hun opdrachten alsook aan de instanties en personen die het voorwerp zijn van een dreiging bedoeld in [...] [artikel] 7”*. Deze dreigingen hebben betrekking op terrorisme, extremisme, spionage, inmenging, proliferatie van massavernietigingswapens, criminele organisaties en schadelijke sekten.

Hoewel de categorieën van bestemmingen ruim omschreven zijn, is het desondanks van belang dat artikel 19, eerste lid W.I&V een exhaustieve lijst van bestemmingen is (zie de bewoordingen *“delen [...] slechts mee aan”*). Hierbij is eveneens van belang dat *“de instanties en personen die het voorwerp zijn van een dreiging”* ontvanger kunnen zijn van inlichtingen van de VSSE.

Artikel 19, eerste lid W.I&V moet samengelezen worden met artikel 20, §§ 1 en 3 W.I&V. Laatstgenoemde stelt:

“§ 1. De inlichtingen- en veiligheidsdiensten, de politiediensten, de administratieve en gerechtelijke overheden zorgen voor een zo doeltreffend mogelijke wederzijdse samenwerking. De inlichtingen- en veiligheidsdiensten zorgen er eveneens voor dat er samenwerking is met de buitenlandse inlichtingen- en veiligheidsdiensten.”

“§ 3. De Nationale Veiligheidsraad bepaalt de in artikel 19, eerste lid, bedoelde voorwaarden waaronder de inlichtingen worden meegedeeld en de voorwaarden van de in § 1 van dit artikel bedoelde samenwerking.”

Het Comité stelt vast dat er geen bijzondere richtlijnen van de Nationale Veiligheidsraad (NVR) voorhanden zijn die de mededeling en doorgifte van inlichtingen regelt ingeval *“die worden ondernomen met de intentie om te verstoren en waarbij verstoren de finaliteit is”* (Cf. de specifieke doelstelling van een mededeling en doorgifte van inlichtingen door de VSSE aan een derde instantie, zoals bepaald door de administrateur-generaal VSSE in de interne dienstnota n° 18-50 van de VSSE).

De gedeeltelijke uitvoering van de wettelijke plicht bedoeld in artikel 20, §3 W.I&V vindt wel men terug in de niet-openbare Richtlijn van 16 februari 2000 ‘op het vlak van de mededeling van inlichtingen en de samenwerking tussen de inlichtingen- en veiligheidsdiensten en de administratieve overheden en diensten’ (NVR-richtlijn BE autoriteiten). Daarnaast is er de niet-openbare Richtlijn van 30 september 2016 ‘aangaande de relaties van de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichtingen en Veiligheid (ADIV) met buitenlandse inlichtingendiensten’ (NVR-richtlijn Buitenlandse Inlichtingendiensten).²⁹

Het Comité is van oordeel dat geen van beide NVR-richtlijnen op afdoende wijze uitgewerkt zijn om tegemoet te komen aan de vereisten in artikel 20, §3 W.I&V. Het Comité erkent wel dat de NVR-richtlijn Buitenlandse Inlichtingendiensten inhoudelijk veel

Wetboek van de Belgische nationaliteit, en artt. 44/2, §2 en 44/11/3ter, §4 WPA i.o. art. 7, §1, eerste lid KB Terrorist Fighters en art. 7, §1, eerste lid KB Haatpropagandisten.

²⁹ Ook ministeriële omzendbrieven, na te zijn overlegd en goedgekeurd in de Nationale Veiligheidsraad, kunnen uitvoering geven aan de wettelijke vereiste bedoeld in artikel 20, §3 W.I&V. Deze werkwijze wordt meestal gevolgd binnen de opvolging van specifieke veiligheidsfenomenen. Een voorbeeld hiervan is de ministeriële omzendbrief Terrorist fighters en haatpropagandisten van 22 mei 2018.

omvangrijker is dan de NVR-richtlijn BE autoriteiten. Bij eerstgenoemde zou de Nationale Veiligheidsraad zich kunnen beperken tot een bijlage van de bestaande richtlijn. Laatstgenoemde is evenwel dusdanig gedateerd en bevat dusdanig weinig concrete inhoud dat een algehele herziening van deze richtlijn noodzakelijk is.

Van belang tot slot is dat noch artikel 19 W.I&V noch enig andere wetsbepaling voorzien in de mogelijkheid dat de instanties en personen van waaruit de dreiging gaat in kennis gesteld kunnen worden dat de VSSE hen opvolgt of heeft opgevolgd.³⁰ De geheimhoudingsplicht geregeld in artikel 36 W.I&V voorziet overigens dat het geheim – zoals bijvoorbeeld het feit dat de VSSE een dossier heeft over een betrokkene – enkel extern doorgegeven kan worden op grond van artikel 19 W.I&V.³¹ In het licht hiervan **rijst** onder meer **de vraag op welke rechtsgrond de VSSE bijvoorbeeld een inkennisgeving zou kunnen doen aan een target (individu of buitenlandse dienst) dat de VSSE hem opvolgt (met bijhorende waarschuwing om hiermee op te houden)**.

PRIMAIRE DISRUPTIE

Vanuit juridisch oogpunt is een primaire disruptiemaatregel het ‘gebruik’ door de VSSE zelf van de door de haar geproduceerde inlichtingen. Zoals vermeld, gaat de VSSE zich in deze niet langer gedragen als inlichtingendienst belast met het detecteren en opvolgen van dreigingen, maar eerder als actiedienst belast met het daadwerkelijk bestrijden van dreigingen.

Traditioneel wordt binnen het inlichtingenwerk een onderscheid gemaakt tussen vier soorten activiteiten: de informatiegaring, de informatiebehandeling, de inlichtingenanalyse en de inlichtingenverstrekking. Juridisch bekeken, vinden we vernoemde vier categorieën van inlichtingenactiviteiten terug in de wettelijke omschrijving van de inlichtingenopdracht. Zowel artikel 7, 1° W.I&V (algemene inlichtingenopdracht) als artikel 3°/1 W.I&V (bijzondere inlichtingenopdracht) bepalen dat de door de VSSE te verrichten activiteiten bestaan uit ‘*het inwinnen, analyseren en verwerken van inlichtingen*’.

De lege lata bestaat er geen wettelijke bepaling die de primaire disruptiemaatregelen van de VSSE regelt noch dekt. Zoals vermeld, bepalen beide vernoemde wetsbepalingen (artt. 7, 1° en 3°/1 W.I&V) dat de door de VSSE te verrichten activiteiten bestaan – en uitsluitend mogen bestaan – uit ‘*het inwinnen, analyseren en verwerken van inlichtingen*’. Operationeel vertaald stellen deze bepalingen dat de taakstelling van de VSSE binnen haar inlichtingenwerk bestaat uit inlichtingenonderzoeken en het navolgend doorgeven van de onderzoeksresultaten aan derden. Het navolgend gebruik door de VSSE van deze onderzoeksresultaten, meer bepaald het verstoringsgeoriënteerd³² aanwenden en exploiteren van de door haar geproduceerde inlichtingen, vindt geen grondslag in vernoemde wetsbepalingen.

³⁰ Ook artikel 13 W.I&V kan hiervoor overigens niet als rechtsgrond dienst doen. Dit is een te algemene bepaling om de inlichtingenverstrekking in zijn geheel te regelen. Net zoals artikel 13 W.I&V overigens een te algemene bepaling is om de informatiegaring in zijn geheel te regelen. Een standpunt dat de wetgever heeft gevolgd via de uitwerking van de gewone, specifieke en uitzonderlijke methoden (art. 14 tot 18/17 W.I&V).

³¹ Of op grond van een andere wetsbepaling die een verplichte doorgifte van inlichtingen regelt, zoals de ambtelijke aangifteplicht (art. 29 Sv) en de meldingsplicht aan het OCAD (art. 6 Wet OCAD).

³² Een andere finaliteit is bijvoorbeeld het gebruik door de VSSE van haar onderzoeksresultaten om oriëntatie te brengen in lopende inlichtingenonderzoeken of om nieuwe onderzoeken te openen.

