EUROPESE
COMMISSIE

HOGE VERTEGENWOORDIGER
VAN DE UNIE VOOR
BUITENLANDSE ZAKEN
EN VEILIGHEIDSBELEID

Brussel, 13.6.2018
JOIN(2018) 14 final

GEZAMENLIJK VERSLAG AAN HET EUROPEES PARLEMENT, DE EUROPESE RAAD EN DE RAAD

over de uitvoering van het gezamenlijk kader voor de bestrijding van hybride dreigingen van juli 2017 tot en met juni 2018

INLEIDING

Het gezamenlijk kader voor de bestrijding van hybride bedreigingen – een reactie van de Europese Unie[1] plaatst omgevingsbewustzijn, weerbaarheid en reactievermogen centraal in het EU-optreden tegen hybride bedreigingen. Om aanvallen beter het hoofd te kunnen bieden en ervan te kunnen herstellen, is het van fundamenteel belang dat wij ons beter in staat stellen om kwaadwillige hybride activiteiten vroegtijdig op te sporen en te begrijpen en de weerbaarheid van kritieke infrastructuur (transport, communicatie, energie, ruimtevaart, financiën) vergroten. De bestrijding van hybride bedreigingen vereist maatregelen van zowel de lidstaten als de Europese instellingen. Het eerste verslag over de uitvoering van de 22 acties die in het gezamenlijk kader zijn vastgesteld, werd op 19 juli 2017 aan de Raad voorgelegd[2]. Deze actualisering van 2018 geeft een overzicht van de vooruitgang die sinds de zomer van vorig jaar is geboekt.

Er is aanzienlijke vooruitgang geboekt op alle vier de prioritaire actiegebieden:

- het omgevingsbewustzijn verbeteren
- de weerbaarheid opbouwen
- de lidstaten en de Unie beter in staat stellen om crisissen te voorkomen, erop te reageren en er snel en op gecoördineerde wijze van te herstellen
- de samenwerking met de NAVO versterken om te zorgen voor maatregelen die elkaar aanvullen

DE HYBRIDE AARD VAN BEDREIGINGEN ERKENNEN

<u>Actie 1</u>: ***Uitvoering van een analyse van de hybride risico's door de lidstaten***

De Raad heeft de Groep vrienden van het voorzitterschap opgericht, voorgezeten door het roulerend voorzitterschap, om de werkzaamheden voort te zetten. In december 2017 hebben de lidstaten een analyse uitgevoerd om hun belangrijkste kwetsbaarheden voor hybride bedreigingen te beoordelen. Op basis van de antwoorden van de lidstaten zal het voorzitterschap waarschijnlijk vóór eind juni 2018 een verslag voorleggen aan het Comité van permanente vertegenwoordigers (Coreper).

Gezien het verstrijken van het mandaat van de groep op het einde van juni 2018 is de Groep vrienden van het voorzitterschap tijdens zijn vergadering in april begonnen met besprekingen over het toekomstige mandaat op basis van het voorstel van het voorzitterschap. Dit voorstel zou het huidige mandaat verlengen tot 2020 en zou de inhoud ervan verbreden; volgens het huidige ontwerp zou het mandaat taken omvatten die verband houden met het analyseren van opties om de paraatheid en weerbaarheid van de lidstaten te versterken en het observeren van nationale ontwikkelingen, het bieden van hulp bij de coördinatie van beleid op het gebied van hybride bedreigingen, en het ondersteunen van de werkzaamheden van de Raad inzake de samenwerking tussen de EU en de NAVO op het gebied van de bestrijding van hybride bedreigingen, de uitwisseling van informatie en de ontwikkeling van een gemeenschappelijke visie op hybride bedreigingen.

---

1. JOIN(2016) 18 final.
2. Gezamenlijk verslag aan het Europees Parlement en de Raad over de uitvoering van het gezamenlijk kader voor de bestrijding van hybride bedreigingen: een reactie van de Europese Unie (JOIN(2017) 30 final).

ORGANISATIE VAN DE EU-REACTIE: BETERE BEWUSTMAKING

Actie 2: ***Oprichting van een EU-Fusiecel voor analyse van hybride bedreigingen***

De EU-Fusiecel voor analyse van hybride bedreigingen, die is opgericht binnen het Centrum van de Europese Unie voor de analyse van inlichtingen als onderdeel van de civiele/militaire gezamenlijke capaciteit op het gebied van inlichtingenanalyse van de EU, maakt gebruik van zowel civiele als militaire analisten en van bijdragen van de inlichtingen- en veiligheidsdiensten van de lidstaten. De Fusiecel bereikte zijn volledige operationele capaciteit in juli 2017, een status die tijdens de parallelle en gecoördineerde oefening met de NAVO in 2017 (PACE17) werd bevestigd. De Fusiecel ontvangt en analyseert gerubriceerde informatie en informatie uit open bronnen over hybride bedreigingen van een breed scala van belanghebbenden. Vervolgens worden verslagen en analyses uitgewisseld tussen de EU-instellingen en de lidstaten als basis voor de besluitvorming. De Fusiecel heeft tot nu toe meer dan 100 producten gecreëerd die betrekking hebben op hybride bedreigingen. Het CERT-EU (het computercrisisresponsteam voor de instellingen van de Europese Unie) draagt bij tot de werkzaamheden van de EU-Fusiecel voor analyse van hybride bedreigingen door informatie te delen over opkomende of bestaande cyberdreigingen. Wat chemische, biologische, radiologische en nucleaire bedreigingen, cyberinlichtingen en contra-inlichtingen betreft, is de specifieke deskundigheid momenteel echter beperkt.

Om deze werkzaamheden te ondersteunen, heeft de EU-Fusiecel voor analyse van hybride bedreigingen een netwerk van nationale contactpunten opgezet. Tot op heden hebben 26 van de 28 lidstaten contactpunten aangewezen die regelmatig bijeenkomen om hun deskundigheid met de cel te delen.

Bovendien wordt dit netwerk weerspiegeld door een gelijkwaardig gezamenlijk netwerk van de Europese Dienst voor extern optreden (EDEO) en de Commissie dat gericht is op de verwezenlijking van diverse weerbaarheidsmaatregelen. Deze bijeenkomsten vinden maandelijks plaats, waarbij de nadruk ligt op thematische kwesties zoals transport, infrastructuur, energie, cyberbeveiliging en vijandige inlichtingenactiviteiten.

Op strategisch niveau ontwikkelt de EU-Fusiecel voor analyse van hybride bedreigingen zijn relatie met het Europees Centrum voor de bestrijding van hybride bedreigingen in Helsinki door deel te nemen aan workshops en oefeningen en via routinebesprekingen over onderwerpen teneinde deskundigheid op het gebied van de bestrijding van hybride bedreigingen op te bouwen.

In het kader van de gezamenlijke verklaring vinden er dagelijks contacten plaats tussen personeelsleden van de Fusiecel en die van de Hybrid Analysis Branch van de NAVO. In september 2017 werd een baanbrekende parallelle en gecoördineerde beoordeling over een hybride onderwerp gepubliceerd. De producten die gepland zijn voor levering in 2018 zullen gericht zijn op hybride uitdagingen uit de zuidelijke en oostelijke regio's.

Actie 3: ***Strategische communicatie***

De strategische communicatie heeft in de EU een extra impuls gekregen, waarbij veel verschillende actoren capaciteiten hebben ontwikkeld. In de mededeling "Bestrijding van online-desinformatie: een Europese benadering"[3] van 26 april 2018 wordt desinformatie erkend als een hybride bedreiging en wordt een aantal maatregelen uiteengezet, waaronder een versterkt netwerk tussen de Commissie, de Europese dienst voor extern optreden en de lidstaten. De positieve ervaringen van de in maart 2015 met een mandaat van de Europese Raad opgerichte East Stratcom Task Force moeten worden ondersteund en versterkt, zoals

[3] COM(2018) 236 final.

voorgesteld in de gezamenlijke mededeling: Strijd tegen hybride bedreigingen: bescherming van de Europeanen[4].

