EUROPESE
COMMISSIE

HOGE VERTEGENWOORDIGER
VAN DE UNIE VOOR
BUITENLANDSE ZAKEN
EN VEILIGHEIDSBELEID

Brussel, 13.6.2018
JOIN(2018) 16 final

GEZAMENLIJKE MEDEDELING VAN HET EUROPEES PARLEMENT, DE EUROPESE RAAD EN DE RAAD

Het opbouwen van weerbaarheid en reactiecapaciteit tegen hybride bedreigingen

1. INLEIDING

Hybride activiteiten door overheids- en niet-overheidsactoren blijven een ernstige en acute bedreiging voor de EU en haar lidstaten. Pogingen om landen te destabiliseren door het publieke vertrouwen in overheidsinstellingen te ondermijnen en maatschappelijke kernwaarden in vraag te stellen, komen steeds vaker voor. Onze maatschappij wordt zwaar op de proef gesteld door actoren die de EU en haar lidstaten schade willen toebrengen, van cyberaanvallen die de economie en openbare diensten ontwrichten over gerichte desinformatiecampagnes tot vijandelijke militaire acties.

Hybride campagnes zijn multidimensioneel: ze bestaan uit een combinatie van dwang en subversie, waarbij gebruik wordt gemaakt van conventionele en niet-conventionele methodes en tactieken (diplomatiek, militair, economisch, technologisch) om de tegenstander te destabiliseren. Ze zijn zodanig ontworpen dat ze moeilijk kunnen worden gedetecteerd of toegeschreven, en kunnen door zowel overheids- als niet-overheidsactoren worden gebruikt. De aanslag met zenuwgas in Salisbury in maart jongstleden[1] benadrukt de verscheidenheid van hybride bedreigingen en de vele tactieken die nu beschikbaar zijn. In reactie hierop heeft de Europese Raad[2] beklemtoond dat de capaciteit van de EU en haar lidstaten om hybride bedreigingen op cybergebied en op het gebied van strategische communicatie en contra-inlichtingen op te sporen, te voorkomen en te bestrijden, moet worden opgedreven. Daarbij werd bijzondere nadruk gelegd op de behoefte aan weerbaarheid tegen chemische, biologische, radiologische en nucleaire bedreigingen.

Bedreigingen met non-conventionele wapens vallen in een aparte categorie wegens de schaal waarop ze schade kunnen veroorzaken. Ze zijn niet alleen moeilijk te detecteren en toe te schrijven, maar het is ook complex om ertegen op te treden. Ook de internationale gemeenschap[3] maakt zich in het algemeen zorgen over chemische, biologische, radiologische en nucleaire bedreigingen die verder reiken dan hybride bedreigingen en ook terroristische bedreigingen omvatten, en met name over het evoluerende risico op proliferatie, zowel geografisch als onder niet-overheidsactoren.

Het versterken van de weerbaarheid tegen deze bedreigingen en het opvoeren van de capaciteit zijn hoofdzakelijk de verantwoordelijkheid van de lidstaten. De EU-instellingen hebben echter al een aantal maatregelen genomen om de nationale inspanningen te helpen versterken. Zij werken bijvoorbeeld nauw samen met andere internationale actoren, zoals de Noord-Atlantische Verdragsorganisatie (NAVO)[4], en deze werkzaamheden kunnen verder worden verdiept om steun te verlenen aan lidstaten op gebieden als snelle reactie[5].

Met deze gezamenlijke verklaring wordt tegemoetgekomen aan het verzoek van de Raad om hier verder werk van te maken. Ze maakt deel uit van een breder pakket dat ook het

---

1 Wat de aanslag in Salisbury betreft, heeft de Europese Raad op 22 maart 2018 verklaard dat hij "het eens [was] met het standpunt van de regering van het Verenigd Koninkrijk dat de Russische Federatie hier hoogstwaarschijnlijk voor verantwoordelijk is en dat er geen aannemelijke alternatieve verklaring is."

2 Conclusies van de Europese Raad van maart 2018.

3 Zie bijvoorbeeld Resolutie S/RES/2325 (2016) van 14 december 2016 van de Veiligheidsraad van de Verenigde Naties.

4 De bestrijding van hybride bedreigingen is een van de zeven gebieden van samenwerking met de Noord-Atlantische Verdragsorganisatie die zijn uiteengezet in de gezamenlijke verklaring die de voorzitter van de Europese Raad, de voorzitter van de Europese Commissie en de secretaris-generaal van de Noord-Atlantische Verdragsorganisatie in juli 2016 in Warschau hebben afgelegd.

5 Op zijn topontmoeting van juni 2018 in Charlevoix heeft ook de G7 ermee ingestemd een G7-snellereactiemechanisme op te zetten om bedreigingen voor democratieën aan te pakken: https://g7.gc.ca/en/official-documents/charlevoix-commitment-defending-democracy-from-foreign-threats/

laatste voortgangsverslag over de Veiligheidsunie[6] omvat, waarin een stand van zaken wordt opgemaakt en een overzicht wordt gegeven van de volgende stappen in de tenuitvoerlegging van het Actieplan voor chemisch, biologisch, radiologisch en nucleair materiaal van oktober 2017[7], alsook het tweede voortgangsverslag[8] over de tenuitvoerlegging van de 22 acties van het Gezamenlijk kader voor de bestrijding van hybride bedreigingen - een reactie van de Europese Unie[9].