Ook de artikelen 13 tot 19 W.I&V (m.n. de diverse bevoegdheden die de VSSE kan aanwenden binnen de uitvoering van haar inlichtingenopdrachten) vormen geen grondslag voor een primaire disruptiemaatregel. Wat de VSSE doet en hoe ze dit doet, wordt namelijk bepaald én begrensd door waarom de dienst dit doet (o.m. krachtens artikel 75, 2° van de Gegevensbeschermingswet). De uitoefening van vernoemde bevoegdheden wordt zodoende begrensd door de finaliteiten opgesomd in artikel 7, 1° en 3°/1 W.I&V. De bevoegdheden bedoeld in de artikelen 13 tot 19 W.I&V moeten m.a.w. uitgeoefend worden met het oogmerk van collecte, verwerking of doorgifte van inlichtingen, niet met het oogmerk van het navolgend gebruik door de VSSE van deze inlichtingen.

Ter illustratie: de VSSE heeft in de huidige wettelijke stand van zaken van de wetgever een observatiebevoegdheid gekregen om informatie in te winnen (cf. artt. 16/1, 18/4 en 18/11 W.I&V), niet om door middel van een niet-discrete, voor het target waarneembare en opvallende observatie een non-verbale boodschap en waarschuwing aan een target over te maken dat hij/zij door de VSSE opgevolgd wordt en op deze wijze verstorend te werken ten aanzien van betrokkene en zijn – door de VSSE als schadelijk gekwalificeerde – activiteiten.

Ter illustratie: de VSSE heeft *de lege lata* de bevoegdheid om menselijke bronnen (human intelligence / HUMINT / informanten) in de zetten (art. 18 W.I&V). Het gaat hierbij om natuurlijke personen die door de inlichtingendienst belast worden met het heimelijk inwinnen van informatie. De VSSE kan in de huidige stand van de wetgeving deze natuurlijke personen niet aanwenden als beïnvloedingsagenten, zijnde natuurlijke personen die door de inlichtingendienst belast worden met het al dan niet heimelijk verstoren van bepaalde (door de VSSE als dreiging gekwalificeerde) activiteiten. De vraag of ze hierbij al dan niet strafbare feiten plegen of uitlokken staat los van de vraag of de door de VSSE beheerde menselijke bronnen ingezet mogen worden als beïnvloedingsagent.

Ter illustratie: de VSSE is bevoegd om personen nationaal en internationaal te seinen (bv. de SIS-signalering³³, zijnde via het Schengen Informatie Systeem van de Europese Unie). Dergelijke instrumenten dienen om informatie in te winnen (bv. discreet de bewegingen van een target in kaart brengen), niet om de activiteiten van personen te verstoren (bv. door een systematische controle van betrokkene op de luchthaven).

Samengevat: **het gebruik van de VSSE van haar bevoegdheden om informatie in te winnen (de zgn. gewone, specifieke en uitzonderlijke inlichtingenmethoden) met een ander doel dan informatiegaring, meer bepaald met als opzet de inlichtingen te gebruiken met een verstoringsfinaliteit, schendt het doelbindings- en finaliteitsbeginsel³⁴ indachtig de huidige opsomming van opdrachten in artikel 7 W.I&V (en de hierin gebruikte wijze van beschrijving van deze opdrachten).**

Een wettelijke verankering van de primaire disruptie wordt door de VSSE evenwel momenteel niet weerhouden: *“In eerste instantie werd nagegaan wat vandaag mogelijk is binnen het bestaande wettelijke kader. Daaruit kwam de redenering met betrekking tot primaire en secundaire verstoringsacties. Secundair wil zeggen het informeren van partners opdat zij hun wettelijk arsenaal kunnen gebruiken om de dreiging tegen te gaan. Partners in dit verband zijn de dienst vreemdelingenzaken (toegang grondgebied) of de gouverneurs (wapendracht). Primair wil zeggen een eigenstandig optreden van de VSSE (door te gaan spreken met een target, met zijn baas...). Voor beide vormen van tussenkomst werden interne procedures*

³³ Het betreffen verzoeken van de VSSE aan het Belgische Sirene-bureau, ingericht bij de federale politie, tot internationale signaleringen via het Schengen Informatie Systeem van de Europese Unie.

³⁴ Ook wel, in het bestuursrecht, het specialiteitsbeginsel genoemd.

*vastgelegd die volgens ons de nodige garanties bieden. Wetswijzigingen vragen we niet. Dat betekent ook dat we niet vragen naar bijkomende middelen om tussen te komen. We menen dat het nuttig is om voor verdere stappen, verplicht te zijn om te werken met partners (o.a. politie en justitie). Dat biedt de meeste garanties voor een democratisch aanvaardbare manier van tegengaan van dreigingen”.*³⁵

Zoals vermeld, achtte de Onderzoekscommissie het evenwel essentieel dat, gezien de impact van het disruptief optreden op de rechten van de geïsoleerde personen of entiteiten, de noodzakelijke juridische waarborgen moesten worden voorzien. *“Dergelijk optreden moet aldus steunen op een te creëren wettelijke basis, waarin niet alleen de wettelijke toepassingsvoorwaarden worden geschetst, maar ook de vereiste controlemechanismen worden voorzien”.*³⁶

In zijn Toezichtonderzoek naar de opvolging van de in de parlementaire onderzoekscommissie Terroristische Aanslagen geformuleerde aanbevelingen met betrekking tot de inlichtingen- en veiligheidsdiensten, stelde het Comité :

“Naar de interpretatie van de minister van Justitie en bij uitbreiding de VSSE, werd voldaan aan deze aanbeveling. Het Comité is evenwel van oordeel dat in een democratische rechtsstaat de primaire verstoringsactiviteiten van de VSSE (m.a.w. het eigenmachtig optreden van de inlichtingendienst tegen een activiteit die ze zelf als bedreiging heeft gekwalificeerd) afzonderlijk gereguleerd moeten worden in een voldoende duidelijke wet in de formele zin van het woord. De achterliggende gedachte is dat er verschillende instanties verantwoordelijk moeten zijn voor het opsporen en onderzoeken van mogelijke nationale veiligheidsdreigingen, voor de dreigingsinschatting (in casu het beoordelen of personen, groeperingen of gebeurtenissen daadwerkelijk een nationale veiligheidsdreiging vormen) en voor het nemen van de nodige maatregelen tegen dergelijke dreigingen. Minstens dient de beslissingsmacht tot het executief optreden in handen te liggen van een instantie andere dan de uitvoerende instantie. Een alternatief bestaat in het inrichten van een externe controle vergelijkbaar met de BIM-controle.

*Primaire verstoringmaatregelen tegenover een natuurlijk persoon hebben vanuit mensenrechtelijk oogpunt een wettelijke basis nodig. Het Comité gaat dan ook niet akkoord met de visie van de VSSE als zou hiervoor geen wettelijke tussenkomst vereist zijn. Elke inmenging in de persoonlijke levenssfeer eist een wettelijke grondslag. Het Comité stelt vast dat de VSSE geen vragende partij is voor bijkomende wettelijke middelen (lees: bijkomende bevoegdheden). Primaire verstoringmaatregelen – zoals het geven van een waarschuwing aan een target (bv. een buitenlandse inlichtingenofficier die op Belgisch grondgebied spioneert), aan zijn werkgever (bv. de buitenlandse inlichtingendienst), het sensibiliseren van zijn slachtoffers of het verstoren van een dreiging aan de hand van een geheime tussenkomst van een menselijke bron op vraag van een inlichtingendienst – **zijn allen verstoringssacties die krachtens artikel 22 Grondwet en artikel 8.2 EVRM een wettelijke***

³⁵ Brief van de Directeur Analyse d.d. 3 augustus 2022 aan de Voorzitter van het Vast Comité I betreffende de aanbevelingen parlementaire onderzoekscommissie aanslagen – reacties VSSE. Zie: VAST COMITÉ I, “Toezichtonderzoek naar de opvolging van de in de parlementaire onderzoekscommissie Terroristische Aanslagen geformuleerde aanbevelingen met betrekking tot de inlichtingen- en veiligheidsdiensten”, pag. 69.

³⁶ *Parl. St.* Kamer, 2016-17, nrs. 54K1752/008, 308.

*grondslag eisen. Het feit dat de VSSE geen vragende partij is voor bijkomende wettelijke middelen wil dus niet zeggen dat er geen wettelijke tussenkomst nodig is.*³⁷

*Het Comité stelt vast dat de parlementaire onderzoekscommissie zich, indachtig het voorwerp van het parlementair onderzoek, heeft beperkt tot disruptie ter bestrijding van het terrorisme, extremisme en radicalisme. Het Comité wenst hierbij de aandacht te vestigen op het (grote) belang van disruptiemaatregelen binnen de contraspionage. Er wordt derhalve geadviseerd om ook de primaire disruptie binnen de contraspionage mee te nemen in een parlementair debat.”*³⁸

Deze evaluatie maakt reeds duidelijk dat het Comité geen bezwaar heeft tegen een primaire disruptiebevoegdheid voor de VSSE. Gelet op het gevoelig karakter ervan moet dit echter voorafgegaan worden door een parlementair debat, met als voorwerp van bespreking de inhoud van primaire disruptie, de toepassingsvoorwaarden, de na te leven procedure alsook de controle op de uitoefening van een dergelijke disruptiebevoegdheid.

