EUROPESE
COMMISSIE

HOGE VERTEGENWOORDIGER
VAN DE UNIE VOOR
BUITENLANDSE ZAKEN
EN VEILIGHEIDSBELEID

Brussel, 19.7.2017
JOIN(2017) 30 final

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

1. INLEIDING

De EU wordt geconfronteerd met een van de grootste veiligheidsdreigingen in haar geschiedenis. Bedreigingen nemen alsmaar vaker niet-conventionele vormen aan: sommige daarvan zijn fysiek, zoals nieuwe vormen van terrorisme; sommige situeren zich in de digitale ruimte, in de vorm van complexe cyberaanvallen. Andere zijn subtieler en bestaan uit het uitoefenen van druk, zoals desinformatiecampagnes en manipulatie van de media. Zij zijn erop gericht Europese kernwaarden zoals menselijke waardigheid, veiligheid en democratie te ondermijnen. Recente gecoördineerde wereldwijde cyberaanvallen, waarvan het moeilijk is gebleken om de daders aan te wijzen, hebben de kwetsbaarheden van onze samenlevingen en instellingen blootgelegd.

In april 2016 hebben de Europese Commissie en de hoge vertegenwoordiger een gezamenlijke mededeling voor de bestrijding van hybride bedreigingen[1] (gezamenlijk kader) aangenomen. Wegens de grensoverschrijdende en complexe aard van hybride bedreigingen wordt in dat kader een overheidsbrede aanpak voorgesteld om de algehele weerbaarheid van onze samenlevingen te versterken. De Raad[2] heeft dit initiatief en de voorgestelde acties verwelkomd en heeft de Commissie en de hoge vertegenwoordiger verzocht om in juli 2017 een voortgangsverslag uit te brengen. Hoewel de EU de lidstaten kan ondersteunen bij het opbouwen van hun weerbaarheid tegen hybride bedreigingen, ligt de verantwoordelijkheid hiervoor in eerste instantie bij de lidstaten, voor zover de bestrijding van hybride bedreigingen betrekking heeft op de nationale veiligheid en defensie.

Dit gezamenlijk kader voor de bestrijding van hybride bedreigingen vormt een belangrijk onderdeel van de alomvattende, meer geïntegreerde benadering van veiligheid en defensie door de EU. Het draagt bij tot een Europa dat beschermt, waartoe voorzitter Juncker in zijn toespraak over de Staat van de Unie van september 2016 heeft opgeroepen. In 2016 heeft de Europese Unie ook de grondslag gelegd voor een sterker Europees defensiebeleid om tegemoet te komen aan de vraag van burgers naar meer bescherming. In de integrale strategie van de EU voor haar buitenlands en veiligheidsbeleid[3] is nader ingegaan op de behoefte aan een geïntegreerde benadering om de interne weerbaarheid te koppelen aan het externe optreden van de EU, en is opgeroepen tot het aangaan van synergieën tussen defensiebeleid en beleid met betrekking tot de eengemaakte markt, de industrie, wetshandhaving en inlichtingendiensten. Na de goedkeuring van het Europees defensieactieplan in november 2016 heeft de Commissie concrete initiatieven voorgesteld die, door de weerbaarheid van de defensietoeleveringsketen te bevorderen en de interne defensiemarkt te versterken, zullen helpen om de EU beter in staat te stellen om op hybride bedreigingen te reageren. Zo heeft de Commissie op 7 juni 2017 het Europees defensiefonds opgericht, waarin voor de periode tot en met 2020 een financiering van 600 miljoen EUR en voor de periode na 2020 een jaarlijkse financiering van 1,5 miljard EUR wordt voorgesteld. In de mededeling over de veiligheidsunie[4] is erkend dat het nodig is om hybride bedreigingen te bestrijden en voor meer coherentie tussen de interne en externe activiteiten op het gebied van veiligheid te zorgen.

[1] Gezamenlijke mededeling aan het Europees Parlement en de Raad - Gezamenlijk kader voor de bestrijding van hybride bedreigingen — een reactie van de Europese Unie, JOIN(2016) 18 final.
[2] Conclusies van de Raad over bestrijding van hybride bedreigingen, persmededeling 196/16, 19 april 2016.
[3] Deze is op 28 juni 2016 door de hoge vertegenwoordiger aan de Europese Raad gepresenteerd.
[4] COM(2016) 230 final van 20.4.2016.

In het debat over de toekomst van Europa hebben de leiders van de EU veiligheid en defensie centraal geplaatst[5]. Dit is bevestigd in de Verklaring van Rome van 25 maart 2017, waarin een visie wordt gegeven van een veilige Unie die streeft naar het versterken van haar gemeenschappelijke veiligheid en defensie. De voorzitters van de Europese Raad en de Europese Commissie en de secretaris-generaal van de NAVO hebben op 8 juli 2016 in Warschau een gezamenlijke verklaring ondertekend om een nieuw elan en nieuwe inhoud te geven aan het strategische partnerschap tussen de EU en de NAVO. In de gezamenlijke verklaring worden zeven concrete gebieden aangehaald waarop nauwer zou moeten worden samengewerkt, waaronder hybride bedreigingen. Aansluitend daarop hebben de Europese Raad en de Noord-Atlantische Raad een gemeenschappelijke reeks van 42 uitvoeringsvoorstellen goedgekeurd; in juni 2017 is hierover een eerste verslag uitgebracht waaruit bleek dat er aanzienlijke vooruitgang is geboekt[6].

In de discussienota van de Commissie over de toekomst van de Europese defensie[7], die in juni 2017 is gepresenteerd, worden vooruitblikkend op 2025 verschillende scenario's voorgesteld om de steeds grotere bedreigingen voor Europa op het vlak van veiligheid en defensie aan te pakken en het eigen defensievermogen van Europa te versterken. In alle drie scenario's worden veiligheid en defensie beschouwd als integrerende onderdelen van het Europese project om onze interne en externe belangen te beschermen en te bevorderen. Europa moet uitgroeien tot een verstrekker van veiligheid en geleidelijk in zijn eigen veiligheid voorzien. Geen enkele lidstaat kan de uitdagingen die ons te wachten staan, alleen het hoofd bieden; dit geldt in het bijzonder voor de bestrijding van hybride bedreigingen. Samenwerking op het gebied van defensie en veiligheid is dan ook geen optie, maar een noodzakelijke voorwaarde voor de totstandbrenging van een Europa dat ons beschermt.

Het doel van dit verslag is een overzicht te geven van de voortgang en van de volgende stappen in de uitvoering van de acties op de vier gebieden die in het gezamenlijk kader worden voorgesteld: het omgevingsbewustzijn verbeteren; weerbaarheid opbouwen; de lidstaten en de Unie beter in staat stellen om crisissen te voorkomen, erop te reageren en er op gecoördineerde wijze van te herstellen; en de samenwerking met de NAVO versterken om te zorgen voor maatregelen die elkaar aanvullen. Het moet worden gelezen in samenhang met de maandelijkse voortgangsverslagen over de totstandbrenging van een echte en doeltreffende Veiligheidsunie.

2. DE HYBRIDE AARD VAN EEN BEDREIGING ERKENNEN

In de Europese veiligheidscontext zijn hybride activiteiten een steeds vaker voorkomend fenomeen. De intensiteit van deze activiteiten neemt toe en leidt tot steeds grotere bezorgdheid over beïnvloeding van verkiezingen, desinformatiecampagnes, kwaadwillige cyberactiviteiten en daders van hybride handelingen die trachten kwetsbare leden van de samenleving te radicaliseren en als handlangers in te zetten. Kwetsbaarheid voor hybride bedreigingen houdt niet op aan de landsgrenzen. Zij vereisen ook op het niveau van de EU en

[5] Het stappenplan van Bratislava van de Europese Raad van 16 september 2016 en de Verklaring van Rome van de leiders van 27 lidstaten en de Europese Raad, het Europees Parlement en de Europese Commissie van 25 maart 2017.
[6] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation
[7] Discussienota over de toekomst van de Europese defensie van 7 juni 2017, https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_nl.pdf

de NAVO een gecoördineerde respons. Uit de gebeurtenissen sinds april 2016 blijkt dat, hoewel bedreigingen nog vaak als losstaande feiten worden beoordeeld, er binnen de Unie steeds meer erkenning en begrip is van de hybride aard van sommige van de waargenomen activiteiten evenals van de noodzaak om op gecoördineerde wijze daartegen op te treden. De EU zal zich verder inspannen om het omgevingsbewustzijn en de samenwerking te verbeteren.

Actie 1: Lidstaten, hierbij in voorkomend geval gesteund door de Commissie en de hoge vertegenwoordiger, wordt verzocht een analyse van de hybride risico's uit te voeren om essentiële zwakke punten te identificeren, inclusief specifieke aan hybride bedreigingen gerelateerde indicatoren, die mogelijkerwijs nationale en pan-Europese structuren en netwerken kunnen treffen.

