Fiche 1: Mededeling weerbaarheid vergroten, versterken capaciteiten om hybride dreigingen aan te pakken

1. Algemene gegevens

a) Titel voorstel
Gezamenlijke mededeling van het Europees Parlement, de Europese Raad en de Raad: Het opbouwen van weerbaarheid en reactiecapaciteit tegen hybride bedreigingen

b) *Datum ontvangst Commissiedocument*
13.06.2018

c) *Nr. Commissiedocument*
JOIN (2018) 16

d) *Eur-Lex*
https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1529312841198&uri=JOIN:2018:16:FIN

e) Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing
Niet opgesteld

f) Behandelingstraject Raad
Raad Buitenlandse Zaken

g) Eerstverantwoordelijk ministerie
Ministerie van Buitenlandse Zaken, in nauwe samenwerking met Justitie en Veiligheid (NCTV), Binnenlandse Zaken en Defensie.

2. Essentie voorstel

In deze mededeling van de Europese Commissie en de Hoge Vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid (HV) worden voorstellen gedaan voor vervolgstappen op het gebied van opsporing, preventie en respons op hybride dreigingen. Hybride conflicten kenmerken zich door gelijktijdige en meestal heimelijke acties op verschillende terreinen en tegen verschillende actoren, gericht op het destabiliseren van de tegenstander. Zowel conventionele als onconventionele middelen kunnen hier onderdeel van uitmaken, zoals cyber, verspreiding van desinformatie, aanval op (vitale) economische processen, maar ook inzet van chemische, biologisch, radiologische en nucleaire middelen (CBRN). Het voorstel volgt op de Europese Raadsconclusies van maart 2018 die uitnodigen tot vergroten van de capaciteit van de EU en haar lidstaten om hybride dreigingen het hoofd te bieden. De mededeling bouwt voort op de 22 actiepunten uit het *Gezamenlijk Kader voor de Bestrijding van Hybride Bedreigingen* (2016)[1],

1 https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

alsmede op het *Chemische, Biologische, Radiologische en Nucleaire Actie Plan* (2017)[2]. De mededeling herbevestigt dat de EU op gecoördineerde wijze wenst te werken om diverse onderdelen die deel uit (kunnen) maken van een hybride campagne te adresseren.

Na een korte samenvatting van reeds gezette stappen in EU-verband de afgelopen twee jaar, worden in de mededeling op vijf deelgebieden voorstellen gedaan om de gezamenlijke respons op hybride dreigingen verder te verbeteren:

(1) Omgevingsbewustzijn – verbeterde capaciteit om hybride dreigingen op te sporen
Om kwaadwillende acties beter te kunnen herkennen en mogelijke verbanden tussen ogenschijnlijk losstaande incidenten te kunnen leggen, wordt voorgesteld de analysecapaciteit van de EDEO Hybrid Fusion Cell[3] uit te breiden. Lidstaten worden tevens verzocht meer inlichtingen met de cel te delen. De instellingen zeggen toe het werk aan kwetsbaarheidsindicatoren te voltooien zodat lidstaten potentiële hybride dreigingen binnen diverse sectoren (zoals bij vitale infrastructuur energie en telecom, alsmede bij overheid) beter kunnen beoordelen.

(2) Versterkte maatregelen tegen chemische, biologische, radiologische en nucleaire dreigingen
De mededeling stelt dat de EU moet onderzoeken welke verdere maatregelen genomen kunnen worden om internationale regels en normen tegen het gebruik van chemische wapens te handhaven, inclusief een specifiek EU-sanctieregime tegen chemische wapens. De Commissie stelt voor om de stappen uit het EU CBRN actieplan 2017[2] op het gebied van risicovolle chemische stoffen, precursoren en opsporing van chemische dreigingen voor einde 2018 te completeren. Ook worden lidstaten aangemoedigd om voorraden van essentiële medische tegenmaatregelen en de inzetbaarheid daarvan te inventariseren.

(3) Strategische communicatie
EDEO en Commissie stellen voor om, binnen de eigen competenties, te komen tot een meer gestructureerde aanpak van desinformatie op EU-niveau. Tevens zullen de Commissie en EDEO bekijken hoe de drie Stratcom Task Forces[4] beter kunnen worden ondersteund om desinformatiecampagnes tegen te gaan. Ook beoogt de Commissie dit najaar evenementen te organiseren over dreiging op gebied van cyber en desinformatie rondom verkiezingen.

