EUROPESE
COMMISSIE

HOGE VERTEGENWOORDIGER
VAN DE UNIE VOOR
BUITENLANDSE ZAKEN
EN VEILIGHEIDSBELEID

Brussel, 6.4.2016
JOIN(2016) 18 final

GEZAMENLIJKE MEDEDELING AAN HET EUROPEES PARLEMENT EN DE RAAD

Gezamenlijk kader voor de bestrijding van hybride bedreigingen

een reactie van de Europese Unie

1. INLEIDING

De afgelopen jaren is de veiligheidssituatie van de Europese Unie drastisch gewijzigd. In het licht van de belangrijkste bedreigingen voor vrede en stabiliteit in de oostelijke en zuidelijke nabuurschap van de EU blijkt hoe noodzakelijk het is dat de Unie zich aanpast en haar capaciteit als verstrekker van veiligheid uitbreidt, met sterke aandacht voor de nauwe band tussen externe en interne veiligheid. Veel van de huidige problemen op het vlak van vrede, veiligheid en welvaart worden veroorzaakt door de instabiliteit in de directe omgeving van de Unie en de veranderende aard van de dreigingen. In zijn politieke beleidslijnen van 2014 benadrukte Commissievoorzitter Jean-Claude Juncker de noodzaak om "ervoor te zorgen dat Europa ook op het gebied van veiligheid en defensie sterker komt te staan" en de Europese en nationale instrumenten doeltreffender te combineren dan voorheen. Aansluitend op deze oproep en op verzoek van de Raad Buitenlandse Zaken van 18 mei 2015 heeft de hoge vertegenwoordiger in nauwe samenwerking met de diensten van de Commissie en het Europees Defensieagentschap (EDA) en in overleg met de EU-lidstaten werkzaamheden verricht om voorliggend gezamenlijk kader in te dienen met uitvoerbare voorstellen ter bestrijding van hybride bedreigingen en ter bevordering van de weerbaarheid van de Unie en haar lidstaten en partners[1]. In juni 2015 heeft de Europese Raad erop gewezen dat EU-instrumenten moeten worden gebruikt om hybride bedreigingen het hoofd te bieden[2].

Hoewel definities van hybride bedreigingen kunnen uiteenlopen en flexibel moeten blijven om te kunnen reageren op het evoluerende karakter van deze dreigingen, is het concept erop gericht een combinatie te omvatten van dwang en subversie, conventionele en niet-conventionele methodes (diplomatiek, militair, economisch, technologisch) die staten of niet-overheidsactoren gecoördineerd kunnen inzetten om specifieke doelstellingen te bereiken zonder over te gaan tot een officiële oorlogsverklaring. Vaak worden hierbij vooral de zwakke punten van het doel uitgebuit en wordt een dubbelzinnige houding aangenomen om besluitvormingsprocessen te ontregelen. Grootschalige desinformatiecampagnes, waarbij gebruik wordt gemaakt van sociale media om het politieke betoog te controleren en handlangers te radicaliseren, rekruteren en aan te sturen, kunnen instrumenten zijn voor hybride bedreigingen.

Voor zover de bestrijding van hybride bedreigingen betrekking heeft op de nationale veiligheid en defensie en de handhaving van de openbare orde, ligt de verantwoordelijkheid in eerste instantie bij de lidstaten, aangezien de meeste nationale kwetsbare punten landspecifiek zijn. Talrijke EU-lidstaten worden evenwel geconfronteerd met gemeenschappelijke bedreigingen, die ook gericht kunnen zijn op grensoverschrijdende netwerken of infrastructuur. Dergelijke bedreigingen kunnen doeltreffender worden aangepakt met een gecoördineerde reactie op EU-niveau door gebruik te maken van EU-beleidsmaatregelen en -instrumenten, een beroep te doen op de Europese solidariteit, wederzijdse bijstand en alle mogelijkheden die het Verdrag van

[1] Conclusies van de Raad met betrekking tot het gemeenschappelijk veiligheids- en defensiebeleid (GVDB), mei 2015 [Consilium 8971/15]

[2] Conclusies van de Europese Raad, juni 2015 [EUCO 22/15].

Lissabon biedt. EU-beleidsmaatregelen en -instrumenten kunnen - en in aanzienlijke mate doen zij dit reeds - een cruciale, waardetoevoegende rol vervullen bij de bewustmaking. Hiermee wordt de weerbaarheid van lidstaten verhoogd om te kunnen reageren op gemeenschappelijke bedreigingen. Het in het raam van dit kader voorgestelde extern optreden van de Unie is gebaseerd op de in artikel 21 van het Verdrag betreffende de Europese Unie (VEU) opgenomen beginselen als democratie, de rechtsstaat, de universaliteit en de ondeelbaarheid van de mensenrechten en de naleving van de beginselen van het Handvest van de Verenigde Naties en het internationale recht[3].

Deze gezamenlijke mededeling heeft tot doel een integrale benadering te bevorderen die de EU in staat zal stellen in samenwerking met de lidstaten specifiek de bedreigingen van hybride aard tegen te gaan door synergie-effecten tot stand te brengen tussen alle betrokken instrumenten en de nauwe samenwerking tussen alle betrokken actoren te bevorderen[4]. De acties bouwen voort op bestaande strategieën en sectorale beleidsmaatregelen die bijdragen tot meer veiligheid. Met name de volgende instrumenten kunnen ook bijdragen tot de bestrijding van hybride bedreigingen: de Europese veiligheidsagenda[5], de geplande globale EU-strategie voor buitenlands en veiligheidsbeleid en het Europees defensieactieplan[6], de EU-cyberbeveiligingsstrategie[7], de Energiezekerheidsstrategie[8] en de maritieme veiligheidsstrategie van de Europese Unie[9].

Aangezien de NAVO ook inspanningen levert om hybride bedreigingen tegen te gaan en de Raad Buitenlandse Zaken heeft voorgesteld om de samenwerking en coördinatie op dit vlak te intensiveren, wordt er met sommige voorstellen naar gestreefd de samenwerking tussen de EU en de NAVO met het oog op de bestrijding van hybride bedreigingen te versterken.

De voorgestelde reactie is toegespitst op de volgende punten: betere bewustmaking, betere bestendigheid, preventie van, reactie op en herstel van crisissituaties.

2. DE HYBRIDE AARD VAN EEN BEDREIGING ERKENNEN

Hybride bedreigingen hebben tot doel de kwetsbaarheden van een land uit te buiten. Met deze bedreigingen wordt vaak getracht de fundamentele democratische waarden en vrijheden te ondermijnen. Als een eerste stap zullen de hoge vertegenwoordiger en

[3] Het Handvest van de grondrechten van de Europese Unie is bindend voor de EU-instellingen en de lidstaten wanneer zij de wetgeving van de Unie ten uitvoer leggen.
[4] Eventuele wetgevingsvoorstellen zullen worden getoetst aan de voorschriften van de Commissie inzake betere regelgeving, overeenkomstig de richtsnoeren inzake betere regelgeving van de Commissie, SWD(2015) 111.
[5] COM(2015) 185 final.
[6] Zal in 2016 worden ingediend.
[7] EU-beleidskader voor cyberdefensie [Consilium 15585/14] en gezamenlijke mededeling over de "Strategie inzake cyberbeveiliging van de Europese Unie: een open, veilige en beveiligde cyberspace", februari 2013 [JOIN(2013)1].
[8] Gezamenlijke mededeling over de "Europese strategie voor energiezekerheid", mei 2014 [SWD(2014) 330].
[9] Gezamenlijke mededeling "Voor een open en veilig mondiaal maritiem domein: onderdelen voor een maritieme veiligheidsstrategie van de Europese Unie - JOIN(2014) 9 final - 6.3.2014.