De Raad heeft een Groep vrienden van het voorzitterschap opgericht, waarin deskundigen uit de lidstaten zijn bijeengebracht; deze groep heeft als opdracht een algemene analyse op te stellen die hen in staat moet stellen een beter zicht te krijgen op de belangrijkste indicatoren van hybride bedreigingen, deze op te nemen in mechanismen voor vroegtijdige waarschuwing en beoordeling van bestaande risico's, en deze zo nodig te delen. Er is overeenstemming bereikt over het mandaat en de werkzaamheden zijn reeds aangevat. De algemene analyse zou klaar moeten zijn tegen eind 2017, waarna de eigenlijke analyses van start gaan. De bescherming tegen hybride bedreigingen zou ons onderling moeten versterken. De lidstaten worden dan ook aangemoedigd om deze analyses zo snel mogelijk uit te voeren, aangezien zij waardevolle informatie zullen opleveren over de mate van kwetsbaarheid en paraatheid in heel Europa.

a. BETERE BEWUSTMAKING

De uitwisseling van inlichtingenanalyses en -beoordelingen is een essentieel hulpmiddel om onzekerheid te verminderen en het omgevingsbewustzijn te vergroten. Het voorbije jaar is op dat gebied aanzienlijke vooruitgang geboekt. De EU-Fusiecel voor analyse van hybride bedreigingen is opgericht en is nu volledig operationeel; ook de oprichting van de East Stratcom Task Force is een feit en Finland heeft het Europees Centrum voor de bestrijding van hybride bedreigingen opgezet. Er is veel werk verricht rond de analyse van de instrumenten en hulpmiddelen die voor desinformatie of propaganda worden ingezet, waarbij goed wordt samengewerkt tussen de EU StratCom Task Force East, de EU-Fusiecel voor analyse van hybride bedreigingen en de NAVO. Dit vormt een goede basis om verder te bouwen aan een cultuur waarin bedreigingen voor onze interne en externe veiligheid systematisch door een "hybride bril" worden geanalyseerd en beoordeeld.

Fusiecel voor analyse van hybride bedreigingen

Actie 2: Oprichting van een EU-Fusiecel voor analyse van hybride bedreigingen binnen de bestaande structuur van het Centrum van de Europese Unie voor de analyse van inlichtingen, die in staat is om gerubriceerde gegevens en informatie uit open bronnen over hybride bedreigingen te ontvangen en te analyseren. De lidstaten wordt verzocht nationale contactpunten betreffende hybride bedreigingen aan te duiden om samenwerking en beveiligde communicatie met de EU-Fusiecel voor analyse van hybride bedreigingen tot stand te brengen.

De EU-Fusiecel voor de analyse van hybride bedreigingen is opgericht binnen het Centrum van de Europese Unie voor de analyse van inlichtingen en is belast met het ontvangen en analyseren van door verschillende belanghebbenden aangeleverde gerubriceerde informatie en informatie uit open bronnen over hybride bedreigingen. Daarna worden de analyses binnen de

EU en tussen lidstaten uitgewisseld en vervolgens benut voor de besluitvorming van de EU, bijvoorbeeld als input voor de op EU-niveau uitgevoerde beoordelingen van de veiligheidsrisico's. De afdeling Inlichtingen van de militaire staf van de EU draagt met militaire analyse bij tot het werk van de Fusiecel. Tot nu toe zijn meer dan vijftig beoordelingen en briefings over onderwerpen van hybride aard opgesteld. Sinds januari 2017 geeft de cel een periodiek verschijnend bulletin uit (het "Hybrid Bulletin"); dit bulletin bevat analyses van actuele bedreigingen en hybride kwesties en wordt rechtstreeks binnen de EU-instellingen en -organen en de nationale contactpunten verspreid[8]. De cel heeft in mei 2017 zoals gepland haar volledige operationele capaciteit bereikt. Tot slot vinden er onderlinge contacten tussen de personeelsleden van de cel en de recent opgerichte Hybrid Analysis Branch van de NAVO plaats, waarbij zowel uit de oprichting van de Fusiecel getrokken lessen als informatie wordt uitgewisseld (waarbij de EU-voorschriften inzake uitwisseling van gerubriceerde informatie ten volle worden nageleefd). De EU-Fusiecel voor analyse van hybride bedreigingen onderzoekt momenteel verdere initiatieven om in de toekomst nauwer samen te werken en zal een sleutelrol spelen bij de in het najaar van 2017 geplande parallelle oefeningen van de EU en de NAVO, waarin het reactievermogen van de EU-Fusiecel voor analyse van hybride bedreigingen zal worden getest en getrokken lessen zullen worden toegepast.

Strategische communicatie

Actie 3: In overleg met de lidstaten zal de hoge vertegenwoordiger onderzoeken op welke wijze de capaciteit voor een proactieve strategische communicatie kan worden geactualiseerd en gecoördineerd en mediamonitoring en taaldeskundigen optimaal kunnen worden ingezet.

De voorbije maanden maakte de toename van desinformatiecampagnes en de systematische verspreiding van valse nieuwsberichten op sociale media deel uit van een spectrum van maatregelen om tegenstanders te ondermijnen. In kringen waar sociale media het favoriete medium is, kan informatie die betrouwbaar en authentiek lijkt, de publieke opinie beïnvloeden ten voordele van bepaalde personen, organisaties of regeringen. Dergelijke hybride tactieken beogen een ruimer doel, namelijk het creëren van verwarring in onze samenlevingen en het in diskrediet brengen van democratische regeringen en van onze structuren, instellingen en verkiezingen. Valse nieuwsberichten worden vaak via onlineplatformen verspreid (zie ook actie 17). De Commissie en de hoge vertegenwoordiger verwelkomen de recente stappen die onlineplatformen en uitgevers van nieuwsmedia hebben ondernomen om desinformatie aan te pakken. De Commissie zal dergelijke vrijwillige maatregelen blijven aanmoedigen.

De hoge vertegenwoordiger heeft de East Stratcom Task Force opgericht, die prognoses opstelt over en reageert op gevallen van desinformatie en desinformatiecampagnes. Dit zorgt voor een steeds betere communicatie over het beleid van de Unie in het oostelijk nabuurschap en versterkt tegelijk het mediaklimaat in deze landen. De taskforce heeft de voorbije twee jaar meer dan 3 000 individuele gevallen van desinformatie in 18 talen aan het licht gebracht. Binnenkort wordt een nieuwe website opgezet: "*#EUvsdisinformation*". Deze met een onlinezoektool uitgeruste website zal de gebruikerstoegang aanzienlijk verbeteren. Uit onderzoek en analyses blijkt echter dat het aantal kanalen en boodschappen waarin dagelijks desinformatie wordt verspreid, aanzienlijk hoger ligt. Het via Horizon 2020 gefinancierde

[8] Tot op heden hebben 21 lidstaten nationale contactpunten aangewezen. Dit zijn personen die in de hoofdsteden van de lidstaten op het gebied van beleid of weerbaarheid werken.

EU-STRAT-project is gericht op de analyse van beleid en media in de landen van het Oostelijk Partnerschap.

De hoge vertegenwoordiger verzoekt de lidstaten om de werkzaamheden van de Stratcom-taskforces te ondersteunen om de opkomst van hybride bedreigingen doeltreffender te bestrijden. Dit moet de Task Force South helpen om de communicatie en contacten met de Arabische wereld — onder andere in het Arabisch — te verbeteren; dit omvat tevens het ontkrachten van mythen en het weergeven van de feiten over de Europese Unie en haar beleid. De contacten met plaatselijke journalisten moeten ervoor zorgen dat de nieuwsitems aan de lokale cultuur worden aangepast. Beide taskforces, die ondersteuning krijgen van de EU-Fusiecel voor analyse van hybride bedreigingen, zijn erop gericht om aanverwante inspanningen van de lidstaten te ondersteunen en aan te vullen. Daarnaast verstrekt de Commissie medefinanciering aan het Europees netwerk voor strategische communicatie, een samenwerkingsnetwerk van 26 lidstaten die analyses, goede praktijken en ideeën uitwisselen over de inzet van strategische communicatie ter bestrijding van gewelddadig extremisme, alsook over desinformatie.

Kenniscentrum voor de bestrijding van hybride bedreigingen

Actie 4: Lidstaten wordt verzocht de oprichting van een kenniscentrum voor de bestrijding van hybride bedreigingen te overwegen.