(4) Het opbouwen van weerbaarheid en afschrikking op het gebied van cyberbeveiliging
Goed functionerende cyberveiligheid wordt binnen de EU-instituties en sommige lidstaten in de weg gezeten door een gebrek aan middelen en gebrekkige coördinatie tussen EU-instellingen en

2 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_action_plan_to_enhance_preparedness_against_chemical_biological_radiological_and_nuclear_security_risks_en.pdf
3 De EDEO Hybrid Fusion Cell is in 2016 opgezet binnen het EU inlichtingen- en situatiecentrum (IntCen) om publieke en geclassificeerde informatie te analyseren en mogelijke hybride aanvallen op te sporen.
4 Sinds 2015 zijn er drie 'Stratcom Taskforces' opgezet (Oost, Zuid en Westelijke Balkan) welke zich richten op het opsporen/ analyseren van, en voorlichten over, desinformatie, alsmede het verzorgen van correcte informatievoorziening.

tussen instellingen en lidstaten[5]. Het niet delen van (geclassificeerde) informatie vormt volgens de Commissie een probleem om tot gecoördineerde attributie, en daarmee afschrikking, van cyberaanvallen te komen. De Commissie roept het Europees Parlement en de Raad op om de onderhandelingen over voorstellen met betrekking tot cybersecurity in 2018 af te ronden[6]. Tevens zullen de instellingen met de lidstaten samenwerken om cyber-elementen in EU-brede crisismanagement- en reactiemechanismes te bevorderen. Ook wordt voorgesteld om een trainings- en onderwijsplatform op te zetten om training over cybersecurity te coördineren.

(5) Weerbaarheid opbouwen tegen vijandige inlichtingenactiviteiten

Om ongewenste inlichtingen-activiteiten tegen te gaan wordt gepleit voor betere coördinatie tussen lidstaten en voor het versterken van capaciteiten van EU-instituties door het vergroten van bewustzijn. Hiertoe willen EDEO en Commissie de *Hybrid Fusion Cell* uitbreiden met CI-expertise. Ook worden het Europees Parlement en de Raad opgeroepen de onderhandelingen over het voorstel inzake investeringsscreening (COM(2017)487) dit jaar af te ronden.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

Nederland ziet meerwaarde om binnen de EU samen op te trekken, en van elkaar te leren hoe hybride dreigingen beter kunnen worden gedetecteerd zodat effectiever kan worden opgetreden tegen mogelijke aanvallen. Daarom is Nederland dit jaar toegetreden tot het *European Centre of Excellence Countering Hybrid Threats*[7] en neemt Nederland actief deel aan besprekingen over dit onderwerp binnen EU- en NAVO-verband. Ook op nationaal vlak zijn stappen gezet op dit terrein. Het kabinet zet hierbij in op een brede aanpak van ongewenste buitenlandse inmenging, waar het tegengaan van desinformatiecampagnes deel van uitmaakt, gericht op een goede informatiepositie, effectieve interbestuurlijke en internationale samenwerking, het voeren van een dialoog met landen van zorg, met als doel het vergroten van de weerbaarheid in Nederland en gecoördineerd optreden wanneer zich incidenten voordoen. Hybride dreigingen en overheidsbrede respons daarop vormen onderdeel van de voor de zomer van 2019 te verschijnen interdepartementale nationale veiligheidsstrategie.

b) Beoordeling + inzet ten aanzien van dit voorstel

De beoordeling van Nederland ten aanzien van de mededeling is positief met een aantal kanttekeningen. De mededeling vormt veelal een herbevestiging en uitwerking van staand Europees beleid en doet geen aanzet tot concreet nieuw beleid. Door de mededeling wordt wel de

5 In dat licht nam de EU eerder een richtlijn aan met maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, en werd een aantal relevante bepalingen opgenomen in de Algemene Verordening Gegevensbescherming.

6 Dit betreft de verordening Europese Verstrekkings- en Bewaringsbevelen voor e-evidence: (COM(2018) 225 final (17.4.2018 en COM(2018) 226 final (17.4.2018).