2. DE REACTIE VAN DE EU

De Commissie en de Hoge Vertegenwoordiger hebben niet-aflatende inspanningen geleverd om de capaciteit van de EU op te bouwen en hebben effectieve steun verleend aan de lidstaten om hybride en chemische, biologische, radiologische en nucleaire bedreigingen te bestrijden. Er zijn al tastbare resultaten bereikt op gebieden als strategische communicatie, situationeel bewustzijn, versterking van de paraatheid, weerbaarheid en crisisresponscapaciteiten.

De East StratCom Task Force, die na de Europese Raad van maart 2015 is opgericht, leidde de werkzaamheden met betrekking tot het voorspellen, opsporen en bestrijden van desinformatie uit buitenlandse bronnen. De deskundigenanalyses en publieke producten[10] van deze taskforce hebben het bewustzijn omtrent de gevolgen van Russische desinformatie aanzienlijk doen toenemen. In de voorbije twee jaar heeft de taskforce meer dan 4 000 afzonderlijke gevallen van desinformatie aan het licht gebracht, waarvan vele doelbewust tegen Europa waren gericht. De focus van de werkzaamheden van de East Stratcom Task Force lag ook op een verbetering van de positieve berichtgeving, vooral in de oostelijke nabuurschapslanden. Dit succes heeft geleid tot de oprichting van twee andere taskforces, met een verschillende geografische focus - een taskforce voor de Westelijke Balkan en een specifieke Task Force South voor de Arabisch sprekende landen.

Er zijn belangrijke stappen gezet om de structuur op te bouwen die nodig is om het situationeel bewustzijn te verbeteren en de besluitvorming te ondersteunen. Binnen het Centrum van de Europese Unie voor de analyse van inlichtingen, dat deel uitmaakt van de Europese Dienst voor extern optreden, is in 2016 een EU-Fusiecel voor analyse van hybride bedreigingen opgericht. De Fusiecel ontvangt en analyseert gerubriceerde en publiek beschikbare informatie over hybride bedreigingen, die afkomstig is van diverse belanghebbenden. Tot dusver zijn meer dan 100 evaluaties en briefings opgesteld, die binnen de EU onder de lidstaten zijn verspreid om te worden meegenomen in de besluitvorming in de EU. De Fusiecel werkt nauw samen met het Europees Kenniscentrum voor de bestrijding van hybride dreigingen in Helsinki. Dit Kenniscentrum, dat in april 2017 is opgericht en tot taak heeft strategisch overleg aan te moedigen en hybride bedreigingen te onderzoeken en te analyseren, telt nu 16 landen[11] als lid en krijgt voortdurend steun van de EU.

---

6 Vijftiende voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie, COM(2018) 470.

7 COM(2017) 610 final.

8 Gezamenlijk verslag over de uitvoering van het gezamenlijk kader voor de bestrijding van hybride bedreigingen (juli 2017-juli 2018), JOIN(2018) 14.

9 JOIN(2016) 18 final.

10 Zie www.euvsdisinfo.eu

11 14 van de 16 huidige leden zijn EU-lidstaten: Tsjechië, Denemarken, Estland, Finland, Frankrijk, Italië, Duitsland, Letland, Litouwen, Nederland, Polen, Spanje, Zweden, het Verenigd Koninkrijk. Het initiatief voor de oprichting ervan werd genomen door het gezamenlijk kader voor de bestrijding van hybride bedreigingen. Het Kenniscentrum kreeg ook actieve steun van de EU en de Noord-Atlantische Verdragsorganisatie in het kader van hun samenwerking.

Er zijn ook belangrijke stappen gezet in de versterking van de paraatheid en weerbaarheid, met name tegen chemische, biologische, radiologische en nucleaire bedreigingen. De voorbije zes maanden is grote vooruitgang geboekt bij het identificeren van hiaten in de paraatheid voor chemische, biologische, radiologische en nucleaire incidenten, met name wat betreft de capaciteit om chemische, biologische, radiologische en nucleaire aanvallen te helpen voorkomen. Op initiatief van de Commissie heeft een consortium van nationale deskundigen een analyse uitgevoerd van de tekortkomingen van de detectieapparatuur in verschillende chemische, biologische, radiologische en nucleaire scenario's. Het verslag met de gapanalyse is verspreid onder de lidstaten, zodat ze geïnformeerde beslissingen kunnen nemen over detectiestrategieën en operationele maatregelen kunnen treffen om de vastgestelde tekortkomingen te verhelpen.

Dit werd gevolgd door metingen van de vooruitgang. De responscapaciteit van de EU op een grootschalige hybride crisis werd in detail getest tijdens de parallelle en gecoördineerde oefening van 2017 (PACE17) met de Noord-Atlantische Verdragsorganisatie. Deze oefening ging verder dan ooit tevoren: niet alleen werd het "EU Hybrid Playbook", de verschillende EU-responsmechanismen en de efficiëntie van hun onderlinge wisselwerking getest, maar ook de wijze waarop de EU-respons op hybride bedreigingen in wisselwerking staat met de acties van de Noord-Atlantische Verdragsorganisatie. Momenteel wordt de oefening voor 2018 voorbereid. Het is niet alleen de ambitie om dergelijke oefeningen jaarlijks te laten plaatsvinden, maar ook om de lidstaten te helpen bij het versterken van hun responscapaciteit op hybride crisissen.