TUSSENBSLUIT

De Onderzoekscommissie Terroristische aanslagen heeft zich in 2017 duidelijk uitgesproken voor de invoering van een disruptiebevoegdheid voor de VSSE, en dit zowel voor maatregelen inzake primaire disruptie alsook inzake secundaire disruptie. De Onderzoekscommissie drong hierbij aan – tot tweemaal toe – op een wetgevende tussenkomst van het parlement. Het Comité stelt vast dat de VSSE geen wettelijke uitwerking en tussenkomst vraagt voor de implementatie van haar disruptietheorie.

Voor wat betreft de secundaire disruptie is het Comité van oordeel dat het huidige wettelijke kader de basis legt. Het Comité beveelt echter aan om, zoals opgelegd in de Inlichtingenwet, de voorwaarden en procedure nader te laten vastleggen door de Nationale Veiligheidsraad. Het Comité dringt hierbij aan om een zekere terughoudendheid aan de dag te leggen met betrekking tot de vraag of een dergelijke NVR-richtlijn geclassificeerd dient te worden. Hierbij wordt in herinnering gebracht dat de (geactualiseerde) dienstnota n° 20-29 van de VSSE eveneens niet geclassificeerd is.³⁹

Ten gronde maakt een secundair disruptiebeleid waarbij beoogd wordt om een bepaalde dreiging (bv. de spionage- en inmengingsactiviteiten van een bepaald land) doelgericht te frustreren en te neutraliseren (bv. door bepaalde sleutelposities binnen het buitenlandse inlichtingenapparaat van dit land te verstoren⁴⁰) een inherent onderdeel uit van de wettelijke inlichtingenopdracht van de VSSE. Juridisch bekeken gaat het over het doelgericht informeren en doordacht adviseren en ondersteunen door de VSSE van andere instanties (bv. de regering en de diplomatie) opdat laatstgenoemden de noodzakelijke maatregelen zouden kunnen nemen ter bestrijding van betrokken veiligheidsdreiging. **Een secundair disruptiebeleid is zodoende in wezen een slimme externe verspreiding door de VSSE van haar inlichtingen, en**

³⁷ Inspiratie kan hiervoor worden gevonden in art. 73 van de Nederlandse wet op de inlichtingen- en veiligheidsdiensten.

³⁸ VAST COMITÉ I, “Toezichtonderzoek naar de opvolging van de in de parlementaire onderzoekscommissie Terroristische Aanslagen geformuleerde aanbevelingen met betrekking tot de inlichtingen- en veiligheidsdiensten”, pag. 70.

³⁹ Ze heeft wel de kwalificatie « beperkte verspreiding ».

⁴⁰ Zie bijvoorbeeld: Veiligheid van de Staat, Intelligence report 2021-2022, pag. 8 en 9.

verdient zonder meer navolging. Het Comité wenst wel de bemerking te maken dat, net zoals elke beleid en zoals vereist door artikel 20 §3 W.I&V, een beleid gevalideerd moet worden door de bevoegde politieke overheden (*i.c.* de Nationale Veiligheidsraad). Een persoonsgebonden verstoringsmaatregel staat daarenboven onder het corrigerend toezicht van het Vast Comité I handelend als gegevensbeschermingsautoriteit.

Voor wat betreft de primaire disruptie is het Comité van oordeel dat vanuit verdragrechtelijk én grondwettelijk oogpunt een wetgevende interventie van het Parlement noodzakelijk is. **Een persoonsgebonden verstoringsmaatregel moet, krachtens artikel 22 Grondwet en artikel 8.2 EVRM, in een formele wet geregeld worden.** Ook vanuit beleidsmatige invalshoek is een primaire disruptiebevoegdheid een te grote paradigmashift binnen het inlichtingenwerk om aan een verdere implementatie ervan geen parlementair debat te laten voorafgaan.

Meer concreet beveelt het Comité aan om, zoals in de Nederlandse wetgeving op de inlichtingen- en veiligheidsdiensten, in de Inlichtingenwet een bepaling toe te voegen bestaande uit de volgende bewoordingen: *“het bevorderen en treffen van maatregelen ter bescherming van de door de dienst te behartigen fundamentele belangen van het land en ter bestrijden van de door de dienst te beteugelen dreigingen”*.⁴¹

Het is belangrijk dat deze bepaling zou toegevoegd worden aan artikel 7 W.I&V (m.n. de opsomming van de opdrachten van de VSSE) en niet als nieuw wetsartikel tussen de artikelen 13 tot 19 W.I&V (m.n. de opsomming van bevoegdheden die de VSSE ter beschikking heeft ter uitvoering van haar opdrachten). Op deze wijze wordt toegemoet gekomen aan de legaliteitsvereiste gesteld in artikel 22 Grondwet en artikel 8.2 EVRM, maar wordt de dienst bij de uitoefening van de disruptieopdracht beperkt door de middelen/bevoegdheden die ze reeds ter beschikking heeft (en hierin beperkt door de legaliteitsvereiste bedoeld in artikel 12

⁴¹ Geïnspireerd op artikel 73 van de Nederlandse wet op de inlichtingen- en veiligheidsdiensten. Deze bepaling stelt:

“1. De diensten zijn bevoegd tot het bevorderen of treffen van maatregelen ter bescherming van door de desbetreffende dienst te behartigen belangen, al dan niet met behulp van een technisch hulpmiddel.

2. De uitoefening van de bevoegdheid, bedoeld in het eerste lid, is slechts toegestaan, indien Onze betrokken Minister of namens deze het hoofd van een dienst daarvoor toestemming heeft verleend. Het hoofd van een dienst kan aan hem ondergeschikte ambtenaren bij schriftelijk besluit aanwijzen die de toestemming, bedoeld in de eerste volzin, namens hem verlenen. Onze betrokken Minister wordt een afschrift van het besluit, bedoeld in de tweede volzin, gezonden.

3. Bij het bevorderen of treffen van een maatregel wordt slechts die maatregel bevorderd of getroffen, die gelet op de omstandigheden van het geval, waaronder de ernst van de bedreiging van de door een dienst te beschermen belangen, voor de betrokkene het minste nadeel oplevert. Artikel 26, tweede tot en met vierde lid, is van overeenkomstige toepassing.”

➔ Vertaald naar de Belgische Inlichtingenwet betreft dit de vereisten inzake subsidiariteit en proportionaliteit.

“4. Het bevorderen of treffen van maatregelen als bedoeld in het eerste lid kan bij een instructie als bedoeld in artikel 41, eerste lid, worden opgedragen aan een natuurlijke persoon als bedoeld in dat artikel.”

➔ Vertaald naar de Belgische Inlichtingenwet betreft dit een menselijke bron.

“5. In het geval dat het bevorderen of treffen van maatregelen wordt opgedragen aan een medewerker van de dienst, is artikel 41, vierde tot en met zevende lid, van overeenkomstige toepassing, met dien verstande dat onder «de natuurlijke persoon» of «persoon» in de desbetreffende artikellieden wordt verstaan: de medewerker van de dienst die wordt belast met de feitelijke uitvoering van de in het eerste lid bedoelde handelingen.”

➔ Vertaald naar de Belgische Inlichtingenwet betreft dit (1) het plegen van een strafbaar feit door een VSSE-agent, (2) het verbod tot uitlokking van een strafbaar feit, (3) de materiële en formele voorwaarden voor het plegen van een strafbaar feit.

W.I&V⁴²). Het vergt een apart debat welke eventuele bijkomende bijvoegdheden de VSSE hierbij verder dient te verkrijgen (*infra*). Het Comité is echter wel van oordeel dat de inlichtingendienst geen specifieke geweldsbevoegdheid mag worden toegekend.⁴³ De VSSE is geen politiedienst en mag dit, *dixit* het Comité, ook niet worden.⁴⁴ Uit eerdere correspondentie van de VSSE valt duidelijk af te leiden dat de dienst hier ook geen vragende partij voor is.⁴⁵ Ook de uitlokking van misdrijven dient, zoals actueel het geval, verboden te blijven. Een beïnvloedingsagent mag geen strafbare feiten provoceren.

