EUROPESE
COMMISSIE

HOGE VERTEGENWOORDIGER
VAN DE UNIE VOOR
BUITENLANDSE ZAKEN
EN VEILIGHEIDSBELEID

Brussel, 10.11.2022
JOIN(2022) 49 final

GEZAMENLIJKE MEDEDELING AAN HET EUROPEES PARLEMENT EN DE RAAD

Het EU-beleid op het gebied van cyberdefensie

I. INLEIDING

De terugkeer van oorlog in Europa, door de militaire agressie van Rusland tegen Oekraïne, zonder aanleiding of grond, is een waarschuwing voor iedereen die vragen stelt bij de aanpak van de EU op het gebied van veiligheid en defensie en haar vermogen om haar visie uit te dragen en haar belangen te verdedigen, ook in cyberspace. Autoritaire regimes trachten de op regels gebaseerde internationale orde in cyberspace aan te vechten en te ondermijnen, waardoor dit domein net als land, zee en lucht en de ruimte steeds meer betwist wordt. Kwaadwillig gedrag in cyberspace van de kant van zowel statelijke als niet-statelijke actoren is de afgelopen jaren toegenomen; dit uit zich onder meer in een toenemend aantal cyberaanvallen op kritieke militaire en civiele infrastructuur in de EU en bij missies en operaties buiten de EU.

De scheidslijnen tussen de civiele en de militaire dimensie van cyberspace zijn vervaagd, zoals blijkt uit recente aanvallen op energienetwerken, vervoersinfrastructuur en ruimtesystemen. Dit illustreert ook de onderlinge afhankelijkheid van de fysieke en de digitale infrastructuur en het potentieel van significante cyberincidenten om kritieke infrastructuur te verstoren of te beschadigen. Het is dus heel duidelijk dat de EU in cyberspace moet zorgen voor nauwe militaire en civiele samenwerking, zodat zij een sterkere rol kan spelen om de veiligheid te waarborgen.

De EU moet meer verantwoordelijkheid nemen voor haar eigen veiligheid. Dat vereist moderne en interoperabele Europese strijdkrachten. De lidstaten zullen zich er dus met spoed en met voorrang toe moeten verbinden om meer te investeren in het volledige spectrum van cyberdefensievermogens, met inbegrip van actieve defensievermogens. De EU blijft zich ten volle committeren aan het internationaal recht en de internationale normen in cyberspace, maar moet zich bereid tonen deze vermogens op gecoördineerde wijze in te zetten in geval van een cyberaanval op een lidstaat.

Om hierin te slagen, moet de EU haar technologische en digitale soevereiniteit op cybergebied waarborgen. Het vermogen van de EU om op te treden, zal afhangen van haar vermogen om geavanceerde technologieën voor cyberbeveiliging en cyberdefensie in de EU te beheersen en te ontwikkelen. Aangezien cybertechnologieën een groot potentieel voor tweeërlei gebruik hebben, moet de sector cyberbeveiliging en cyberdefensie, met inbegrip van onderzoek, ontwikkeling en innovatie, de vermogens beter ontwikkelen door veel synergetischer te werk te gaan.

Gemeenschappelijke preventie en opsporing zijn belangrijke onderdelen van de defensievermogens van de EU. De EU moet de capaciteit hebben om aanvallen in een vroeg stadium op te sporen. Opsporingsgegevens moeten worden omgezet in voor uitvoering vatbare inlichtingen die zowel voor cyberbeveiliging als voor cyberdefensie kunnen dienen. Zo'n samenwerking tussen de cybergemeenschappen op defensie- en civiel gebied vormt de basis voor een beter gemeenschappelijk situationeel bewustzijn in cyberspace en is evenzeer cruciaal voor een gecoördineerde crisisrespons op zowel technisch als operationeel niveau.

Het gewapende conflict in Oekraïne heeft ook aangetoond hoe waardevol nauwe samenwerking met de particuliere sector is en hoezeer het noodzakelijk is toegang te hebben tot particuliere betrouwbare aanbieders die als cyberreserves optreden om de respons op grote cyberaanvallen te verbeteren. Daarom moet erop worden toegezien dat de lidstaten kunnen

rekenen op de steun van betrouwbare cyberreserves, en dat een en ander op een veilige en gecoördineerde manier gebeurt.

Deze gezamenlijke mededeling bouwt voort op het EU-beleidskader voor cyberdefensie[1] en stelt een ambitieuze strategie voor die de EU en haar lidstaten in staat moet stellen in cyberspace zelfverzekerd en assertief op te treden. Doel is de cyberdefensievermogens te vergroten door middel van individueel of gezamenlijk optreden van de lidstaten, en de coördinatie en de samenwerking tussen de cybergemeenschappen in de EU te versterken. Er zal ook voor worden gezorgd dat de EU op het gebied van kritieke cybertechnologieën strategisch minder afhankelijk wordt en dat de Europese technologische en industriële defensiebasis (EDTIB) wordt versterkt. Het beleid zal de spelregels van de EU bepalen en manieren voorstellen om de solidariteit, die het hart van de EU vormt op het gebied van cyberdefensie, te versterken en in samenwerking met de particuliere sector de respons op grote cyberaanvallen te verbeteren. Gezien de transnationale aard van cyberdreigingen zullen wederzijds voordelige en op maat gesneden partnerschappen op het gebied van cyberdefensie worden ontwikkeld, onder meer voor capaciteitsopbouw op het gebied van cyberdefensie, en zal de cyberweerbaarheid van de partnerlanden worden versterkt.

Zoals voorgesteld in het strategische kompas voor veiligheid en defensie[2], dat de Raad in maart 2022 heeft aangenomen, zal het huidige beleid inzake cyberdefensie het vermogen versterken om op de EU en haar lidstaten gerichte cyberaanvallen te voorkomen, deze op te sporen, zich ertegen te verdedigen, ervan te herstellen en dergelijke aanvallen te ontmoedigen, met gebruikmaking van alle beschikbare middelen. Dit is in overeenstemming met de digitale prioriteiten van de Commissie, de ambitie van de EU-strategie inzake cyberbeveiliging van 2020[3], de aankondiging van voorzitter Von der Leyen in haar toespraak over de Staat van de Unie 2021[4] en de conclusies van de Raad over de ontwikkeling van de cyberstrategie van de Europese Unie[5] van 23 mei 2022. In de gezamenlijke mededeling van 2022 over lacunes op het gebied van defensie-investeringen[6] werden de EU en haar lidstaten ook aangemoedigd om te werken aan een cyberdefensievermogen dat het hele spectrum bestrijkt (van onderzoek, opsporing en bescherming tot respons).