Uit deze concrete stappen blijkt dat de door de EU opgezette beleidskaders vruchten afwerpen: de voorbije twee jaar zijn een aantal kaders opgezet om de werkzaakheden van de EU te helpen aansturen en focussen.

In het *Gezamenlijk kader voor de bestrijding van hybride bedreigingen - een reactie van de Europese Unie*[12] uit april 2016 wordt een overheidsbrede aanpak aangemoedigd, met 22 actiedomeinen, om **hybride bedreigingen** te bestrijden en de weerbaarheid van de EU, haar lidstaten en internationale partners te verbeteren. De meeste acties van dat gezamenlijk kader hebben tot doel het situationeel bewustzijn te verbeteren, weerbaarheid op te bouwen en de reactiecapaciteit aan te scherpen. Ze hebben onder meer betrekking op het versterken van de capaciteit van de EU om inlichtingen te analyseren, betere bescherming van kritieke infrastructuur en cyberbeveiliging om radicalisering en gewelddadig extremisme te bestrijden. Ook de bestrijding van cyberbedreigingen en cyberaanvallen behoren tot de kerntaken van het gezamenlijk kader. Het tweede voortgangsverslag over de tenuitvoerlegging van het gezamenlijk kader, dat samen met deze gezamenlijke mededeling wordt vastgesteld, toont aan dat tastbare vooruitgang is geboekt met deze acties en bevestigt dat de inspanningen van de EU om hybride bedreigingen te bestrijden, zijn versterkt en verdiept[13].

9 mei 2018 was een belangrijke datum wat **cyberbeveiliging** betreft: het was de uiterste termijn voor de omzetting van de richtlijn inzake de beveiliging van netwerk- en informatiesystemen, de eerste juridisch bindende en voor de hele EU geldende reeks maatregelen op het gebied van cyberbeveiliging. Dit is een belangrijk onderdeel van de bredere aanpak die is uiteengezet in de *Gezamenlijke mededeling inzake weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU*[14] van september 2017, die een breed gamma aan concrete maatregelen bevat om een krachtige impuls te geven aan de cyberbeveiligingsstructuren en -capaciteiten van de EU. Centraal in deze

---

13 Eerste tenuitvoerleggingsverslag (juli 2017): JOIN(2017) 30 final.

14 JOIN(2017) 450 final.

mededeling stond de opbouw van de weerbaarheid van de EU tegen cyberaanvallen en de versterking van de cyberbeveiligingscapaciteit van de EU, de totstandbrenging van een doeltreffende strafrechtelijke respons, en de verbetering van de wereldwijde stabiliteit door internationale samenwerking. Deze mededeling ging vergezeld van een voorstel voor een cyberbeveiligingsverordening, teneinde de steun op EU-niveau te versterken[15], en werd gevolgd door een reeks voorstellen die nu verder ten uitvoer moeten worden gelegd (zie hieronder).

Desinformatie is schadelijk voor onze democratieën omdat het de burgers belemmert om geïnformeerde beslissingen te nemen en deel te nemen aan het democratische proces. Het internet heeft de hoeveelheid en de diversiteit aan berichtgeving die beschikbaar is voor de burgers enorm doen toenemen. Nieuwe technologieën kunnen echter worden gebruikt om op een nooit eerder geziene schaal en met een nooit eerder geziene snelheid desinformatie te verspreiden, die doelbewust gericht is op het zaaien van wantrouwen en het creëren van maatschappelijke spanningen. In de mededeling van de Commissie *"Bestrijding van online-desinformatie: een Europese benadering*[16]*"* wordt een Europese aanpak van dit probleem uiteengezet, waarbij diverse belanghebbenden, met name online-platforms maar ook mediabedrijven, worden opgeroepen om actie te ondernemen. Deze acties hebben betrekking op een breed spectrum aan relevante domeinen, zoals grotere transparantie, betrouwbaarheid en verantwoordingsplicht van online-platforms, beter beveiligde en schokbestendige verkiezingsprocessen, het stimuleren van onderwijs en mediageletterdheid, steun voor journalistiek van goede kwaliteit, en bestrijding van desinformatie via strategische communicatie. De eerste concrete stappen zijn een praktijkcode betreffende desinformatie, die moet worden opgesteld door een Multi-stakeholderforum inzake desinformatie en een netwerk van factcheckers; deze code moet voor de zomer klaar zijn. De eerste vergadering van het Multi-stakeholderforum inzake desinformatie vond plaats op 29 mei 2018; tijdens deze vergadering werd overeenstemming bereikt over de stappen die moeten worden gezet om de code in juli 2018 te kunnen goedkeuren. De Commissie zal eind 2018 de voortgang bij de bestrijding van dit probleem evalueren en beslissen of extra ingrepen nodig zijn op dit gebied. De geplande activiteiten zullen samenhangend en complementair zijn met die van de East Stratcom Task Force.