Commissie met de lidstaten samenwerken om het omgevingsbewustzijn te vergroten door het monitoren en beoordelen van de risico's die de kwetsbare punten van de EU kunnen bedreigen. De Commissie ontwikkelt momenteel methoden op het gebied van veiligheidsrisicobeoordeling om beleidsmakers te informeren en een risicogebaseerde beleidsvorming te bevorderen op gebieden die gaan van luchtvaartbeveiliging tot terrorismefinanciering en witwassen van geld. Daarnaast zou een analyse door de lidstaten, waarin de terreinen worden afgebakend die kwetsbaar zijn voor hybride bedreigingen, nuttig zijn. Het doel zou zijn indicatoren van hybride bedreigingen te identificeren, op te nemen in mechanismen voor vroegtijdige waarschuwing en bestaande instrumenten voor risicobeoordeling, en in voorkomend geval uit te wisselen.

***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.**

3. ORGANISATIE VAN DE EU-REACTIE: BETERE BEWUSTMAKING

3.1. De EU-Fusiecel voor analyse van hybride bedreigingen

Het is essentieel dat de EU in overleg met haar lidstaten over voldoende omgevingsbewustzijn beschikt om wijzigingen in de veiligheidsomgeving op te sporen die verband houden met hybride bedreigingen die door staten en/of niet-overheidsactoren worden veroorzaakt. Met het oog op de doeltreffende bestrijding van hybride bedreigingen is het belangrijk de gegevensuitwisseling te verbeteren en een nuttige uitwisseling van inlichtingen tussen sectoren en binnen de Europese Unie en haar lidstaten en partners te bevorderen.

Een EU-Fusiecel voor analyse van hybride bedreigingen zal zich specifiek toespitsen op het onderzoek van hybride bedreigingen en zal worden opgericht binnen het Centrum van de Europese Unie voor de analyse van inlichtingen (EU INTCEN) van de Europese Dienst voor extern optreden (EDEO). Deze Fusiecel zou belast worden met het ontvangen, analyseren en delen van gerubriceerde gegevens en informatie uit open bronnen die in het bijzonder verband houden met indicatoren en waarschuwingen over hybride bedreigingen en die worden aangeleverd door verschillende betrokken partijen binnen de EDEO (inclusief EU-delegaties), de Commissie (met inbegrip van de EU-agentschappen[10]) en lidstaten. In samenwerking met bestaande soortgelijke organen op Europees[11] en nationaal niveau zou de Fusiecel externe aspecten van de hybride bedreigingen, die de EU en haar nabuurschap raken, onderzoeken om een snelle analyse te kunnen opstellen van de desbetreffende incidenten en aan te reiken aan de strategische besluitvormingsprocessen van de EU, inclusief het verstrekken van input aan de op het

[10] Overeenkomstig hun mandaten.
[11] Bijvoorbeeld het Europees Centrum voor de bestrijding van cybercriminaliteit en het Europees Centrum voor terrorismebestrijding van Europol, Frontex, het computercrisisteam van de EU (CERT)-EU.

niveau van de EU uitgevoerde beoordelingen van de veiligheidsrisico's. De resultaten van de door de Fusiecel uitgevoerde analyse zouden dan kunnen worden verwerkt en behandeld overeenkomstig de EU-voorschriften voor de beveiliging van gerubriceerde informatie en gegevens[12]. De Fusiecel zal contacten onderhouden met bestaande organen op Europees en nationaal niveau. Lidstaten zouden nationale contactpunten kunnen oprichten die als schakel met de EU-Fusiecel voor analyse van hybride bedreigingen fungeren. Personeelsleden binnen en buiten de EU (inclusief degenen die werkzaam zijn bij EU-delegaties, operaties en missies) en in de lidstaten moeten ook worden opgeleid om eerste tekenen van hybride bedreigingen te herkennen.

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 (EU-Intcen), die belast is van het ontvangen en analyseren van gerubriceerde gegevens en informatie uit open bronnen over hybride bedreigingen. Lidstaten wordt verzocht nationale contactpunten op te richten over hybride bedreigingen om samenwerking en beveiligde communicatie met de EU-Fusiecel voor analyse van hybride bedreigingen tot stand te brengen.

3.2. Strategische communicatie

Hybride bedreigingen kunnen de vorm aannemen van het systematisch verspreiden van desinformatie, onder meer door gerichte campagnes op de sociale media, waarbij zij ernaar streven individuen te radicaliseren, de samenleving te destabiliseren en het politieke betoog te controleren. Het vermogen om te reageren op hybride bedreigingen door gebruik te maken van een deugdelijke strategie op het vlak van **strategische communicatie** is essentieel. Het verstrekken van snelle feitelijke antwoorden en het bewustmaken van de bevolking van de hybride bedreigingen zijn belangrijke factoren voor het opbouwen van maatschappelijke weerbaarheid.

Strategische communicatie moet ten volle gebruik maken van sociale media alsook van de traditionele audiovisuele en internetmedia. Hierbij kan de EDEO voortbouwen op de activiteiten van de *East and Arab Stratcom* taskforces en moet de EDEO optimaal gebruik maken van linguïsten die vloeiend de desbetreffende niet-EU-talen spreken en van socialemediadeskundigen, die niet-EU-informatie kunnen monitoren en gericht kunnen communiceren als reactie op desinformatie. Om hybride bedreigingen aan het licht te brengen, moeten lidstaten coördinatiemechanismen voor strategische communicatie opzetten om de toewijzing van middelen te ondersteunen en desinformatie te bestrijden.

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.

[12] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995.

3.3. Kenniscentrum voor de bestrijding van hybride bedreigingen

Voortbouwend op de ervaring die door sommige lidstaten en partnerorganisaties[13] is opgedaan, zou een multinationale instelling of een netwerk van multinationale instellingen kunnen optreden als een kenniscentrum voor de bestrijding van hybride bedreigingen. In een dergelijk kenniscentrum kan worden onderzocht hoe hybride strategieën zijn toegepast en kan de ontwikkeling worden bevorderd van nieuwe concepten en technologieën binnen de particuliere sector en de industrie om lidstaten te ondersteunen bij het opbouwen van weerbaarheid. Het onderzoek zou kunnen bijdragen tot de onderlinge afstemming van Europese en nationale beleidsmaatregelen, doctrines en concepten en zou ervoor kunnen zorgen dat bij de besluitvorming rekening wordt gehouden met de complexiteit en dubbelzinnigheid waarmee hybride bedreigingen gepaard gaan. In een dergelijk kenniscentrum zouden programma's kunnen worden opgezet om het onderzoek te bevorderen en praktische oplossingen te bedenken voor de bestaande problemen die door hybride bedreigingen worden veroorzaakt. Het sterke punt van een dergelijk centrum zou de deskundigheid zijn die wordt ontwikkeld door de multinationale en sectoroverschrijdende samenwerking tussen civiele, militaire, particuliere en academische sectoren.

Een dergelijk centrum zou nauw samenwerken met de bestaande kenniscentra bij de EU[14] en de NAVO[15]om gebruik te maken van de inzichten in hybride bedreigingen die kenniscentra op het vlak van cyberdefensie, strategische communicatie, civiele en militaire samenwerking, energievraagstukken en crisisrespons ondertussen reeds hebben opgeleverd.

<u>Actie 4</u>: Lidstaten wordt verzocht de oprichting van een kenniscentrum van de bestrijding van hybride bedreigingen te overwegen.