De meeste werkzaamheden van East Stratcom zijn gericht op het ondersteunen van de EU-delegaties in de regio van het Oostelijk Partnerschap en Rusland, voornamelijk en tot op zekere hoogte in Centraal-Azië, teneinde de verspreiding van positieve boodschappen te verbeteren en een groter nationaal of regionaal publiek te bereiken. De Commissie ondersteunt deze activiteiten met een meerjarig regionaal informatie- en communicatieprogramma. De East Stratcom Task Force coördineert zijn activiteiten regelmatig, ook met de lidstaten en de NAVO. Naast het monitoren van desinformatie heeft de East Stratcom Task Force bewustmakingsactiviteiten in de landen van het Oostelijk Partnerschap en de lidstaten over de gevolgen van Russische desinformatie. De Commissie intensiveerde ook de opleiding van het personeel in landen van het Oostelijk Partnerschap om hun Stratcom-capaciteit en hun weerbaarheid tegen desinformatie te vergroten. In de toekomst is meer samenwerking met het NAVO-hoofdkwartier en de kenniscentra in Riga en Helsinki gepland, zoals het delen van analyses en opleidingsseminars voor journalisten uit de regio van het Oostelijk Partnerschap of Rusland.

Naar aanleiding van de nieuwe strategie van de EU voor de Westelijke Balkan is een op de Westelijke Balkan gerichte taskforce opgericht om het EU-beleid doeltreffender bekend te maken bij een breder publiek in de regio en tegelijkertijd het bewustzijn te vergroten over desinformatieactiviteiten die op de Westelijke Balkan zijn gericht en dergelijke activiteiten aan te pakken. De taskforce en de Commissie hebben een intensieve samenwerking tot stand gebracht met als doel meer strategische en gerichte communicatie en berichtgeving naar de regio op basis van beste praktijken en met de nadruk op thematische campagnes. Er is echter een gebrek aan bewustzijn van de groeiende bedreigingen die specifiek op de instellingen zijn gericht. Er moet een veiligheidsbewustzijn tot stand worden gebracht en de instellingen moeten beter in staat worden gesteld om hybride bedreigingen het hoofd te bieden.

De in 2017 opgerichte Task Force South heeft zijn mandaat aangepast om rekening te houden met een verschuiving van het prisma van terrorismebestrijding naar een meer genuanceerde aanpak gericht op het verbeteren van de communicatie en contacten met de Arabische wereld, ook in het Arabisch. Aangezien Da'esh of Islamitische Staat (IS) niet de enige bedreiging in termen van radicalisering is, tracht de taskforce de wijdverbreide desinformatie en misvatting van de EU te beperken. Dit gebeurt door in nauwe samenwerking met de Commissie positieve verhalen over de Europese Unie en haar beleid te brengen met het oog op een beter begrip van de Unie, door strategischer te communiceren over de activiteiten van de Unie in de Arabische wereld en door gedeelde waarden en belangen te bevorderen. De Commissie ondersteunt deze activiteiten met een meerjarig regionaal informatie- en communicatieprogramma.

<u>Actie 4:</u> ***Kenniscentrum voor de bestrijding van hybride bedreigingen.***

Het in 2017 opgerichte Europees Centrum voor de bestrijding van hybride bedreigingen fungeert als een expertisecentrum ter ondersteuning van de individuele en collectieve inspanningen van de deelnemende landen om hybride bedreigingen te bestrijden door middel van onderzoek, opleiding, onderwijs en oefeningen. Zowel EU-lidstaten als NAVO-bondgenoten kunnen zich bij het centrum aansluiten. Onlangs zijn Italië, Nederland, Denemarken en Tsjechië lid geworden, waarmee het totaal op 16 landen komt. Zowel de EU als de NAVO maken als waarnemers deel uit van de stuurgroep.

In 2018 bereikte het centrum een akkoord over een begroting en een werkplan, ontwikkelde het zijn conceptueel kader en richtte het drie belangengemeenschappen op: hybride beïnvloeding, Kwetsbaarheden en weerbaarheid en Strategie en defensie. Er is een subgroep

[4] Verwijzing in te voegen wanneer bekend.

voor niet-overheidsactoren opgericht die onderzoekt hoe verschillende terroristische groepen en hun handlangers te werk gaan. Het centrum heeft een aantal analyses van hybride bedreigingen gepubliceerd en heeft verschillende bijeenkomsten op hoog niveau georganiseerd om tot een gemeenschappelijke visie op hybride bedreigingen te komen, beste praktijken uit te wisselen en gemeenschappelijke antwoorden te zoeken in de EU- en NAVO-gemeenschappen.

ORGANISATIE VAN DE EU-REACTIE: WEERBAARHEID OPBOUWEN

Het opbouwen van weerbaarheid vereist maatregelen op veel beleidsterreinen. Deze maatregelen zijn niet noodzakelijk specifiek voor het hybride karakter van de bedreigingen, maar kunnen er samen voor zorgen dat een weerbaardere EU beter is toegerust om het hoofd te bieden aan hybride bedreigingen. Wanneer dit relevant is voor de beschrijving van de vooruitgang die in het kader van elke actie is geboekt, wordt derhalve verwezen naar het specifieke beleidskader en de acties van de Unie, met name de acties in het kader van de werkzaamheden met het oog op de totstandbrenging van een veiligheidsunie. Dit verslag moet daarom worden gelezen in samenhang met de maandelijkse voortgangsverslagen over de totstandbrenging van een echte en doeltreffende veiligheidsunie, die op dezelfde dag zijn goedgekeurd.[5]

Actie 5: *Bescherming en weerbaarheid van kritieke infrastructuur*

De Commissie heeft een ontwerphandboek over kwetsbaarheidsindicatoren en de weerbaarheid van kritieke infrastructuur tegen hybride bedreigingen in de EU opgesteld. Dit ontwerphandboek wordt momenteel gevalideerd via overleg met de lidstaten. De definitieve versie van het handboek zal naar verwachting in november 2018 worden goedgekeurd. Voorts zullen de kwetsbaarheidsindicatoren worden getest tijdens de parallelle en gecoördineerde oefening in 2018 met de NAVO (PACE18), maar ook door individuele lidstaten die belangstelling hebben getoond. Bijzondere aandacht moet worden besteed aan de verdere ontwikkeling van detectie-indicatoren die een vroegtijdige waarschuwing bij het begin van een hybride aanval op kritieke infrastructuur moeten vergemakkelijken. Bij de komende evaluatie van de Europese richtlijn inzake de bescherming van kritieke infrastructuur zal ook rekening worden gehouden met hybride bedreigingen. Voorts versterkt de Commissie de wetenschappelijke ondersteuning om de meervoudige en transversale kenmerken van hybride bedreigingen aan te pakken, met bijzondere aandacht voor de identificatie van kwetsbaarheden, vroege opsporing en indicatoren, weerbaarheid, bewustmaking en oefeningen.

Om de belangrijkste activa van de Unie te beschermen, heeft de Commissie bovendien een voorstel ingediend voor een verordening tot vaststelling van een kader voor screening van buitenlandse directe investeringen in de Europese Unie als het waarschijnlijk is dat zij van invloed zullen zijn op de veiligheid of openbare orde[6]. Het voorstel van de Commissie heeft betrekking op directe investeringen door personen of ondernemingen van derde landen die onder meer van invloed kunnen zijn op de kritieke infrastructuur (met inbegrip van energie, transport, communicatie, gegevensopslag, ruimtevaart en andere gevoelige faciliteiten), kritieke technologieën (met inbegrip van kunstmatige intelligentie, cyberbeveiliging, technologieën in toepassingen die mogelijk voor tweeërlei gebruik geschikt zijn), de voorzieningszekerheid van kritieke grondstoffen of investeringen die toegang geven tot gevoelige informatie of het vermogen om dergelijke informatie te controleren.