II. EU-CYBERDEFENSIE OM CYBERAANVALLEN OP TE SPOREN, TE BESTRIJDEN EN ONS ERTEGEN TE BESCHERMEN EN VERDEDIGEN

1. Samen werken aan een sterkere cyberdefensie

Cyberaanvallen zijn vaak grensoverschrijdend van aard en kunnen fysieke gevolgen hebben voor kritieke infrastructuur in de EU. Significante cyberincidenten kunnen zodanig verstorend werken dat een of enkele getroffen lidstaten er niet zelfstandig tegen kunnen optreden. Zulke

[1] EU-beleidskader voor cyberdefensie (CDPF) (bijgewerkt in 2018), 19 november 2018, https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/nl/pdf
[2] Een strategisch kompas voor veiligheid en defensie – Voor een Europese Unie die haar burgers, waarden en belangen beschermt en bijdraagt aan de internationale vrede en veiligheid
[3] EU-strategie inzake cyberbeveiliging voor het digitale decennium, JOIN/2020/18 final.
[4] https://ec.europa.eu/commission/presscorner/detail/nl/SPEECH_21_4701
[5] Document 9364/22
[6] JOIN(2022) 24 final

incidenten kunnen onderdeel zijn van grootschaligere hybride aanvallen vanuit derde landen, bedoeld om de economie en de samenleving te destabiliseren, kritieke infrastructuur voor de veiligheid van de EU te verzwakken en het functioneren van de democratie te ondermijnen en te verstoren, onder meer door aanvallen op verkiezingsinfrastructuur.

De EU heeft in 2018 cyberspace aangemerkt als een domein van militaire operaties. In het in 2021 aangenomen document over militaire visie en strategie inzake cyberspace als een domein van operaties[7] worden de randvoorwaarden vastgesteld en worden de doelen, manieren en middelen beschreven die nodig zijn om cyberspace te benutten als operationeel domein ter ondersteuning van operaties in het kader van het gemeenschappelijk veiligheids- en defensiebeleid (GVDB) van de EU. Cyberdefensie en de inzet van daarmee verband houdende vermogens over het volledige spectrum van militaire cyberspaceoperaties zijn een nationaal prerogatief van de lidstaten. Zij steunen echter op een breder ecosysteem, met inbegrip van een sterke industriële basis die wordt ondersteund door vermogensontwikkeling op EU-niveau.

De cyberdefensiegemeenschap van de EU, die bestaat uit de defensieautoriteiten van de lidstaten en ondersteund wordt door EU-instellingen, -organen en -agentschappen (EU-IOA's), heeft bepaalde specifieke kenmerken in vergelijking met de andere cybergemeenschappen[8] en gebruikt een ander governancemodel. Het ontbreken van een vast kader voor informatie-uitwisseling en samenwerking tussen de militaire computercrisisteams van de EU (milCERT's), onder meer ter ondersteuning van militaire GVDB-missies en -operaties, is een probleem, gezien de toegenomen cyberdreigingen die van zowel overheids- als niet-overheidsactoren uitgaan.

Samenwerking tussen cybergemeenschappen op civiel, diplomatiek en rechtshandhavingsgebied en hun evenknieën op defensiegebied zal voor alle betrokken actoren een grote toegevoegde waarde opleveren. Het is daarom cruciaal dat we een dergelijke samenwerking mogelijk maken door te voorzien in geschikte en veilige middelen voor informatie-uitwisseling en door deel te nemen aan oefeningen en andere activiteiten die bevorderlijk zijn voor vertrouwen en gemeenschappelijk begrip.

Bovendien verlenen de lidstaten elkaar momenteel slechts in beperkte mate wederzijdse operationele bijstand. Verdere uitbreiding van het concept van snellereactieteams op cybergebied in de hele EU moet worden geëxploreerd. Daarbij moeten we voortbouwen op het aanverwante project voor snellereactieteams bij cyberincidenten en wederzijdse bijstand op het gebied van cyberbeveiliging (CRRT)[9] in het kader van de permanente gestructureerde samenwerking (Pesco), onder meer in de context van artikel 42, lid 7, (clausule inzake wederzijdse bijstand) van het Verdrag betreffende de Europese Unie (VEU)[10] en artikel 222 (solidariteitsclausule) van het Verdrag betreffende de werking van de Europese Unie (VWEU)[11]. Een van de lessen die uit de succesvolle Oekraïense cyberdefensie in de context van de Russische aanvalsoorlog zijn getrokken, is dat de particuliere sector een beslissende rol

[7] European Union Military Vision and Strategy on Cyberspace as a Domain of Operations, EEAS(2021) 706 REV4

[8] Cybergemeenschappen op civiel, diplomatiek en rechtshandhavingsgebied.

[9] Cyber Rapid Response Teams and Mutual Assistance in Cyber Security.

[10] Verdrag betreffende de Europese Unie, geconsolideerde versie: Publicatieblad C 326 van 26.2.2006, blz. 1.

[11] Verdrag betreffende de werking van de Europese Unie, geconsolideerde versie: Publicatieblad C 326 van 26.2.2006, blz. 1.

speelt. Daarom moet worden onderzocht in welke mate de particuliere sector ook kan bijdragen tot een betere cyberrespons.

1.1. Versterking van het gemeenschappelijke situationeel bewustzijn en coördinatie binnen de defensiegemeenschap

Gezien de omvang van het risico van cyberaanvallen moeten de lidstaten beschikken over een zo volledig mogelijk collectief situationeel bewustzijn, met inbegrip van capaciteit voor vroegtijdige opsporing, en de middelen om adequaat te reageren en de situatie op solidaire en gecoördineerde wijze te herstellen.