Wat **chemische, biologische, radiologische en nucleaire** risico's betreft, zijn in het *Actieplan*[17] van de Commissie van oktober 2017 23 praktische acties en maatregelen voorgesteld om de burgers en de infrastructuur beter te beveiligen tegen dergelijke bedreigingen, onder meer via nauwere samenwerking tussen de EU en haar lidstaten en met de Noord-Atlantische Verdragsorganisatie. Dit actieplan, dat deel uitmaakt van de maatregelen van de Veiligheidsunie om de bescherming en weerbaarheid tegen terrorisme te verbeteren, volgt een preventieve aanpak die gebaseerd is op de redenering dat de waarschijnlijkheid van chemische, biologische, radiologische en nucleaire risico's laag is, maar de gevolgen in het geval van een aanval groot en langdurig zullen zijn. De aanval in Salisbury en de toenemende bezorgdheid omtrent de belangstelling van terroristen in chemische, biologische, radiologische en nucleaire materialen en hun vermogen om deze zowel binnen als buiten de EU te gebruiken[18], tonen aan dat chemische, biologische, radiologische en nucleaire stoffen een reële bedreiging vormen. Dit toont nogmaals aan dat het Actieplan zo snel mogelijk volledig ten uitvoer moet worden gelegd. Het volgt een benadering voor alle mogelijke risico's en focust op vier doelstellingen: de

15 COM (2017) 477, zie hieronder.
16 COM (2018) 236 final.
17 COM(2017) 610 final.
18 Europol, Terrorism Situation and Trend report (TE-SAT) 2017, blz. 16, beschikbaar op: www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf. Zie ook de verklaringen van de directeur-generaal van de OPCW: www.globaltimes.cn/content/1044644.shtml.

toegankelijkheid van CBRN-materiaal beperken; een betere paraatheid bij en respons op veiligheidsincidenten met CBRN-materiaal garanderen; op intern en extern niveau zorgen voor sterkere banden op het gebied van CBRN-beveiliging met belangrijke regionale en internationale EU-partners; en de kennis van CBRN-risico's vergroten. In het laatste voortgangsverslag over de Veiligheidsunie, dat samen met deze gezamenlijke mededeling wordt vastgesteld, wordt in detail verslag uitgebracht over de tastbare vooruitgang bij de tenuitvoerlegging van het Actieplan.

Om de effectiviteit van de inspanningen ter bestrijding van hybride bedreigingen te vergroten en de boodschap van eenheid tussen de EU-lidstaten en de bondgenoten van de Noord-Atlantische Verdragsorganisatie (NAVO) te versterken, is in de *Gezamenlijke Verklaring van Warschau*[19] van juli 2016 vastgesteld dat samenwerking bij het bestrijden van hybride bedreigingen een kerngebied is van de **samenwerking tussen de EU en de NAVO**. Op dit ogenblik heeft bijna één derde van alle gezamenlijke voorstellen voor samenwerking betrekking op hybride bedreigingen[20]. De hierboven beschreven oefeningen en het "EU Playbook[21]" worden dit jaar uitgebouwd, waarbij de samenwerking verder wordt verdiept.

3. KRACHTIGER REAGEREN OP DE EVOLUERENDE BEDREIGINGEN

3.1. Situationeel bewustzijn - verbeterde capaciteit om hybride bedreigingen op te sporen

Inspanningen om hybride bedreigingen te bestrijden, moeten worden geschraagd door een capaciteit om kwaadwillige cyberactiviteiten en de bronnen daarvan, zowel intern als extern, op te sporen en de mogelijke verbanden tussen ogenschijnlijk niet met elkaar in verband staande gebeurtenissen te begrijpen. Daartoe is het van essentieel belang dat gebruik wordt gemaakt van alle beschikbare gegevensstromen, met inbegrip van publiek beschikbare informatie.

De Fusiecel die binnen de Europese Dienst voor extern optreden is opgericht als enig EU-focuspunt voor de analyse van hybride bedreigingen, is een belangrijke factor, maar moet over de nodige deskundigheid beschikken om het hoofd te kunnen bieden aan het volledige spectrum aan hybride bedreigingen, met inbegrip van chemische, biologische, radiologische en nucleaire bedreigingen en contra-inlichtingen. Bredere deskundigheid ter aanvulling van de civiele en militaire inlichtingen op deze specifieke gebieden zou zorgen voor betere ondersteuning van de reactie van de EU op toekomstige crisissen. Dit kan worden ondersteund door acties van de lidstaten om de bijdragen van hun nationale inlichtingendiensten aan de Fusiecel op te drijven en om het netwerk van nationale contactpunten met de Fusiecel beter in staat te stellen tijdkritieke informatie te verstrekken en te verwerken. Een volgende stap houdt in dat de lidstaten kijken hoe ze de bijdragen van hun nationale inlichtingendiensten aan het Inlichtingen- en situatiecentrum van de Europese Unie (INTCEN) kunnen opdrijven, teneinde een diepere analyse van potentiële dreigingen mogelijk te maken.

---

19 Deze verklaring, die door voorzitter Juncker, voorzitter Tusk, en NAVO secretaris-generaal Stoltenberg is ondertekend, vormt de basis voor de samenwerking tussen de EU en de NAVO.

20 15283/16 en 14802/17.

21 SWD(2017) 227 final.

Toekomstige maatregelen

- De Hoge Vertegenwoordiger zal de EU-Fusiecel uitbreiden met componenten die gespecialiseerd zijn in chemische, biologische, radiologische en nucleaire inlichtingen en in cyberanalyse. De lidstaten worden verzocht om meer inlichtingen te verstrekken aan de Fusiecel, zodat bestaande en ontluikende hybride bedreigingen beter kunnen worden geanalyseerd.