Het is van betekenis dat hierbij, net zoals in Nederland, in de wet ook een vereiste inzake subsidiariteit en proportionaliteit wordt ingevoegd. Het Comité laat de vraag open of bij de uitvoering van een primaire disruptiemaatregel, net zoals dit het geval is in de Nederlandse regelgeving, de VSSE gebruik moet kunnen maken worden van een menselijke bron (*supra*, een beïnvloedingsagent), van een technisch hulpmiddel, en van een VSSE-agent die beschikt over de bevoegdheid tot het plegen van misdrijven.

Het Comité pleit tot slot dat bij de uitvoering ervan een externe controle gepaard gaat vergelijkbaar met de BIM-controle, MPLUS-controle⁴⁶ (met verplichte ambtshalve notificatie aan het Comité) of de DPA-controle van het Comité. Hierbij gaat het Comité een toezicht uitoefenen met de bevoegdheid om bij een vastgestelde onwettigheid corrigerende maatregelen te nemen.

1.2.3 Verschillende soorten disruptiemaatregelen

Bij de dienstnota n° 18-50 van 5 november 2018 hoort een geclassificeerde bijlage “Werkset verstoring VSSE” (ook wel “disruptietoolkit” genoemd). Deze werkset bevat een opsomming van primaire en secundaire disruptiemaatregelen. Hoewel de betrokken dienstnota intussen

⁴² Artikel 12 W.I&V: “Om hun opdrachten te vervullen, mogen de inlichtingen- en veiligheidsdiensten slechts dwangmiddelen gebruiken onder de voorwaarden die door de wet worden bepaald.”

⁴³ Binnen de VSSE beschikt het Incident Response Team (het zgn. interventieteam *cf.* art. 22 W.I&V) wel over een geweldsbevoegdheid. Meer hierover: VERSCHAEVE, B., “Het Incident Response Team van de Staatsveiligheid. De interne beveiligingsdienst van de burgerlijke inlichtingendienst toegelicht”, *Politie en Recht* nr. 1/2022, pag. 3-20.

⁴⁴ De VSSE-agenten kunnen uitzonderlijk – net zoals overigens elke burger – wel (proportioneel) geweld toepassen en zelfs kortstondig (in afwachting van de aankomst van de politie) een persoon van zijn vrijheid beroven in het kader van de wettige verdediging (art. 416 Sw). In dit kader rijzen er overigens vragen bij de recente beslissing van de minister van Justitie waarbij de VSSE-agenten andere dan de IRT-operatoren wel over een handvuurwapen maar niet langer over handboeien beschikken in het kader van hun voorgeschreven uitrusting. Een proportioneel geweldsgebruik in het kader van de uitoefening van de wettige verdediging eist immers dat, in bepaalde gevallen, VSSE-agenten over handboeien beschikken. Indien een VSSE-agent in een noodweersituatie louter een handvuurwapen draagt (bv. tijdens een observatie) waarbij een aanvaller onder schot dient te worden gehouden doch waarbij het louter dreigen met schieten niet langer effectief is, dan is daadwerkelijk schieten het enige alternatief wanneer deze VSSE-agent niet over handboeien beschikt om de aanvaller (tot de komst van de politie) te immobiliseren. Het niet beschikken over handboeien (de klassieke metalen of de toelaatbare plasticen) in dergelijke situatie leidt onverminderd tot een disproportioneel geweldsgebruik. Zie: artikel 3 Ministerieel besluit van 16 juni 2022 tot bepaling van de voorgeschreven uitrusting van de agenten van de Veiligheid van de Staat en tot vaststelling van bijzondere bepalingen betreffende het voorhanden hebben, het dragen en het bewaren van de bewapening (*BS* 19 oktober 2022).

⁴⁵ Brief van de Directeur Analyse d.d. 3 augustus 2022 aan de Voorzitter van het Vast Comité I betreffende de aanbevelingen parlementaire onderzoekscommissie aanslagen – reacties VSSE. Zie: VAST COMITÉ I, “Toezichtonderzoek naar de opvolging van de in de parlementaire onderzoekscommissie Terroristische Aanslagen geformuleerde aanbevelingen met betrekking tot de inlichtingen- en veiligheidsdiensten”, pag. 69.

⁴⁶ Bedoeld wordt de gewone inlichtingenmethoden in de artikelen 16/2 tot 16/4 W.I&V, waar een bijzondere controlemechanisme wordt uitgewerkt.

werd vervangen door de dienstnota n° 20-29 van 11 juni 2020 is de werkset nog steeds geldig. De dienstnota n° 18-50 stelt terzake: *“Medewerkers die verstoring overwegen kunnen zich inspireren op de werkset verstoring [...]. Het is mogelijk om een of meerdere versturende maatregelen in te zetten, ook een combinatie van primaire en secundaire maatregelen kan overwogen worden.”*⁴⁷

Zowel de dienstnota n° 18-50 alsook de geactualiseerde dienstnota n° 20-29 verplichten het gebruik van een standaarddocument/template voor de procedure primaire verstoring. Dit omstandig formulier bevat de evaluatie en motivatie met betrekking tot een voorstel tot primaire disruptie (m.n. de verantwoording voor de verstoring, de beoogde doelstellingen, de beschrijving van de beoogde maatregel, de evaluatie van diverse soorten risico's waaronder van operationele, juridische, diplomatieke, organisatorische en veiligheidsmatige aard, het standpunt van de betrokken dossierbeheerders, de beslissing van de hiërarchische lijn), alsook de uiteindelijke beslissing van de administrateur-generaal. Zoals de dienstnota's n° 18-50 en n° 20-29 zelf reeds stellen, is de 'Werkset verstoring VSSE' in de eerste plaats een inspiratiebron. De uiteindelijke keuze van de beoogde maatregel wordt in het disruptieformulier bepaald en beschreven. **Het Comité juicht zonder meer dit formulier toe.** Een klein aanpassing waarbij meer de nadruk wordt gelegd op de vereisten inzake subsidiariteit en proportionaliteit is evenwel aangewezen. Het Comité beveelt aan dat bij een toekomstgerichte en in de wet nader uitgewerkte toezicht van het Comité dit formulier wordt aangewend als beginpunt van de externe controle.

Het ontbreken van een exhaustieve lijst van primaire disruptiemaatregelen, gevalideerd door de Nationale Veiligheidsraad, op grond van algemene beginselen en beperkingen vastgelegd door een democratisch verkozen wetgevende vergadering, doet echter in de huidige stand van zaken vragen rijzen rond de legaliteit en democratische legitimiteit van de implementatie van de (primaire) disruptietheorie door de VSSE. Het kan geenszins de bedoeling zijn dat de VSSE zelf bepaalt welke actiemogelijkheden ze ter beschikking heeft om de door haar als dreiging gekwalificeerde activiteiten eigenmachtig (dus via primaire disruptiemaatregelen) te verstoren. Het is overigens nog maar de vraag of de VSSE hier zelf vragende partij voor is, indachtig haar bestendig verzoek doorheen de jaren om belangrijke aangelegenheden (bijv. het vastleggen van haar prioriteiten) te laten goedkeuren door de Nationale Veiligheidsraad.

1.3 TOEPASSINGSVOORWAARDEN

1.3.1 Actueel

In de dienstnota's n° 18-50 en 20-29 bepaalt de VSSE: *“Verstoren is het dermate hinderen van dreigingen dat deze niet langer plaatsvinden of dat de schadelijkheid ervan aanzienlijk wordt teruggebracht.”* De Onderzoekscommissie⁴⁸, die de VSSE wat betreft de definitie van de VSSE woordelijk herhaalt⁴⁹, stelt: *“De onderzoekscommissie [...] meent dat aan de VSSE [...] de mogelijkheid moet worden geboden om bepaalde schadelijke activiteiten dermate te verstoren dat zij niet langer plaatsvinden of dat minstens de schadelijkheid ervan wordt*

⁴⁷ Dienstnota n° 18-50, pag. 2.

⁴⁸ *Parl. St.*, Kamer, 2015-2016, nr. 54-1752/008, pag. 56 en 308.

⁴⁹ Nota van 31 augustus 2016 van de administrateur-generaal van de VSSE gericht aan de Voorzitter van de Parlementaire Onderzoekscommissie Terroristische aanslagen, aan de Ministers van Justitie en van Binnenlandse Zaken en aan de Voorzitter van het Vast Comité I, pag. 24 (m.b.t. het disruptie-project).

gereduceerd. Dergelijke disruptie kan niet alleen gericht zijn op personen, maar ook op andere entiteiten, zoals bijvoorbeeld een radicale boekhandel of een extremistische onderwijsinstelling.”