Wat het militair situationeel bewustzijn betreft, moet een **EU-coördinatiecentrum voor cyberdefensie (EUCDCC)** worden opgezet ter ondersteuning van een versterkt situationeel bewustzijn binnen de defensiegemeenschap, waaronder alle militaire GVDB-commandanten in de EU. De hoge vertegenwoordiger zal aan de lidstaten het voorstel voor het EUCDCC voorleggen, dat voortbouwt op het Pesco-project voor het coördinatiecentrum voor het cyber- en informatiedomein (CIDCC)[12]. Doel is een holistische analyse te maken van cyberspace, de elektromagnetische omgeving en het cognitieve domein door verschillende informatiebronnen bijeen te brengen op militair strategisch en operationeel niveau. In het kader van de gezamenlijke capaciteit op het gebied van inlichtingenanalyse moeten passende koppelingen worden gemaakt tussen het EUCDCC en het Inlichtingen- en situatiecentrum van de EU (EU Intcen) alsook het directoraat inlichtingen van de militaire staf van de EU. Als aanvulling op de externe informatiebronnen zou het EUCDCC een onafhankelijk actief informatietechnologiesensorsysteem moeten opzetten en integreren om beter toezicht te kunnen houden op door de EU beheerde knooppunten ter ondersteuning van militaire GVDB-missies en -operaties. Het EUCDCC zal zorgen voor versterkte opsporingsvermogens en een nieuwe informatielaag creëren ter verdere verbetering van de informatiebasis voor cyberrisicobeoordeling en situationeel bewustzijn.

Daarvoor zijn vermogens nodig die instelling en onderhoud mogelijk maken van een beeld van cyberspace dat 24/7 operationeel is en waar mogelijk wordt erkend, met inbegrip van de lopende en op handen zijnde cyberoperaties van zowel tegenstanders als bevriende krachten. Zo'n beeld zou bijdragen tot de planning en uitvoering van militaire GVDB-missies en -operaties van de EU. Het EUCDCC moet derhalve de militaire bijdrage gaan leveren die de EU bewuster maakt van kwaadwillige acties in cyberspace en haar in staat stelt daarop beter te reageren.

Om het vertrouwen te versterken en betrouwbare en tijdige strategische informatie over grote cyberincidenten uit te wisselen, zal de **EU-conferentie van cybercommandanten** verder worden ontwikkeld en versterkt[13]. De conferentie zal ten minste tweemaal per jaar bijeenkomen om operationele en andere relevante onderwerpen te bespreken, met deelname van de militaire staf van de EU. Het Europees Defensieagentschap (EDA) treedt op als secretariaat.

[12] Het doel van het project is het ontwikkelen, oprichten en exploiteren van een multinationaal coördinatiecentrum voor het cyber- en informatiedomein (CIDCC) als permanente multinationale militaire component.

[13] Naar aanleiding van de eerste twee bijeenkomsten van de strategische EU-conferentie van cybercommandanten (CyberCo) in januari en juni 2022 hebben de EU-cybercommandanten besloten op hun niveau een meer permanent forum op te zetten.

Er zal een operationeel netwerk voor **milCERT's (MICNET)** worden opgezet, ondersteund door het EDA. Alle lidstaten worden opgeroepen deel te nemen aan MICNET, dat naar verwachting in januari 2023 operationeel zal zijn.

MICNET faciliteert de uitwisseling van informatie tussen milCERT's en zal zo een robuustere en beter gecoördineerde respons op cyberdreigingen ten aanzien van defensiesystemen in de EU bevorderen, waaronder ook systemen die worden gebruikt bij militaire GVDB-missies en -operaties. MICNET zal het ook mogelijk maken dat de opleidingsprocessen en de continue vaststelling van nieuwe eisen voor de milCERT-gemeenschappen worden voortgezet. De komende vier jaar zal het EDA samen met de lidstaten een infrastructuur en bijbehorende instrumenten en procedures ontwikkelen ter ondersteuning van de informatie-uitwisseling tussen milCERT's. MICNET zal ook het kader bieden voor een jaarlijkse oefening waarmee nieuwe vereisten en oplossingen zullen worden getest, gevalideerd en geïdentificeerd.

1.2. Betere coördinatie met civiele gemeenschappen

MICNET moet dienen als kader en infrastructuur voor de uitwisseling van informatie tussen de verschillende niveaus binnen de cyberdefensiegemeenschap en met externe belanghebbenden.

Naarmate MICNET verder wordt ontwikkeld, zal het EDA de lidstaten ondersteunen bij het verkennen van de mogelijkheden voor samenwerking met het netwerk van Computer Security Incident Response Teams (CSIRT), dat nationale CSIRT's en het computercrisisresponsteam van de EU-IOA's (CERT-EU) samenbrengt. Deze samenwerking kan inhouden dat gezamenlijke bijeenkomsten en oefeningen worden georganiseerd. Ook moet de betrokkenheid van de particuliere sector bij relevante inspanningen op het gebied van informatie-uitwisseling en respons op incidenten worden onderzocht.

Om efficiënter cybercrisisbeheer mogelijk te maken, zal de EU-conferentie van cybercommandanten samenwerken met het EU-netwerk van verbindingsorganisaties voor cybercrises (CyCLONe), in het kader waarvan de lidstaten en de Commissie samen de coördinatie en het beheer van grootschalige cyberincidenten in de EU ondersteunen. Deze aanpak zal militaire ervaring en civiel situationeel bewustzijn op strategisch en operationeel niveau combineren.

Aangezien het EUCDCC moet fungeren als centraal knooppunt voor het verzamelen, analyseren, beoordelen en eindelijk verspreiden van informatie over cyberdefensie, met name voor militaire GVDB-missies en -operaties, zou het ook kunnen worden gekoppeld aan de interinstitutionele taskforce voor cybercrises[14], die is opgericht om geïnformeerde besluitvorming en een gecoördineerde respons van de EU-IOA's op grote cybercrises op strategisch en operationeel niveau te waarborgen.

Om analyses en doeltreffendere ondersteuning van crisisbeheer te bieden, kan het EUCDCC ook relevante informatie uitwisselen met een cybersituatie- en -analysecentrum dat bij de Commissie wordt opgericht, met de steun van het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) en CERT-EU.

[14] Een informele groep van betrokken diensten van de Commissie, de EDEO, het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), CERT-EU en Europol, die door de Commissie en de hoge vertegenwoordiger gezamenlijk wordt voorgezeten.

Het ontbreken van door de meeste betrokkenen gedeelde of interoperabele beveiligde communicatie-instrumenten en -platforms tussen de lidstaten en de relevante EU-IOA's is nog steeds een belangrijk obstakel. De Commissie en de betrokken instellingen inventariseren momenteel de bestaande instrumenten voor veilige communicatie op cybergebied. Op basis van deze inventarisatie van de bestaande instrumenten zal de Commissie eind 2022 aanbevelingen aan de Raad voorleggen om tot overeenstemming te komen over verdere maatregelen.