4. ORGANISATIE VAN DE EU-REACTIE: OPBOUW VAN WEERBAARHEID

Weerbaarheid is het vermogen stresssituaties te weerstaan en te boven te komen, gesterkt door de uitdagingen. Voor een doeltreffende bestrijding van hybride bedreigingen moeten de potentiële zwakke punten van de cruciale infrastructuur, toeleveringsketens en de maatschappij worden aangepakt. Door een beroep te doen op instrumenten en beleidsmaatregelen van de EU kan de weerbaarheid van de infrastructuur op Europees niveau worden versterkt.

4.1. Bescherming van kritieke infrastructuur

Het is belangrijk om kritieke infrastructuur (bv. energietoeleveringsketens, transport) te beschermen, aangezien een onconventionele aanval in de vorm hybride bedreigingen op elk zacht doelwit zou kunnen resulteren in ernstige economische of maatschappelijke

[13] Kenniscentra van de NAVO.
[14] Bv. het Instituut voor veiligheidsstudies van de EU (EU ISS), thematische EU-kenniscentra inzake CBRN-vraagstukken.
[15] http://www.nato.int/cps/en/natohq/topics_68372.htm.

verstoringen. Om de bescherming te waarborgen van kritieke infrastructuur voorziet het Europees programma voor de bescherming van kritieke infrastructuur[16] (EPCIP) in een sectoroverschrijdende benadering voor alle mogelijke risico's, waarbij rekening wordt gehouden met de onderlinge afhankelijkheid en wordt uitgegaan van de uitvoering van activiteiten op het vlak van preventie, paraatheid en respons. De richtlijn betreffende Europese kritieke infrastructuren[17] voorziet in een procedure voor de identificatie en de aanmerking van Europese kritieke infrastructuren (ECI) en een gemeenschappelijke aanpak voor de beoordeling van de noodzaak om de bescherming ervan te verbeteren. In het kader van deze richtlijn moeten met name de werkzaamheden worden hervat om de bestendigheid van kritieke transportinfrastructuur te versterken (bv. de belangrijkste luchthavens en koopvaardijhavens van de EU). De Commissie zal nagaan of gemeenschappelijke instrumenten moeten worden ontwikkeld, met inbegrip van indicatoren, voor een versterking van de bestendigheid van kritieke infrastructuur tegen hybride bedreigingen in alle relevante sectoren.

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 bestendigheid van kritieke infrastructuur te verbeteren ten aanzien van hybride bedreigingen in relevante sectoren.

4.1.1. Energienetwerken

De ononderbroken opwekking en distributie van stroom is van vitaal belang voor de EU en een aanzienlijke stroomuitval zou nadelige gevolgen kunnen hebben. Essentieel bij de bestrijding van hybride bedreigingen is een verdere diversificatie van energiebronnen, leveranciers en transportroutes van de EU om te voorzien in een veiligere en bestendigere energievoorziening. De Commissie voert ook risico- en veiligheidsbeoordelingen (stresstests) uit van de kerncentrales in de EU. Om de energiediversificatie tot stand te brengen, worden de werkzaamheden in het kader van de energie-unie opgevoerd: bv. de zuidelijke gascorridor voor gastoevoer vanuit de Kaspische regio naar Europa en de oprichting van hubs voor vloeibaar gas met meerdere leveranciers in Noord-Europa. Dit voorbeeld moet worden gevolgd in Midden- en Oost-Europa en in het Middellandse-Zeegebied, waar momenteel wordt gewerkt aan een Mediterrane gashub[18]. De zich ontwikkelende markt voor vloeibaar aardgas zal ook op een positieve manier bijdragen tot het realiseren van deze doelstelling.

Wat betreft nucleair materiaal en nucleaire installaties, ondersteunt de Commissie de ontwikkeling en invoering van de striktste veiligheidsnormen, waardoor de bestendigheid van de nucleaire infrastructuur verder wordt versterkt. De Commissie vindt dat gewerkt

[16] Mededeling van de Commissie betreffende een Europees programma voor de bescherming van kritieke infrastructuur, 12.12.2006, COM(2006) 786 final.
[17] Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren, PB L 345 van 23.12.2008.
[18] Voor de tot nu toe geboekte vooruitgang, zie Stand van zaken rond de energie-unie 2015 (COM (2015) 572 final.)

moet worden aan de consequente omzetting en tenuitvoerlegging van de richtlijn inzake nucleaire veiligheid[19], waarin de voorschriften zijn vastgelegd voor de voorkoming van ongevallen en de beperking van de gevolgen van ongevallen, en van de bepalingen van de basisnormenrichtlijn[20] over de internationale samenwerking op het vlak van noodplannen en rampenbestrijding, in het bijzonder tussen buurlanden en met buurlanden.

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.

4.1.2 Transport en beveiliging van de toeleveringsketen

Transport is essentieel voor de werking van de Unie. Hybride aanvallen op transportinfrastructuur (luchthavens, wegeninfrastructuur, havens en spoorwegen) kunnen zware gevolgen hebben en resulteren in verstoringen van het reizigersvervoer en toeleveringsketens. Bij de implementatie van de wetgeving inzake veiligheid van lucht- en zeevaart[21] voert de Commissie regelmatige inspecties[22] uit en in het kader van haar werkzaamheden op het vlak van de beveiliging van het vervoer over land streeft zij ernaar het hoofd te bieden aan opkomende hybride bedreigingen. In dit verband wordt overleg gepleegd over een EU-kader in het raam van de herziene Verordening inzake luchtvaartveiligheid[23], als onderdeel van de luchtvaartstrategie voor Europa[24]. Daarnaast komen bedreigingen voor maritieme veiligheid aan de orde in de maritieme

[19] Richtlijn 2009/71/Euratom van de Raad van 25 juni 2009 tot vaststelling van een communautair kader voor de nucleaire veiligheid van kerninstallaties, zoals gewijzigd bij Richtlijn 2014/87/Euratom van de Raad van 8 juli 2014.

[20] Richtlijn 2013/59/Euratom van de Raad van 5 december 2013 tot vaststelling van de basisnormen voor de bescherming tegen de gevaren verbonden aan de blootstelling aan ioniserende straling, en houdende intrekking van de Richtlijnen 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom en 2003/122/Euratom.

[21] Verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad van 11 maart 2008 inzake gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart en tot intrekking van Verordening (EG) nr. 2320/2002; Uitvoeringsverordening (EU) nr. 2015/1998 van de Commissie van 5 november 2015 houdende vaststelling van gedetailleerde maatregelen voor de toepassing van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart; Richtlijn 2005/65/EG van het Europees Parlement en de Raad van 26 oktober 2005 betreffende het verhogen van de veiligheid van havens; Verordening (EG) nr. 725/2004 van het Europees Parlement en de Raad van 31 maart 2004 betreffende de verbetering van de beveiliging van schepen en havenfaciliteiten.

[22] Krachtens het EU-recht moet de Commissie inspecties uitvoeren om de correcte uitvoering door de lidstaten van de vereisten op het vlak van de beveiliging van lucht- en zeevaart te garanderen. Hierbij gaat het om inspecties van de voor deze beveiliging in de lidstaat bevoegde autoriteit alsook om inspecties op luchthavens, havens, vliegtuigen, schepen en instanties aan wie de uitvoering van de veiligheidsmaatregelen is toevertrouwd. De inspecties van de Commissie hebben tot doel ervoor te zorgen dat EU-normen door de lidstaten volledig worden uitgevoerd.

[23] Verordening (EU) 2016/4 van de Commissie van 5 januari 2016 tot wijziging van Verordening (EG) nr. 216/2008 van het Europees Parlement en de Raad met betrekking tot essentiële eisen inzake milieubescherming; Verordening (EG) nr. 216/2008 van 20.2.2008 tot vaststelling van gemeenschappelijke regels op het gebied van burgerluchtvaart en tot oprichting van een Europees Agentschap voor de veiligheid van de luchtvaart.