Het Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS II – overlegforum voor duurzame energie in de defensie- en veiligheidssector) van het

[5] COM(2018) 470 final.
[6] COM(2017) 487 final.

Europees Defensieagentschap zal in het kader van de tweede fase verder steun verlenen aan de ontwikkeling van het door de deskundigengroep Protection of Critical Energy Infrastructures (PCEI – bescherming van kritieke energie-infrastructuur) opgesteld conceptdocument en zal dit document vertalen naar een als richtsnoer bedoeld beleidsdocument op EU-niveau. Hierin wordt een kader voorgesteld voor het vaststellen van beste beheerpraktijken voor ministeries van Defensie ter versterking van de bescherming en weerbaarheid van alle defensiegerelateerde kritieke energie-infrastructuur.

<u>Actie 6:</u> ***Vergroting van de energievoorzieningszekerheid van de EU en verhoging van de bestendigheid van nucleaire infrastructuur.***

Na haar toezegging in september 2017 (gezamenlijke mededeling "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU"[7]) zal de Commissie steun blijven verlenen aan het European Energy Information Sharing and Analysis Centre (Europees Centrum voor uitwisseling en analyse van informatie over energie) op het gebied van cyberbeveiliging.

Om gasvoorzieningscrisissen te voorkomen, leggen de lidstaten de vorig jaar aangenomen verordening betreffende de veiligstelling van de aardgasvoorziening ten uitvoer, terwijl de Commissie de tenuitvoerlegging ervan en de samenwerking tussen de lidstaten binnen de risicogroepen vergemakkelijkt. De gemeenschappelijke risicobeoordelingen moeten uiterlijk op 1 oktober 2018 bij de Commissie worden ingediend. De Commissie zal de preventieve actieplannen en de noodplannen tegen 1 maart 2019 ontvangen. De lidstaten moeten uiterlijk op 1 december 2018 de bilaterale solidariteitsafspraken maken.

Om de bestaande leemte in de regelgeving op het gebied van de risicoparaatheid in de elektriciteitssector aan te pakken, zou de risicoparaatheidsverordening, waarover momenteel wordt onderhandeld, onder meer het volgende omvatten: regels voor de beoordeling van risico's, de verplichting voor de lidstaten om een risicoparaatheidsplan met bepaalde verplichte elementen op te stellen, een beschrijving van hoe crisissituaties moeten worden aangepakt en een beschrijving van hoe de voorzieningszekerheid moet worden gemonitord. De risicoparaatheidsplannen moeten ook afspraken over regionale samenwerking bevatten, met name afspraken over het beheer van gelijktijdige elektriciteitscrisissen. Bij de tenuitvoerlegging van de risicoparaatheidsverordening zouden de lidstaten twee jaar na de inwerkingtreding van de verordening de eerste nationale risicoparaatheidsplannen moeten opstellen. Daarna moeten de plannen om de drie jaar worden bijgewerkt. In de toekomstige risicoparaatheidsverordening zal ook worden bepaald dat de lidstaten regelmatig gezamenlijke oefeningen moeten houden om een elektriciteitscrisis te simuleren. De Commissie is reeds begonnen met de voorbereiding van dergelijke gezamenlijke oefeningen met geïnteresseerde lidstaten, het Gemeenschappelijk Centrum voor Onderzoek (JRC) en de Coördinatiegroep voor elektriciteit.

Met het oog op de bestendigheid van nucleaire infrastructuur zal de informatie-uitwisseling met en tussen de lidstaten en de Commissie over nucleaire-veiligheidskwesties op korte termijn worden verbeterd en is een analyse van aanvullende initiatieven gepland. Er zal een analyse van de verordening inzake nucleaire-veiligheidscontrole worden uitgevoerd en er zullen eventuele richtsnoeren worden opgesteld om de lidstaten te helpen beter om te gaan met (radioactieve) hoogactieve ingekapselde bronnen. Op langere termijn is de Commissie voornemens de activiteiten op nucleair vlak te versterken op gebieden waar de lidstaten een gemeenschappelijk belang hebben en waar informatie-uitwisseling en samenwerking een overeengekomen voordeel opleveren. De Commissie zal ook passende maatregelen bestuderen voor de effectieve tenuitvoerlegging, binnen de EU, van het internationale Verdrag inzake de fysieke beveiliging van kernmateriaal en kerninstallaties.

[7] JOIN(2017) 450 final.

Wat de defensiesector betreft, heeft het Consultation Forum for Sustainable Energy in the Defence and Security Sector de "Roadmap for Sustainable Energy Management in the Defence and Security Sector" (routekaart voor duurzaam energiebeheer in de defensie- en veiligheidssector) opgesteld om de defensiesector te ondersteunen bij het verbeteren van het beheer van de energie-infrastructuur. Het overlegforum zal blijven onderzoeken hoe de defensiesector in staat kan worden gesteld efficiënter om te gaan met energiebronnen en zal een aantal technologieën voor het genereren van projecten voor potentiële exploitatie door de defensiesector (bijv. windenergie, zonne-energie, slimme netten, energieopslag, biobrandstoffen, biomassa en energiewinning uit afval) evalueren.

In deze context heeft het Energy and Environment Programme (energie- en milieuprogramma) van het Europees Defensieagentschap zijn werkzaamheden voortgezet via het onderzoeksproject "Smart Blue Water Camps" om de mogelijkheden te onderzoeken voor technologische ingrepen op het gebied van duurzaam waterbeheer in militaire kampen "thuis" en via het onderzoekscontract "Smart Camps Technical Demonstrator", waarin de haalbaarheid wordt onderzocht van de integratie van een breder scala aan energie- en milieutechnologieën op grotere schaal in een militaire omgeving om de energie-, water- en afvalproblematiek aan te pakken en tegelijkertijd de kosten en militaire doeltreffendheid van GVDB-missies te verbeteren.

<u>Actie 7</u>: ***Beveiliging van het transport en de toeleveringsketen***

Voor alle transportdomeinen, met name de burgerluchtvaart, het transport over zee en het transport over land, heeft de Commissie de besprekingen met de lidstaten, de industrie en andere belanghebbenden over opkomende hybride veiligheidsdreigingen geïntensiveerd om kennis te vergaren en lessen te trekken uit ervaringen.

In het kader van de uitvoeringsactiviteiten en de herziening van het EU-actieplan voor een maritieme-veiligheidsstrategie analyseert de Commissie tendensen op het gebied van maritieme veiligheid – waaronder ook piraterij en maritieme geschillen vallen – die de scheepvaart- en handelsroutes zouden kunnen verstoren en de belangen van de EU zouden kunnen schaden. Gezien het feit dat de EER-lidstaten de controle hebben over meer dan 40 procent van de mondiale koopvaardijvloot en dat de EU een belangrijk handelsblok is, zouden hybride aanvallen op de maritieme handelsroutes aanzienlijke verstorende effecten hebben op de waarde- en toeleveringsketens in Europa. Risicoanalyses en monitoring van opkomende bedreigingen op maritiem gebied kunnen leiden tot voorstellen om de specifieke transportwetgeving waar nodig bij te werken. Het vormt ook de basis voor continu werken aan de verbetering van het maritieme bewustzijn, onder meer in de ontwikkelingscontext van de gemeenschappelijke gegevensuitwisselingsstructuur (CISE), waar begin 2018 drie nieuwe projecten zijn toegewezen na een nieuwe oproep tot het indienen van voorstellen ter ondersteuning van de lidstaten bij het verbeteren van de IT-interoperabiliteit tussen nationale maritieme autoriteiten.