7 Dit Europese kenniscentrum op gebied van hybride dreiging is in 2017 opgezet als uitvloeisel van het *EU Gezamenlijk Kader voor de Bestrijding van Hybride Bedreigingen*. Zestien landen hebben zich inmiddels aangesloten.

urgentie om tot verdere uitwerking van afgesproken stappen te komen, benadrukt. Hieronder volgt een korte beoordeling en inzet per deelonderwerp:

(1) Omgevingsbewustzijn – verbeterde capaciteit om hybride dreigingen op te sporen

Het herkennen van hybride dreigingen is noodzakelijk om actie te kunnen ondernemen. Door het multidimensionale en veelal heimelijke karakter van hybride conflictvoering kan deze alleen worden onderkend wanneer breed gecoördineerd en actief wordt gezocht naar deze acties. Het kabinet ziet het samenbrengen en delen van informatie door de EU dan ook als een goede ontwikkeling en ondersteunt deze. Voor het reeds opgestarte proces om te komen tot kwetsbaarheidsindicatoren heeft Nederland de gevraagde informatie aan de instellingen geleverd.

(2) Versterkte maatregelen tegen chemische, biologische, radiologische en nucleaire bedreigingen

De mededeling bevestigt de Nederlandse inzet en analyse met betrekking tot de dreiging die uitgaat van chemische, biologische, radiologische en nucleaire strijdmiddelen, die zowel in de Geïntegreerde Buitenland- en Veiligheidsstrategie als de Defensienota aan de orde is gesteld. In Nederland is na de publicatie van het eerste CBRN Action Plan (2010-2015) al veel gebeurd op het terrein van CBRN. Het in 2017 vastgestelde EU CBRN Actieplan is een goed vervolg hierop en vormt een basis voor EU-inzet voor opbouw van capaciteit, weerbaarheid en coördinatie. De door de Commissie voorgestelde stappen passen in dat kader en kunnen dan ook gesteund worden. Hoewel een incident als in Salisbury het CBRN-dossier beïnvloedt, is de Nederlandse beleidsmatige benadering van de dreiging systeem- en niet incident-gedreven. Een goed werkend systeem dient namelijk ook onbekende dreigingen en stoffen te kunnen mitigeren.

(3) Strategische communicatie

Nederland deelt de analyse dat gerichte desinformatiecampagnes een bedreiging vormen voor het vertrouwen in de rechtsstaat, de mogelijkheid om geïnformeerde beslissingen te nemen en te participeren in de democratische samenleving. De Europese Commissie presenteerde recentelijk een Europese aanpak van desinformatie met gerichte maatregelen om de invloed van desinformatie te verminderen. Nederland onderkent het grensoverschrijdende karakter van online desinformatie en kan de Europese aanpak, voor zover deze bestaande bevoegdheden en de onafhankelijkheid van de media waarborgt, verwelkomen. Zie voor de Nederlandse aanpak en de inzet op de aangekondigde maatregelen het BNC-fiche (22112-2608). De voorliggende mededeling over hybride dreigingen bevat geen nadere uitwerking van de eerdere voorstellen.

De Europese Commissie en de Hoge Vertegenwoordiger zijn voornemens te komen tot een beter gestructureerde aanpak van desinformatie op EU-niveau. Nederland beoogt een afgebakende rol van Europese en nationale overheidsinstellingen in het adresseren van de dreiging die uitgaat van desinformatiecampagnes, namelijk slechts daar waar deze campagnes afkomstig zijn van statelijke actoren of aan staten gelieerde actoren in derde landen. Tevens hecht Nederland bijzonder aan het respecteren van nationale bevoegdheden en een ondersteunende rol van de EU. Ook mogen

vrijheid van meningsuiting en onafhankelijke en pluralistische media niet wordt aangetast. Zolang deze voorwaarden worden gerespecteerd, kan Nederland de voornemens ondersteunen.
Het staat de Commissie en EDEO vrij om in overleg met de lidstaten evenementen te organiseren over de dreiging van cyber en desinformatie rondom verkiezingen. Waar het gaat om de verkiezingen en het verkiezingsproces in het bijzonder is het Nederlandse standpunt dat dit een nationale aangelegenheid is. Nederland ondersteunt wel het uitwisselen van informatie en best practices tussen lidstaten om risico's/ dreigingen te onderkennen en maatregelen te treffen.