- In samenwerking met de Hoge Vertegenwoordiger zal de Commissie de werkzaamheden met betrekking tot kwetsbaarheidsindicatoren voltooien, zodat de lidstaten de mogelijkheid op hybride bedreigingen in verschillende sectoren beter kunnen beoordelen. Deze werkzaamheden zullen ook de EU-analyse van hybride tendensen ondersteunen.

3.2. **Versterkte maatregelen tegen chemische, biologische, radiologische en nucleaire bedreigingen**

Het Actieplan tegen chemische, biologische, radiologische en nucleaire bedreigingen van de beveiliging uit oktober 2017 vormt het kader voor maatregelen ter versterking van de paraatheid, weerbaarheid en coördinatie op EU-niveau. De acties hebben betrekking op een reeks maatregelen ter ondersteuning van de lidstaten: bundeling van deskundigheid, gezamenlijke capaciteitsopbouw, uitwisseling van kennis en goede praktijken en versterking van de operationele samenwerking. De lidstaten en de Commissie moeten samenwerken om het actieplan zo snel mogelijk volledig ten uitvoer te leggen. Voortbouwend op de vooruitgang die al is geboekt met de gapanalyse van de opsporingscapaciteit en de uitwisseling van goede praktijken in de nieuw opgerichte Adviesgroep inzake chemische, biologische, radiologische en nucleaire beveiliging, moet de Unie nu verdere maatregelen nemen om ontluikende en evoluerende bedreigingen aan te pakken. Dit geldt met name voor chemische bedreigingen. Naar het voorbeeld van de werkzaamheden om de toegang tot precursoren voor explosieven te beperken[22], moet de EU snel operationele maatregelen nemen om de toegang tot risicovolle chemische materialen beter te controleren en de capaciteit om dergelijke materialen in een zo vroeg mogelijk stadium op te sporen, te optimaliseren. De lidstaten moeten ook overwegen om verdere gapanalyses en inventarisaties uit te voeren op EU-niveau, bijvoorbeeld met betrekking tot chemische, biologische, radiologische en nucleaire weerbaarheid en activa en benaderingen voor decontaminatie. De voorbereiding op en het beheer van de gevolgen van een chemische, biologische, radiologische of nucleaire aanval vergt versterkte samenwerking en coördinatie tussen de lidstaten, en met name tussen de autoriteiten voor civiele bescherming. Het Uniemechanisme voor civiele bescherming kan een sleutelrol spelen in dit proces, dat tot doel heeft de collectieve voorbereidings- en responscapaciteit te versterken.

Internationale samenwerking is eveneens een belangrijk element in deze werkzaamheden; de EU kan steunen op koppelingen met de regionale chemische, biologische, radiologische

[22] In het kader van de werkzaamheden in de Veiligheidsunie om de armslag voor terroristen en criminelen te beperken, heeft de Commissie krachtdadige maatregelen getroffen om de toegang tot precursoren voor explosieven waarvan misbruik kan worden gemaakt om zelfgemaakte explosieven te vervaardigen, te beperken. In oktober 2017 heeft de Commissie een aanbeveling gepresenteerd inzake onmiddellijke actie ter voorkoming van misbruik van precursoren voor explosieven, op basis van bestaande regels (Aanbeveling C(2017) 6950 final). Voortbouwend hierop heeft de Commissie in april 2018 een voorstel vastgesteld om de bestaande Verordening 98/2013 over het op de markt brengen en het gebruik van precursoren voor explosieven te herzien en te versterken (COM(2018) 209 final).

en nucleaire excellentiecentra en streven naar synergieën met de Noord-Atlantische Verdragsorganisatie en de programma's voor preventie van, paraatheid voor en reactie op natuurrampen en door de mens veroorzaakte rampen in de landen van het Oostelijk en het Zuidelijk Nabuurschap[23].

Toekomstige maatregelen

- De EU moet maatregelen onderzoeken om de naleving van internationale regels en normen tegen het gebruik van chemische wapens te garanderen, eventueel via een specifieke EU-sanctieregeling tegen chemische wapens.
- Om het Actieplan voor chemisch, biologisch, radiologisch en nucleair materiaal verder uit te werken, zal de Commissie met de lidstaten samenwerken om tegen eind 2018:
  - een lijst op te stellen van chemische stoffen die een specifieke bedreiging vormen; deze lijst moet de basis vormen voor operationele maatregelen om de toegang tot die stoffen te beperken;
  - een dialoog op te zetten met private actoren in de toeleveringsketen, teneinde de evoluerende dreiging van chemische stoffen die als precursoren kunnen worden gebruikt, samen aan te pakken;
  - de dreigingsscenario's sneller opnieuw te bekijken en de bestaande opsporingsmethoden te analyseren, teneinde chemische bedreigingen beter te kunnen opsporen, met als doel operationele richtsnoeren op te stellen die de lidstaten kunnen gebruiken om hun opsporingscapaciteiten te verbeteren.
- De lidstaten moeten een inventaris opmaken van hun voorraden aan essentiële medische tegenmaatregelen, laboratoriumbehandelingen en andere capaciteiten. De Commissie zal met de lidstaten samenwerken om de beschikbaarheid van deze voorraden in de hele EU regelmatig in kaart te brengen, zodat ze bij een aanval sneller kunnen worden ingezet.