[24] Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's: Een luchtvaartstrategie voor Europa, COM/2015/0598 final, 7.12.2015

veiligheidsstrategie van de Europese Unie en het bijhorende actieplan[25]. Met dit actieplan moeten de EU en haar lidstaten maritieme veiligheidsvraagstukken op alomvattende wijze kunnen aanpakken, inclusief het bestrijden van hybride bedreigingen door een sectoroverschrijdende samenwerking tussen civiele en militaire actoren om bescherming te bieden aan de maritieme kritieke infrastructuur, de wereldwijde toeleveringsketen, de maritieme handel en de maritieme natuurlijke hulp- en energiebronnen. De beveiliging van de internationale toeleveringsketen komt ook aan de orde in de strategie en het actieplan voor douanerisicobeheer van de Europese Unie[26].

***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 de strategie en het actieplan voor douanerisicobeheer van de Europese Unie en het bijhorende actieplan, onderzoeken de Europese Commissie en de hoge vertegenwoordiger (binnen hun respectieve bevoegdheden) in samenwerking met de lidstaten hoe op hybride bedreigingen moeten worden gereageerd, in het bijzonder op de bedreigingen die betrekking hebben op kritieke transportinfrastructuur.**

4.1.3 Ruimtevaart

Hybride bedreigingen kunnen gericht zijn op ruimtevaartinfrastructuur met multisectorale gevolgen. De EU heeft het ondersteuningskader voor ruimtebewaking en -monitoring[27] geconcipieerd om middelen die in handen zijn van de lidstaten door middel van een netwerk te verbinden om ruimtebewakings- en -monitoringsdiensten[28] te kunnen verstrekken aan welbepaalde gebruikers (lidstaten, EU-instellingen, eigenaren en exploitanten van ruimtevaartuigen en instanties voor civiele bescherming). In het kader van de komende ruimtevaartstrategie voor Europa zal de Commissie de verdere ontwikkeling van dit ondersteuningskader onderzoeken om de hybride bedreigingen voor ruimtevaartinfrastructuur te monitoren.

Satellietcommunicatie (SatCom) is essentieel voor crisisbeheer, rampenbestrijding, politietoezicht, grens- en kustbewaking. Zij vormt de ruggengraat van grootschalige infrastructuur, zoals transport- en ruimtevaartsystemen of systemen voor op afstand bestuurde luchtvaartuigen. In overeenstemming met de oproep van de Europese Raad om de volgende generatie van overheidssatellietcommunicatie voor te bereiden (GovSatCom) gaat de Commissie in samenwerking met het Europees Defensieagentschap na hoe de vraag naar satellietcommunicatie kan worden gebundeld

[25] In december 2014 heeft de Raad een actieplan vastgesteld om de maritieme veiligheidsstrategie van de Europese Unie uit te voeren. http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf

[26] Mededeling van de Commissie aan het Europees Parlement, de Raad en het Europees Economisch en Sociaal Comité over de EU-strategie en het actieplan voor douanerisicobeheer: risico's aanpakken, veiligheid van de toeleveringsketen vergroten en handel vergemakkelijken, COM (2014) 527 final.

[27] Zie Besluit nr. 541/2014/EU van het Europees Parlement en de Raad.

[28] Zoals waarschuwingen voor het voorkomen van botsingen in de satellietbaan, waarschuwingen met betrekking tot het uiteenvallen, botsingen en de riskante terugkeer van voorwerpen uit de ruimte in de dampkring van de aarde.

in het kader van de komende ruimtevaartstrategie en het actieplan voor een Europese defensie.

Heel wat kritieke infrastructuur is afhankelijk van exacte tijdsbepalingen voor de synchronisatie van de netwerkinfrastructuur (bv. energie en telecommunicatie) of om transacties van een tijdstempel te voorzien (bv. financiële markten). De afhankelijkheid van een tijdsynchronisatiesignaal dat afkomstig is van één enkel wereldwijd satellietnavigatiesysteem, biedt niet de bestendigheid die noodzakelijk is om te kunnen weerstaan aan hybride bedreigingen. Met Galileo, het Europese wereldwijde satellietnavigatiesysteem, zou een beroep kunnen worden gedaan op een tweede betrouwbare tijdsbron.

***Actie 8*: Binnen het kader van de toekomstige ruimtevaartstrategie en het actieplan voor een Europese Defensie zal de Commissie voorstellen om de bestendigheid 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, de voorbereiding van de volgende generatie overheidssatellietcommunicatie op Europees niveau en de invoering van Galileo in kritieke infrastructuur die afhankelijk is van tijdsynchronisatie.**

4.2. Defensiecapaciteit

De defensiecapaciteit moet worden versterkt om de weerbaarheid van de EU tegen hybride bedreigingen te versterken. Het is belangrijk om de essentiële werkterreinen - bv. capaciteit op het vlak van surveillance en verkenning - af te bakenen. Het Europees Defensieagentschap zou de aanzet kunnen geven voor de ontwikkeling van een militaire capaciteit (bv. door kortere cycli voor de ontwikkeling van defensievermogens, investeringen in technologie, systemen en prototypes, introductie van innovatieve commerciële technologieën in defensiebedrijven) die gericht is op de bestrijding van hybride bedreigingen. Mogelijke acties zouden kunnen worden overwogen in het kader van het komende actieplan voor een Europese defensie.

***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 defensiecapaciteiten en de ontwikkeling van een relevante EU-capaciteit, in het bijzonder om hybride bedreigingen tegen een of meerdere lidstaten te bestrijden.**

4.3. Bescherming van de volksgezondheid en voedselzekerheid

De volksgezondheid zou in gevaar kunnen komen door de doelbewuste verspreiding van besmettelijke ziekten of door de besmetting van levensmiddelen en de verontreiniging van bodem, lucht en drinkwater met chemische, biologische, radiologische en nucleaire (CBRN) materialen. Voorts kan het met opzet verspreiden van dier- of plantenziekten de voedselzekerheid van de Unie ernstig in het gedrang brengen en belangrijke economische en sociale gevolgen hebben voor essentiële onderdelen van de EU-voedselketen. De bestaande EU-structuren voor gezondheidsbeveiliging, milieubescherming en

voedselveiligheid kunnen worden gebruikt om het hoofd te bieden aan hybride bedreigingen waarbij deze methoden worden gebruikt.

In het kader van de EU-wetgeving over grensoverschrijdende gezondheidsbedreigingen[29] voorzien bestaande mechanismen in een coördinatie van de voorbereiding op ernstige grensoverschrijdende bedreigingen voor de volksgezondheid, waarbij lidstaten, EU-agentschappen en wetenschappelijke comités[30] via het systeem voor vroegtijdige waarschuwing en maatregelen worden betrokken. Het Gezondheidsbeveiligingscomité, dat de reactie van de lidstaten op de bedreigingen coördineert, kan optreden als een contactpunt over de zwakke punten in de volksgezondheid[31] en hierbij voorzien in een verankering van hybride bedreigingen (en in het bijzonder bioterrorisme) in de richtsnoeren voor crisiscommunicatie en in de oefeningen voor capaciteitsopbouw met de lidstaten (crisissimulatietests). Op het vlak van voedselveiligheid kunnen de bevoegde autoriteiten via het systeem voor snelle waarschuwingen voor levensmiddelen en diervoeders (RASFF) en het gemeenschappelijk douanerisicobeheersysteem (CRMS) risicoanalyse-informatie uitwisselen om de gezondheidsrisico's als gevolg van besmette levensmiddelen te monitoren. Wat dier- en plantgezondheid betreft, zullen in het kader van de lopende herziening van het EU-rechtskader[32] nieuwe onderdelen worden toegevoegd aan het bestaande instrumentarium[33], om ook op hybride bedreigingen beter voorbereid te zijn.