In de dienstnota n° 18-50 gaat de VSSE dieper in om de randvoorwaarden die, eventueel, aanwezig moeten zijn opdat tot verstoren zou kunnen overgegaan worden. Hier wordt voorgeschreven dat “[v]erstoren [...] in een dossier en/of op een target overwogen [kan] worden op het moment dat bv.

- *de dreiging groot is en het risico niet langer beheerst is,*
- *het louter verzamelen van inlichtingen en het inzetten van inlichtingmethoden niet meer zinvol is,*
- *bepaalde gebeurtenissen in het dossier opportuniteiten bieden tot verstoren,*
- *een dreiging geïdentificeerd is die onvoldoende ernstig is om verdere inzet van mensen en middelen te verantwoorden, maar waar het dossier wel mogelijkheden tot verstoren biedt,*
- *de aard van de dreiging de VSSE verplicht externe partners te betrekken bij het verstoren,*
- *de initiële doelstellingen in het dossier werden behaald en het dossier kan worden afgerond.”⁵⁰*

In de dienstnota n° 20-29, die dienstnota n° 18-50 opheft en vervangt, wordt deze passage niet hernomen noch worden nieuwe materiële voorwaarden ingesteld.

1.3.2 Toekomstgericht

In de huidige interne regelgeving wordt zeer weinig tot geen aandacht besteed aan de materiële voorwaarden die a priori aanwezig moeten zijn vooraleer tot disruptie overgegaan kan worden. Dossiermatig moeten de agenten van de VSSE die in een bepaalde casus wensen over te gaan tot disruptie de nodige motivering verstrekken. Maar deze verplichting verandert logischerwijs niets aan het feit dat er binnen de inlichtingendienst geen algemene toepassingsvoorwaarden bestaan, m.a.w. voorwaarden die op algemene wijze (lees: op alle dossiers) aanwezig moet zijn bij het nemen van een primaire en/of secundaire disruptiemaatregel. In de dienstnota n° 18-50 werd hier nog enige aandacht aan besteed. Al stelt het Comité vast dat betrokken voorwaarden niet exhaustief, weinig coherent en niet afdwingbaar zijn/waren. In de dienstnota n° 20-29 werd deze bepaling geschrapt.

Het Comité beveelt aan dat de wetgever (m.b.t. de primaire disruptie) en de Nationale Veiligheidsraad (m.b.t. de secundaire disruptie) de toepassingsvoorwaarden vastlegt om over te gaan tot verstoring. Het Comité wenst hier te benadrukken dat vanuit grondrechtelijk en mensenrechtelijk oogpunt het geenszins mogelijk is dat dergelijke bepaling in een NVR-richtlijn (in zijn geheel) geïdentificeerd wordt.

⁵⁰ Dienstnota n° 18-50, pag. 2.

1.4 PROCEDURES

1.4.1 Actueel

De dienstnota n° 20-29 behandelt, naast een herinnering van de door de VSSE aangewende definitie van disruptie, uitsluitend de interne procedures/werkprocessen inzake de primaire en secundaire disruptie.

Overleg en akkoord interne partners

“De eerste stap in de procedure betreft een overleg en akkoord tussen de interne partners die inhoudelijk betrokken zijn bij het dossier (analyse en buitendiensten) en de interne partners die nodig zijn bij het uitvoeren van de verstoring (bv. verbindingsofficieren, humint). De dossierbeheerder aka OWNER van het dossier organiseert dit overleg.

De thema’s die in het overleg aan bod komen zijn de opportuniteit voor verstoren, de haalbaarheid van de gekozen maatregel(en), de aanvaardbaarheid van eventuele risico’s en de beschikbaarheid van personeel voor een correcte uitvoering van de verstoring.

Bij primaire verstoring is JUR⁵¹ verplicht bij dit overleg aanwezig. Zij staat in voor de juridische evaluatie van de primaire disruptiemaatregelen.

Indien de verstoring een combinatie van primaire en secundaire maatregelen omvat, is het volgen van de procedure primaire verstoring verplicht.”.

Procedure primaire verstoring

Vervolgens wordt in de dienstnota een opsomming gegeven van de opeenvolgende fasen:

- de dossierbeheerder vervult de nodige voorbereidende werkzaamheden, meer bepaald registratie in de VSSE-gegevensbank en invulling van het disruptieformulier aan de hand van de beslissingen genomen op het voorafgaande overleg;
- het disruptieformulier volgt de hiërarchische lijn;
- bespreking van het disruptiedossier door de VSSE-directie;
- eindbeslissing (uitvoering of niet uitvoering disruptie) door het VSSE-hoofd.

Procedure secundaire verstoring

“Voor secundaire disruptie is er geen wijziging ten aanzien van de huidige procedure. De aanvraag, middels NE of NA aan een externe partner, volgt de hiërarchische lijn.”. Zoals vermeld, geschiedt de uitvoering van een secundaire disruptiemaatregel via een nota aan een Belgische (overheids)instantie (NA) en/of via een nota aan een buitenlandse inlichtingen- en veiligheidsdienst (NE).

⁵¹ De Juridische dienst van de VSSE.

De VSSE heeft ook de nodige aandacht voor het verstrekken van contextuele informatie aan de betrokken Belgische (overheids)instantie en/of de betrokken buitenlandse inlichtingen- en veiligheidsdienst: de dienstnota verduidelijkt dat “[e]en duidelijke, open en volledige interne communicatie met de verbindingsofficier (die de relatie met de betrokken externe partner onderhoudt) over de strategische doelstelling van de verstoring, inclusief eventuele alternatieve scenario’s, helpt misverstanden te voorkomen.”

1.4.2 Toekomstgericht

In de huidige interne regelgeving wordt afdoende aandacht besteed aan de te volgen interne procedures vooraleer tot disruptie overgegaan kan worden.

Het Comité beveelt wel aan dat de wetgever (m.b.t. de primaire disruptie) en de Nationale Veiligheidsraad (m.b.t. de secundaire disruptie) de beslissingsbevoegdheid vastlegt om over te gaan tot verstoring.

Voor primaire disruptie is het Comité van oordeel dat dit de (adjunct-)administrateur-generaal moet zijn zonder mogelijkheid tot delegatie (cf. de BIM-procedure).

Voor secundaire disruptie is het Comité de mening toebedeeld dat dit de (adjunct-)administrateur-generaal moet zijn, maar met een mogelijkheid tot delegatie. Het Comité beveelt sterk aan om een delegatiemogelijkheid te beperken tot het niveau van directeur, zijnde het niveau net onder de adjunct-administrateur-generaal VSSE. Gelet op de graad van inmenging op de persoonlijke levenssfeer is het niet verdedigbaar dat een disruptiebevoegdheid kan gedelegeerd worden aan een lager niveau.

Tot slot beveelt het Comité aan om in de Inlichtingenwet een meldingsplicht te creëren waarbij de inlichtingen- en veiligheidsdiensten worden verplicht om veiligheidsdreigingen die ze gedetecteerd hebben gedurende de uitoefening van hun inlichtingenopdracht door te geven aan de veiligheidsoverheden (bv. de NVO voor wat betreft veiligheidsmachtigingen, -attesten en -adviezen) ingeval de persoon het voorwerp uitmaakt van een veiligheidsscreening.

1.5 POLITIEKE MANDATARISSEN⁵²

Bijzondere aandacht verdienen de passages in de dienstnota n° 20-29 handelend over disruptie ingeval een politieke mandataris betrokken is.

Hierin wordt bepaald: “Indien een politieke mandataris betrokken is bij de primaire verstoring⁵³, dient de OWNER⁵⁴ het vakje politieke mandataris in het document “model 90”⁵⁵ aan te vinken en ook een NA op te maken voor de voogdijminister en de Premier. Een kopie van deze NA wordt gericht aan de voorzitter van het Comité I. [...] AG⁵⁶ wordt persoonlijk geïnformeerd over de aanpak en de timing indien een rechtstreeks gesprek met een politieke

⁵² Over ‘de opvolging van politieke mandatarissen’ voerde het Comité al diverse toezichtonderzoeken uit. Zie: VAST COMITÉ I, *Activiteitenverslag* 1998, 67 e.v., *Activiteitenverslag* 1999, 12 e.v., *Activiteitenverslag* 2008, 23 e.v., *Activiteitenverslag* 2013, 3 en *Activiteitenverslag* 2021, 32-33.