Met de vaststelling van het grens- en kustwachtpakket[8] in september 2016 hebben het Europees Parlement en de Raad in de oprichtingsverordeningen van het Europees Grens- en kustwachtagentschap, het Europees Bureau voor visserijcontrole (EFCA) en het Europees Agentschap voor maritieme veiligheid (EMSA) een gemeenschappelijk artikel opgenomen waarin hen wordt opgedragen hun samenwerking te versterken, elk binnen zijn mandaat, zowel met elkaar als met de nationale autoriteiten die kustwachtfuncties uitvoeren[9], teneinde

[8] Verordening (EU) 2016/1624 betreffende de Europese grens- en kustwacht.

[9] De kustwachtfuncties zijn: 1) beheer van de maritieme veiligheid en de zeescheepvaart; 2) hulpverlening bij scheepsongevallen en hulpverlening op zee; 3) visserijcontrole en -inspectie; 4) bewaking van de zeegrenzen; 5) bescherming van het mariene milieu; 6) preventie en bestrijding van illegale handel en smokkel en de daarmee verband houdende handhaving van het zeerecht; 7) opsporing en redding op zee;

het maritieme situationele bewustzijn te vergroten en coherente en kostenefficiënte maatregelen te ondersteunen. In 2017 is hierover een studie gepubliceerd waarin gemeenschappelijke kenmerken en manieren zijn vastgesteld om de interoperabiliteit en samenwerking op het gebied van risicobeoordeling tussen autoriteiten die kustwachtfuncties uitoefenen te verbeteren[10].

Transportgerelateerde thema's en opkomende bedreigingen – met inbegrip van maar niet beperkt tot havens – zijn cyberdreigingen voor de luchtvaartveiligheid, gps-storing en -spoofing, bedreigingen voor satellieten of problemen in het hoge noorden en het noordpoolgebied. Het Europees Centrum voor de bestrijding van hybride bedreigingen in Helsinki draagt ook bij aan de analyse van deze transportgerelateerde hybride bedreigingen en heeft onlangs een analyse voor havenbescherming uitgevoerd.

De douanediensten in de EU spelen een sleutelrol bij het waarborgen van de veiligheid van de buitengrenzen en de toeleveringsketen en dragen zo bij tot de veiligheid van de Europese Unie. De Commissie is bezig met een aanzienlijke upgrade van het systeem voor voorafgaande vrachtinformatie en douanerisicobeheersysteem om ervoor te zorgen dat de douanediensten in de EU alle noodzakelijke informatie verkrijgen, deze informatie doeltreffender aan de lidstaten meedelen, gemeenschappelijke en lidstaatspecifieke risicoregels toepassen en risicovolle zendingen doeltreffender aanpakken. Een hoofdprioriteit van het EU-actieplan inzake chemisch, biologisch, radiologisch en nucleair materiaal[11] is het waarborgen van de grensbeveiligings- en opsporingscapaciteit tegen de illegale binnenkomst van CBRN-materiaal. Aanpassing van de vrachtinformatiesystemen is van essentieel belang om het toezicht op en de risicogebaseerde controles van internationale toeleveringsketens te versterken, zodat CBRN-materiaal de EU niet illegaal binnenkomt. In het vijftiende verslag over de totstandbrenging van een doeltreffende en echte Veiligheidsunie worden nadere bijzonderheden verstrekt over de EU-maatregelen ter verbetering van de paraatheid bij CBRN-risico's, en met name over de acties die op EU-niveau zijn ondernomen in het kader van het actieplan van de Commissie ter verbetering van de paraatheid bij veiligheidsrisico's op chemisch, biologisch, radiologisch en nucleair gebied.

Om de obstakels voor militaire mobiliteit in de EU uit de weg te ruimen, hebben de hoge vertegenwoordiger en de Commissie op 28 maart 2018 een actieplan gepresenteerd om de mogelijkheden voor civiel-militair gebruik van het trans-Europese netwerk te onderzoeken, de douaneformaliteiten voor militair transport te vereenvoudigen en regelgevings- en procedurele kwesties in verband met het transport van gevaarlijke goederen voor militaire doeleinden aan te pakken. De Commissie heeft een budget van 6,5 miljard euro voorgesteld in het kader van de cluster Defensie van het meerjarig financieel kader die via de financieringsfaciliteit voor Europese verbindingen zou worden uitgevoerd ter ondersteuning van de transportinfrastructuur om deze aan te passen aan de behoeften op het gebied van militaire mobiliteit. Het doel is een civiel-militair gebruik van de transportinfrastructuur mogelijk te maken.

<u>Actie 8</u>: ***Weerbaarheid van ruimtevaartinfrastructuur opbouwen***

In het voorstel van de Commissie voor een ruimtevaartprogramma van de Unie[12] zijn veiligheidsaspecten geïntegreerd, onder meer in Copernicus, Govsatcom en het ondersteuningskader voor ruimtebewaking en -monitoring, die aspecten van de weerbaarheid tegen hybride bedreigingen zouden omvatten, naast reeds bestaande maatregelen voor Galileo en Egnos.

---

8) maritiem toezicht en maritieme bewaking; 9) maritieme-douaneactiviteiten; 10) respons bij ongevallen en rampen op zee en 11) maritieme veiligheid en veiligheid van schepen en havens.

10 https://publications.europa.eu/nl/publication-detail/-/publication/217db2fc-15d6-11e7-808e-01aa75ed71a1

11 COM(2017) 610 final, 18.10.2017.

12 COM(2018) 447 final, 6.6.2018.

Het ondersteuningskader voor ruimtebewaking en -monitoring[13] heeft tot doel de beschikbaarheid op lange termijn van Europese en nationale ruimtevaartinfrastructuur, -faciliteiten en -diensten te ondersteunen. In juli 2016 begon het met de levering van de eerste diensten ter voorkoming van botsingen, het uiteenvallen en de ongecontroleerde terugkeer van voorwerpen uit de ruimte. De nationale operationele centra voor ruimtebewaking en -monitoring en het Satellietcentrum van de Europese Unie hebben maatregelen op het gebied van gegevensbeveiliging geïmplementeerd waarin wordt rekening gehouden met de aanbevelingen van de Raad inzake de veiligheidsaspecten van het Gegevensbeleid voor omgevingsbewustzijn in de ruimte[14].

Wat Galileo betreft, onderneemt de Commissie nieuwe stappen om te zorgen voor een betere bescherming van de levering van gegevens die essentieel zijn voor de goede werking van kritieke infrastructuur die voor timing en synchronisatie afhankelijk is van satellietnavigatie. Er wordt overwogen Galileo te gebruiken voor de levering van diensten in kritieke infrastructuur, zoals energienetten, telecommunicatienetwerken en financiële markten. In dit verband worden in het voorstel van de Commissie voor een verordening tot vaststelling van een kader voor screening van buitenlandse directe investeringen de Europese programma's voor wereldwijde satellietnavigatiesystemen (GNSS) Galileo en Egnos genoemd als voorbeelden van projecten of programma's van EU-belang die relevant kunnen zijn voor de screening van buitenlandse directe investeringen in het kader van de voorgestelde verordening.[15]

Het EU-initiatief voor satellietcommunicatie voor overheidsgebruik zal een gegarandeerde en beveiligde toegang tot satellietcommunicatie bieden voor missies, operaties en belangrijke infrastructuur van de Unie en de lidstaten. Dit is een belangrijk instrument om hybride bedreigingen voor bepaalde infrastructuur, waaronder ruimtevaart-, transport- en energie-infrastructuur, te bestrijden.