3.3. **Strategische communicatie - coherente verspreiding van informatie**

Een belangrijke uitdaging met betrekking tot hybride bedreigingen is het bewustzijn te vergroten en het grote publiek te leren hoe zij informatie van desinformatie kunnen onderscheiden. Voortbouwend op de ervaring van de East Stratcom Task Force, de EU-Fusiecel, het Europees Kenniscentrum voor de bestrijding van hybride bedreigingen en andere inspanningen van de Commissie[24], zullen de Commissie en de Hoge Vertegenwoordiger de strategische communicatiecapaciteit van de EU verder ontwikkelen en professionaliseren door te zorgen voor systematische interactie en samenhang tussen de bestaande structuren. Dit zal verder worden uitgebreid naar andere EU-instellingen en

[23] In het Oostelijk en het Zuidelijk Nabuurschap worden opleidingen en oefeningen voor civiele bescherming georganiseerd in het kader van regionale programma's voor preventie van, paraatheid voor en reactie op natuurrampen en door de mens veroorzaakte rampen.

[24] Ook de Vertegenwoordigingen van de Commissie houden zich actief bezig met het natrekken van feiten en het ontkrachten van mythes. Verscheidene Vertegenwoordigingen hebben tools ontwikkeld die zijn aangepast aan de lokale omstandigheden, zoals *Les Décodeurs de l'Europe* in Frankrijk, UE Vero Falso in Italië, een wedstrijd voor cartoons over het ontkrachten van EU-mythes in Oostenrijk, een vergelijkbare cartoonreeks in Roemenië en Euromyths A-Z van de Vertegenwoordiging van het VK. Er zijn nog meer van dergelijke projecten in de maak.

lidstaten, onder meer door gebruik te maken van het aangekondigde beveiligde onlineplatform inzake desinformatie.

Betere coördinatie en samenwerking met betrekking tot strategische communicatie in alle EU-instellingen, met de lidstaten en met partners en internationale organisaties is van essentieel belang en vereist voorbereiding en oefening alvorens op een echte crisis kan worden gereageerd.

Verkiezingen zijn strategisch een bijzonder gevoelige periode voor cyberaanvallen en pogingen om conventionele (offline) garanties en regels, zoals stilteperioden, transparante financieringsregels en gelijke behandeling van kandidaten online te omzeilen. In het verleden hebben derde landen bijvoorbeeld online aanvallen gelanceerd tegen verkiezingsinfrastructuur en IT-systemen voor verkiezingscampagnes en grootschalige politiek gemotiveerde desinformatiecampagnes en cyberaanvallen georganiseerd, met als doel het vertrouwen in en de geloofwaardigheid van democratische verkiezingen te ondermijnen. De EU heeft verscheidene werkpunten vooropgesteld om het bewustzijn in de lidstaten te vergroten, teneinde de voorbereiding en respons op deze evoluerende bedreigingen te verbeteren. In de Raad zullen de cyberbeveiligingsautoriteiten van de lidstaten[25] vrijwillig richtsnoeren en gemeenschappelijke beste praktijken opstellen om verkiezingstechnologie doorheen de volledige verkiezingscyclus te beveiligen tegen cyberbedreigingen. Dit omvat informatiesystemen en ICT-oplossingen die worden gebruikt om kiezers en kandidaten te registreren, stemmen te verzamelen en te tellen en resultaten bekend te maken, alsook hulpsystemen die rechtstreeks gekoppeld zijn aan de legitimiteit van de verkiezingsresultaten.

In het geval van hybride aanvallen moet het grote publiek ook snel betrouwbare en consequente informatie krijgen. Omdat chemische, biologische, radiologische en nucleaire incidenten of gebeurtenissen met een vergelijkbare impact tot publieke verontwaardiging leiden, moeten de burgers snel een antwoord krijgen. Strategische berichtgeving speelt een belangrijke rol tussen internationale organisaties, die mogelijk afzonderlijk responsplannen aan het opstellen zijn.

Toekomstige maatregelen

- De Europese Dienst voor extern optreden en de Commissie zullen, binnen hun respectieve bevoegdheidsgebieden, tot een meer gestructureerde samenwerking inzake strategische communicatie trachten te komen, teneinde desinformatie van binnen en buiten de EU aan te pakken en vijandelijke desinformatie en hybride inmenging door buitenlandse overheden te bestrijden.

- De Commissie zal in het najaar evenementen op hoog niveau organiseren met lidstaten en relevante belanghebbenden, waaronder het grondrechtencolloquium inzake democratie, om goede praktijken en richtsnoeren te bevorderen met betrekking tot de wijze waarop cybergerelateerde en desinformatiebedreigingen voor verkiezingen kunnen worden voorkomen, ingeperkt en bestreden.

- De Hoge Vertegenwoordiger en de Commissie zullen bekijken hoe de werkzaamheden van de drie Stratcom-taskforces beter kunnen worden ondersteund, wat middelen en hulpbronnen betreft, teneinde te garanderen dat de EU-inspanningen volstaan om het hoofd te bieden aan de complexiteit van desinformatiecampagnes van vijandige actoren.

[25] Onder de auspiciën van de samenwerkingsgroep die is opgericht in het kader van de richtlijn inzake de beveiliging van netwerk- en informatiesystemen.

3.4. **Het opbouwen van weerbaarheid en afschrikking op het gebied van cyberbeveiliging**

Cyberbeveiliging is van cruciaal belang voor onze welvaart en veiligheid. Naarmate ons dagelijks leven en onze economieën meer vervlochten raken met digitale technologieën, worden we kwetsbaarder.