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

4.4. Cyberbeveiliging

De EU heeft veel voordeel bij de interconnectie en digitalisering van de samenleving. Cyberaanvallen zouden de digitale dienstverlening binnen de EU kunnen verstoren. Dergelijke aanvallen kunnen deel uitmaken van hybride bedreigingen. Een grotere bestendigheid van de communicatie- en informatiesystemen in Europa is belangrijk om de digitale interne markt te ondersteunen. De EU-cyberbeveiligingsstrategie en de

[29] Besluit nr. 1082/2013/EU van het Europees Parlement en de Raad van 22 oktober 2013 over ernstige grensoverschrijdende bedreigingen van de gezondheid en houdende intrekking van Beschikking nr. 2119/98/EG, PB L 293/1 van 5.11.2013.

[30] Commission Decision C(2015) 5383 of 7.8.2015 on establishment of Scientific Committees in the field of public health, consumer safety and the environment. (*Besluit van de Commissie tot oprichting van wetenschappelijke comités op het gebied van consumentenveiligheid, volksgezondheid en milieu*)

[31] Overeenkomstig Besluit nr. 1082/2013/EU van het Europees Parlement en de Raad van 22 oktober 2013 over ernstige grensoverschrijdende bedreigingen van de gezondheid en houdende intrekking van Beschikking nr. 2119/98/EG, PB L 293/1.

[32] Verordening 2016/429 van het Europees Parlement en de Raad betreffende overdraagbare dierziekten en houdende wijziging en intrekking van bepaalde handelingen op het gebied van diergezondheid ("diergezondheidswetgeving"), PB L 84 van 31.3.2016. Wat betreft de verordening van het Europees Parlement en de Raad betreffende beschermende maatregelen tegen plaagorganismen bij planten ("de plantgezondheidswetgeving"), hebben het Europees Parlement en de Raad op 16 december 2015 een politieke overeenkomst over de tekst bereikt.

[33] Bv. EU-vaccinbanken, gesofisticeerde digitale informatiesystemen over dierziekten, opleggen van extra maatregelen voor laboratoria en andere entiteiten die met ziekteverwekkers werken.

Europese Veiligheidsagenda voorzien in het algemene strategische kader voor EU-initiatieven op het vlak van cyberbeveiliging en cybercriminaliteit. De EU heeft zich actief beziggehouden met bewustmaking, samenwerkingsmechanismen en reacties in het kader van de doelstellingen van de cyberbeveiligingsstrategie. Met name in de voorgestelde Richtlijn netwerk- en informatiebeveiliging[34] komen cyberveiligheidsrisico's aan de orde voor een brede waaier van essentiële dienstenleveranciers op het vlak van energie, vervoer, financiën en gezondheid. Deze dienstenleverancies alsook de leveranciers van essentiële digitale diensten (bv. cloudcomputingdiensten) moeten passende veiligheidsmaatregelen nemen en ernstige incidenten rapporteren aan de nationale autoriteiten, waarbij zij melding moeten maken van kenmerken die wijzen op hybride bedreigingen. Na de vaststelling van de richtlijn door de medewetgevers zal de daadwerkelijke omzetting en tenuitvoerlegging ervan de cyberbeveiligingscapaciteiten van de lidstaten bevorderen en resulteren in een versterkte samenwerking op het vlak van cyberbeveiliging door uitwisseling van informatie en beste praktijken bij de bestrijding van hybride bedreigingen. De richtlijn voorziet met name in de oprichting van een netwerk van 28 nationale Computer Security Incident Response Teams (CSIRT) en het CERT-EU[35] om operationele samenwerking op vrijwillige basis voort te zetten.

Om de publiek-private samenwerking en een EU-brede aanpak van cyberbeveiliging te bevorderen, heeft de Commissie het NIB-platform opgericht, dat richtsnoeren verstrekt voor beste praktijken op het vlak van risicobeheer. De lidstaten bepalen de veiligheidsvereisten en -voorschriften voor de aanmelding van nationale incidenten en de Commissie streeft naar een hoge mate van convergentie bij risicobeheersing, waarbij met name een beroep wordt gedaan op het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa).

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

4.4.1. Industrie

Het toegenomen gebruik van cloudcomputingdiensten en big data heeft geleid tot grotere kwetsbaarheid voor hybride bedreigingen. De strategie voor een digitale eengemaakte

[34] Voorstel van de Commissie voor een richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen COM(2013) 48 final - 7/2/2013. De Raad en het Europees Parlement hebben een politiek akkoord bereikt over de voorgestelde richtlijn en de richtlijn moet binnenkort formeel worden aangenomen.

[35] Computercrisisteam (CERT-EU) voor de EU-instellingen.

markt voorziet in een contractueel publiek-privaat partnerschap inzake cyberveiligheid[36], dat is toegespitst op onderzoek en innovatie en ervoor zorgt dat de Unie beschikt over sterke technologische capaciteit op dit terrein. Met het contractueel publiek-privaat partnerschap kan vertrouwen worden opgebouwd tussen verschillende marktdeelnemers en kunnen synergieën worden ontwikkeld tussen de vraag- en de aanbodzijde. Hoewel het contractueel publiek-privaat partnerschap en de begeleidende maatregelen in eerste instantie zijn toegespitst op producten en diensten voor civiele cyberbeveiliging, moeten de resultaten van deze initiatieven ervoor zorgen dat technologiegebruikers beter beschermd zijn tegen hybride bedreigingen.

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

4.4.2. Energie

Slimme woningen en toepassingen, de ontwikkeling van het slimme energienetwerk en de toegenomen digitalisering van het energiesysteem brengen een grotere kwetsbaarheid voor cyberaanvallen met zich. Met de Europese strategie voor energiezekerheid[37] en de strategie voor de Energie-Unie[38] wordt een benadering voor alle mogelijke risico's ondersteund, waarin weerbaarheid tegen hybride bedreigingen is opgenomen. Het thematisch netwerk voor de bescherming van kritieke energie-infrastructuur bevordert de samenwerking tussen exploitanten in de energiesector (olie, gas, elektriciteit). De Commissie heeft een internetplatform ontwikkeld om de gegevens over bedreigingen en incidenten te analyseren en uit te wisselen[39]. Samen andere belanghebbenden[40] concipieert de Commissie momenteel ook een alomvattende strategie voor de energiesector met betrekking tot de cyberbeveiliging van de werking van slimme energienetten om de infrastructuur minder kwetsbaar te maken. Hoewel de integratie van de elektriciteitsmarkten sterk is toegenomen, zijn de regelgeving en de procedures om het hoofd te bieden aan crisissituaties nog steeds nationaal. We moeten ervoor zorgen dat regeringen samenwerken ter voorbereiding op en voorkoming en beperking van risico's, waarbij alle betrokken partijen optreden op basis van een gemeenschappelijk geheel van regels.

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

[36] Moet medio 2016 van start gaan.
[37] Mededeling van de Commissie aan het Europees Parlement en de Raad: Europese strategie voor energiezekerheid - COM/2014/0330 final.
[38] Mededeling over "Een kaderstrategie voor een schokbestendige energie-unie met een toekomstgericht beleid inzake klimaatverandering" (COM(2015) 080 final).
[39] Incident and Threat Information Sharing EU Centre – ITIS (*EU-centrum voor gegevensuitwisseling over incidenten en bedreigingen*)
[40] In de vorm van het Energy Expert CyberSecurity Platform - EECSP (*cyberbeveiligingsplatform voor energiedeskundigen*).