<u>Actie 9</u>: ***Aanpassing van defensievermogens en ontwikkeling van een relevante EU-capaciteit***

Het Europees Defensiefonds, dat op 7 juni 2017 werd gelanceerd, is een belangrijke stap voorwaarts om de lidstaten ertoe aan te zetten hun samenwerking op defensiegebied in Europa te intensiveren en vol te houden teneinde effectief op de strategische uitdagingen te kunnen reageren. In het kader van het vermogensonderdeel van het Fonds zal de EU met name de nationale financiering voor samenwerkingsprojecten voor de ontwikkeling van defensievermogens aanvullen. Daartoe heeft de Commissie in juni 2017 een voorstel ingediend voor een verordening tot instelling van een industrieel ontwikkelingsprogramma voor de Europese defensie met een begroting van 500 miljoen euro voor de periode 2019-2020. Op 22 mei 2018 bereikten het Europees Parlement en de Raad een voorlopig akkoord over de ontwerpverordening. Voor het volgende meerjarig financieel kader van de EU heeft de Commissie een geïntegreerd Europees Defensiefonds voorgesteld met een ambitieus budget van 13 miljard euro, waarbij meer dan 8,90 miljard euro is voorzien voor samenwerkingsprojecten voor de ontwikkeling van defensievermogens. Het potentiële effect van de bestrijding van hybride bedreigingen op de vermogensontwikkeling zal worden verwerkt in het herziene vermogensontwikkelingsplan, waarover de lidstaten in juni 2018 overeenstemming moeten bereiken.

---

13 Besluit nr. 541/2014/EU van het Europees Parlement en de Raad van 16 april 2014 tot oprichting van een ondersteuningskader voor ruimtebewaking en -monitoring.

14. Gegevensbeleid voor omgevingsbewustzijn in de ruimte (14698/12), 9.10.2012.

15 Zie de bijlage in COM(2017) 487 final.

<u>Actie 10</u>: ***Mechanismen voor paraatheid en coördinatie op gezondheidsgebied***

Paraatheid op gezondheidsgebied is een zeer belangrijk onderdeel van de algemene paraatheid bij CBRN-risico's. Om die reden heeft de Commissie stappen ondernomen in het kader van haar actieplan ter verbetering van de paraatheid bij veiligheidsrisico's op chemisch, biologisch, radiologisch en nucleair gebied. Er zijn met name inspanningen geleverd ter ondersteuning van initiatieven voor een doeltreffende uitwisseling van expertise.

Daarom heeft de Commissie Chimera opgezet, een oefening voor de sectoren gezondheid, civiele bescherming en veiligheid in de hele EU en in derde landen om de paraatheid en reactieplanning bij ernstige grensoverschrijdende bedreigingen te testen. Het fictieve scenario van de oefening omvatte de opzettelijke verspreiding van een overdraagbare ziekte in combinatie met cyberaanvallen op kritieke infrastructuur, waaronder ziekenhuizen, om de bestaande mechanismen, systemen en communicatie-instrumenten op nationaal en EU-niveau te testen in reactie op een hybride bedreiging. De EU-brede oefening vond plaats op 30 en 31 januari 2018 in Luxemburg. Ze heeft bijgedragen tot de ondersteuning van sectoroverschrijdende capaciteitsopbouw, de verbetering van de interoperabiliteit en coördinatie tussen de sectoren gezondheid, civiele bescherming en veiligheid op het niveau van de EU en de lidstaten en de samenwerking met internationale partners. De oefening heeft ook geholpen bij het in kaart brengen van de huidige verantwoordelijkheden en rollen van alle belanghebbenden bij crisisbeheersing van hybride bedreigingen. Het systeem voor vroegtijdige waarschuwing en maatregelen (EWRS), het sectoroverschrijdende waarschuwingssysteem van de Commissie (ARGUS), het gemeenschappelijk noodcommunicatie- en informatiesysteem (CECIS) en de geïntegreerde EU-regeling politieke crisisrespons (IPCR) van de Raad zijn getest op hun interactie. In het vijftiende verslag over de totstandbrenging van een doeltreffende en echte Veiligheidsunie worden nadere bijzonderheden verstrekt over de EU-maatregelen ter verbetering van de paraatheid bij CBRN-risico's.

In april 2018 publiceerde de Commissie een mededeling en diende ze een voorstel voor een aanbeveling van de Raad in om de EU-samenwerking op het gebied van door vaccinatie te voorkomen ziekten te versterken, met als doel dat deze aanbeveling vóór eind 2018 wordt goedgekeurd. Ze is bedoeld om de terughoudendheid tegenover vaccinatie aan te pakken, de duurzaamheid van vaccinatieprogramma's te verbeteren en de doeltreffendheid van onderzoek en ontwikkeling op het gebied van vaccins te verhogen.

Wat het Europees medisch korps betreft, werd het Noorse medische urgentieteam door de Wereldgezondheidsorganisatie (WHO) geclassificeerd, wat betekent dat het aan minimale kwaliteitsnormen voldeed. In april 2018 vond de eerste regionale WHO-bijeenkomst van medische urgentieteams van de Europese regio plaats; een bijeenkomst die gezamenlijk werd georganiseerd door de Commissie, de Wereldgezondheidsorganisatie en de Belgische gezondheidsautoriteiten, als voorzitter van de regionale groep.

Momenteel worden in nauwe samenwerking met de European Burns Association (Europese Brandwondenvereniging) en de lidstaten voorbereidingen getroffen om een mechanisme voor het beheer van rampen met zeer veel brandwondenslachtoffers te ontwikkelen. Begin oktober 2018 komen de Commissie en de lidstaten bijeen in een workshop om het werk af te ronden.

<u>Actie 11</u>: ***CSIRT-netwerk (Cyber Security Incident Response Teams) en het CERT-EU (het computercrisisresponsteam voor de instellingen van de Europese Unie) en de netwerk- en informatiebeveiligingsrichtlijn***

Het CERT-EU brengt op periodieke en ad-hocbasis inschattingen van cyberdreigingen in kritieke sectoren uit. Voor verschillende transportwijzen (lucht-, zee- en landtransport) ziet de Commissie er regelmatig op toe en zorgt zij ervoor dat sectorale initiatieven met betrekking

tot cyberdreigingen consistent zijn met sectoroverschrijdende capaciteiten die onder de richtlijn inzake de beveiliging van netwerk- en informatiesystemen (NIS-richtlijn) vallen.

In september 2017 organiseerden het Europees Defensieagentschap en het Estse voorzitterschap van de Raad van de Europese Unie een strategische simulatieoefening rond cyberbeveiliging voor EU-ministers van Defensie, CYBRID17 genaamd, om meer bewustzijn te creëren wat betreft de coördinatie van cyberbeveiligingsincidenten op politiek niveau en de potentiële effecten van offensieve cybercampagnes. De nadruk lag op omgevingsbewustzijn, crisisresponsmechanismen en strategische communicatie. Het Europees Defensieagentschap zal de elementen van deze oefening overbrengen naar het platform voor onderwijs, opleiding, evaluatie en oefeningen op cybergebied van de Europese Veiligheids- en defensieacademie, die in september 2018 zal worden opgericht. Soortgelijke oefeningen op hoog niveau door EU-voorzitterschappen worden overwogen voor de toekomst.

Actie 12: ***Contractueel publiek-privaat partnerschap (cPPP) voor cyberbeveiliging***

De Commissie heeft een publiek-privaat partnerschap voor cyberbeveiliging ondertekend met de European Cyber Security Organisation (ECSO, Europese organisatie voor cyberbeveiliging) om het concurrentievermogen en de innovatiecapaciteit van de digitale-beveiligingsindustrie en privacyindustrie in Europa te stimuleren. De EU zal tot 450 miljoen euro in dit partnerschap investeren om gebruikers en infrastructuur tegen cyberaanvallen te beschermen. Verwacht wordt dat het cPPP tegen 2020 1,8 miljard euro aan investeringen zal opleveren.