(4) Het opbouwen van weerbaarheid en afschrikking op het gebied van cyberbeveiliging
Dit gedeelte van de Mededeling bevat veelal een herbevestiging van reeds ingezette trajecten en geen aanzet tot concreet nieuw beleid. Wel wordt aansporing gedaan om deze trajecten snel af te ronden, danwel opgeroepen tot betere beleidsuitvoering. Dit laatste bijvoorbeeld door vervolgacties van lidstaten zoals betere inlichtingendeling.

Het in deze paragraaf geschetste beeld wordt deels onderschreven. Afgelopen jaren zijn al diverse concrete stappen gezet om cyberbeveiliging in Europees verband te versterken[8]. Tegelijkertijd blijft in het licht van de ontwikkeling van de cyberdreiging permanente aandacht voor cyberbeveiliging nodig.

Met betrekking tot het voorstel om een specifiek training en educatieplatform voor cyberdefensie op te zetten is Nederland van mening dat het meerwaarde kan hebben om bestaande EDA-initiatieven zoals het Cyber Defence Training & Excercises Coordination Platform (CD TEXP) en Demand Pooling for Cyber Defence Training and Exercise (DePoCyTE) te versterken en overlap daarmee wordt voorkomen. In ieder geval is Nederland geen voorstander van een geheel nieuw platform. Gezochte synergie met NAVO wordt toegejuicht, mits ook hier doublures worden voorkomen.
Nederland deelt voorts de inschatting van de Commissie dat van attributie van cyberaanvallen een afschrikwekkende werking uit kan gaan. Om die reden is het van belang dat lidstaten hun informatie-uitwisseling verder versterken. Daarnaast is vanwege de inherente grenzeloosheid van het internet internationale samenwerking tussen landen in de opsporing en vervolging van cybercrime zeer belangrijk, alsmede optimalisering van de huidige vormen van samenwerking en waar nodig ontwikkeling van aanvullende of nieuwe Europese of internationale juridische kaders. De voorstellen kunnen ook worden gezien in relatie tot de recente voorstellen voor het verbeteren

[8] Genoemde trajecten zijn o.a. de Cybersecurity Strategie van de EU van 2013, de relevante bepalingen in de reeds aangenomen AVG en NIB-richtlijn, en het in september 2017 door de Commissie gepubliceerde EU-cyberpakket waaronder de vernieuwing van het ENISA-mandaat, de verordening inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie, het voorstel voor oprichting van een netwerk van (nationale) kenniscentra voor cyberbeveiliging met een centraal Europees onderzoeks- en kenniscentrum voor cyberbeveiliging, de Recommendation for Coordinated Response to Large Scale Cybersecurity Incidents and Crises ("Blueprint") en de zgn. 'Cyber Diplomacy Toolbox' (Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities), waarbij recente inzet van het toolbox instrumentarium als voorbeeld wordt genoemd. In concreto gaat het om aanname van Raadsconclusies waarin kwaadwillend gebruik van informatie- en communicatietechnologie (zoals bv. de WannaCry en NonPetya cyberaanvallen) wordt veroordeeld.

van grensoverschrijdende toegang van elektronisch bewijs. De voorstellen van de Commissie zijn dienstig aan versnelde besluitvorming op relevante trajecten en verbeterde weerbaarheid van de EU en kunnen dan ook worden gezien als constructieve en haalbare stappen ten behoeve van betere cyberveiligheid.

(5) Weerbaarheid opbouwen tegen vijandige inlichtingenactiviteiten

Nederland heeft geen bezwaren tegen de oproep tot snelle afronding van de onderhandelingen over het voorstel inzake investeringsscreening (COM(2017)487) en ziet ook het belang van het creëren van een dergelijk mechanisme (zie ook Kamerstuk 22 112, nr. 2437: Mededeling en Verordening Investeringstoets). Echter mist Nederland een solide onderbouwing waarom dit voorstel van belang is voor het vergroten van de weerbaarheid tegen de activiteiten van vijandige diensten. Nederland heeft twijfels aan deze link aangezien het investeringstoetsvoorstel een kader creëert bij de toetsing op basis van nationale veiligheid van buitenlandse investeringen in de EU. Het voorstel verplicht EULS niet om te toetsen. Voorts steunt Nederland het vergroten van de kennis over contra-inlichtingen bij de Hybrid Fusion Cell en het vergroten van de weerbaarheid van EU instituties.

c) Eerste inschatting van krachtenveld

Het onderwerp hybride dreigingen is voor velen geen eenduidig begrip, hetgeen eraan bijdraagt dat er het onderwerp vanuit verschillende hoeken wordt benaderd. De focus gaat in de meeste landen uit naar de onderdelen strategische communicatie en cyberveiligheid. Het opvoeren van CBRN binnen deze discussie is een relatief recente ontwikkeling. In algemene zin is er grote steun onder lidstaten voor het werk binnen de EU op hybride dreigingen en strategische communicatie. Dit geldt met name voor de landen in met name noord-, midden- en oost Europa die externe dreiging voelen.