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

4.4.3. Zorgen voor solide financiële systemen

De EU-economie heeft nood aan een veilig financieel en betaalsysteem. De bescherming van het financiële systeem en zijn infrastructuur tegen cyberaanvallen - ongeacht het motief of de aard van de aanvaller - is essentieel. Om het hoofd te kunnen bieden aan hybride bedreigingen tegen de financiële dienstverlening van de EU, moet de financiële sector begrijpen met welke bedreiging hij wordt geconfronteerd, zijn verdediging hebben getest en over de noodzakelijke technologie beschikken om beveiligd te zijn tegen aanvallen. Bijgevolg is gegevensuitwisseling over bedreigingen tussen financiële-marktpartijen en met de desbetreffende autoriteiten en de belangrijkste dienstverleners of klanten van cruciaal belang. Deze gegevensuitwisseling moet evenwel beveiligd zijn en beantwoorden aan de voorschriften inzake gegevensbescherming. Overeenkomstig de werkzaamheden in internationale fora, met inbegrip van de activiteiten van de G7 in deze sector, zal de Commissie zich inspannen om de factoren te bepalen die de passende gegevensuitwisseling belemmeren en zal zij oplossingen voorstellen. Het is belangrijk dat de beveiligingsprotocollen voor de financiële sector en de desbetreffende infrastructuur op gezette tijden worden getest en verbeterd, inclusief een voortdurende verbetering van technologieën waarmee de beveiliging verder kan worden versterkt.

Actie 14: In samenwerking met Enisa[41], de lidstaten, de desbetreffende internationale, Europese en nationale autoriteiten en de financiële instellingen zal de Commissie platformen en netwerken voor gegevensuitwisseling over bedreigingen bevorderen en faciliteren en de factoren aanpakken die een dergelijke gegevensuitwisseling belemmeren.

4.4.4. Transport

Moderne transportsystemen (vervoer per spoor en over de weg, lucht- en scheepvaart) maken gebruik van informatiesystemen, die het doelwit kunnen vormen van cyberaanvallen. Gezien de grensoverschrijdende dimensie heeft de EU een specifieke rol te vervullen. In coördinatie met de lidstaten zal de Commissie de cyberdreigingen en risico's blijven analyseren die betrekking hebben op wederrechtelijke verstoringen van transportsystemen. De Commissie ontwikkelt momenteel een routekaart inzake cyberveiligheid voor de luchtvaart in samenwerking met het Europees Agentschap voor de veiligheid van de luchtvaart (EASA)[42]. Cyberdreigingen voor maritieme veiligheid

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

[42] Naar aanleiding van het door de Commissie in december 2015 ingediende voorstel is er momenteel overleg tussen het Europees Parlement en de Raad over de nieuwe EASA-verordening. Voorstel voor een Verordening van het Europees Parlement en de Raad inzake gemeenschappelijke regels op het gebied van burgerluchtvaart en tot oprichting van een Agentschap van de Europese Unie voor de veiligheid van de luchtvaart, en tot intrekking van Verordening (EG) nr. 216/2008 van het Europees Parlement en de Raad, COM(2015) 613 final, 2015/0277 (COD).

komen ook aan de orde in de maritieme veiligheidsstrategie van de Europese Unie en het bijhorende actieplan.

<u>Actie 15</u>: 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 die welke betrekking hebben op cyberaanvallen binnen de transportsector.

4.5. Drooglegging van de financiering van hybride bedreigingen

Voor het uitvoeren van hybride bedreigingen is financiering noodzakelijk om deze activiteiten te kunnen handhaven. Financiering kan worden gebruikt om terroristische groeperingen of meer subtiele vormen van destabilisatie te ondersteunen, zoals het verlenen van bijstand aan drukkingsgroepen en extremistische politieke partijen. De EU heeft haar inspanningen opgevoerd op het vlak van de bestrijding van criminele financiële transacties en terrorismefinanciering, zoals blijkt uit de Europese Veiligheidsagenda, en in het bijzonder het bijhorende actieplan[43]. Met name kan met het herziene EU-kader voor de strijd tegen het witwassen van geld de strijd tegen terrorismefinanciering en het witwassen van geld verder worden opgevoerd, waarbij het opsporen en traceren van verdachte geldovermakingen en gegevensuitwisselingen door de nationale financiële-inlichtingeneenheden (FIE's) worden vergemakkelijkt en de traceerbaarheid van geldoverdrachten in de Europese Unie is gegarandeerd. Deze aanpak kan dus ook bijdragen tot de bestrijding van hybride bedreigingen. In het kader van de GBVB-instrumenten kunnen ook gerichte en doeltreffende beperkende maatregelen worden geconcipieerd om het hoofd te bieden aan hybride bedreigingen.

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

4.6. Weerbaarheid opbouwen tegen radicalisering en gewelddadig extremisme

Hoewel terroristische daden en gewelddadig extremisme niet per se een hybride karakter hebben, kunnen hybride bedreigingen zich specifiek richten op kwetsbare leden van de samenleving voor rekrutering, waarbij deze laatsten worden geradicaliseerd met de inzet van moderne communicatiekanalen (met inbegrip van internet, sociale media en handlangers) en propaganda.

Voor de bestrijding van extremistische content op het internet onderzoekt de Commissie momenteel - in het kader van de strategie voor een digitale eengemaakte markt - of nieuwe maatregelen eventueel noodzakelijk zijn, met inachtneming van de gevolgen van die maatregelen voor de grondrechten van vrijheid van meningsuiting en informatie. Hierbij kan het gaan om strikte procedures voor het verwijderen van illegale inhoud die

[43] Mededeling van de Commissie aan het Europees Parlement en de Raad inzake een actieplan ter versterking van de strijd tegen terrorismefinanciering (COM (2016) 50 final)

tegelijkertijd voorkomen dat legale inhoud ontoegankelijk wordt gemaakt ("melding en actie") en grotere verantwoordelijkheid en zorgvuldigheid van intermediaire organisaties bij het beheer van hun netwerken en systemen. Dit zou een aanvulling zijn op de bestaande vrijwillige aanpak, waarbij internet- en socialemediabedrijven (met name in het kader van het EU-Internetforum) in samenwerking met de EU-eenheid voor de melding van internetuitingen van Europol, terroristische propaganda snel verwijderen.

In het kader van de Europese Veiligheidsagenda wordt radicalisering bestreden door uitwisseling van ervaring en de ontwikkeling van beste praktijken, met inbegrip van samenwerking in derde landen. Het Adviesteam voor strategische communicatie inzake Syrië streeft ernaar de ontwikkeling en verspreiding van alternatieve boodschappen te versterken om een tegenwicht te bieden voor de terroristische propaganda. Het netwerk voor voorlichting over radicalisering verleent bijstand aan lidstaten en mensen op het terrein die in contact moeten komen met geradicaliseerde personen (inclusief buitenlandse terroristische strijders) of met diegenen van wie wordt vermoed dat ze kwetsbaar zijn radicalisering. Het netwerk voor voorlichting over radicalisering voorziet in opleidingsactiviteiten en advies en zal bijstand verlenen aan prioritaire derde landen die blijk geven van een bereidheid om samen te werken. Daarnaast ondersteunt de Commissie de justitiële samenwerking op het vlak van strafrecht, onder meer met Eurojust, om terrorisme en radicalisering in de lidstaten te bestrijden, inclusief de aanpak van buitenlandse terroristische strijders en terugkeerders.