Naar aanleiding van de oproep tot oprichting van een kenniscentrum heeft Finland in april 2017 het Europees Centrum voor de bestrijding van hybride bedreigingen opgezet. Tien EU-lidstaten[9], Noorwegen en de VS zijn lid van het centrum, en zowel de Europese Unie als de NAVO zijn gevraagd om de stuurgroep te ondersteunen[10]. Het centrum heeft als opdracht de strategische dialoog te bevorderen en in samenwerking met belangengemeenschappen onderzoek en analyses uit te voeren om de weerbaarheid en het reactievermogen te verbeteren en zo bij te dragen tot de bestrijding van hybride bedreigingen. Verwacht wordt dat het centrum ook zal dienen als locatie voor toekomstige oefeningen rond hybride bedreigingen. Het centrum heeft reeds nauwe contacten gelegd met de EU-Fusiecel voor analyse van hybride bedreigingen en de werkzaamheden van beide organisaties zouden elkaar moeten aanvullen. De EU bekijkt momenteel hoe zij het centrum concrete ondersteuning kan verlenen.

b. WEERBAARHEID OPBOUWEN

In het gezamenlijk kader wordt de focus van het EU-optreden gericht op weerbaarheid (bv. van vervoer, communicatie, energie, de financiële sector of regionale veiligheidsinfrastructuur) tegen propaganda en informatiecampagnes, pogingen om het bedrijfsleven, samenlevingen en economische stromen te ondermijnen, alsook tegen aanvallen op IT- en cybergerelateerde infrastructuur. Het stelt voor om weerbaarheid op te bouwen als een preventieve en afschrikkende maatregel om, zowel binnen als buiten de EU, samenlevingen robuuster te maken en escalatie van crisissen te vermijden. De toegevoegde waarde van de EU ligt in de ondersteuning van lidstaten en partners bij het opbouwen van hun weerbaarheid, daarbij steunend op een breed scala aan bestaande instrumenten en programma's. Er is aanzienlijke vooruitgang geboekt in het kader van acties om weerbaarheid

[9] Duitsland, Estland, Spanje, Frankrijk, Letland, Litouwen, Polen, Finland, Zweden en het Verenigd Koninkrijk.
[10] Andere EU-lidstaten en NAVO-bondgenoten kunnen zich bij het centrum aansluiten.

op te bouwen, bijvoorbeeld op het gebied van cyberbeveiliging, kritieke infrastructuur, beveiliging van het financiële systeem tegen illegaal gebruik en inspanningen ter bestrijding van gewelddadig extremisme en radicalisering.

Bescherming van kritieke infrastructuur

Actie 5: In samenwerking met de lidstaten en de betrokken partijen zal de Commissie gemeenschappelijke instrumenten, met inbegrip van indicatoren, selecteren om de bescherming en weerbaarheid van kritieke infrastructuur te verbeteren ten aanzien van hybride bedreigingen in relevante sectoren.

In het kader van het Europees programma voor de bescherming van kritieke infrastructuur (EPCIP) gaat de Commissie verder met de inspanningen om gemeenschappelijke instrumenten op te zetten, waaronder kwetsbaarheidsindicatoren, teneinde de weerbaarheid van kritieke infrastructuur tegen hybride bedreigingen in relevante sectoren te verbeteren. In mei 2017 heeft de Commissie een workshop georganiseerd rond hybride bedreigingen voor kritieke infrastructuur, waaraan nagenoeg alle lidstaten, exploitanten van kritieke infrastructuur en de EU-Fusiecel voor analyse van hybride bedreigingen hebben deelgenomen en waarbij de NAVO als waarnemer aanwezig was. Hier is overeenstemming bereikt over een gemeenschappelijke routekaart en stappen voor verdere inspanningen, op basis van een vragenlijst die naar de nationale autoriteiten in de lidstaten was verstuurd. In het najaar zal de Commissie verder overleg plegen met de betrokken partijen om tegen eind 2017 een aantal indicatoren overeen te komen.

Het Europees Defensieagentschap is momenteel bezig met het opsporen van tekortkomingen in gemeenschappelijk vermogen en onderzoek als gevolg van het kluwen aan energie-infrastructuren en defensievermogens. In het najaar van 2017 zal het Europees Defensieagentschap een conceptdocument opstellen en proefacties voor holistische methoden ontwikkelen.

De energievoorzieningszekerheid van de EU vergroten

Actie 6: In samenwerking met de lidstaten zal de Commissie de inspanningen ondersteunen op het vlak van de diversificatie van energiebronnen en de bevordering van de veiligheids- en beveiligingsnormen om de bestendigheid van de nucleaire infrastructuur te verhogen.

In december 2016 heeft de Commissie in het pakket voorzieningszekerheid concrete voorstellen gedaan en in april 2017 hebben de Raad en het Europees Parlement een akkoord bereikt over de nieuwe verordening betreffende de veiligstelling van de aardgasvoorziening, die bedoeld is om gasvoorzieningscrisissen te voorkomen. De nieuwe regels zullen ervoor zorgen dat de lidstaten op een regionaal gecoördineerde en gemeenschappelijke wijze te werk gaan bij het treffen van maatregelen betreffende de leveringszekerheid. Hierdoor zal de EU zich beter kunnen voorbereiden op en beter kunnen omgaan met gastekorten in geval van een crisis of een hybride aanval. Voor de eerste maal zal het solidariteitsbeginsel van toepassing zijn. De lidstaten zullen buurlanden kunnen bijstaan wanneer zich een ernstige crisis of aanval voordoet, zodat de Europese huishoudens en bedrijven gespaard blijven van black-outs.

De EU heeft ook vorderingen geboekt bij de ontwikkeling van belangrijke projecten om haar energiebevoorradingsroutes en -bronnen te diversifiëren in overeenstemming met de kaderstrategie voor de energie-unie en de Europese strategie voor energiezekerheid. Zo zijn langs de zuidelijke gascorridor bouwwerkzaamheden gaande voor alle belangrijke

pijplijnprojecten: uitbreiding van de Zuidelijke Kaukasus-pijpleiding en de Trans-Anatolische en Trans-Adriatische pijpleidingen, de upstreampijpleiding Shah Deniz II, alsmede de uitbreiding van de zuidelijke gascorridor naar Centraal-Azië, met name Turkmenistan. De invoer van vloeibaar aardgas (LNG) naar Europa neemt toe en is afkomstig van nieuwe leveranciers, zoals de VS. Het voorbeeld van de terminal in Litouwen toont aan hoe diversificatieprojecten de afhankelijkheid van één enkele leverancier kunnen verminderen. Het opdrijven van energie-inspanningen en een betere aanwending van eigen energiebronnen, vooral hernieuwbare, draagt ook bij tot de diversificatie van energieroutes en -bronnen.

Op het gebied van nucleaire veiligheid draagt de Commissie actief bij — met name via workshops met nationale autoriteiten en toezichthouders — tot een consistente en doeltreffende uitvoering van de twee richtlijnen inzake nucleaire veiligheid en basisnormen voor bescherming, die de lidstaten respectievelijk tegen eind 2017 en 2018 in nationaal recht moeten omzetten. Daarnaast draagt het Euratom-programma voor onderzoek en opleiding bij tot de verhoging van de nucleaire veiligheid.

Beveiliging van het vervoer en de toeleveringsketen

Actie 7: De Commissie houdt toezicht op de opkomende bedreigingen in de transportsector en actualiseert indien nodig de wetgeving. Bij de uitvoering van de EU-strategie voor maritieme veiligheid en van de strategie voor douanerisicobeheer van de Europese Unie en de bijhorende actieplannen, onderzoeken de Europese Commissie en de hoge vertegenwoordiger (binnen hun respectieve bevoegdheden) in samenwerking met de lidstaten hoe op hybride bedreigingen moet worden gereageerd, in het bijzonder op bedreigingen betreffende kritieke transportinfrastructuur.

In overeenstemming met de mededeling over de veiligheidsunie draagt de Commissie bij tot veiligheidsrisicobeoordelingen op EU-niveau in samenwerking met de lidstaten, het Centrum van de Europese Unie voor de analyse van inlichtingen en betrokken agentschappen om bedreigingen voor de beveiliging van het vervoer te identificeren en de ontwikkeling van doeltreffende en proportionele beperkingsmaatregelen te ondersteunen. Het neerhalen van vlucht MH17 van Malaysian Airlines boven het oosten van Oekraïne in 2014 heeft de aandacht gevestigd op het risico dat gepaard gaat met het overvliegen van conflictgebieden. In overeenstemming met de aanbevelingen van de Europese taskforce op hoog niveau inzake conflictgebieden[11] heeft de Commissie met de steun van nationale luchtvaart- en veiligheidsdeskundigen en de EDEO een methode voor "gemeenschappelijke EU-risicobeoordeling" ontwikkeld, die het mogelijk maakt om gerubriceerde informatie uit te wisselen en een gemeenschappelijk risicobeeld op te stellen. In maart 2017 heeft het Europees Agentschap voor de veiligheid van de luchtvaart (EASA) op basis van de resultaten van deze gemeenschappelijke EU-risicobeoordeling het eerste voorlichtingsbulletin over conflictgebieden (Conflict Zones Information Bulletin)[12] uitgebracht. De Commissie overweegt de risicobeoordelingsactiviteiten op het gebied van luchtvaartbeveiliging uit te breiden naar andere vervoerswijzen (bv. vervoer via spoor, over zee) en zal hierover in 2018 voorstellen indienen. In juni 2017 hebben de Commissie, de EDEO en de lidstaten een risicobeoordelingsoefening rond de beveiliging van treinverkeer opgestart om eventuele lacunes op te sporen en risicobeperkende maatregelen vast te stellen.