EU-cybersolidariteit voor meer gemeenschappelijke detectie en een beter situationeel bewustzijn

Met civiele ondersteuningsacties kan het gemeenschappelijk situationeel bewustzijn verder worden versterkt. De cyberdefensiegemeenschap zal baat hebben bij sterkere vermogens op het gebied van civiele detectie en situationeel bewustzijn die voor de bescherming van kritieke infrastructuur in de EU worden ontwikkeld. Daarom bereidt de Commissie een initiatief voor ter bevordering van de uitrol van een EU-infrastructuur voor operationele beveiligingscentra (SOC's), waarvan een eerste fase de komende weken van start zal gaan en vervolgens zou kunnen worden uitgebreid en op grotere schaal uitgerold[15]. Uiteindelijk moet die infrastructuur bestaan uit verschillende SOC-platforms, waarvan elk een aantal nationale SOC's samenbrengt. Het programma Digitaal Europa (DEP)[16] verleent steun ter aanvulling van de nationale financiering. Wetswijzigingen in het kader van het programma Digitaal Europa zouden op langere termijn mogelijk maken dat financiële steun wordt verleend voor gezamenlijke aanbestedingen van ultrabeveiligde instrumenten en infrastructuur van de volgende generatie. Daardoor zou de geplande SOC-infrastructuur van de EU kunnen zorgen voor verbetering van de collectieve detectiecapaciteit door gebruik te maken van de meest geavanceerde artificiële intelligentie (AI) en gegevensanalyse, ook met betrekking tot civiele communicatienetwerken. Dankzij deze geavanceerde methode voor bruikbare inlichtingen op het gebied van cyberdreigingen kunnen instanties en betrokken entiteiten tijdig worden gewaarschuwd, zodat zij ernstige incidenten kunnen detecteren en doeltreffend kunnen aanpakken. De omvang en de reikwijdte van de infrastructuur zullen afhangen van de financiering die op nationaal niveau en door de EU kan worden geboden, en die afhankelijk is van het beschikbare budget in het kader van het meerjarig financieel kader.

Dergelijke meerlanden-SOC's zouden ook de deelname van defensie-entiteiten mogelijk kunnen maken. Daarvoor zou dan een "defensiepijler" moeten worden opgezet om aspecten te regelen zoals de bestuursvorm en het soort gedeelde informatie. Deze "defensiepijler" zou in samenwerking met de hoge vertegenwoordiger worden ontwikkeld en zou een specifiek mechanisme kunnen omvatten voor de uitwisseling van informatie met militaire actoren, waaronder het EUCDCC, waarvoor dan beveiligingsnormen op defensieniveau zouden kunnen worden ontwikkeld.

[15] De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk (JOIN(2020) 18 final) en de EU-strategie voor de veiligheidsunie (COM(2020) 605).

[16] Verordening (EU) 2021/694 van het Europees Parlement en de Raad van 29 april 2021 tot oprichting van het programma Digitaal Europa en tot intrekking van Besluit (EU) 2015/2240 (PB L 166 van 11.5.2021, blz. 1, wordt mogelijk gewijzigd).

EU-cybersolidariteit op het gebied van paraatheid, respons en herstel

Significante cyberincidenten kunnen vaak dusdanig verstorend werken dat een of meer getroffen lidstaten er niet zelfstandig tegen kunnen optreden. In dergelijke gevallen moeten de lidstaten een beroep kunnen doen op wederzijdse bijstand en solidariteit, onder meer in het kader van artikel 42, lid 7, VEU en artikel 222 VWEU. De hoge vertegenwoordiger zal samen met de Commissie en de lidstaten onderzoeken welke mogelijkheden er zijn om het **concept van snellereactieteams bij cyberincidenten (CRRT) uit te breiden** op basis van het aanverwante CRRT-project in het kader van Pesco, zodat de EU-lidstaten en GVDB-missies en -operaties betere ondersteuning kan worden geboden. Die teams zouden tot taak hebben om op verzoek, afhankelijk van de specifieke behoeften, op korte termijn op maat gesneden en gerichte bijstand te verlenen. Voor zover relevant kan er ook in worden voorzien dat betrouwbare particuliere partners voor efficiënte respons- en herstelmaatregelen zorgen.

In het kader van het EU-initiatief voor cybersolidariteit bereidt de Commissie maatregelen voor om de paraatheids- en responsacties in de hele EU te versterken. Dit houdt in dat **essentiële entiteiten die kritieke infrastructuur exploiteren, worden getest op potentiële kwetsbaarheden op basis van EU-risicobeoordelingen** – waarbij wordt voortgebouwd op maatregelen die de Commissie al samen met Enisa heeft geïnitieerd – en dat responsmaatregelen worden genomen om de impact van ernstige incidenten te beperken, onmiddellijk herstel te ondersteunen en/of de werking van essentiële diensten te herstellen[17].

Het EU-initiatief voor cybersolidariteit zou steun kunnen bieden voor de **geleidelijke totstandbrenging van een cyberreserve op EU-niveau met diensten van betrouwbare particuliere aanbieders**, die op verzoek van de lidstaten in actie zou kunnen komen bij ernstige grensoverschrijdende incidenten. Om ervoor te zorgen dat de steun uit de cyberreserve op EU-niveau wordt verleend waar die nodig is en een aanvulling vormt op andere mogelijke vormen van bijstand, moeten de taken en verantwoordelijkheden duidelijk worden omschreven en volledig worden gecoördineerd met de bestaande instanties. De reikwijdte van de maatregelen en de toewijzing van de kosten van specifieke interventies zijn afhankelijk van de beschikbare EU-financiering, maar de EU zou ook meerwaarde kunnen bieden door ervoor te zorgen dat een dergelijke reserve op EU-niveau beschikbaar is en klaar staat. Om een hoog niveau van vertrouwen te waarborgen, zal de Commissie ook de mogelijkheden overwegen om steun te bieden voor de ontwikkeling van certificeringsregelingen voor cyberbeveiliging voor dergelijke particuliere cyberbeveiligingsbedrijven.