Op dit ogenblik is er in de EU een gebrek aan investeringen en coördinatie om tot effectieve cyberbeveiliging te komen. De EU tracht hier iets aan te doen door capaciteit op te bouwen via ondersteunende maatregelen, sterkere coördinatie en nieuwe structuren om de uitrol van cyberbeveiligingstechnologie te bevorderen[26]. In de richtlijn inzake beveiliging van netwerk- en informatiesystemen[27] is bepaald aan welk minimumniveau de beveiliging van netwerk- en informatiesystemen in de hele EU moet voldoen. Om de cyberweerbaarheid te verbeteren, is het van essentieel belang dat alle lidstaten deze richtlijn volledig ten uitvoer leggen. Dit is een cruciale eerste stap. De algemene verordening gegevensbescherming bevat de verplichting om inbreuken betreffende persoonsgegevens te melden aan de bevoegde toezichthoudende autoriteit. Andere belangrijke maatregelen zijn een sterker en gemoderniseerd agentschap van de Europese Unie voor cyberbeveiliging en een Europees certificeringskader voor ICT-producten en -diensten[28], teneinde het consumentenvertrouwen op te bouwen. Er zijn ook werkzaamheden aan de gang om bijstand te verlenen aan het netwerk van kenniscentra van de lidstaten, teneinde de ontwikkeling en uitrol van cyberbeveiligingsoplossingen te stimuleren en de inspanningen voor capaciteitsopbouw op dit domein in de EU en op nationaal niveau aan te vullen. Hierbij wordt voortgebouwd op de werkzaamheden van het op 6 juni door de Commissie voorgestelde programma Digitaal Europa[29], dat nieuwe prioriteit verleent aan EU-investeringen in cyberbeveiliging.

Tegelijk wordt in de aanbeveling inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises (de "blauwdruk")[30] uiteengezet hoe de samenwerking tussen de lidstaten en diverse EU-actoren moet verlopen wanneer zij moeten reageren op een grootschalige grensoverschrijdende cyberaanval. In die aanbeveling wordt benadrukt dat situationeel bewustzijn van essentieel belang is voor effectieve coördinatie op technisch, operationeel en strategisch/politiek niveau. De in het kader van de richtlijn inzake beveiliging van netwerk- en informatiesystemen opgerichte samenwerkingsgroep werkt eveneens aan een verbetering van de uitwisseling van informatie tussen relevante partijen, waarbij een gemeenschappelijke classificatie voor de beschrijving van incidenten wordt opgesteld. Deze aanpak zal tijdens de volgende oefeningen worden getest. De Fusiecel stelt strategische analyses op van actuele en ontluikende cyberbedreigingen, op basis van de bijdragen van de inlichtingendiensten van de lidstaten.

Het onlangs goedgekeurde kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten (het "instrumentarium voor cyberdiplomatie") betekende een grote stap voorwaarts in operationele termen, en bevat maatregelen in het kader van

---

[26] In het kader van de versterking van innovatie in de regio's van Europa, is in december 2017 een nieuw interregionaal proefproject opgezet om de cyberbeveiligingswerkzaamheden van EU-regio's te bundelen.

[27] 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.

[28] COM (2017) 477.

[29] Voorstel voor een verordening tot vaststelling van het programma Digitaal Europa voor de periode 2021-2027, COM(2018) 434.

[30] C (2017) 6100.

het gemeenschappelijk buitenland- en veiligheidsbeleid, waaronder ook beperkende maatregelen die kunnen worden gebruikt voor een sterkere EU-respons op activiteiten die schadelijk zijn voor de politieke, veiligheids- en economische belangen. Het afschrikkend effect van dit kader hangt af van de mate waarin de lidstaten er ten volle gebruik van maken. De Raad Buitenlandse zaken heeft in zijn conclusies inzake kwaadwillige cyberactiviteiten van april jongstleden het kwaadwillige gebruik van informatie- en communicatietechnologieën streng veroordeeld, onder meer naar aanleiding van de Wannacry- en NotPetya-aanvallen, die aanzienlijke schade en economische verliezen hebben veroorzaakt in de EU en daarbuiten.

De EU en haar lidstaten moeten hun inlichtingenuitwisseling opschroeven om de verantwoordelijken van cyberaanvallen te kunnen aanwijzen. Dit zou potentiële daders afschrikken en de kans vergroten dat ze ter verantwoording worden geroepen. Het afschrikkend effect vergroten is een kerndoelstelling van de strategische benadering van de Commissie ter verbetering van de cyberbeveiliging. De recente voorstellen van de Commissie die gericht zijn op een verbetering van de grensoverschrijdende vergaring van elektronische bewijzen voor strafrechtelijke procedures zouden de rechtshandhavingsmogelijkheden om cybercriminaliteit te onderzoeken en te vervolgen, eveneens aanzienlijk vergroten.

Sterke cyberweerbaarheid vraagt om een collectieve en brede aanpak. Hiervoor zijn robuustere en doeltreffendere structuren nodig om de cyberbeveiliging te bevorderen en om te reageren op cyberaanvallen in de lidstaten, maar ook tegen de instellingen, agentschappen, delegaties, missies en activiteiten van de EU: het gebrek aan een gezamenlijk beveiligd communicatienetwerk tussen de Europese instellingen is een belangrijke tekortkoming. Het bewustzijn van cyberbeveiliging in de instellingen en onder het personeel van de EU moet worden vergroot door een verbeterde beveiligingscultuur en intensievere opleiding.