Als aanvulling op de bovenstaande maatregelen op het vlak van haar **externe optreden** werkt de EU mee aan de bestrijding van gewelddadig extremisme, onder meer met externe samenwerking en voorlichting, preventie (bestrijding van radicalisering en terrorismefinanciering) alsook met maatregelen die toegespitst zijn op onderliggende economische, politieke en maatschappelijke omstandigheden waarin terroristische groepen zich kunnen ontplooien.

Actie 17: ***De Commissie voert momenteel de acties tegen radicalisering uit die zijn opgenomen in de Europese Veiligheidsagenda 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.***

4.7. Sterkere samenwerking met derde landen

Zoals is benadrukt in de Europese Veiligheidsagenda, heeft de EU haar inspanningen meer toegespitst op de capaciteitsopbouw van de veiligheidssector in ***partnerlanden***, door onder andere aandacht te besteden aan het verband tussen veiligheid en bij de herziening van het Europees nabuurschapsbeleid te voorzien in een

veiligheidsdimensie[44]. Met deze acties kan ook de weerbaarheid van de partners tegen hybride activiteiten worden bevorderd.

De Commissie is voornemens om indien nodig de uitwisseling van operationele en strategische informatie met de uitbreidingslanden en binnen het Oostelijk Partnerschap en de Zuidelijke Nabuurschap te intensiveren om het hoofd te kunnen bieden aan de georganiseerde misdaad, terrorisme, irreguliere migratie en handel in handvuurwapens. Op het vlak van terrorismebestrijding streeft de EU naar een intensievere samenwerking met derde landen door een modernisering van de veiligheidsdialogen en de actieplannen.

De financieringsinstrumenten voor het externe optreden van de EU hebben tot doel goed functionerende en verantwoording verschuldigde instellingen op te bouwen in derde landen[45], hetgeen een noodzakelijke voorwaarde is om doeltreffend te reageren wanneer de veiligheid in het gedrang is en om de weerbaarheid te versterken. In dit kader zijn de hervorming van de veiligheidssector en de capaciteitsopbouw ter ondersteuning van veiligheid en ontwikkeling[46] essentieel. Met behulp van het instrument voor bijdrage aan stabiliteit en vrede[47] heeft de Commissie acties opgezet voor de versterking van het vermogen weerstand te bieden tegen cyberbedreigingen en de capaciteiten van partners om cyberaanvallen en cybercriminaliteit op te opsporen en af te slaan. Hiermee kan het hoofd worden geboden aan hybride bedreigingen in derde landen. De EU financiert de capaciteitsopbouw in partnerlanden om de aan CBRN-vraagstukken gerelateerde veiligheidsrisco's te beperken[48].

Ten slotte zouden de lidstaten in de lijn van de alomvattende benadering van het crisisbeheer instrumenten en missies kunnen inzetten die deel uitmaken van het gemeenschappelijk veiligheids- en defensiebeleid (GVDB) en die afzonderlijk of als aanvulling bij ingezette EU-instrumenten kunnen worden gebruikt om partners te helpen bij de uitbreiding van hun capaciteit. Hierbij kunnen de volgende maatregelen worden overwogen: i) steun voor strategische communicatie, ii) ondersteunend advies aan cruciale overheidsdiensten die blootgesteld zijn aan hybride bedreigingen, iii) extra steun voor grensbeheer bij crisissituaties. Er kan worden gezocht naar verdere synergie-

[44] Gezamenlijke mededeling aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's - Herziening van het Europees nabuurschapsbeleid, 18.11.2015, JOIN(2015) 50 final.

[45] Idem; Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's - EU-uitbreidingsstrategie, 10.11.2015, COM(2015) 611 final; Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's Het effect van het EU-ontwikkelingsbeleid vergroten: een agenda voor verandering, 13.10.2011, COM(2011) 637 final.

[46] Gezamenlijke mededeling "Capaciteitsopbouw voor veiligheid en ontwikkeling - De partners in staat stellen crises te voorkomen en te beheersen" (JOIN (2015) 17 final).

[47] Verordening (EU) nr. 230/2014 van het Europees Parlement en de Raad van 11 maart 2014 tot vaststelling van een instrument voor bijdrage aan stabiliteit en vrede, PB L 77/1 van 15.3.2014.

[48] Hierbij gaat het onder meer over grenstoezicht, crisisbeheer, eerste reactie, illegale handel, exportcontrole betreffende producten voor tweeërlei gebruik, surveillance en beheersing van ziekten, nucleair forensisch onderzoek, herstel na incidenten, beveiliging van hoog-risico-inrichtingen. Beste praktijken die tot stand zijn gekomen met behulp van instrumenten die binnen het CBRN-actieplan van de EU zijn ontwikkeld, zoals het Europees opleidingscentrum voor nucleaire beveiliging en deelname van de EU aan de internationale werkgroep voor grenstoezicht, kunnen met derde landen worden gedeeld.

effecten tussen GVDB-instrumenten en actoren op het gebied van beveiliging, douane en justitie, inclusief de betrokken EU-agentschappen[49], Interpol en het Europees Gendarmeriekorps, conform hun mandaten.

<u>Actie 18</u>: 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 bij andere EU-instrumenten - worden ingezet om bijstand te verlenen aan partners bij de versterking van hun capaciteiten.

5. PREVENTIE, REACTIE OP CRISISSITUATIES EN HERSTEL

Zoals in afdeling 3.1. is uiteengezet, heeft de voorgestelde EU-Fusiecel voor analyse van hybride bedreigingen tot doel de relevante indicatoren te analyseren om hybride bedreigingen te voorkomen, erop te reageren en beleidsmakers te informeren. Door het voeren van een langetermijnbeleid op nationaal en Europees niveau kan de vatbaarheid voor 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 zijn uitgelokt, is essentieel. In dit verband kan het faciliteren van nationale civiele-beschermingsacties en de capaciteit van het Europees Coördinatiecentrum voor respons in noodsituaties[50] een doeltreffend reactiemechanisme zijn voor de aspecten van hybride bedreigingen die met civiele beschermingsmaatregelen moeten worden beantwoord. Dit kan tot stand komen in samenwerking met andere responsmechanismen en systemen voor vroegtijdige waarschuwing van de EU, met name het situatiecentrum van de EDEO voor de externe veiligheidsdimensie en het centrum voor strategische analyse en respons voor interne veiligheid.

De solidariteitsclausule (artikel 222 van het VWEU) voorziet in een optreden van de Unie en een optreden van de lidstaten indien een lidstaat wordt getroffen door een terroristische aanval, een natuurramp of een door de mens veroorzaakte ramp. Een optreden van de Unie om bijstand te verlenen aan de lidstaat komt tot stand door toepassing van Besluit 2014/415/EU van de Raad[51]. Een regeling voor de coördinatie in het kader van de Raad moet gebaseerd zijn op de geïntegreerde EU-regeling politieke crisisrespons [52]. In het kader van deze regelingen stellen de Commissie en de hoge vertegenwoordiger (binnen hun respectieve bevoegdheden) de desbetreffende Unie-

[49] EUROPOL, FRONTEX, CEPOL, EUROJUST
[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en
[51] Besluit 2014/415/EU van de Raad inzake de regeling voor de toepassing van de solidariteitsclausule door de Unie, PB L 192 van 1.7.2014, blz. 53.
[52] http://www.consilium.europa.eu/en/documents-publications/publications/2014/eu-ipcr/

instrumenten vast en stellen zij aan de Raad besluiten inzake uitzonderlijke maatregelen voor.