Oefeningen zijn een essentieel onderdeel van de opbouw van paraatheid. Zij bevorderen de ontwikkeling van een gemeenschappelijke kennisbasis en een gemeenschappelijk inzicht in cyberdefensie, waardoor de operationele paraatheid wordt versterkt. Gemeenschappelijke cyberdefensieoefeningen bevorderen ook de interoperabiliteit en het vertrouwen tussen belanghebbenden, onder meer ter ondersteuning van militaire GVDB-missies en -operaties. Voortbouwend op CYBER PHALANX[18] en de oefeningen in het kader van milCERT zal **het EDA een nieuw project opzetten, CyDef-X, dat alle lidstaten samenbrengt en dat als kader zal dienen voor EU-oefeningen op het gebied van cyberdefensie**. Dit project kan ook

[17] Oproep van Nevers om de cyberbeveiligingsvermogens van de EU te versterken.
[18] https://eda.europa.eu/publications-and-data/factsheets/factsheet-cyber-phalanx

zijn nut hebben voor het testen van wederzijdse bijstand uit hoofde van artikel 42, lid 7, VEU. Het gebruik van specifieke omgevingen voor testen, opleidingen en oefenomgevingen op het gebied van cyberdefensie (bv. de Cyber Ranges Federation) moet ook worden onderzocht, onder meer door gebruik te maken van het Pesco-project op dat gebied[19].

Oefeningen kunnen ook een belangrijke rol spelen om de samenwerking tussen civiele en militaire entiteiten te verbeteren. Bij het organiseren van oefeningen moeten Enisa, EDA en andere relevante entiteiten daarom altijd overwegen deelnemers uit andere cybergemeenschappen erbij te betrekken.

In het kader van de versterking van de capaciteit van de EU om cyberaanvallen te voorkomen, af te wenden en erop te reageren, en in overeenstemming met de EU-strategie inzake cyberbeveiliging van 2020 en het strategisch kompas, zal de hoge vertegenwoordiger in 2023 opties voorstellen om het EU-instrumentarium voor cyberdiplomatie[20] verder te versterken op basis van de onderdelen van de cyberstrategie van de EU en de lessen die zijn getrokken uit de uitvoering van het instrumentarium sinds de vaststelling ervan.

Maatregelen op het gebied van cyberdefensie

- Een EU-coördinatiecentrum voor cyberdefensie opzetten als centrum voor een gemeenschappelijk militair situationeel bewustzijn, en de mogelijkheden onderzoeken voor samenwerking met het situatie- en analysecentrum van de Commissie.
- De EU-conferentie van EU-cybercommandanten verder ontwikkelen en versterken.
- De lidstaten aanmoedigen actief deel te nemen aan MICNET, het netwerk van militaire CERT's, en streven naar samenwerking met het civiele CSIRT-netwerk.
- Een nieuw kaderproject CyDef-X ontwikkelen ter ondersteuning van cyberdefensieoefeningen in EU-verband.
- De mogelijkheden verkennen om het concept van snellereactieteams bij cyberincidenten verder te ontwikkelen op basis van het CRRT-project in het kader van Pesco.
- De mogelijkheden verkennen voor de verdere ontwikkeling van projecten op het gebied van Cyber Ranges Federation.

Civiele ondersteunende maatregelen

- Een EU-initiatief voor cybersolidariteit opzetten, met inbegrip van mogelijke wetgeving tot wijziging van het programma Digitaal Europa:
    - ter versterking van de gemeenschappelijke vermogens van de EU op het gebied van opsporing, situationeel bewustzijn en respons;
    - met het oog op de geleidelijke totstandkoming van een EU-cyberreserve met diensten van betrouwbare particuliere aanbieders;
    - ter ondersteuning van het testen van kritieke entiteiten op potentiële kwetsbaarheden op basis van EU-risicobeoordelingen.

[19] https://www.pesco.europa.eu/project/cyber-ranges-federations-crf/

[20] Conclusies van de Raad over een kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten ("Instrumentarium voor cyberdiplomatie").

- De mogelijkheden onderzoeken voor de ontwikkeling van regelingen voor cyberbeveiligingscertificering op EU-niveau, gericht op de cyberbeveiligingssector en particuliere ondernemingen.
- De samenwerking op strategisch, operationeel en technisch niveau tussen de cyberdefensiegemeenschap en andere cybergemeenschappen versterken.

2. Het defensie-ecosysteem van de EU beveiligen

De afgelopen jaren is het aantal cyberaanvallen drastisch toegenomen, waaronder ook aanvallen op de toeleveringsketen met als doel cyberspionage, ransomware of verstoring. In 2020 werden bv. wereldwijd meer dan 18 000 organisaties, waaronder overheidsinstanties, grote bedrijven en defensiebedrijven, getroffen door SolarWinds[21]. De exploitatie van een kwetsbaarheid in de Log4J-software van Apache[22] heeft duidelijk gemaakt dat ook softwarecomponenten die niet als zeer risicovol of kritiek worden beschouwd, als wapen kunnen worden gebruikt om in de EU succesvolle aanvallen uit te voeren op grote bedrijven of overheden, ook op defensiegebied. Dit toont duidelijk aan dat moet worden gewerkt aan verdere versterking van de cyberweerbaarheid van entiteiten die actief zijn in het defensie-ecosysteem van de EU, met inbegrip van militaire entiteiten, de defensie-industrie en particuliere actoren.

De strijdkrachten zijn voor hun mobiliteit, communicatie en energie in hoge mate afhankelijk van kritieke civiele infrastructuur. De Russische aanval op het KA-SAT-satellietnetwerk[23], waardoor de communicatie van verschillende overheidsinstanties en de Oekraïense strijdkrachten werd verstoord, is een voorbeeld van een dergelijke afhankelijkheidsrelatie. Dergelijke kritieke infrastructuur moet derhalve worden beveiligd.

Om problemen in verband met de beveiliging van hun communicatie- en informatiesystemen aan te pakken, ontwikkelen de lidstaten hun eigen beveiligingsnormen en -eisen voor militaire systemen. Daarbij wordt niet altijd rekening gehouden met de noodzaak van interoperabiliteit, noch met het bestaan van civiele normen voor producten voor tweeërlei gebruik. Dit heeft negatieve gevolgen voor het vermogen van de lidstaten om gezamenlijk op te treden in cyberspace, ook in de context van militaire GVDB-missies en -operaties, en vormt belemmeringen voor de verlening van wederzijdse bijstand. Daarnaast moet ook worden gestreefd naar sterkere synergie tussen militaire en civiele normalisatietrajecten, aangezien de verplichting om voor civiele en militaire afnemers vergelijkbare, maar verschillende normen te hanteren leidt tot hogere productiekosten voor de ontwikkeling van producten voor tweeërlei gebruik door de industrie.