11 https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf

12 https://ad.easa.europa.eu/czib-docs/page-1

Ook in de projecten rond veiligheidsonderzoek binnen het zevende kaderprogramma en Horizon 2020 zijn aanzienlijke inspanningen geleverd op het gebied van luchtvaartbeveiliging en luchtverkeersbeheer (ATM). Op het gebied van de burgerluchtvaart werkt de Commissie samen met het Europees Agentschap voor de veiligheid van de luchtvaart en belanghebbenden aan de ontwikkeling van twee initiatieven ter versterking van de cyberbeveiliging, waarin eveneens hybride bedreigingen worden aangepakt: de oprichting van het Computer Emergency Response Team on Aviation en het opzetten van een taskforce voor cyberbeveiliging in de Gemeenschappelijke Onderneming Sesar (Single European Sky Air Traffic Management System Research), die verantwoordelijk is voor het beheer van het luchtverkeer in het gemeenschappelijke Europese luchtruim. Het Europees Defensieagentschap levert militaire input rond cyberbeveiliging in de luchtvaart aan zowel de Gemeenschappelijke Onderneming Sesar als aan het Europees Agentschap voor de veiligheid van de luchtvaart via het "Europees strategisch coördinatieplatform inzake cyberbeveiliging", dat op verzoek van de lidstaten en de sector ondersteuning zal bieden aan de coördinatie op EU-niveau van alle luchtvaartgerelateerde activiteiten. Overeenkomstig de routekaart inzake cyberveiligheid in de luchtvaart heeft het Europees Agentschap in 2016 voor de veiligheid van de luchtvaart analyses van lacunes in de bestaande voorschriften verricht en ook een Europees centrum voor cyberveiligheid in de luchtvaart omschreven en opgericht; dat laatste is nu operationeel en brengt samen met het computercrisisteam van de EU (CERT-EU) (memorandum van overeenstemming ondertekend in februari 2017) analyses uit van bedreigingen voor de luchtvaart; het werkt ook samen met Eurocontrol (er is een routekaart voor samenwerking vastgesteld) en er is een website voor de verspreiding van analyses uit open bronnen ontwikkeld. Tegen het najaar van 2017 wordt een normalisatieprogramma en een beveiligd kanaal voor informatie-uitwisseling vastgesteld.

Douanerisicobeheer

Met betrekking tot de douane richt de Commissie zich op een aanzienlijke verbetering van de vroegtijdige uitwisseling van informatie over ladingen en van het douanerisicobeheersysteem. Dit beslaat het volledige spectrum van douanerisico's, met inbegrip van risico's voor de veiligheid en integriteit van internationale toeleveringsketens en relevante kritieke infrastructuur (bv. directe bedreigingen voor zeehavenfaciliteiten, luchthavens of landgrenzen als gevolg van de invoer). De verbetering is bedoeld om ervoor te zorgen dat de douaneautoriteiten in de EU van handelaars alle noodzakelijke informatie over het verkeer van goederen verkrijgen; dat zij deze informatie doeltreffender met de lidstaten kunnen delen; dat zij zowel gemeenschappelijke als lidstaatspecifieke risicobeheersingsvoorschriften toepassen; en dat zij risicovolle zendingen doeltreffender kunnen aanpakken door intensiever samen te werken met andere autoriteiten, met name andere wetshandhavings- en veiligheidsdiensten. De benodigde IT-ontwikkelingen om de Commissie in staat te stellen deze verbetering door te voeren, bevinden zich momenteel in de opstartfase; in de komende maanden zullen hiervoor op centraal niveau de desbetreffende investeringen worden verricht.

Ruimtevaart

Actie 8: Binnen het kader van de toekomstige ruimtevaartstrategie en het actieplan voor een Europese Defensie zal de Commissie voorstellen om de weerbaarheid van de ruimtevaartinfrastructuur tegen hybride bedreigingen te versterken, in het bijzonder door een mogelijke uitbreiding van de reikwijdte van het ondersteuningskader voor ruimtebewaking en -monitoring om hybride bedreigingen te kunnen opsporen, door de voorbereiding van de

volgende generatie overheidssatellietcommunicatie op Europees niveau en door de invoering van Galileo in kritieke infrastructuur die afhankelijk is van tijdsynchronisatie.

Bij de voorbereiding van het regelgevingskader inzake satellietcommunicatie voor overheidsgebruik en het ondersteuningskader voor ruimtebewaking en -monitoring tegen 2018 zal de Commissie weerbaarheid tegen hybride bedreigingen opnemen in haar beoordelingscriteria. In overeenstemming met de ruimtevaartstrategie zal de Commissie bij het voorbereiden van de verdere ontwikkeling van het Galileo- en het Copernicusprogramma nagaan hoe deze diensten de kwetsbaarheid van kritieke infrastructuur kunnen helpen beperken. Het evaluatieverslag zou in het najaar van 2017 klaar moeten zijn en het voorstel betreffende de volgende generatie van Copernicus en Galileo is gepland voor 2018. Het Europees Defensieagentschap is bezig met het opzetten van samenwerkingsprojecten voor vermogensontwikkeling op het gebied van in de ruimte gebaseerde communicatie, militaire plaatsbepaling, navigatie en tijdsbepaling en aardobservatie. In het licht van huidige en opkomende hybride bedreigingen zullen alle projecten op weerbaarheidsvereisten gericht zijn.

Defensievermogens

Actie 9: In voorkomend geval met steun van de lidstaten en in overleg met de Commissie zal de hoge vertegenwoordiger projecten voorstellen voor de aanpassing van de defensievermogens en de ontwikkeling van een relevante EU-capaciteit, in het bijzonder om hybride bedreigingen tegen één of meer lidstaten te bestrijden.

In 2016 en 2017 heeft het Europees Defensieagentschap samen met de Commissie, de EDEO en deskundigen uit de lidstaten drie theoretische simulatie-oefeningen gehouden rond scenario's met hybride bedreigingen. Hun bevindingen zullen worden verwerkt in het vermogensontwikkelingsplan zodat de daaruit voortvloeiende ontwikkeling van belangrijke vermogens die nodig zijn voor de bestrijding van hybride bedreigingen in de nieuwe prioriteiten inzake vermogensontwikkeling van de EU worden opgenomen. Bij de herziening van de behoeftencatalogus 2005 zal met het gegeven van hybride bedreigingen rekening worden gehouden. In april 2017 heeft het Europees Defensieagentschap een analyseverslag over militaire implicaties van hybride aanvallen op kritieke haveninfrastructuur afgerond; dit zal in oktober 2017 op een workshop met maritieme deskundigen worden besproken. Een andere specifieke analyse van de militaire rol bij de bestrijding van minidrones is gepland voor 2018. Voorts zouden vermogensprioriteiten ter versterking van de weerbaarheid tegen door de lidstaten vastgestelde hybride bedreigingen vanaf 2019 ook in aanmerking kunnen komen voor steun uit hoofde van het Europees Defensiefonds. De Commissie roept de medewetgevers op om voor een snelle goedkeuring te zorgen en verzoekt de lidstaten om voorstellen in te dienen voor vermogensprojecten ter versterking van de weerbaarheid van de EU tegen hybride bedreigingen.

Actie 10: In samenwerking met de lidstaten zal de Commissie zorgen voor een grotere bewustwording van en weerbaarheid tegen hybride bedreigingen binnen de bestaande mechanismen voor paraatheid en coördinatie, met name het Gezondheidsbeveiligingscomité.

Met het oog op het versterken van de paraatheid en weerbaarheid tegen hybride bedreigingen, met inbegrip van capaciteitsopbouw in de gezondheidszorg en de levensmiddelensector, ondersteunt de Commissie lidstaten via opleiding, simulatie-oefeningen en door de totstandbrenging van richtsnoeren voor de uitwisseling van ervaringen te bevorderen en gezamenlijke acties te financieren. Dit vindt met name plaats binnen het EU-kader voor gezondheidsbeveiliging tegen ernstige grensoverschrijdende bedreigingen van de gezondheid

en in het kader van het volksgezondheidsprogramma tot uitvoering van de Internationale Gezondheidsregeling, een verzameling voorschriften die bindend zijn voor 196 landen, waaronder de lidstaten, met als doel om acute grensoverschrijdende risico's voor de volksgezondheid in de hele wereld te voorkomen en aan te pakken. Om sectoroverschrijdende paraatheid en reactievermogen in de gezondheidssector te testen, zullen de diensten van de Commissie in het najaar van 2017 een oefening rond complexe en multidimensionale hybride bedreigingen houden. De Commissie en de lidstaten bereiden een gezamenlijke actie rond vaccinatie voor, bestaande uit onder andere de levering van vaccins, het voorspellen van de vraag en onderzoek naar innovatieve processen voor de productie van vaccins, met als doel op EU-niveau (2018-2020) de vaccinvoorziening te versterken en de gezondheidsbeveiliging te verbeteren. De Commissie werkt ook samen met de Europese Autoriteit voor voedselveiligheid en het Europees Centrum voor ziektepreventie en -bestrijding om zich aan te passen aan geavanceerde wetenschappelijke onderzoekstechnieken, met het oog op een nauwkeurigere identificatie van gezondheidsbedreigingen en de bronnen ervan, en een daaruit voortvloeiend snel beheer van bedreigingen voor de voedselveiligheid. De Commissie heeft een netwerk van onderzoeksfinanciers (Global Research Collaboration for Infectious Disease Preparedness) opgezet om binnen 48 uur na een belangrijke uitbraak een gecoördineerde onderzoeksrespons in gang te kunnen zetten.