Wat cyberbeveiliging betreft, zijn in de gezamenlijke mededeling van september 2017 over "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU"[16] maatregelen beschreven om de cyberbeveiligingsstructuren en -capaciteiten van de EU een krachtige impuls te geven, zoals uiteengezet in de gezamenlijke mededeling. Doeltreffende cyberbeveiliging in de EU wordt echter gehinderd door onvoldoende investeringen en coördinatie. De EU streeft ernaar dit probleem aan te pakken zoals uiteengezet in de gezamenlijke mededeling.

Actie 13: ***Weerbaarheid van de energiesector***

In juni 2018 zal de Commissie in het kader van de NIS-samenwerkingsgroep een sectorale werkstroom opzetten om de specifieke kenmerken van de energiesector aan te pakken en de lidstaten richtsnoeren te verstrekken voor de tenuitvoerlegging van de richtlijn inzake de beveiliging van netwerk- en informatiesystemen (NIS-richtlijn) voor deze sector. Tegelijkertijd werkt de Commissie aan specifieke richtsnoeren inzake cyberbeveiliging die verder gaan dan de NIS-richtlijn teneinde goede praktijken op het gebied van cyberbeveiliging in de energiesector vast te stellen en die gericht zijn op exploitanten die niet onder de NIS-richtlijn vallen. De Commissie zal het initiatief blijven nemen tot evenementen voor het delen van informatie over cyberbeveiligingsproblemen in de energiesector om het bewustzijn te vergroten, beste praktijken uit te wisselen, de samenwerking te verbeteren (over de grenzen heen en tussen transmissie- en distributienetbeheerders), en fysieke maatregelen, nieuwe risico's en onderwijs en vaardigheden te bespreken.

Op lange termijn zal de Commissie een netcode voor sectorspecifieke regels inzake cyberbeveiliging opstellen, zoals voorgesteld in de herschikking van de elektriciteitsverordening[17] die zich momenteel in het wetgevingsproces bevindt.

---

16 JOIN(2017) 450 final.

17 Voorstel voor een verordening van het Europees Parlement en de Raad betreffende de interne markt voor elektriciteit (herschikking) – COM(2016) 861 final.

<u>Actie 14</u>: Weerbaarheid van de financiële sector: platforms en netwerken voor informatie-uitwisseling

In het Fintech-actieplan van de Commissie worden de potentiële belemmeringen aangepakt die de uitwisseling van informatie over cyberbedreigingen tussen financiële-marktdeelnemers beperken en worden mogelijke oplossingen voor het wegwerken van deze belemmeringen aangedragen. Voorts speelt het CERT-EU een rol bij de uitwisseling van informatie over incidenten.

<u>Actie 15</u>: Weerbaarheid tegen cyberaanvallen in de transportsector

De bescherming van transportwijzen tegen cyberaanvallen is een hoge prioriteit voor de Commissie. In de burgerluchtvaart is de vooruitgang op het gebied van cyberbeveiliging goed gevorderd, maar de kwetsbaarheid van de systemen als gevolg van een technische storing of als gevolg van een bedreiging voor de cyberveiligheid kan nooit worden genegeerd, zoals het recente IT-incident in EUROCONTROL, dat de helft van de vluchten in Europa heeft getroffen, heeft aangetoond. De Commissie werkt op transportgebied nauw samen met het Europees Agentschap voor de veiligheid van de luchtvaart. Het CERT-EU heeft een "service level agreement" met EUROCONTROL en een memorandum van samenwerking met het Europees Agentschap voor de veiligheid van de luchtvaart ondertekend om deze entiteiten en hun belanghebbenden te helpen bij de aanpak van cyberdreigingen.

In het zeetransport heeft de scheepvaartsector richtsnoeren inzake cyberbeveiliging uitgevaardigd, die vervolgens op het niveau van de Internationale Maritieme Organisatie zijn besproken en aangenomen, vanuit een overwegend mondiaal perspectief en met een overwegend mondiale aanpak. Cyberbeveiliging in Europese havens en havenfaciliteiten blijft een hoge beleidsprioriteit die in het kader van de invoering en de follow-up van de NIS-richtlijn wordt overwogen en regelmatig wordt besproken met de lidstaten, de industrie en de belanghebbenden.

De Commissie is voornemens een holistisch en interactief kennisinstrumentarium voor cyberbeveiliging te ontwikkelen met aanbevolen goede praktijken om beveiligingsmanagers en -professionals in de transportsector te helpen cyberbeveiligingsrisico's beter te identificeren, te beoordelen en te beperken.

<u>Actie 16</u>: Bestrijding van terrorismefinanciering

Het afgelopen jaar heeft de Commissie aanzienlijke inspanningen geleverd om de financiering van terrorisme te bestrijden, zoals gerapporteerd in de periodieke verslagen van de Veiligheidsunie. Onlangs nog heeft de Commissie in haar veiligheidspakket van april 2018[18] verdere maatregelen genomen om de samenwerking tussen de autoriteiten die verantwoordelijk zijn voor de bestrijding van zware criminaliteit en terrorisme te intensiveren en hun toegang tot en gebruik van financiële informatie te verbeteren, met een voorstel voor een richtlijn[19] ter vergemakkelijking van het gebruik van financiële en andere informatie met het oog op het voorkomen, opsporen, onderzoeken of vervolgen van ernstige strafbare feiten. Nadere bijzonderheden over het recente werk dat op EU-niveau is verricht om de financiering van terrorisme te bestrijden, zijn te vinden in het vijftiende voortgangsverslag over de totstandbrenging van een doeltreffende en echte veiligheidsunie.

Om de sancties voor het witwassen van geld te harmoniseren, heeft de Commissie wetgeving voorgesteld die medio 2018 zou moeten worden aangenomen. Bovendien werd in mei van dit jaar de vijfde antiwitwasrichtlijn aangenomen ter versterking van een aantal maatregelen, zoals verscherpte controles van derde landen met een hoog risico, controles van platforms

[18] COM(2018) 211 final.
[19] COM(2018) 213 final.

voor het wisselen van virtuele valuta's, transparantiemaatregelen die van toepassing zijn op vooruitbetaalde instrumenten, nieuwe bevoegdheden voor financiële-inlichtingeneenheden en snelle toegang tot informatie over de houders van bank- en betaalrekeningen, via centrale registers of elektronische systemen voor gegevensontsluiting voor financiële-inlichtingeneenheden.

<u>Actie 17</u>: ***Acties tegen radicalisering en analyse van de noodzaak om procedures voor verwijdering van illegale inhoud aan te scherpen***

De preventie van gewelddadige radicalisering, zowel offline als online, was de afgelopen jaren een prioriteit voor de Commissie. Om het werk op EU-niveau op te voeren, heeft de Commissie een deskundigengroep op hoog niveau inzake radicalisering opgericht die aanbevelingen moet doen over de coördinatie, de reikwijdte en het effect van het preventiebeleid van de EU. Deze deskundigengroep diende op 18 mei 2018 zijn eindverslag in, waarin wordt aanbevolen om een EU-samenwerkingsmechanisme op te zetten.

Wat de aanpak van illegale online-inhoud betreft, wordt na de goedkeuring van de aanbeveling van de Commissie van 1 maart 2018 de aandacht toegespitst op het verbeteren van de toegankelijkheid van dergelijke online-inhoud. De Commissie is een effectbeoordeling gestart om te bepalen of de huidige inspanningen toereikend zijn of dat er aanvullende maatregelen nodig zijn om ervoor te zorgen dat illegale online-inhoud snel en proactief wordt opgespoord en verwijderd, met inbegrip van mogelijke wetgevende maatregelen ter aanvulling van het bestaande regelgevingskader. De werkzaamheden van de Commissie op dit gebied zijn nader uiteengezet in het vijftiende voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie.