Artikel 222 VWEU heeft ook betrekking op situaties waarbij een of meerdere lidstaten rechtstreekse bijstand verlenen aan een lidstaat die getroffen werd door een terroristische aanval of een ramp. In dit kader is Besluit 2014/415/EU van de Raad niet van toepassing. Gezien de dubbelzinnige aard van hybride activiteiten moet de eventuele toepasselijkheid van de solidariteitsclausule als uiterste middel door de Commissie en de hoge vertegenwoordiger (binnen hun respectieve bevoegdheden) worden beoordeeld wanneer een EU-lidstaat met aanzienlijke hybride bedreigingen geconfronteerd wordt.

In tegenstelling tot artikel 222 VWEU zou artikel 42, lid 7, VEU kunnen worden ingeroepen om passend en tijdig te reageren indien meervoudige ernstige hybride bedreigingen ertoe leiden dat een EU-lidstaat gewapenderhand wordt aangevallen. Uitgebreide en ernstige hybride bedreigingen kunnen ook een intensievere samenwerking en coördinatie met de NAVO vereisen.

Bij de voorbereiding van hun strijdkrachten worden de lidstaten aangespoord om rekening te houden met potentiële hybride bedreigingen. Om bij een hybride aanval snel en doeltreffend besluiten te kunnen nemen, moeten de lidstaten op operationeel en politiek niveau regelmatig oefeningen houden om de slagkracht van de nationale en multinationale besluitvorming te testen. Er moet worden gestreefd naar een gemeenschappelijk operationeel protocol tussen de lidstaten, de Commissie en de hoge vertegenwoordiger, waarin de bij een hybride aanval te volgen effectieve procedures - vanaf de initiële identificatiefase tot de slotfase van de aanval - zijn afgebakend en de rol van elke EU-instelling en elke hierbij betrokken actor is vastgelegd.

Als een belangrijk onderdeel van het GVDB zouden middelen kunnen worden ingezet voor a) civiele en militaire opleiding, b) mentorschap en adviesmissies om de veiligheids- en defensiecapaciteit van een bedreigde staat te verbeteren, c) noodplanning om signalen van hybride bedreigingen op te sporen en de capaciteit voor vroegtijdige waarschuwing te versterken, d) ondersteuning van het beheer van grenscontroles bij noodsituaties, e) steun op specifieke terreinen zoals CBRN-risicobeperking en evacuatie-operaties van non-combattanten.

***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.**

***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 uitgebreide en ernstige hybride aanval.**

<u>Actie 21</u>: In overleg met de lidstaten zorgt de hoge vertegenwoordiger voor de opname, inzet en coördinatie van de capaciteiten van een militair optreden bij de bestrijding van hybride bedreigingen in het kader van het gemeenschappelijk veiligheids- en defensiebeleid.

6. NAUWERE SAMENWERKING MET DE NAVO

Hybride bedreigingen zijn niet alleen een probleem voor de EU, maar ook voor andere belangrijke partnerorganisaties zoals de Verenigde Naties (VN), de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE) en in het bijzonder de NAVO. Voor een doeltreffende reactie moet zowel op politiek als operationeel niveau een dialoog en coördinatie tussen organisaties tot stand komen. Een nauwere interactie tussen de EU en de NAVO zou moeten resulteren in een betere voorbereiding en meer doeltreffende reactie van beide organisaties op hybride bedreigingen, waarbij zij op basis van het inclusiviteitsbeginsel in hun optreden elkaar aanvullen en wederzijds ondersteunen en elkaars besluitvormingsautonomie en gegevensbeschermingsregels in acht nemen.

Beide organisaties hebben gedeelde waarden en worden geconfronteerd met gelijkaardige problemen. De EU-lidstaten en NAVO-bondgenoten verwachten dat hun respectieve organisaties hen zullen ondersteunen, waarbij zij in een crisissituatie snel, doortastend en gecoördineerd optreden of in het ideale geval kunnen verhinderen dat de crisis zich voordoet. Er zijn een aantal terreinen afgebakend voor nauwere samenwerking en coördinatie tussen de EU en NAVO. Hierbij gaat het onder meer over omgevingsbewustzijn, strategische communicatie, cyberbeveiliging en crisispreventie en respons. De lopende informele dialoog tussen de EU en de NAVO over hybride bedreigingen moet worden versterkt om de activiteiten die beide organisaties op dit vlak ontplooien, met elkaar in overeenstemming te brengen.

Met het oog op de complementariteit van reacties van de EU en de NAVO is het belangrijk dat beide organisaties vóór en tijdens een crisissituatie eenzelfde situationeel bewustzijn delen. Dit kan door op gezette tijden analyses en opgedane ervaring uit te wisselen, maar ook door een directe samenwerking tot stand te brengen tussen de EU-Fusiecel voor analyse van hybride bedreigingen en de NAVO-cel voor hybride bedreigingen. Even belangrijk is om vertrouwd te worden met elkaars procedures voor crisisbeheer om snel en doeltreffend te kunnen reageren. Weerbaarheid kan ook worden versterkt door te zorgen voor complementariteit bij het bepalen van benchmarks voor essentiële onderdelen van hun infrastructuur en door nauwe samenwerking op het vlak van strategische communicatie en cyberdefensie. Volledig inclusieve gezamenlijke oefeningen op politiek en technisch niveau zouden de besluitvormingscapaciteit van beide organisaties doeltreffender maken. Onderzoek naar nieuwe samenwerkingsmogelijkheden inzake opleiding kan bijdragen tot de totstandkoming van een vergelijkbaar niveau van deskundigheid op essentiële terreinen.

<u>Actie 22</u>: In samenwerking met de Commissie zet de hoge vertegenwoordiger de informele dialoog verder, 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.

7. CONCLUSIES

In deze gezamenlijke mededeling worden de acties aangegeven die ontworpen zijn om de hybride bedreigingen te helpen bestrijden en de weerbaarheid te bevorderen op zowel Europees als nationaal niveau, en worden de partners voor de uitvoering van de acties vermeld. Aangezien de nadruk ligt op **een betere bewustmaking**, wordt voorgesteld specifieke mechanismen in te stellen voor de uitwisseling van informatie met lidstaten en om de EU-capaciteit voor strategische communicatie te coördineren. Er zijn acties geconcipieerd om **bestendigheid tot stand te brengen** op terreinen zoals cyberbeveiliging, kritieke infrastructuur, beveiliging van het financiële systeem tegen illegaal gebruik en inspanningen ter bestrijding van gewelddadig extremisme en radicalisering. Op elk van deze terreinen vormen de uitvoering van de door de EU en de lidstaten overeengekomen strategieën en de volledige uitvoering door de lidstaten van de bestaande wetgeving eerste stappen. Enkele concretere maatregelen zijn voorgesteld om deze inspanningen verder te versterken.

Wat betreft **preventie van, reactie op en herstel van hybride bedreigingen** wordt voorgesteld de haalbaarheid te onderzoeken van de toepassing van de solidariteitsclausule van artikel 222 VWEU (zoals aangegeven in het desbetreffende besluit) en artikel 42, lid 7, VEU bij een uitgebreide en ernstige hybride aanval. De capaciteit op het vlak van strategische besluitvorming kan worden verstrekt door de totstandkoming van een gemeenschappelijk operationeel protocol.

Ten slotte wordt voorgesteld **de samenwerking** en **coördinatie** tussen **de EU en de NAVO** te intensiveren waarbij gezamenlijke inspanningen worden geleverd om het hoofd te bieden aan hybride bedreigingen.

Bij de uitvoering van dit gezamenlijk kader hebben de hoge vertegenwoordiger en de Commissie zich ertoe verbonden de hiervoor geschikte EU-instrumenten in te zetten waarover zij beschikken. Het is cruciaal dat de EU samen met de lidstaten ernaar streeft de risico's te verminderen die gepaard gaan met een blootstelling aan potentiële hybride bedreigingen die door staten en niet-overheidsactoren worden veroorzaakt.