[21] https://cybernews.com/security/solarwinds-hack-the-mystery-of-one-of-the-biggest-cyberattacks-ever/
[22] https://www.ncsc.nl/onderwerpen/log4j
[23] Verklaring van de hoge vertegenwoordiger namens de Europese Unie over kwaadwillige cyberactiviteiten van hackers en hackersgroepen in de context van de Russische agressie tegen Oekraïne: https://www.consilium.europa.eu/nl/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/

2.1. Versterking van de cyberweerbaarheid van het defensie-ecosysteem

Om de cyberweerbaarheid van het defensie-ecosysteem te versterken, zijn gerichte maatregelen en investeringen nodig van een grote verscheidenheid aan entiteiten, van de militaire infrastructuur van de lidstaten en GVDB-missies en -operaties tot kritieke infrastructuur, de defensie-industrie en relevante onderzoeksorganisaties.

Informatie die noodzakelijk is voor een geïnformeerde besluitvorming moet worden beschermd, willen GVDB-missies en -operaties succes hebben. De EU en haar lidstaten moeten hun militaire commando- en controlestructuren verder versterken en hun infrastructuur verder ontwikkelen en beveiligen. Dat geldt ook voor het politiek-militair overleg in de vroege stadia van crisisbeheer met het oog op de effectieve inzet van het operationeel hoofdkwartier, met inbegrip van het militair plannings- en uitvoeringsvermogen (MPCC). Aan dit punt zal met name aandacht worden geschonken in het kader van de verdere ontwikkeling van het operationele wide area network van de EU.

In het kader van militaire missies en operaties gebruiken cyberdefensieactoren informatie in allerlei vormen en classificaties, afkomstig uit allerlei bronnen. De toepassing van beveiligde geavanceerde technologie, zoals AI, met steun van de industrie, is dan ook van het allergrootste belang.

De beveiliging van de infrastructuur van communicatie- en informatiesystemen moet worden verbeterd door onderling overeengekomen managementprocedures toe te passen en daardoor het vertrouwen onder belanghebbenden in de integriteit van de beschikbare informatie te bevorderen. Bovendien zal de hoge vertegenwoordiger, ook als hoofd van het EDA, met de steun van de Commissie de lidstaten bijstaan bij de ontwikkeling van **niet-juridisch bindende aanbevelingen voor de defensiegemeenschap, geïnspireerd op de richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS2)**[24] (defensie is namelijk van het toepassingsgebied van de richtlijn uitgesloten). Hiermee wordt bijgedragen tot een grotere algehele maturiteit op het gebied van cyberdefensie.

Het voorstel van de Commissie voor een verordening betreffende cyberweerbaarheid[25], die tot doel heeft vereisten inzake cyberbeveiliging vast te stellen voor producten met digitale elementen, zal ook zorgen voor een verkleining van het aanvalsoppervlak van producten voor tweeërlei gebruik die bijvoorbeeld door de defensie-industrie en overheidsactoren op defensiegebied worden gebruikt in hun communicatie- en informatiesystemen. Volgens het voorstel zouden fabrikanten verplicht zijn kwetsbaarheden die actief worden uitgebuit, binnen 24 uur te melden aan Enisa, dat de betrokken nationale CSIRT's op de hoogte zal brengen. In dit verband zou het ook belangrijk zijn ervoor te zorgen dat de defensiegemeenschap snel wordt geïnformeerd over kwetsbaarheden in producten met digitale elementen, en over alle beschikbare en/of reeds toegepaste patches en mitigerende maatregelen.

[24] Richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148. De medewetgevers hebben onlangs overeenstemming bereikt over deze tekst, die naar verwachting eind dit jaar formeel zal worden vastgesteld.

[25] Voorstel voor een verordening betreffende horizontale cyberbeveiligingseisen voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020 (COM(2022) 454 final).

Met name ook omdat het leger afhankelijk is van kritieke civiele infrastructuur, is het **noodzakelijk dat de bescherming van kritieke infrastructuur tegen grootschalige cyberaanvallen verder wordt verbeterd**. Op verzoek van de Raad[26] ontwikkelen de Commissie, de hoge vertegenwoordiger en de NIS-samenwerkingsgroep[27] risicoscenario's voor de beveiliging van digitale infrastructuur. Daarbij zal de nadruk in eerste instantie liggen op cyberbeveiliging in de sectoren energie, telecommunicatie, vervoer en ruimtevaart. Daarnaast zullen ook gerichte cyberbeveiligingsrisicobeoordelingen worden opgesteld voor communicatie-infrastructuur en -netwerken in de EU (met inbegrip van vaste en mobiele infrastructuur, satellieten, onderzeese kabels en internetrouting)[28]. Ten aanzien van de bescherming van kritieke infrastructuur tegen door de mens veroorzaakte dreigingen, waaronder hybride dreigingen, worden de lidstaten in het voorstel voor een aanbeveling van de Raad betreffende een gecoördineerde aanpak van de Unie om de veerkracht van kritieke infrastructuur te versterken[29] er onder meer toe opgeroepen te zorgen voor passende stresstests en crisiscoördinatie. De kritieke maritieme infrastructuur, met inbegrip van de bescherming van onderzeese gegevenskabels, zal verder worden behandeld in het kader van de komende herziening van de EU-strategie voor maritieme veiligheid en het bijbehorende actieplan. Verdere maatregelen ter versterking van de cyberbeveiliging van kritieke infrastructuur in het energiesysteem zijn opgenomen in het EU-actieplan voor de digitalisering van het energiesysteem[30].