***Actie 11*: De Commissie spoort de lidstaten aan om zo snel mogelijk een netwerk tussen de 28 CSIRT's en het CERT-EU (computercrisisteam van de EU) alsook een kader voor strategische samenwerking op te richten en dit optimaal te benutten. In samenwerking met de lidstaten moet de Commissie ervoor zorgen dat sectorale initiatieven op het vlak van cyberdreigingen (bv. luchtvaart, energie, zeevaart) in overeenstemming zijn met de in de richtlijn netwerk- en informatiebeveiliging opgenomen sectoroverschrijdende vermogens voor het bundelen van informatie, deskundigheid en snelle reacties.**

Uit de recente wereldwijde cyberaanvallen waarbij ransomware en malware werden gebruikt om duizenden computersystemen plat te leggen, is opnieuw gebleken dat de cyberweerbaarheid en beveiligingsmaatregelen binnen de EU dringend moeten worden versterkt. Zoals aangekondigd in de tussentijdse evaluatie van de digitale eengemaakte markt zijn de Commissie en de hoge vertegenwoordiger momenteel bezig met een herziening van de EU-strategie voor cyberbeveiliging van 2013, met name door de goedkeuring van een voor september 2017 gepland pakket. De doelstelling is te zorgen voor een doeltreffendere sectoroverschrijdende reactie op deze bedreigingen en zo het vertrouwen in de digitale maatschappij en de digitale economie te vergroten. Ook wordt het mandaat van het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa) herzien om zijn rol in het veranderde ecosysteem op het gebied van cyberbeveiliging vast te stellen. De Europese Raad juicht toe dat de Commissie de strategie voor cyberbeveiliging wil herzien[13].

De vaststelling van de richtlijn netwerk- en informatiebeveiliging (NIS-richtlijn)[14] in juli 2016 was een belangrijke stap in de opbouw van weerbaarheid op het gebied van cyberbeveiliging op Europees niveau. In de richtlijn worden de eerste EU-brede voorschriften inzake cyberbeveiliging vastgesteld, worden de cyberbeveiligingsvermogens versterkt en wordt de samenwerking tussen de lidstaten opgevoerd. Krachtens de richtlijn zijn ondernemingen in kritieke sectoren ook verplicht passende veiligheidsmaatregelen te treffen en alle ernstige

[13] Conclusies van de Europese Raad van 22-23 juni 2017.

[14] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).

cyberincidenten aan de desbetreffende nationale autoriteit te melden. Het gaat onder meer om de sectoren energie, vervoer, water, gezondheidszorg, het bankwezen en de infrastructuur van de financiële markten. Aanbieders van onlinemarktplaatsen, cloudcomputingdiensten en zoekmachines zullen vergelijkbare maatregelen moeten treffen. De samenwerkingsgroep voor netwerk- en informatiediensten (in 2016 door de Commissie opgericht), die belast is met het voorkomen van marktfragmentatie, zal voor een consistente sector- en grensoverschrijdende uitvoering zorgen. De NIS-richtlijn wordt in deze context beschouwd als het referentiekader voor alle sectorale initiatieven op het gebied van cyberbeveiliging. Voorts voorziet de richtlijn in de oprichting van het netwerk van Computer Security Incident Response Teams (CSIRT's), waarin alle relevante belanghebbenden zijn vertegenwoordigd. De Commissie en CERT-EU oefenen tegelijkertijd actief toezicht uit op cyberdreigingen en wisselen informatie uit met nationale autoriteiten om ervoor te zorgen dat de IT-systemen van de EU-instellingen beveiligd en weerbaar zijn tegen cyberaanvallen. Het incident met de ransomware WannaCry in mei 2017 was een eerste gelegenheid voor het netwerk om operationele informatie uit te wisselen en samen te werken door advies te verspreiden. Het CERT-EU onderhield nauw contact met het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) bij Europol en met de CSIRT's, cybercriminaliteitseenheden en belangrijke partners in de bedrijfstak van de getroffen landen om de dreiging te beperken en slachtoffers bij te staan. De uitwisseling van nationale situatieverslagen heeft in de hele EU tot een gemeenschappelijk omgevingsbewustzijn geleid. Door deze ervaring was het netwerk beter voorbereid op de volgende incidenten (bv. de ransomware NonPetya). Er zijn ook verschillende problemen vastgesteld, die momenteel worden aangepakt.

***Actie 12*: In samenwerking met de lidstaten werkt de Commissie in het kader van een contractueel publiek-privaat partnerschap voor cyberbeveiliging met de bedrijfstak samen om technologieën te ontwikkelen en te testen die gebruikers en infrastructuur beter beschermen tegen de cyberaspecten van hybride bedreigingen.**

In juli 2016 is de Commissie in overleg met de lidstaten een contractueel publiek-privaat partnerschap voor cyberbeveiliging met de bedrijfstak aangegaan, waarbij meer dan 450 miljoen EUR uit het onderzoeks- en innovatieprogramma Horizon 2020 wordt geïnvesteerd om technologieën te ontwikkelen en te testen die gebruikers en infrastructuur beter moeten beschermen tegen cyber- en hybride bedreigingen. In het kader van het partnerschap is de eerste pan-Europese strategische onderzoeksagenda opgesteld, die gericht was op het verhogen van de weerbaarheid van kritieke infrastructuur en burgers tegen cyberaanvallen. Via het partnerschap is de coördinatie tussen belanghebbenden versterkt, wat efficiëntie- en doeltreffendheidswinsten in de Horizon 2020-financiering voor cyberbeveiliging heeft opgeleverd. Binnen het partnerschap wordt parallel gewerkt aan kwesties rond cyberbeveiligingsgerelateerde certificatie van informatie- en communicatietechnologie en aan manieren om het nijpende tekort aan cyberbeveiligingsprofessionals op de arbeidsmarkt aan te pakken. Gezien de aanzienlijke behoeften aan civiel onderzoek en de hoge weerbaarheid die nodig is voor defensie, draagt de Cyber Research and Technology Group ("groep voor cyberonderzoek en -technologie") van het Europees Defensieagentschap bij aan de onderzoeksgebieden die door de Europese organisatie voor cyberbeveiliging in hun strategische onderzoeks- en innovatieagenda zijn vastgesteld.

***Actie 13*: De Commissie zal richtsnoeren uitvaardigen voor eigenaars van slimme netwerken om de cyberbeveiliging van hun installaties te verbeteren. In het kader van het initiatief betreffende de opzet van de elektriciteitsmarkt zal de Commissie overwegen om draaiboeken en procedurele regels**

voor te stellen voor gegevensuitwisseling en organisatie van solidariteit tussen lidstaten bij crisissituaties, inclusief regels over hoe cyberaanvallen kunnen worden voorkomen en beperkt.

In de energiesector werkt de Commissie via de oprichting van het Energy Expert Cyber Security Platform aan een sectorale strategie inzake cyberbeveiliging, met als doel de uitvoering van de NIS-richtlijn te versterken. In een studie in februari 2017 zijn ter ondersteuning van het platform beste beschikbare technieken geïdentificeerd om het niveau van cyberbeveiliging van slimme metersystemen te verhogen. De Commissie heeft ook een onlineplatform opgezet onder de naam "Incident and Threat Information Sharing EU Centre", dat informatie over cyberdreigingen en incidenten in de energiesector analyseert en deelt.

De weerbaarheid van de financiële sector tegen hybride bedreigingen vergroten

Actie 14: In samenwerking met Enisa[15], de lidstaten, de desbetreffende internationale, Europese en nationale autoriteiten en financiële instellingen zal de Commissie platformen en netwerken voor gegevensuitwisseling over bedreigingen bevorderen en faciliteren en de factoren aanpakken die een dergelijke gegevensuitwisseling belemmeren.

De Commissie erkent dat cyberdreigingen een van de belangrijkste risico's vormen voor de financiële stabiliteit en heeft daarom het regelgevingskader voor betalingsdiensten in de Europese Unie, dat momenteel ten uitvoer wordt gelegd, aan een herziening onderworpen. In de herziene richtlijn betalingsdiensten[16] zijn nieuwe bepalingen opgenomen om de veiligheid van betalingsinstrumenten te versterken en sterke cliëntauthenticatie in te voeren teneinde fraude — met name bij onlinebetalingen — te verminderen. Deze nieuwe wetgeving wordt met ingang van januari 2018 van toepassing. Met de hulp van de Europese Bankautoriteit en in overleg met belanghebbenden is de Commissie momenteel bezig met de ontwikkeling van technische reguleringsnormen — die naar verwachting eind 2017 worden bekendgemaakt — inzake sterke cliëntauthenticatie en gemeenschappelijke en beveiligde communicatie met het oog op de beveiliging van betalingstransacties. Op internationaal vlak heeft de Commissie nauw met de respectieve G7-partners samengewerkt aan de "grondbeginselen van de G7 inzake cyberbeveiliging in de financiële sector", die in oktober 2016 door de ministers van Financiën en presidenten van de centrale banken van de G7 zijn bekrachtigd. De beginselen zijn opgesteld voor (private en publieke) entiteiten in de financiële sector en dragen bij tot een gecoördineerde benadering van cyberbeveiliging binnen de financiële sector teneinde gezamenlijk om te gaan met cyberdreigingen, met name de toename ervan in frequentie en complexiteit.