De gedragscode voor de strijd tegen illegale online haatuitingen op Facebook, Twitter, Google (YouTube) en Microsoft levert snel positieve resultaten op. De gedragscode heeft ervoor gezorgd dat ondernemingen aanzienlijke vooruitgang hebben geboekt bij de snelle controle en verwijdering van veronderstelde illegale haatuitingen die hen worden gemeld. Uit het derde monitoringverslag van de Commissie over de uitvoering van de gedragscode, dat in januari 2018 werd gepubliceerd, is gebleken dat gemiddeld 70 % van de haatuitingen wordt verwijderd en dat controles op haatuitingen binnen 24 uur worden uitgevoerd, zoals voorgeschreven in de gedragscode. De gedragscode is een industriestandaard geworden en de recente beslissing van Instagram en Google+ om zich bij de gedragscode aan te sluiten is bemoedigend. In maart 2018 heeft de Commissie ook aanvullende maatregelen voor onlineplatforms voorgesteld, zoals automatische detectie, transparantie en feedback aan gebruikers, en waarborgen ter bescherming van de vrijheid van meningsuiting[20].

Naast de reeds genomen maatregelen tegen radicalisering en online haatuitingen moeten ook maatregelen worden genomen om cyberbedreigingen voor verkiezingen te voorkomen en te beperken.

<u>Actie 18</u>: ***Intensivering van de samenwerking met nabuurschapsregio's en derde landen***

De Europese Unie heeft zich verder toegespitst op het opbouwen van capaciteit en weerbaarheid in de veiligheidssector in partnerlanden, onder meer door de veiligheidsdimensie van het herziene Europese nabuurschapsbeleid verder uit te werken. Om de partners beter in staat te stellen hybride bedreigingen te bestrijden, worden specifieke analyses van hybride risico's uitgevoerd om de kritieke kwetsbaarheden van de partners te identificeren en gerichte steun te verlenen. De Europese Dienst voor extern optreden (EDEO) heeft in samenwerking met de Commissie een analyse uitgevoerd met de Republiek Moldavië. In 2018 hebben Jordanië en Georgië de EU officieel verzocht om

[20] COM(2018) 1177 final.

kwetsbaarheidsanalyses op hen uit te voeren, waarbij de eerste stap erin bestond de vragenlijst op hun specifieke behoeften af te stemmen. In Oekraïne zijn aanvullende werkzaamheden voor capaciteitsopbouw op het gebied van cyberbeveiliging, met name van kritieke infrastructuur, uitgevoerd via technische-bijstandsmissies. Begin 2018 heeft de Commissie ook een uitgebreid nieuw programma gelanceerd om de cyberweerbaarheid in derde landen, met name in Afrika en Azië, te vergroten.

De EU blijft plannen en programma's voor capaciteitsopbouw op het gebied van nucleaire beveiliging bespreken met de Internationale Organisatie voor Atoomenergie en de Amerikaanse overheid in de Border Monitoring Working Group (werkgroep voor grenstoezicht). Het Europees opleidingscentrum voor nucleaire beveiliging (EUSECTRA) geeft opleidingen in preventie en detectie op het gebied van nucleaire beveiliging en de reactie op nucleaire incidenten. Het actieplan van de Commissie ter verbetering van de paraatheid bij veiligheidsrisico's op chemisch, biologisch, radiologisch en nucleair gebied omvat specifieke acties op het gebied van samenwerking met belangrijke internationale partners, onder meer in de context van terrorismebestrijding en de veiligheidsdialoog met relevante derde landen.

Het door de EU gefinancierde initiatief "CBRN-kenniscentra", dat bijna alle nabuurschapspartners omvat[21], blijft werken aan het vergroten van de nationale en regionale capaciteit van partnerlanden op het gebied van preventie, paraatheid en reactie op deze bedreigingen, ook in verband met "harde-veiligheidsstructuren".

In het oostelijke en zuidelijke nabuurschap worden opleidingen en oefeningen op het gebied van civiele bescherming georganiseerd in het kader van de regionale programma's voor preventie, paraatheid en reactie op natuurrampen en door de mens veroorzaakte rampen (PPRD). De derde fase van het PPRD-programma voor het zuidelijke nabuurschap ging van start in 2018. De tweede fase van het PPRD-programma voor het oostelijk nabuurschap eindigt in november 2018, maar zal mogelijk worden verlengd. Er wordt gezorgd voor nauwe contacten met de regionale CBRN-kenniscentra en PPRD-programma's voor het zuidelijke en oostelijke nabuurschap.

PREVENTIE VAN, REACTIE OP EN HERSTEL VAN CRISISSITUATIES

Door het voeren van een langetermijnbeleid op nationaal en Europees niveau kunnen de gevolgen van hybride bedreigingen worden beperkt. Op korte termijn blijft het evenwel essentieel om de capaciteit van de lidstaten en de Unie te versterken om de preventie van, de reactie op en het herstel van hybride bedreigingen snel en gecoördineerd te laten verlopen. Een snelle reactie op gebeurtenissen die door hybride bedreigingen worden uitgelokt, is essentieel. Het afgelopen jaar is op dit gebied veel vooruitgang geboekt: de EU heeft nu een operationeel protocol waarin het crisisbeheersingsproces in het geval van een hybride aanval is vastgelegd. In de toekomst zal regelmatig toezicht worden gehouden en zullen regelmatig oefeningen plaatsvinden.

<u>Actie 19</u>: ***Een gemeenschappelijk operationeel protocol en oefeningen om de capaciteit van de strategische besluitvorming bij complexe hybride bedreigingen te verbeteren***

Het operationeel EU-protocol werd in juni 2016 in een gezamenlijk werkdocument van de diensten van de Commissie vastgesteld. Het bood de basisrichtsnoeren voor een crisisrespons van alle instellingen. Tijdens EUPACE17 werd het protocol getest aan de hand van een hybride scenario en bleek het van onschatbare waarde als instrument om de interconnectie tussen diensten te vergemakkelijken. Bovendien bood het aanknopingspunten voor interactie

[21] Met regionale CBRN-kenniscentra in Rabat, Algiers, Amman en Tbilisi.

tussen de verschillende responsniveaus: politiek strategisch, operationeel en technisch, alsook tussen de drie belangrijkste EU-responsmechanismen, namelijk crisisrespons (voor externe crisissen), ARGUS (het interne IT-platform voor informatie-uitwisseling van de Commissie) en het platform van de Raad voor geïntegreerde politieke crisisrespons. Het protocol heeft ook zijn waarde bewezen tijdens de parallelle oefening met de NAVO op CMX'17. De volgende oefening in de reeks PACE'18-oefeningen vindt in november 2018 plaats en om rekening te houden met eventuele geleerde lessen zal worden overwogen om het protocol bij te werken.