Vanuit de ruimte opererende diensten zijn voor defensie steeds belangrijker, of het nu gaat om surveillance, situationeel bewustzijn, nauwkeurige positionering of ultrabeveiligde communicatie. Het betreft hier dan ook belangrijke strategische troeven voor technologische soevereiniteit. Verstoring van diensten die vanuit de ruimte opereren, kan grote gevolgen hebben voor defensiesystemen, maar ook voor de samenleving en de economie in het algemeen. De weerbaarheid van dergelijke diensten is cruciaal voor de algehele weerbaarheid van cyberdefensie, aangezien zij het doelwit kunnen zijn van kwaadwillige aanvallen. Zoals blijkt uit de aanvallen op de KA-SAT-netwerken, worden in de ruimte gestationeerde systemen in toenemende mate blootgesteld aan cyberdreigingen die van invloed kunnen zijn op de beschikbaarheid of continuïteit van diensten die vanuit de ruimte opereren. Dit brengt een risico met zich mee voor de strategische en veiligheidsbelangen van de EU in het ruimtedomein, alsook voor de ruimtevermogens die cyberdefensie mogelijk maken en ondersteunen. De in het strategisch kompas[31] aangekondigde EU-ruimtestrategie voor veiligheid en defensie zal maatregelen bevatten om de robuustheid en cyberweerbaarheid van ruimtevaartinfrastructuren en aanverwante diensten te verbeteren en dreigingen voor gevoelige ruimtesystemen en -diensten in de EU af te wenden en te beantwoorden, waarbij met name op cyberdreigingen wordt ingegaan.

---

[26] Conclusies van de Raad over de ontwikkeling van de cyberstrategie van de Europese Unie (ST09364/22 van 23 mei 2022).

[27] https://digital-strategy.ec.europa.eu/nl/policies/nis-cooperation-group

[28] Oproep van Nevers om de cyberbeveiligingsvermogens van de EU te versterken.

[29] Voorstel voor een aanbeveling van de Raad betreffende een gecoördineerde aanpak van de Unie om de veerkracht van kritieke infrastructuur te versterken (COM(2022) 551 final).

[30] Digitalisering van het energiesysteem – EU-actieplan (COM(2022) 552 final).

[31] Een strategisch kompas voor veiligheid en defensie, 21 maart 2022: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/nl/pdf

De Commissie roept de lidstaten ook op om dringend werk te maken van de uitvoering van de maatregelen die worden aanbevolen in de EU-toolbox voor cyberbeveiliging van 5G[32]. Lidstaten die nog geen beperkingen ten aanzien van leveranciers met een hoog risico hebben ingevoerd, zouden dit onverwijld moeten doen, aangezien elke vertraging de netwerken in de EU kwetsbaarder kan maken. Dergelijke risico's kunnen relevant zijn voor militaire middelen en gevolgen hebben voor de algemene defensieomgeving van de lidstaten.

Wat de **cyberweerbaarheid van de Europese defensie-industrie en van de onderzoeks- en ontwikkelingsentiteiten op defensiegebied** betreft: op deze entiteiten is de NIS 2-richtlijn van toepassing, tenzij de lidstaten dat uitdrukkelijk hebben uitgesloten. Dit vereist dat die entiteiten beschikken over een programma voor cyberbeveiligingsrisicobeheer dat zowel de beveiliging van de toeleveringsketen als de melding van incidenten omvat. Aangezien in het defensie-ecosysteem de particuliere sector een grote rol speelt bij de verlening van cyberbeveiligingsdiensten, moeten de lidstaten bovendien gebruikmaken van regelingen voor cyberbeveiligingscertificering. Een **EU-certificeringsregeling voor cyberbeveiliging voor bedrijven die diensten verlenen aan de defensie-industrie** kan bijdragen tot een geharmoniseerd niveau van vertrouwen op de markt, waarbij kan worden voortgebouwd op de ervaring van Enisa.

2.2. Interoperabiliteit op het gebied van cyberdefensie en samenhangende normen in de EU

Interoperabiliteit en gemeenschappelijkheid zijn belangrijke vereisten die vanaf de ontwerpfase van cyberdefensievermogens in overweging moeten worden genomen. Daarbij moet ook rekening worden gehouden met de lessen die zijn getrokken uit lopende missies en operaties, zoals onder leiding van de militaire staf van de EU en met de steun van het EDA vastgesteld. De beginselen, processen en normen die in het kader van Federated Mission Networking (FMN)[33] zijn overeengekomen, moeten de leidraad vormen voor de ontwikkeling van nationale cyberdefensievermogens, teneinde de interoperabiliteit ervan te waarborgen.

De samenwerking kan worden gefaciliteerd door harmonisatie van de vereisten die voor cyberdefensievermogens van de volgende generatie gelden. Die harmonisatie kan leiden tot gezamenlijke ontwikkelings- en aankoopinitiatieven en geïntegreerde levenscyclusondersteuning. Het EDA en de militaire staf van de EU zullen daarom **aanbevelingen opstellen voor een aantal interoperabiliteitsvereisten op het gebied van cyberdefensie in de EU**. De vereisten moeten bij alle planning in aanmerking worden genomen om normalisatie, een cruciale factor voor interoperabiliteit, in alle aspecten te waarborgen. De test-, evaluatie- en certificeringsvereisten zijn eveneens een cruciale factor.

In het kader van de voorgestelde verordening cyberweerbaarheid[34] zullen geharmoniseerde normen op het gebied van cyberbeveiliging worden ontwikkeld voor hardware- en softwareproducten en -componenten. Die normen zullen gelden voor alle civiele producten en producten voor tweeërlei gebruik die digitale elementen hebben. Daaronder valt een groot deel

[32] Cyberbeveiliging van 5G-netwerken – EU-toolbox met risicobeperkende maatregelen – De digitale toekomst van Europa vormgeven (europa.eu)
[33] https://dnbl.ncia.nato.int/FMNPublic/SitePages/Home.aspx
[34] COM(2022) 454 final.

van de producten die in de defensiesector worden gebruikt. Waar mogelijk zal de Commissie de samenhang met defensiegerelateerde cyberbeveiligingsnormen voor digitale producten aanmoedigen. Zoals uiteengezet in het actieplan voor synergieën tussen de civiele, defensie- en ruimtevaartindustrieën[35] ("actieplan voor synergieën") zal de Commissie in nauwe samenwerking met de belangrijkste belanghebbenden een plan presenteren om de toepassing van bestaande hybride civiele en defensienormen en de ontwikkeling van nieuwe normen te bevorderen. Alle belanghebbenden, met inbegrip van de Europese normalisatieorganisaties, de Noord-Atlantische Verdragsorganisatie (NAVO) en andere partners, moeten hun samenwerking verder ontwikkelen, waarbij zij optimaal gebruik kunnen maken van de diensten van het Europees normalisatiecomité voor defensie. In dezelfde geest moeten militaire normalisatie-instanties, wanneer zij nieuwe cyberbeveiligingsnormen ontwikkelen voor defensieproducten met digitale elementen, de geharmoniseerde normen die in het kader van de verordening cyberweerbaarheid zijn ontwikkeld, als uitgangspunt nemen[36].