Vervoer

Actie 15: In samenwerking met de lidstaten onderzoeken de Commissie en de hoge vertegenwoordiger (binnen hun respectieve bevoegdheden) hoe het hoofd kan worden geboden aan hybride bedreigingen, in het bijzonder aan cyberaanvallen binnen de transportsector.

[15] Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging.

[16] Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt (PB L 337 van 23.12.2015, blz. 35).

De uitvoering van het actieplan voor de maritieme veiligheidsstrategie van de EU[17] zal bijdragen tot het doorbreken van het hokjesdenken bij de uitwisseling van informatie en het gedeelde gebruik van middelen door civiele en militaire autoriteiten. Via een overheidsbrede benadering is een nauwere samenwerking tussen verschillende actoren tot stand gebracht. Tegen eind 2017 moet een gezamenlijke civiel-militaire strategische onderzoeksagenda voor de Commissie en de EDEO klaar zijn, met een afsluitende workshop rond de bescherming van kritieke maritieme infrastructuur. Deze inspanningen zouden in de toekomst kunnen worden uitgebreid naar de opkomende bedreiging voor onderzeese pijpleidingen, energie-overdracht en glasvezel- en traditionele communicatiekabels door verstoring buiten nationale wateren.

In een recent onderzoek[18] is een evaluatie uitgevoerd van de risicobeoordelingscapaciteit van nationale autoriteiten die kustwachttaken verrichten. Hierin is een overzicht opgesteld van de belangrijkste belemmeringen voor samenwerking en zijn aanbevelingen gedaan voor praktische manieren om de samenwerking tussen maritieme autoriteiten op EU- en nationaal niveau op dit specifieke gebied te verbeteren. Risicobeoordeling is van essentieel belang bij het bestrijden van maritieme bedreigingen en speelt een zelfs nog grotere rol bij de evaluatie en preventie van hybride bedreigingen, aangezien daar verdere en complexere overwegingen aan te pas komen. De resultaten van dit onderzoek worden aan verschillende fora betreffende de kustwacht voorgelegd zodat de voorgestelde aanbevelingen kunnen worden beoordeeld en uitgevoerd om zo de samenwerking op dit gebied vooral met het oog op paraatheid en de respons op hybride bedreigingen te vergroten.

Bestrijding van terrorismefinanciering

Actie 16: De Commissie zal de uitvoering van het actieplan inzake terrorismefinanciering benutten om bij te dragen tot de bestrijding van hybride bedreigingen.

De daders achter hybride bedreigingen en de personen die hun steun verlenen, hebben geld nodig om hun plannen uit te voeren. De inspanningen van de EU tegen criminaliteit en terrorismefinanciering in het kader van de Europese Veiligheidsagenda en het actieplan inzake terrorismefinanciering kunnen ook bijdragen tot de bestrijding van hybride bedreigingen. In december 2016 heeft de Commissie drie wetgevingsvoorstellen gedaan, namelijk over het strafbaar stellen van witwassen van geld, over de aanpak van illegaal contantenverkeer, en over het bevriezen en confisqueren van vermogensbestanddelen[19].

Alle lidstaten moesten tegen 26 juni 2017 de vierde antiwitwasrichtlijn[20] omzetten en in juli 2016 heeft de Commissie een doelgericht wetgevingsvoorstel ingediend om deze richtlijn met extra maatregelen aan te vullen en te versterken[21].

---

[17] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf en het tweede verslag over het actieplan voor de maritieme veiligheidsstrategie van de EU, dat op 21 juni 2017 aan de lidstaten is voorgesteld.

[18] "Evaluation of risk assessment capacity at the level of Member States' authorities performing coast guard functions", 2017, https://ec.europa.eu/maritimeaffairs/documentation/studies

[19] Derde voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie (COM(2016) 831 final).

[20] Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie (Voor de EER relevante tekst) (PB L 141 van 5.6.2015, blz. 73).

Op 26 juni 2017 heeft de Commissie de in de vierde antiwitwasrichtlijn vastgestelde supranationale risicobeoordeling uitgebracht. Zij heeft ook een voorstel ingediend voor een verordening om de invoer en opslag in de EU van illegaal uit derde landen uitgevoerde cultuurgoederen te voorkomen[22]. Later dit jaar zal de Commissie verslag uitbrengen over haar doorlopende beoordeling van de behoefte aan eventuele extra maatregelen om terrorismefinanciering in de EU te traceren. De Commissie is ook bezig met een herziening van de wetgeving inzake de bestrijding van fraude en vervalsing van andere betaalmiddelen dan contanten[23].

Het achtste verslag over de totstandbrenging van een doeltreffende en echte Veiligheidsunie bevat meer details over de voortgang van de uitvoering van het actieplan tegen terrorismefinanciering.

De gemeenschappelijke waarden van de EU en inclusieve, open en weerbare samenlevingen bevorderen

Weerbaarheid opbouwen tegen radicalisering en gewelddadig extremisme

Religieuze en ideologische radicalisering, etnische conflicten en conflicten met minderheden kunnen door externe actoren worden uitgelokt via ondersteuning van specifieke groepen of door inspanningen om conflicten tussen groepen aan te wakkeren. Er zijn extra uitdagingen opgedoken, zoals dreigingen van "lone wolves", nieuwe radicaliseringstrajecten — mogelijk in de context van de migratiecrisis — alsook de opkomst van rechts-extremisme (met inbegrip van geweld tegen migranten) en risico's van polarisering. Terwijl de inspanningen op het gebied van radicalisering worden voortgezet in het kader van de veiligheidsunie, kan dit ook indirect relevant zijn voor hybride bedreigingen, aangezien personen die kwetsbaar zijn voor radicalisering, gemanipuleerd kunnen worden door de daders achter hybride bedreigingen.

***Actie 17:* De Commissie voert momenteel de acties tegen radicalisering uit die in de Europese Veiligheidsagenda zijn opgenomen en onderzoekt de noodzaak voor de aanscherping van de procedures voor verwijdering van illegale inhoud, waarbij zij een beroep doet op de zorgvuldigheid van de intermediaire organisaties bij het beheer van netwerken en systemen.**

Radicalisering voorkomen

De Commissie gaat voort met de uitvoering van haar veelomvattende reactie op radicalisering, zoals uiteengezet in de mededeling van juni 2016 over ondersteuning bij de bestrijding van radicalisering die tot gewelddadig extremisme leidt[24]; essentiële maatregelen in dit kader zijn het propageren van op integratie gericht onderwijs en gemeenschappelijke waarden, het tegengaan van terroristische propaganda op het internet, het aanpakken van radicalisering in gevangenissen, het versterken van de samenwerking met derde landen en het

[21] Zie voor nadere informatie het derde verslag over de totstandbrenging van een doeltreffende en echte Veiligheidsunie (COM(2016) 831 final) en het achtste verslag over de totstandbrenging van een doeltreffende en echte Veiligheidsunie (COM(2017) 354 final).
[22] COM(2017) van 26.6.2017, COM(2017) 340 final, SWD(2017) 275 final.
[23] Achtste voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie (COM(2017) 354 final).
[24] http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf

opvoeren van onderzoeksinspanningen om een beter inzicht in de veranderende aard van radicalisering te verwerven en beleidsmaatregelen beter te onderbouwen. Het netwerk voor voorlichting over radicalisering (RAN) is een van de voortrekkers geweest van de inspanningen van de Commissie om lidstaten op dit gebied te ondersteunen, door met praktijkwerkers op lokaal niveau te werken. In het achtste verslag over de totstandbrenging van een doeltreffende en echte Veiligheidsunie[25] wordt hierover nadere informatie verstrekt.

Radicalisering en haatuitingen op het internet

In overeenstemming met de Europese Veiligheidsagenda[26] heeft de Commissie stappen ondernomen om de beschikbaarheid van illegale inhoud op het internet te beperken, met name via de EU-eenheid voor de melding van internetuitingen bij Europol en het EU-internetforum[27]. Ook in het kader van de gedragscode tot bestrijding van illegale haatuitingen op het internet[28] is aanzienlijke vooruitgang geboekt. In het achtste verslag over de totstandbrenging van een doeltreffende en echte Veiligheidsunie[29] wordt hierover nadere informatie verstrekt. Deze acties worden nog opgevoerd, onder meer in het licht van de conclusies van de Europese Raad[30], de G7-top[31] en de G20-top in Hamburg[32].

Onlineplatformen hebben een sleutelrol bij de aanpak van illegale of potentieel gevaarlijke inhoud. In het kader van de strategie voor een digitale eengemaakte markt, zoals uiteengezet in de tussentijdse evaluatie[33], zal de Commissie voor een betere coördinatie van de dialoog met onlineplatformen zorgen en daarbij focussen op de mechanismen en technische oplossingen om illegale inhoud te verwijderen. In voorkomend geval moet ernaar worden gestreefd deze mechanismen te onderbouwen met richtsnoeren over aspecten zoals de melding en verwijdering van illegale inhoud. De Commissie zal ook richtsnoeren uitbrengen over aansprakelijkheidsregels.