Toekomstige maatregelen

- Het Europees Parlement en de Raad moeten vaart zetten achter de onderhandelingen over de cyberbeveiligingsvoorstellen om vóór het einde van het jaar een akkoord te bereiken; zij moeten ook overeenstemming bereiken over de voorgestelde wetgeving inzake het verzamelen van elektronisch bewijsmateriaal.

- De Commissie en de Hoge Vertegenwoordiger zullen nauw samenwerken met de lidstaten om vooruitgang te boeken met de cyberaspecten van de EU-mechanismen voor crisisbeheer en -respons. De lidstaten worden verzocht om hun werkzaamheden met betrekking tot de toewijzing van cyberaanvallen en het praktische gebruik van het instrumentarium voor cyberdiplomatie voort te zetten, teneinde de politieke respons op cyberaanvallen te vergroten.

- Om tegemoet te komen aan de behoefte om onze cyberverdedigingscapaciteiten op te drijven, wordt een specifiek opleiding- en onderwijsplatform opgezet om de door de lidstaten aangeboden opleidingsmogelijkheden op het gebied van cyberverdediging te helpen coördineren. Er wordt gestreefd naar synergieën met soortgelijk inspanningen van de Noord-Atlantische Verdragsorganisatie.

3.5. **Weerbaarheid opbouwen tegen vijandige inlichtingenactiviteiten**

Optreden tegen vijandige inlichtingenactiviteiten vergt in de eerste plaats een versterkte en effectieve coördinatie tussen de lidstaten, overeenkomstig relevante EU- en nationale voorschriften en regelingen. Het is echter ook van essentieel belang dat de EU-instellingen hun capaciteiten vergroten om de groeiende dreiging af te weren van activiteiten die specifiek tegen de instellingen zijn gericht en bouwen aan een cultuur van beveiligingsbewustzijn, ondersteund door verbeterde opleiding en fysieke beveiliging. De instellingen kunnen ook met de lidstaten samenwerken om een robuuster EU-accreditatiesysteem op te zetten. Een dergelijk systeem moet gebaseerd zijn op proactieve rapportering, waardoor de lidstaten en instellingen zich beter bewust worden van mogelijke vijandige actoren, met name die welke reeds door lidstaten zijn geïdentificeerd.

Coördinatie tussen lidstaten onderling en tussen lidstaten en andere relevante internationale organisaties, met name de Noord-Atlantische Verdragsorganisatie, zou een hefboomeffect hebben op de contra-inlichtingen tegen vijandige activiteiten in de EU. De screening van investeringen, op basis van een in september 2017 door de Commissie voorgestelde verordening[31] inzake de screening van buitenlandse directe investeringen door de lidstaten om redenen van veiligheid of openbare orde, is een voorbeeld van een domein dat baat zou hebben bij betere coördinatie tussen de lidstaten. Verbeterde coördinatie tussen de lidstaten is ook belangrijk voor het onderzoeken van financiële transacties, aangezien vijandige inlichtingendiensten steeds vaker ingewikkelde financiële regelingen gebruiken om hun activiteiten tegen de EU te financieren.

Toekomstige maatregelen

- De Europese Dienst voor extern optreden en de Commissie zullen verbeterde praktische maatregelen nemen teneinde het vermogen van de EU om samen met de lidstaten op te treden tegen vijandige inlichtingenactiviteiten die specifiek tegen de instellingen zijn gericht, in stand te houden en te ontwikkelen.

- De versterkte Fusiecel zal worden aangevuld met deskundigheid op het gebied van contra-inlichtingen, zodat ze gedetailleerde analyses en briefings kan opstellen over de aard van waarschijnlijk geachte vijandige inlichtingenactiviteiten tegen individuen en de instellingen.

- Het Europees Parlement en de Raad moeten vaart zetten achter de onderhandelingen over het voorstel inzake de screening van investeringen, teneinde vóór het einde van het jaar overeenstemming te bereiken.

4. **CONCLUSIE**

Hybride en chemische, biologische, radiologische en nucleaire bedreigingen staan hoog op de agenda van de EU. Het incident dat in maart plaatsvond in het VK benadrukte het brede spectrum aan hybride oorlogsvoering en de bijzondere behoefte aan weerbaarheid tegen chemische, biologische, radiologische en nucleaire bedreigingen.

[31] Voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van een kader voor de screening van buitenlandse directe investeringen in de Europese Unie, COM(2017) 487.

De Commissie en de Hoge Vertegenwoordiger hebben een aantal initiatieven voorgesteld en goedgekeurd om het hoofd te bieden aan de uitdagingen van hybride bedreigingen. De Commissie zet ook vaart achter de tenuitvoerlegging van het actieplan van 2017 om de voorbereiding op chemische, biologische, radiologische en nucleaire risico's te verbeteren.

Deze gezamenlijke mededeling heeft tot doel de Europese Raad op de hoogte te brengen van de lopende werkzaamheden en na te gaan op welke gebieden intensiever moet worden opgetreden om de essentiële bijdrage van de EU tot de bestrijding van deze bedreigingen te verdiepen en te versterken. Het is nu aan de lidstaten, de Commissie en de Hoge Vertegenwoordiger om te zorgen voor snelle follow-up.