4. Grondhouding ten aanzien van bevoegdheid, subsidiariteit, proportionaliteit, financiële gevolgen en gevolgen op het gebied van regeldruk en administratieve lasten

a) Bevoegdheid

De Nederlandse grondhouding ten aanzien van de bevoegdheid is positief. Op grond van artikel 4, lid 2, VEU, eerbiedigt de Unie de essentiële staatsfuncties, zoals de handhaving van de openbare orde en de bescherming van de nationale veiligheid. Met name de nationale veiligheid blijft de uitsluitende verantwoordelijkheid van elke lidstaat. De mededeling raakt aan verschillende beleidsterreinen zoals het Gemeenschappelijk Buitenlands en Veiligheidsbeleid (GBVB), waar ook het Gemeenschappelijk Veiligheids- en Defensiebeleid (GVDB) onder valt, en het terrein van de civiele bescherming. Op het terrein van het GBVB is sprake van een gedeelde bevoegdheid tussen de EU en de lidstaten (artikel 2, lid 4 VWEU). Voor het GBVB (artikel 2, lid 4 VWEU) geldt dat de lidstaten bevoegd zijn om extern naast de Unie op te treden. Voor zover de EU een positie heeft ingenomen, dienen de lidstaten deze te respecteren. Met betrekking tot civiele bescherming geldt dat de EU een aanvullende bevoegdheid heeft (artikel 6, sub f, VWEU). Dat wil zeggen dat de Unie

bevoegd is om met betrekking tot de Europese dimensie van civiele bescherming het optreden van de lidstaten te ondersteunen, te coördineren of aan te vullen.

b) Subsidiariteit

De Nederlandse grondhouding ten aanzien van de subsidiariteit van de gezamenlijke mededeling is positief. De mededeling geeft duidelijk aan dat voor zover de bestrijding van hybride dreigingen betrekking heeft op de nationale veiligheid en defensie en de handhaving van de openbare orde, de verantwoordelijkheid in eerste instantie bij de lidstaten ligt, aangezien de meeste nationale kwetsbare punten landspecifiek zijn. Talrijke lidstaten worden echter geconfronteerd met gemeenschappelijke bedreigingen, die ook gericht kunnen zijn op grensoverschrijdende netwerken of infrastructuur. Dergelijke bedreigingen kunnen doeltreffender worden aangepakt met een gecoördineerde reactie op EU-niveau, dan (enkel) door afzonderlijk optreden van de lidstaten. Optreden op EU-niveau heeft naar de mening van het kabinet dus een duidelijke toegevoegde waarde.

c) Proportionaliteit

De grondhouding van het kabinet ten aanzien van de proportionaliteit van de mededeling is positief. Het kabinet acht deze mededeling een geschikt instrument om het politieke belang van samenwerking inzake mogelijke hybride dreigingen gebundeld onder de aandacht te brengen. De mededeling voorziet daar op passende wijze in door middel van de voorgestelde afspraken zoals bijvoorbeeld het verzoek aan lidstaten om meer inlichtingen te verstrekken, nadere uitwerking van het actieplan CBRN, meer gestructureerde samenwerking inzake strategische samenwerking tussen de EDEO en Commissie. Deze mededeling gaat ook niet verder dan noodzakelijk.

d) Financiële gevolgen

Uit deze mededeling vloeien geen kosten voort. Mocht het om nu nog niet voorzienbare redenen komen tot kosten voor Nederland, dan zullen deze budgettaire gevolgen worden ingepast op de begroting van de beleidsverantwoordelijke departementen, conform de regels van de budgetdiscipline.

e) Gevolgen voor regeldruk, administratieve lasten en concurrentiekracht

Uit deze mededeling vloeit geen nieuwe regelgeving voort, omdat de mededeling uitgaat van vrijwilligheid. Gevolgen voor de regeldruk en de administratieve lasten zijn er niet.