Sterkere samenwerking met derde landen

Actie 18: ***In samenwerking met de Commissie zal de hoge vertegenwoordiger een onderzoek naar hybride risico's uitvoeren in de nabuurschapsregio's. De hoge vertegenwoordiger, de Commissie en de lidstaten zullen de instrumenten benutten waarover zij elk beschikken om de capaciteiten bij hun partners op te bouwen en de weerbaarheid van hun partners tegen hybride bedreigingen te versterken. GVDB-missies kunnen — onafhankelijk of aanvullend op andere EU-instrumenten — worden ingezet om partners bijstand te verlenen bij de versterking van hun capaciteiten.***

[25] COM(2017) 354 final.
[26] Zie voor nadere informatie het achtste verslag over de totstandbrenging van een doeltreffende en echte Veiligheidsunie (COM(2017) 354 final).
[27] Zie voor nadere informatie het achtste verslag over de totstandbrenging van een doeltreffende en echte Veiligheidsunie (COM(2017) 354 final).
[28] Code of Conduct on illegal online hate speech, 31 mei 2016, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf
[29] Zie voor nadere informatie het achtste verslag over de totstandbrenging van een doeltreffende en echte Veiligheidsunie (COM(2017) 354 final).
[30] Conclusies van de Raad van 22-23 juni 2017.
[31] G7-top in Taormina in Italië van 26 tot en met 27 mei 2017.
[32] G20-top in Hamburg in Duitsland van 7 tot en met 8 juli 2017.
[33] Zie voornoemde mededeling van de Commissie COM(2017) 228 final.

De Europese Unie heeft haar inspanningen verder toegespitst op het opbouwen van capaciteit en weerbaarheid in de veiligheidssector in partnerlanden, onder andere door aandacht te besteden aan het verband tussen veiligheid en ontwikkeling, door bij de herziening van het Europees nabuurschapsbeleid in een veiligheidsdimensie te voorzien en door een dialoog rond terrorismebestrijding en veiligheid op te zetten met landen rond de Middellandse Zee. Hiertoe is in samenwerking met de republiek Moldavië een proefproject voor een risicoanalyse opgezet. Deze analyse is bedoeld als hulpmiddel bij het identificeren van de belangrijkste kwetsbaarheden van het land en om ervoor te zorgen dat EU-steun specifiek op die gebieden wordt toegespitst. Uit de resultaten van het proefproject is gebleken dat de analyse op zich als nuttig werd beschouwd. Voortbouwend op de opgedane ervaring zullen de Commissie en de EDEO aanbevelingen doen om voorrang te geven aan acties op het gebied van doeltreffendheidsopbouw, strategische communicatie, bescherming van kritieke infrastructuur en cyberbeveiliging.

In de toekomst zouden ook andere buurlanden de analyse kunnen benutten en daarbij voortbouwen op deze eerste ervaring; zij het met aanpassingen aan de lokale situatie in die landen en de specifieke dreigingen, waarbij overlapping met lopende inspanningen op het vlak van veiligheid en terrorismebestrijding moet worden vermeden. Meer in het algemeen hebben de Commissie en de hoge vertegenwoordiger op 7 juni 2017 een gezamenlijke communicatie over "Een strategische aanpak van weerbaarheid in het externe optreden van de EU"[34] aangenomen. Hiermee wordt beoogd partnerlanden te helpen om weerbaarder te worden tegen de mondiale uitdagingen van vandaag. In de mededeling wordt erkend dat het nodig is om van crisisbeheersing naar een meer gestructureerde langetermijnbenadering van kwetsbaarheden te gaan, met de nadruk op anticipatie, preventie en paraatheid.

Cyberweerbaarheid voor ontwikkeling

De EU biedt ondersteuning aan landen buiten Europa bij het weerbaarder maken van hun informatienetwerken. De steeds toenemende digitalisering heeft een intrinsieke veiligheidsdimensie die specifieke uitdagingen met zich meebrengt voor de weerbaarheid van informatienetwerken over de hele wereld, want cyberaanvallen houden niet op aan de grenzen. De EU ondersteunt derde landen bij de opbouw van hun vermogen om op passende wijze onverwachte storingen en cyberaanvallen te voorkomen en aan te pakken. Na een proefproject rond cyberbeveiliging in de voormalige Joegoslavische Republiek Macedonië, Kosovo[35] en Moldavië, dat in 2016 is afgerond, zal de Commissie een nieuw programma opstarten ter versterking van de cyberweerbaarheid van derde landen, waaronder hoofdzakelijk landen in Afrika en Azië voor de periode 2017-2020, maar ook Oekraïne. Het is bedoeld om de beveiliging en paraatheid van kritieke informatie-infrastructuur en netwerken in derde landen te verhogen door middel van een overheidsbrede aanpak, met inachtneming van de mensenrechten en de rechtsstaat.

Beveiliging van de luchtvaart

[34] Gezamenlijke mededeling aan het Europees Parlement en de Raad: Een strategische aanpak van weerbaarheid in het externe optreden van de EU (JOIN (2017) 21 final).

[35] Deze benaming laat de standpunten over de status van Kosovo onverlet en is in overeenstemming met Resolutie 1244 van de VN-Veiligheidsraad en het advies van het Internationaal Gerechtshof over de onafhankelijkheidsverklaring van Kosovo.

De burgerluchtvaart blijft een belangrijk en symbolisch doelwit voor terroristen, maar kan ook in het vizier worden genomen als onderdeel van een hybride campagne. Hoewel de EU een solide kader voor de beveiliging van de luchtvaart heeft ontwikkeld, zijn vluchten uit derde landen mogelijk kwetsbaarder. In overeenstemming met resolutie 2309 (2016) van de VN-Veiligheidsraad vergroot de Commissie haar inspanningen om capaciteit op te bouwen in derde landen. In januari 2017 heeft de Commissie een nieuwe geïntegreerde risicobeoordeling ingevoerd om te zorgen voor de prioritering en coördinatie van inspanningen voor capaciteitsopbouw die worden geleverd op het niveau van de EU en de lidstaten, evenals in samenwerking met internationale partners. In 2016 heeft de Commissie een vierjarig project opgezet inzake beveiliging van de burgerluchtvaart in Afrika en op het Arabisch schiereiland om de terrorismedreiging voor de burgerluchtvaart te bestrijden. Het project is gericht op de uitwisseling van expertise tussen partnerlanden en deskundigen van lidstaten van de Europese Burgerluchtvaartconferentie, en op mentor-, opleidings- en coachingactiviteiten. De activiteiten zullen in 2017 verder worden opgevoerd.

c. 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 voorbije jaar is er op dit gebied veel vooruitgang geboekt. Zo beschikt de EU nu over een operationeel protocol waarin de procedure voor crisisbeheer in het geval van een hybride aanval is vastgelegd. Hierop zal in de toekomst regelmatig worden toegezien en dit zal geregeld worden geoefend.

Actie 19: ***In overleg met de lidstaten stellen de hoge vertegenwoordiger en de Commissie een gemeenschappelijk operationeel protocol op en houden zij regelmatig oefeningen om de capaciteit van de strategische besluitvorming bij complexe hybride bedreigingen te verbeteren, waarbij zij voortbouwen op de procedures voor crisisbeheer en de geïntegreerde EU-regeling politieke crisisrespons.***

In het gezamenlijk kader wordt aanbevolen om mechanismen voor een snelle respons op gebeurtenissen die door hybride bedreigingen worden uitgelokt, in te stellen en om de andere responsmechanismen[36] en vroegewaarschuwingssystemen van de EU onderling te coördineren. Met dat doel voor ogen hebben de diensten van de Commissie en de EDEO het operationeel EU-protocol voor de bestrijding van hybride bedreigingen (EU-draaiboek) opgesteld[37]. Hierin worden de werkwijzen vastgelegd voor de coördinatie van de respons, de bundeling en analyse van inlichtingen, de onderbouwing van besluitvormingsprocessen, oefeningen en opleiding, en de samenwerking met partnerorganisaties, met name de NAVO, in geval van een hybride bedreiging. De NAVO heeft in dezelfde trant een draaiboek ontwikkeld voor intensievere samenwerking met de EU om hybride bedreigingen op het gebied van cyberverdediging, strategische communicatie, omgevingsbewustzijn en

[36] De geïntegreerde EU-regeling politieke crisisrespons (IPCR) van de Raad, het Argus-systeem van de Commissie en het crisisresponsmechanisme van de EDEO.
[37] Werkdocument van de diensten van de Commissie (2016) 227, goedgekeurd op 7 juli 2016.

crisisbeheersing te voorkomen en te bestrijden. Het EU-draaiboek zal worden getest aan de hand van een oefening in het najaar van 2017, als onderdeel van de parallelle en gecoördineerde EU-oefening, waarbij met de NAVO zal worden samengewerkt.

Actie 20: De Commissie en de hoge vertegenwoordiger onderzoeken (binnen hun respectieve bevoegdheden) de toepasselijkheid en de praktische gevolgen van artikel 222 VWEU en artikel 42, lid 7, VEU bij een omvangrijke en ernstige hybride aanval.