In september en oktober 2017 hield de EU de eerste parallelle en gecoördineerde oefening met de NAVO (PACE17), waarbij de paraatheid en de interactie tussen de twee organisaties in het geval van een grootschalige hybride crisis werden getest. In de voorbereidingsfase vonden intensieve personeelsuitwisselingen plaats over de vier de gebieden van de draaiboeken voor hybride bedreigingen: Vroegtijdige waarschuwing/Omgevingsbewustzijn; Strategische communicatie; Cyberverdediging; Crisispreventie en -respons. De omvang van de interactie tussen personeelsleden van de EU en de NAVO tijdens EUPACE17 is ongekend. Het was ook de eerste keer dat de NAVO deelnam aan een door het voorzitterschap voorgezeten rondetafelbijeenkomst over een geïntegreerde politieke crisisrespons; hoge EU-ambtenaren hebben deelgenomen aan de besprekingen van de Noord-Atlantische Raad. Het leerervaringsproces spitste zich toe op verschillende aspecten, waaronder de interactie tussen de crisisresponsmechanismen van de EU en de NAVO en de uitdagingen in verband met de uitwisseling van gerubriceerde informatie tussen personeelsleden van de EU en de NAVO, met inbegrip van de behoefte aan veilige communicatie, met name om in de toekomst een snelle en veilige uitwisseling te waarborgen, met volledige inachtneming van de noodzaak van controle door de verstrekker.

De planning voor de parallelle en gecoördineerde oefening in 2018 waarvoor de EU de leidende organisatie zal zijn, is aan de gang.

<u>Actie 20</u>: ***Onderzoek van de toepasselijkheid en praktische gevolgen van artikel 222 VWEU en artikel 42, lid 7, VEU bij een omvangrijke en ernstige hybride aanval***

De toepasselijkheid van de solidariteitsclausule van de EU en haar mechanisme voor wederzijdse bijstand alsook de wisselwerking daarvan met elkaar en de responsmechanismen van de NAVO, met inbegrip van collectieve verdediging overeenkomstig artikel 5, worden verder besproken en getest in oefeningen rond scenario's met hybride bedreigingen. Het Europees Centrum voor de bestrijding van hybride bedreigingen in Helsinki is geïnteresseerd en bereid om verder te werken op het gebied van zowel onderzoek als oefeningen en zo bij te dragen tot de ontwikkeling van een gemeenschappelijke visie tussen de lidstaten en bondgenoten.

<u>Actie 21</u>: ***Opname, inzet en coördinatie van de vermogens voor een militair optreden bij de bestrijding van hybride bedreigingen in het kader van het gemeenschappelijk veiligheids- en defensiebeleid***

Als reactie op de opdracht om militaire vermogens op te nemen in het gemeenschappelijk buitenlands en veiligheidsbeleid/gemeenschappelijk veiligheids- en defensiebeleid en na een seminar met militaire deskundigen in december 2016 en het uitbrengen van richtsnoeren door de Werkgroep van het Militair Comité van de Europese Unie in mei 2017 werd in juli 2017 het militair advies betreffende "de militaire bijdrage van de EU aan de bestrijding van hybride bedreigingen in het kader van het gemeenschappelijk veiligheids- en defensiebeleid" afgerond. Dit werk wordt voortgezet in het kader van het "Concept Development Implementation Plan". In overleg met het Europees Centrum voor de bestrijding van hybride

bedreigingen ontwikkelt de Militaire Staf van de EU een concept over de wijze waarop het leger kan bijdragen aan de bestrijding van hybride bedreigingen, onder meer door middel van missies en operaties in het kader van het gemeenschappelijk veiligheids- en defensiebeleid.

Bovendien maken de Militaire Staf van de EU en de lidstaten dagelijks een betere vroegtijdige waarschuwing mogelijk door militaire inlichtingen te verstrekken aan de Fusiecel voor analyse van hybride bedreigingen. De "Single Analytical Intelligence Capability" ondersteunt de Stratcom-taskforces van de EDEO door militair advies te verstrekken om desinformatiecampagnes te helpen bestrijden die gericht zijn op de EU en individuele lidstaten.

Tijdens de parallelle en gecoördineerde oefening met de NAVO in 2018 (PACE18) zal gebruik worden gemaakt van militaire vermogens om hybride bedreigingen te bestrijden. Op basis van het hybride scenario van PACE18 zullen de Militaire Staf van de EU en de Internationale Militaire Staf van de NAVO op het EU-NAVO-scenario gebaseerde informele besprekingen voeren om te zorgen voor complementariteit bij de bestrijding van hybride bedreigingen, indien de vereisten elkaar overlappen, op basis van het inclusiviteitsbeginsel en met inachtneming van de beslissingsautonomie en de gegevensbeschermingsregels van elke organisatie.

SAMENWERKING TUSSEN DE EU EN DE NAVO

Actie 22: ***Samenwerking tussen de EU en de NAVO op het gebied van omgevingsbewustzijn, strategische communicatie, cyberveiligheid en "crisispreventie en -respons"***

De bestrijding van hybride bedreigingen blijft een belangrijk actieterrein in de interactie tussen de EU en de NAVO. Het is gebaseerd op het besef dat, in het geval van een hybride bedreiging, de middelen en capaciteiten die de twee organisaties kunnen mobiliseren, elkaar aanvullen en de lidstaten en de bondgenoten beter in staat stellen dergelijke bedreigingen te voorkomen, tegen te gaan en te beantwoorden. In het kader van de PACE17-oefening zijn de draaiboeken van beide organisaties getest en daarmee hun vermogen om snel en effectief samen te werken ter ondersteuning van hun getroffen leden. In het licht van de opgedane ervaring zullen de twee draaiboeken worden herzien en bijgewerkt. Op het gebied van strategische communicatie heeft overleg plaatsgevonden over steun aan Oekraïne, Bosnië en Herzegovina, de Republiek Moldavië en Georgië.

In september 2017 heeft een EU-NAVO-workshop over weerbaarheid deskundigen uit kritieke strategische sectoren bijeengebracht om informatie uit te wisselen over hun respectieve activiteiten en om voorstellen voor verdere werkzaamheden te onderzoeken, met name op het gebied van de bescherming van kritieke infrastructuur.

In 2018 is Militaire Mobiliteit opgezet, een project om verplaatsingen van militair materieel en personeel te vergemakkelijken. Daarbij zou rekening kunnen worden gehouden met de uitdagingen van hybride bedreigingen die specifiek zijn ontworpen om de reactietijden van de lidstaten en de bondgenoten te vertragen. Dit is een gebied voor toekomstige parallelle oefeningen en zal in de EUPACE19/20-reeks aan bod komen.

De coördinatie van inspanningen op het gebied van cyberopleidingen is een belangrijk gebied voor nauwere interactie. De NAVO nam in juni 2018 ook als waarnemer deel aan de simulatieoefening CyberEurope van het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (ENISA).

CONCLUSIE

Het verbeteren van het omgevingsbewustzijn en het opbouwen van weerbaarheid tegen zich ontwikkelende hybride bedreigingen uit verschillende bronnen blijft een uitdaging en vereist een voortdurende inspanning van de EU. Het gezamenlijk kader omvat een breed scala aan acties, gaande van het verbeteren van de samenvoeging en uitwisseling van informatie tot een betere bescherming van kritieke infrastructuur en cyberveiligheid en het opbouwen van samenlevingen die weerbaar zijn tegen radicalisering en gewelddadig extremisme. Via het EU-kader voor de bestrijding van hybride bedreigingen kan steun worden verleend aan lidstaten door middel van een reeks maatregelen ter versterking van het vermogen van de EU en de lidstaten om stress te weerstaan, op gecoördineerde wijze te reageren op schadelijke aanvallen en zich ten slotte daarvan te herstellen.

De reactie van de EU op hybride bedreigingen is ook met succes getest en samen met de NAVO getraind in een aantal oefeningen, en het plan is in die richting verder te gaan. Nauwe samenwerking tussen alle relevante actoren binnen de EU en met de NAVO is een essentieel onderdeel van de inspanningen om weerbaarheid op te bouwen. Bovendien draagt de ondersteuning van naburige partnerlanden bij het identificeren van hun kwetsbaarheden en het versterken van hun weerbaarheid tegen hybride bedreigingen bij tot een beter begrip van de aard van externe bedreigingen en daardoor tot een grotere veiligheid voor de buurlanden van de EU.