⁵³ Onderstreeping door het Vast Comité I.

⁵⁴ De dossierbeheerder.

⁵⁵ Het disruptieformulier.

⁵⁶ De administrateur-generaal van de VSSE.

mandataris onderdeel uitmaakt van de disruptie.”⁵⁷ Voor wat betreft de secundaire disruptie wordt vermeld: “Indien een politieke mandataris betrokken is bij de secundaire verstoring, dient de OWNER van het VESTA-QUANTUM dossier⁵⁸ wel de NA op te maken [...]”.

In zijn Activiteitenverslag 2021 schreef het Comité:

“Veelvuldig werd in (parlementaire) debatten de vraag gesteld of en in welke mate de Belgische inlichtingendiensten politieke mandatarissen (mogen) opvolgen en welke regels ze daarbij in acht moeten nemen. Vanaf begin 2018 wordt in deze binnen de VSSE een als ‘vertrouwelijk’ geclassificeerde dienstnota toegepast. Conform deze nota, die werd geactualiseerd in juni 2020⁵⁹, zendt de VSSE twee types van rapporten naar de minister van Justitie en de Premier, met kopie naar het Vast Comité I. Het betreft enerzijds punctuele rapporten over politieke mandatarissen die bijdragen aan de totstandkoming van een dreiging alsook een trimestrieel overzicht van het geheel van documenten waarin melding wordt gemaakt van deze mandatarissen. De minister van Justitie stemde daarbij in met het ‘principe de vérifications par le Comité R qui s’avèrent nécessaires conformément à la loi organique du 18 juillet 1991’.⁶⁰

Gezien nergens wordt vermeld wat het Comité wordt geacht aan te vangen met voormelde informatie, nam het zelf het initiatief een methodologie uit te werken omtrent de ‘problematiek van de opvolging van de politieke mandatarissen door de inlichtingendiensten en de rol van het Vast Comité I’. Deze methodologie werd in 2020 door de parlementaire Begeleidingscommissie goedgekeurd.”⁶¹

De bedoelde politieke mandatarissen zijn de ministers van de diverse regeringen, de Belgische commissaris in de Europese Commissie en de leden van de verschillende Parlementen, inclusief de Belgische leden van het Europees Parlement. Het gaat niet om andere verkozenen of aangeduide mandatarissen (bijv. op gemeentelijk vlak, zoals schepenen, of op provinciaal vlak, bijv. de gouverneurs).⁶²

Voor wat betreft de problematiek inzake disruptie ingeval een politieke mandataris betrokken is, moet de dienstnota n° 20-29 samengelezen worden met de VSSE-dienstnota n° 20-28.⁶³ Laatstgenoemde dienstnota regelt de wijze waarop de medewerkers van de VSSE dienen om te gaan ingeval bepaalde politieke mandatarissen opduiken in documenten van de VSSE.

Deze stelt: “Politieke mandatarissen kunnen te allen tijde (in de uitvoering van hun mandaat/in de marge van een dreiging) voorkomen in de informatie die de VSSE verzamelt. Ze kunnen genoemd worden door menselijke bronnen, opduiken in berichten van zusterdiensten, vermeld worden in krantenartikels, voorkomen in lijsten die ontstaan door toepassing van technische middelen (bv. telefonielijsten). In dergelijke gevallen loopt de politicus eerder toevallig door het beeld van de inlichtingendienst.”⁶⁴

⁵⁷ Dienstnota n° 20-29, pag. 2-3.

⁵⁸ De VSSE-gegevensbank.

⁵⁹ Deze geactualiseerde dienstnota is, in tegenstelling tot de eerdere dienstnota, niet geclassificeerd.

⁶⁰ In: Brief van de minister van Justitie gericht aan het Vast Comité I d.d. 26 juli 2018 over ‘Le recueil d’informations par un service de renseignement concernant une personne exerçant un mandat politique’, vermeld in: VAST COMITÉ I, *Activiteitenverslag 2021*, pag. 32, voetnoot 59.

⁶¹ VAST COMITÉ I, *Activiteitenverslag 2021*, 32-33.

⁶² Dienstnota n° 20-28, pag. 2.

⁶³ Dienstnota n° 20-28 van 11 juni 2020 van de administrateur-generaal van de VSSE inzake politieke mandatarissen (beperkte verspreiding).

⁶⁴ Dienstnota n° 20-28, pag. 4.

Verder wordt gesteld: *“Politieke mandatarissen worden in de operationele werking van de VSSE niet anders behandeld dan andere beroepsgroepen. Indien er redenen zijn om de eventuele betrokkenheid van een politieke mandataris bij de totstandkoming van een dreiging nader te bekijken, dan dient dit ook te gebeuren. Behalve natuurlijk in die gevallen waarbij de politieke mandataris als slachtoffer betrokken is bij de totstandkoming van een dreiging. Omdat het om politieke mandatarissen gaat dienen wel een aantal mechanismen toegepast te worden opdat de dienst geen misbruik zou maken van haar positie. Met name de plicht om bevoegde ministers te informeren van zodra er een vermoeden ontstaat dat een politieke mandataris bijdraagt tot de totstandkoming van een dreiging, is één van die mechanismen.”*⁶⁵

Van onmiddellijk belang voor voorliggende juridische analyse betreft volgend voorschrift:

“Zodra op basis van beschikbare informatie een betrokkenheid van een politieke mandataris kan vastgesteld worden bij de totstandkoming van een dreiging, wordt dit eerst via een intern verslag en vervolgens na goedkeuring door de directie-generaal, met een NA gemeld aan de minister van Justitie en de Premier (in kopie naar het Comité I). Het moet hier gaan om bevestigde of zeer waarschijnlijk geachte informatie die werd geanalyseerd en geverifieerd.

De NA bevat minstens volgende onderdelen:

- *De beschrijving van de wijze waarop de politieke mandataris bijdraagt tot de totstandkoming van de dreiging.*
- *Een inschatting van de mogelijke gevolgen die deze betrokkenheid kan doen ontstaan of heeft doen ontstaan.*
- *Hoe het dossier verder zal opgevolgd worden door de VSSE.*
- *Maatregelen die de dienst zal nemen in dit concrete geval (bv. informeren van gerechtelijke instanties / de Parlementsvoorzitter / de minister-President, gesprek met betrokkene / ...). Indien er sprake zou zijn van het inzetten van verstorende maatregelen dient dienstnota DNS 20-29 gevolgd te worden.*⁶⁶
- *Indien nuttig worden aanbevelingen geformuleerd t.a.v. de minister van Justitie en de Premier.”*⁶⁷

Uit de dienstnota's n° 20-28 en n° 20-29 blijkt duidelijk dat de VSSE zichzelf bevoegd acht om verstorend op te treden tegen als problematisch gekwalificeerde activiteiten van federale en regionale parlementsleden en ministers, en dit klaarblijkelijk niet enkel voor secundaire disruptie (m.n. het inkennisstellen en adviseren van de bevoegde instanties) maar ook voor primaire disruptie (m.n. zelf executief optreden).

Gelet op het belang voor voorliggende problematiek wenst het Comité vooreerst zijn aanbevelingen in het Toezichtonderzoek naar de opvolging van de aanbevelingen van de Onderzoekscommissie Terroristische Aanslagen in herinnering te brengen:

“Het Comité is [...] van oordeel dat in een democratische rechtsstaat de primaire verstoringactiviteiten van de VSSE (m.a.w. het eigenmachtig optreden van de inlichtingendienst tegen een activiteit die ze zelf als bedreiging heeft gekwalificeerd) afzonderlijk gereguleerd moeten worden in een voldoende duidelijke wet in de formele zin van het woord. De achterliggende gedachte is dat er verschillende instanties

⁶⁵ Dienstnota n° 20-28, pag. 4-5.

⁶⁶ Onderstreeping door het Vast Comité I.

⁶⁷ Dienstnota n° 20-28, pag. 6-7.

verantwoordelijk moeten zijn voor het opsporen en onderzoeken van mogelijke nationale veiligheidsdreigingen, voor de dreigingsinschatting (in casu het beoordelen of personen, groeperingen of gebeurtenissen daadwerkelijk een nationale veiligheidsdreiging vormen) en voor het nemen van de nodige maatregelen tegen dergelijke dreigingen. Minstens dient de beslissingsmacht tot het executief optreden in handen te liggen van een instantie andere dan de uitvoerende instantie. Een alternatief bestaat in het inrichten van een externe controle vergelijkbaar met de BIM-controle.