In artikel 42, lid 7, VEU wordt verwezen naar een gewapende aanval op het grondgebied van een lidstaat, terwijl in artikel 222 VWEU (solidariteitsclausule) wordt verwezen naar een terroristische aanval, een natuurramp of een door de mens veroorzaakte ramp op het grondgebied van een lidstaat. Laatstgenoemde zal waarschijnlijk vaker worden gebruikt in geval van hybride aanvallen, die een mix zijn van criminele/subversieve activiteiten. Wanneer de solidariteitsclausule wordt ingeroepen, vindt de coördinatie plaats op het niveau van de Raad (geïntegreerde regeling politieke crisisrespons) en wordt een beroep gedaan op de relevante EU-instellingen, -agentschappen en -organen, evenals steunprogramma's en -mechanismen van de EU. Besluit 2014/415/EU van de Raad voorziet in een regeling voor de toepassing van de solidariteitsclausule door de Unie. Deze toepassingsvoorwaarden blijven geldig en het is niet nodig het besluit van de Raad te herzien. Indien een hybride aanval gepaard gaat met een gewapende aanval, kan ook artikel 42, lid 7, worden ingeroepen. In dergelijke gevallen moeten zowel de lidstaten als de EU hulp en bijstand verlenen. De Commissie en de hoge vertegenwoordiger zullen blijven evalueren hoe dergelijke aanvallen zo doeltreffend mogelijk kunnen worden aangepakt.

Die evaluatie wordt rechtstreeks ondersteund via de goedkeuring van het bovengenoemde operationeel EU-protocol, dat in oktober 2017 als onderdeel van de parallelle en gecoördineerde EU-oefening (PACE) zal worden toegepast. Tijdens deze oefening zullen verschillende mechanismen van de EU en haar interactievermogen op de proef worden gesteld om in de toekomst sneller beslissingen te kunnen nemen in gevallen waarin door een hybride bedreiging veroorzaakte ambiguïteit tot onduidelijkheid leidt.

Actie 21: In overleg met de lidstaten zorgt de hoge vertegenwoordiger voor de 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 GBVB/GVDB 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, is in juli 2017 het militair advies betreffende "de militaire bijdrage van de EU aan de bestrijding van hybride bedreigingen in het kader van het GVDB" afgerond, waarna het in het Concept Development Implementation Programme wordt opgenomen.

d. SAMENWERKING TUSSEN DE EU EN DE NAVO

Actie 22: In samenwerking met de Commissie zet de hoge vertegenwoordiger de informele dialoog voort, waarbij de samenwerking en coördinatie met de NAVO over omgevingsbewustzijn, strategische communicatie, cyberveiligheid en "crisispreventie en respons" wordt versterkt om het hoofd te bieden aan hybride bedreigingen, met inachtneming van de beginselen van inclusiviteit en de autonomie van elke organisatie bij haar besluitvormingsproces.

Op basis van de gezamenlijke verklaring die op 8 juli 2016 door de voorzitters van de Europese Raad en de Europese Commissie en de secretaris-generaal van de NAVO in Warschau is ondertekend, hebben de EU en de NAVO een gemeenschappelijk pakket van 42 uitvoeringsvoorstellen opgesteld, dat vervolgens in afzonderlijke parallelle procedures op 6 december 2016 door zowel de Europese Raad als de Noord-Atlantische Raad is bekrachtigd[38]. In juni 2017 hebben de hoge vertegenwoordiger/vicevoorzitter van de Europese Commissie en de secretaris-generaal van de NAVO een verslag uitgebracht over de algehele voortgang met de uitvoering van de 42 acties van de gezamenlijke verklaring. De bestrijding van hybride bedreigingen vormt een van de zeven samenwerkingsgebieden die in de gezamenlijke verklaring zijn vastgesteld, en omvat tien van de 42 acties. Uit het verslag blijkt dat bij de gezamenlijke inspanningen van het voorbije jaar aanzienlijke resultaten zijn geboekt. Heel wat specifieke acties ter bestrijding van hybride bedreigingen zijn hier al aan bod gekomen, zoals het Europees Centrum voor de bestrijding van hybride bedreigingen, beter omgevingsbewustzijn, de oprichting van de EU-Fusiecel voor analyse van hybride bedreigingen en haar interactie met de pas opgerichte Hybrid Analysis Branch van de NAVO, en de samenwerking tussen teams voor strategische communicatie. Voor de eerste maal zullen personeelsleden van de NAVO en de EU samen hun respons op een hybride scenario oefenen. In het kader van deze oefening wordt naar verwachting meer dan een derde van de gemeenschappelijke voorstellen getest. De EU zal dit jaar haar eigen parallelle en gecoördineerde oefening houden en bereidt zich voor om in 2018 een voortrekkersrol op te nemen.

Personeelsleden van de EU en de NAVO hebben al gezamenlijke briefings over weerbaarheid gehouden, zo ook over de EU-regeling geïntegreerde politieke crisisrespons. Door middel van regelmatige contacten tussen personeelsleden van de NAVO en de EU, met inbegrip van workshops en de NAVO of deelname aan de raad van bestuur van het Europees Defensieagentschap kon informatie worden uitgewisseld over de basisvereisten van de NAVO voor nationale weerbaarheid. Verdere uitwisselingen tussen de Commissie en de NAVO over het versterken van de weerbaarheid staan gepland voor het najaar. In het volgende voortgangsverslag over de samenwerking tussen de EU en de NAVO zullen mogelijkheden worden voorgesteld om de samenwerking tussen de twee organisaties uit te breiden.

3. CONCLUSIE

In het gezamenlijk kader worden acties voorgesteld die bedoeld zijn om hybride bedreigingen te helpen bestrijden en de weerbaarheid te bevorderen op zowel Europees als nationaal niveau, evenals bij partners. Hoewel de Commissie en de hoge vertegenwoordiger in nauwe samenwerking met de lidstaten en de partners resultaten boeken op alle gebieden, is het van essentieel belang dat, ten aanzien van de bestaande en voortdurend veranderende hybride bedreigingen, dit elan wordt vastgehouden. Het zijn de lidstaten die in eerste instantie verantwoordelijk zijn voor het bestrijden van hybride bedreigingen betreffende de nationale veiligheid en de handhaving van de openbare orde. Nationale weerbaarheid en gezamenlijke inspanningen om zich te beschermen tegen hybride bedreigingen moeten worden gezien als onderling versterkende elementen binnen dezelfde algemene inspanning. De lidstaten worden dan ook aangemoedigd om zo spoedig mogelijk analyses van de hybride risico's uit te voeren, aangezien deze waardevolle informatie zullen opleveren over de mate van kwetsbaarheid en paraatheid in heel Europa. Voortbouwend op de aanzienlijke vooruitgang bij de verbetering van het bewustzijn moet het potentieel van de EU-Fusiecel voor analyse van hybride

[38] http://www.consilium.europa.eu/en/press/press-releases/2016/12/06-eu-nato-joint-declaration/

bedreigingen maximaal benut worden. De hoge vertegenwoordiger verzoekt de lidstaten om de werkzaamheden van de Stratcom-taskforces te ondersteunen om de opkomst van hybride bedreigingen doeltreffender te bestrijden. De EU zal het door Finland geleide Europees Centrum voor de bestrijding van hybride bedreigingen ten volle ondersteunen.

De unieke kracht van de EU ligt in de ondersteuning van lidstaten en partners bij het opbouwen van hun weerbaarheid, waarbij zij beschikt over een breed scala aan bestaande instrumenten en programma's. Er is aanzienlijke vooruitgang geboekt met acties voor de opbouw van weerbaarheid, bijvoorbeeld in sectoren als vervoer, energie, cyberbeveiliging en kritieke infrastructuur, evenals bij de bescherming van het financiële systeem tegen illegaal gebruik, en bij de inspanningen ter bestrijding van gewelddadig extremisme en radicalisering. De EU zal haar inspanningen voor de opbouw van weerbaarheid voortzetten, aangezien de aard van hybride bedreigingen evolueert. Meer bepaald zal de EU indicatoren ontwikkelen om de bescherming en weerbaarheid van kritieke infrastructuur te verbeteren ten aanzien van hybride bedreigingen in relevante sectoren.

Via het Europees Defensiefonds kunnen samen met lidstaten vermogensprioriteiten worden medegefinancierd om de weerbaarheid tegen hybride bedreigingen te versterken. In het kader van het aanstaande cyberbeveiligingspakket en de sectoroverschrijdende maatregelen voor de uitvoering van de richtlijn netwerk- en informatiebeveiliging zullen in de hele EU nieuwe platformen voor de bestrijding van hybride bedreigingen worden gecreëerd.

De Commissie en de hoge vertegenwoordiger roepen de lidstaten en belanghebbenden op om waar nodig snel overeenstemming te bereiken en te zorgen voor een snelle en doeltreffende uitvoering van de talrijke weerbaarheidsversterkende maatregelen die in deze mededeling zijn opgenomen. De EU zal haar samenwerking met de NAVO, die nu al haar vruchten afwerpt, verder uitbouwen en verdiepen.

De Unie blijft vastbesloten alle relevante EU-instrumenten in te zetten om complexe hybride bedreigingen aan te pakken. De ondersteuning van de lidstaten bij hun inspanningen blijft een prioriteit voor de Unie, die zal optreden als een sterkere en responsievere veiligheidsverstrekker, zij aan zij met haar belangrijkste partners.