Primaire verstoringmaatregelen tegenover een natuurlijk persoon hebben vanuit mensenrechtelijk oogpunt een wettelijke basis nodig. Het Comité gaat dan ook niet akkoord met de visie van de VSSE als zou hiervoor geen wettelijke tussenkomst vereist zijn. Elke inmenging in de persoonlijke levenssfeer eist een wettelijke grondslag. [...].⁶⁸

Ten tweede wenst het Comité in herinnering te brengen **dat bij de toepassing van primaire disruptie – indachtig het ontbreken van een wettelijk kader – de VSSE eigenmachtig bepaalt wanneer een activiteit aanzien moet worden als een dreiging voor de veiligheid van de Staat, dat de inlichtingendienst eigenmachtig bepaalt wanneer er een primaire disruptiemaatregel moet worden ingezet, dat ze eigenmachtig bepaalt welke maatregel ze zal inzetten, en dat er geen noemenswaardige algemene toepassingsvoorwaarden voorhanden zijn.**

Als deze vaststelling in bovenstaande analyse door het Comité als problematisch wordt bestempeld tegenover ‘gewone’ targets, dan geldt dit minstens evenzeer bij het nemen en uitvoeren van primaire disruptiemaatregelen tegenover vernoemde politieke mandatarissen.

Ten derde stelt zich de vraag op grond van welk criterium de VSSE invulling heeft gegeven aan het begrip “politieke mandataris”. De dienst vult dit momenteel in als de ministers van de diverse regeringen, de Belgische commissaris in de Europese Commissie en de leden van de verschillende Parlementen. Het Comité is van oordeel dat een meer objectief criterium zou bestaan uit alle personen die vallen onder de toepassing van de aangifteplicht mandaten aan het Rekenhof zoals bepaald in de Wetten van 2 mei 1995.

DEEL II. VERSTORING DOOR DE ADIV

2.1 ALGEMEEN

De disruptietheorie werd door de VSSE gecreëerd naar aanleiding van de werkzaamheden en hoorzittingen van de Onderzoekscommissie Terroristische aanslagen. In een nota van de VSSE aan de Voorzitter van de Onderzoekscommissie werd deze aangelegenheid voor de eerste maal naar voor gebracht.

Er bestaat binnen de ADIV geen algemene disruptietheorie. Noch in de nota van 2 september 2016 van de Chef ADIV gericht aan de Voorzitter van de Parlementaire Onderzoekscommissie

⁶⁸ VAST COMITÉ I, “Toezichtonderzoek naar de opvolging van de in de parlementaire onderzoekscommissie Terroristische Aanslagen geformuleerde aanbevelingen met betrekking tot de inlichtingen- en veiligheidsdiensten”, pag. 70.

Terroristische aanslagen⁶⁹, noch gedurende zijn hoorzitting op 5 oktober 2016 voor de Onderzoekscommissie⁷⁰ kwam de disruptietheorie of een vergelijkbaar concept aan bod. De Onderzoekscommissie heeft ook geen aanbeveling ten aanzien van de ADIV geformuleerd met betrekking tot de disruptieproblematiek.

Dit verbaast. Hoewel bovenstaande analyse aantoont dat er op vlak van juridische uitwerking nog belangrijk werk te verrichten is – niet in het minst in het licht van de rechtsbescherming van de burger – is het beleidsmatig en operationeel concept van disruptie lovenswaardig. **De idee dat een inlichtingendienst zich actiever dient te gedragen in de strijd tegen activiteiten die een gevaar betekenen voor de veiligheid van de Staat verdient ook binnen de militaire inlichtingendienst nadere uitwerking.** De Onderzoekscommissie zelf verwoordt dit overigens zeer accuraat door te stellen dat *“[i]n België [...] traditioneel [wordt] uitgegaan van de opvatting dat inlichtingendiensten in wezen een informerende rol hebben, die tot uiting komt in het overmaken van intelligence aan andere overheidsdiensten. De onderzoekscommissie acht het aangewezen om aan de VSSE een meer uitgebreide verantwoordelijkheid toe te kennen op het vlak van de bestrijding van radicalisering, extremisme en terrorisme. De onderzoekscommissie sluit zich op dit punt aan bij de door de administrateur-generaal van de VSSE voorgestelde disruptietheorie en meent dat aan de VSSE inderdaad de mogelijkheid moet worden geboden om bepaalde schadelijke activiteiten dermate te verstoren dat zij niet langer plaatsvinden of dat minstens de schadelijkheid ervan wordt gereduceerd.”*⁷¹ **Het Comité is van oordeel dat deze aanbeveling, en dan vooral wat betreft de secundaire disruptie, evenzeer op de ADIV van toepassing dient te zijn.**

Hierbij hoort echter een belangrijke aanvulling. Ondanks het feit dat er binnen de ADIV geen algemene disruptietheorie bestaat, is er binnen de dienst wel sprake van een disruptie binnen bepaalde specifieke aangelegenheden. Meer zelfs, in tegenstelling tot de VSSE heeft de wetgever in het verleden wel al aan deze problematiek aandacht besteed in het kader van de activiteiten van de ADIV. Zowel in de wetbepalingen die de opdrachten van de ADIV opsommen (m.n. art. 11 W.I&V) als in de bepalingen die bepaalde cyberbevoegdheden van de ADIV regelen (o.m. art. 44/1 W.I&V) bevinden zich instrumenten die gehecht kunnen worden aan een ADIV-disruptietheorie. Dus hoewel er binnen de ADIV geen algemene disruptietheorie bestaat, kan vastgesteld worden dat er binnen het wettelijk kader van de ADIV wel al een (begin van) juridische uitwerking aanwezig is voor bepaalde vormen van disruptie.

⁶⁹ Deze ADIV-nota van 2 september 2016 is eveneens gericht aan de Minister van Defensie, de Chef Defensie en het Vast Comité I.

⁷⁰ Bijlage nr. 1 bij het Derde Tussentijds Verslag over het onderdeel “veiligheidsarchitectuur” namens de Parlementaire onderzoekscommissie (...) – Integrale verslagen van de openbare vergaderingen, , *Parl. St.*, Kamer, 2015-2016, nr. 54-1752/008, pag. 78-100.

⁷¹ Derde Tussentijds Verslag over het onderdeel “veiligheidsarchitectuur” namens de Parlementaire onderzoekscommissie belast met het onderzoek naar de omstandigheden die hebben geleid tot de terroristische aanslagen van 22 maart 2016 in de luchthaven Brussel-Nationaal en in het metrostation Maalbeek te Brussel, met inbegrip van de evolutie en de aanpak van de strijd tegen het radicalisme en de terroristische dreiging, *Parl. St.*, Kamer, 2015-2016, nr. 54-1752/008, pag. 308-309.

2.2 WETTELIJK KADER

We verwijzen hierbij naar volgende onderdelen in de Inlichtingenwet:

Artikel 11, §1, 1° W.I&V, dat **de inlichtingenopdracht van de ADIV** bevat, stelt dat de dienst belast is met het verrichten van inlichtingenonderzoeken naar bepaalde gebeurtenissen en dreigingen alsook *“er de bevoegde ministers onverwijld over inlichten alsook de regering, op haar verzoek, **advies te verlenen** bij de omschrijving van haar binnen- en buitenlands beleid inzake veiligheid en defensie”*. Een dergelijk advies sluit naadloos aan bij het voorstel van het VSSE-hoofd aan de Onderzoekscommissie: *“Als wij tot nu toe onze rol vaak beperkten tot het louter informeren van de autoriteiten, dan denk ik dat wij nu actiever moeten proberen te communiceren inzake de inlichtingen die door onze dienst kunnen worden verstrekt. Eventueel kunnen die vergezeld gaan van een soort van beleidsadvies, waarbij wij bepaalde zaken aanraden om te doen.”*⁷² Aanvullend dient wel opgemerkt te worden dat artikel 11, §1, 1° W.I&V zich eerder situeert binnen het verstrekken van advies binnen de uitwerking van strategische krijtlijnen⁷³, daar waar de administrateur-generaal van de VSSE ook en veeleer verwijst naar het doelgericht voorstellen aan de bestemmingen van haar inlichtingen om in concrete individuele dossiers bepaalde maatregelen te nemen (bv. intrekken van de verblijfstitel van een vreemdeling die op Belgisch grondgebied optreedt als agent van een buitenlandse inlichtingendienst).

Artikel 11, §1, 2° en 2°/1 W.I&V bevat **de cybersecurity-opdracht van de ADIV**. In het kader hiervan is de militaire inlichtingendienst, onder meer, belast met het neutraliseren van een cyberaanval op bepaalde informatica- en verbindingssystemen *“en er de daders van identificeren, onverminderd het recht onmiddellijk met **een eigen cyberaanval** te reageren overeenkomstig de bepalingen van het internationaal recht”*.⁷⁴

Artikel 44/1 W.I&V tot slot bepaalt dat de ADIV *“kan overgaan tot de intrusie in een informaticasysteem dat zich in het buitenland bevindt, er de beveiliging van opheffen, er technische voorzieningen in aanbrengen teneinde **de door het informaticasysteem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen, te decoderen, op te slaan en te manipuleren en het informaticasysteem te verstoren en te neutraliseren [...]**”*. Ook de VSSE heeft de bevoegdheid om zich toegang te verschaffen tot informaticasystemen (cf. art. 18/16 W.I&V). Deze bevoegdheid betreft echter een (uitzonderlijke) methode voor het verzamelen van gegevens. Op grond hiervan mag de VSSE (en de ADIV voor informaticasystemen die zich niet in het buitenland bevinden) geenszins digitale gegevens

⁷² Hoorzitting op 5 oktober 2016 van de administrateur-generaal van de VSSE, *Parl. St.*, Kamer, 2015-2016, nr. 54-1752/008, pag. 118.

⁷³ Zie ook: *Parl. St.* Kamer 2015-2016, nr. 54-2043/001, 8, 32-33.

⁷⁴ Ter info: K. CLERIX, “Knack duikt in de digitale loopgraven: wat doet het nieuwe Cyber Command van het Belgische leger?”, *Knack* 17 oktober 2022; J. MATRICHE, “Cyberespace, le nouveau champ de bataille de l’armée belge”, *Le Soir* 18 octobre 2022; “Defensie houdt Cybercommando boven het doopvont”, *Belga* en *De Morgen* 18 oktober 2022; P. DE LOBEL, “Cyber Command moet beschermen én vechten”, *De Standaard* 20 oktober 2022; J. VAN HORENBEEK, “Hoofd nieuwe Cyber Command: ‘We zullen te werk gaan zoals een sluipschutter. Kijken, wachten en indien nodig toeslaan’.”, *De Morgen* 20 oktober 2022.

manipuleren, noch informaticasystemen verstoren en neutraliseren. Dit wordt zelfs uitdrukkelijk wettelijk verboden.⁷⁵

Als onderdeel van de Krijgsmacht is van belang dat de werkzaamheden van de ADIV, naast de Inlichtingenwet, ook deels geregeld worden in de Wet van 20 mei 1994 betreffende [...] de aanwending en de paraatstelling van de Krijgsmacht en in diens uitvoeringsbesluiten. In dergelijk geval handelt de ADIV als dusdanig als militaire actiedienst. Aangezien het Vast Comité I de wettelijke opdracht heeft toezicht uit te oefenen op de ADIV en al zijn activiteiten, werd het Comité door de wetgever als dusdanig belast met het toezicht op de ADIV ingeval deze verstoringsmaatregelen verricht.

2.3 CYBER

De cybersecurity-opdracht wordt uitgeoefend door de ADIV-eenheid Cyber Command. Deze structuur werd opgericht in oktober 2022 en is de opvolger van de directie Cyber van de ADIV. Ze staat onder leiding van een generaal-majoor (de zgn. Cyber Commander).

Over de inrichting van deze nieuwe eenheid deelde de pas aangestelde Cyber Commander in de media mee:

“We zijn een onderdeel van de militaire inlichtingendienst ADIV. We worden gecontroleerd door het Comité I en de commissie Landsverdediging.”⁷⁶

De operationalisering van de cybersecurity-opdracht geschiedt zodoende aan de hand van een aparte militaire cybercapaciteit en vindt plaats via volgende functionaliteiten:

- cyberdefensie (defensieve cybercapaciteit)
- cyberintelligence (inlichtingenwerk in de virtuele wereld)
- cyberoperations (offensieve cybercapaciteit)

Specifiek over de offensieve cybercapaciteit stelde de Cyber Commander:

“Vergelijk het met een scherpschutter. 99 procent van de tijd zit je verborgen om een legitiem doelwit te volgen, slechts 1 procent van de tijd zul je schieten. Met zo min mogelijk collaterale schade. Vertaald naar de cyberwereld: zodra je binnen raakt in een netwerk, camoufleer je je en wacht je. Tot je op een gegeven moment in actie komt en een onderdeel van het netwerk tijdelijk neutraliseert. Als je tegenstrever het netwerk gebruikt om tanks te vervoeren van punt A naar punt B bijvoorbeeld.”⁷⁷

Voor een concrete invulling en operationalisering van de cybersecurity-opdracht van de ADIV dient men o.m. gebruik te maken van de ‘Glossary of terms and definitions’ van het NATO Standardization Office (NSO). In de (laatste) editie 2021 worden diverse nieuwe cyber-termen ingevoerd, waaronder het begrip ‘offensive cyberspace operation’ / ‘opération cybernétique

⁷⁵ Artikel 18/16, derde lid W.I&V: “Het in het eerste lid bedoelde binnendringen door de inlichtingen- en veiligheidsdiensten in de informaticasystemen kan enkel het verzamelen van relevante gegevens die erin werden opgeslagen, verwerkt of doorgestuurd tot doel hebben, zonder dat er een onomkeerbare vernietiging of wijziging van deze gegevens gebeurt.”

⁷⁶ K. CLERIX, “België maakt zich klaar voor de cyberoorlog. Op bezoek bij het nieuwe Cyber Command”, *Knack* 19 oktober 2022, 39.

⁷⁷ *Ibid.*, 40.

offensive' (afgekort: OCO): "Actions in or through cyberspace that create effects to achieve military objectives."⁷⁸

DEEL III. CONCLUSIES EN AANBEVELINGEN

In het licht van voorliggende juridische analyse wenst het Comité volgende aanbevelingen te formuleren:

VOOR WAT BETREFT DE SECUNDAIRE DISRUPTIE

- Ter uitvoering van de aanbeveling met betrekking tot disruptie van de Parlementaire Onderzoekscommissie Terroristische aanslagen, de goedkeuring van **een Richtlijn van de Nationale Veiligheidsraad** (cf. art. 20, §3 W.I&V) die de materiële en formele voorwaarden vastlegt waaronder de VSSE en de ADIV mogen overgaan tot het nemen en uitvoeren van maatregelen inzake **secundaire disruptie** (zowel voor wat betreft de nationale als de internationale inlichtingenverstrekking).
- De creatie van een wettelijke meldingsplicht, waarbij de VSSE en de ADIV worden verplicht om veiligheidsdreigingen die ze gedetecteerd hebben gedurende de uitoefening van hun inlichtingenopdracht door te geven aan de veiligheidsoverheden (bv. de NVO voor wat betreft veiligheidsmachtigingen, -attesten en -adviezen) ingeval de persoon het voorwerp uitmaakt van een veiligheidsscreening.

VOOR WAT BETREFT DE PRIMAIRE DISRUPTIE

- Ter uitvoering van de aanbeveling met betrekking tot disruptie van de Parlementaire Onderzoekscommissie Terroristische aanslagen, de goedkeuring van **een formele wet** (cf. art. 22 Grondwet en art. 8.2 EVRM) die de materiële en formele voorwaarden vastlegt waaronder de VSSE en de ADIV mogen overgaan tot het nemen en uitvoeren van maatregelen inzake **primaire disruptie**.
- Bijzondere aandacht hierbij verdienen:
 - Het uitwerken van een specifieke externe controle op de beslissing en de uitvoering van primaire disruptiemaatregelen.
 - Het luik politieke mandatarissen binnen de primaire disruptie.
- Het vastleggen van een exhaustieve lijst van primaire disruptiemaatregelen door de **Nationale Veiligheidsraad** die door de VSSE, overeenkomstig de wettelijke toepassingsvoorwaarden en procedure, mag ingezet worden.

VOOR WAT BETREFT DE OFFENSIEVE CYBEROPERATIES VAN DE ADIV

- Het vastleggen van **de interne werkprocessen** van de eenheid Cyber Command van de ADIV, onder meer tot regeling van **de offensieve cyberoperaties**.

⁷⁸ AAP-06, ed. 2021, NATO Glossary of terms and definitions.