Maatregelen op het gebied van cyberdefensie

- De lidstaten ondersteuning bieden bij de ontwikkeling van juridisch niet-bindende aanbevelingen voor de defensiegemeenschap, geïnspireerd op NIS2, teneinde bij te dragen tot een grotere algehele maturiteit op het gebied van cyberdefensie op nationaal niveau.
- Aanbevelingen ontwikkelen met betrekking tot de interoperabiliteitseisen van de EU op het gebied van cyberdefensie.
- De samenwerking met alle relevante actoren op het gebied van defensiegerelateerde normen versterken in het kader van het Europees Comité voor normalisatie op defensiegebied.

Civiele ondersteunende maatregelen

- Risicoscenario's ontwikkelen voor kritieke infrastructuur die van belang is voor militaire communicatie en mobiliteit, met het oog op de gerichte inzet van paraatheidsacties, onder meer door penetratietests.
- De samenwerking tussen civiele en militaire normalisatie-instanties stimuleren met het oog op de ontwikkeling van geharmoniseerde normen voor producten voor tweeërlei gebruik.

3. Investeren in cyberdefensievermogens

De afgelopen jaren zijn de investeringen in cyberdefensie in de EU gegroeid in verband met de toename van kwaadwillige cyberactiviteiten van de kant van zowel overheids- als niet-overheidsactoren. Het is essentieel dat de EU haar cyberdefensievermogens versterkt. Gezien de Russische aanvalsoorlog tegen Oekraïne is er des te meer behoefte aan investeringen om

[35] COM(2021) 70 final.

[36] Er wordt momenteel gewerkt aan normen met betrekking tot de cyberbeveiligingsvoorschriften voor radioapparatuur op basis van Gedelegeerde Verordening (EU) 2022/30. Als de Commissie deze gedelegeerde verordening intrekt, of zodanig wijzigt dat zij niet langer van toepassing is op bepaalde producten die onder de verordening cyberbeveiliging vallen, moeten de Commissie en de Europese normalisatieorganisaties bij het opstellen en ontwikkelen van geharmoniseerde normen ter facilitering van de uitvoering van de verordening cyberbeveiliging rekening houden met de normalisatiewerkzaamheden die zijn verricht in het kader van Uitvoeringsbesluit C(2022) 5637 van de Commissie betreffende een normalisatieverzoek ter ondersteuning van genoemde gedelegeerde verordening.

ervoor te zorgen dat de lidstaten kunnen beschikken over geavanceerde cyberdefensievermogens, zowel stationair als inzetbaar.

Technologische verbeteringen zijn van essentieel belang, willen we onze voorsprong op concurrenten en tegenstanders, die ook zwaar investeren in nieuwe technologieën, in stand kunnen houden. De EU en de lidstaten moeten dan ook de samenwerking en interoperabiliteit op het gebied van cyberdefensie versterken door middel van gezamenlijke vermogensontwikkeling en meer investeringen in onderzoek en ontwikkeling.

Daarnaast moeten kwetsbaarheden die voortvloeien uit strategische afhankelijkheden en de versnippering van de EDTIB[37] worden aangepakt. Vooral vaardigheden en competenties zijn van essentieel belang om de strategische afhankelijkheden op het gebied van cyberbeveiliging en cyberdefensie in Europa te ondervangen. De Europese defensie-industrie moet belangrijke vaardigheden behouden en nieuwe vaardigheden verwerven om in een mondiale context in staat te blijven hightechoplossingen aan te bieden[38]. Ontbreken die vaardigheden, dan heeft dat negatieve gevolgen voor de defensiesector, aangezien de vermogensontwikkeling op alle gebieden daaronder te lijden heeft. Alle acties zullen volledig in overeenstemming zijn met de benadering die is aangekondigd in het actieplan voor synergieën, de routekaart voor kritieke technologieën voor veiligheid en defensie[39] ("de routekaart") en de analyse van de lacunes op het gebied van defensie-investeringen[40].

3.1. Geavanceerde cyberdefensievermogens over het volledige spectrum ontwikkelen

De verantwoordelijkheid en de bevoegdheid voor de inzet van cyberdefensievermogens berusten bij de lidstaten, terwijl de EU een belangrijke rol speelt bij de ondersteuning van de verdere ontwikkeling van specifieke militaire vermogens over het volledige spectrum van doctrine, organisatie, opleiding, materieel, leiderschap, personeel, faciliteiten en interoperabiliteit (DOTMLPF-I) om vrijheid van handelen in cyberspace tot stand te brengen. De aanpak van cyberdefensie moet verder worden geharmoniseerd op alle vermogensdomeinen en moet worden aangepast aan de veranderende geopolitieke omgeving. De ontbrekende elementen in de bestaande vermogens moeten daarom in kaart worden gebracht en de ontwikkeling van nieuwe vermogens moet op gecoördineerde en meetbare wijze worden ondersteund.

De betrokkenheid van de lidstaten bij gezamenlijke ontwikkelingsprojecten op het gebied van cyberdefensie is tot op heden echter ontoereikend en moet worden vergroot om het effect op EU-niveau te maximaliseren. Alle lidstaten moeten meer investeren in gezamenlijke ontwikkeling van cyberdefensievermogens over het volledige spectrum. De lidstaten moeten

[37] Bijvoorbeeld zoals aangegeven in de analyse van de lacunes op het gebied van defensie-investeringen.
[38] Er zijn verschillende initiatieven gelanceerd, waaronder het Europees partnerschap voor defensievaardigheden.
[39] In de routekaart voor kritieke technologieën voor veiligheid en defensie heeft de Commissie opgeroepen tot versterking van de samenwerking op het gebied van technologieën die cruciaal zijn voor de veiligheid en defensie van Europa op de lange termijn en de inspanningen die vereist zijn om de daarmee samenhangende strategische afhankelijkheden te overwinnen.
[40] De gezamenlijke mededeling over de analyse van de lacunes op het gebied van defensie-investeringen en de te volgen koers (JOIN(2022) 24 final), waarin de Commissie en de hoge vertegenwoordiger maatregelen hebben voorgesteld om te waarborgen dat de industrie van de EU op zowel de korte als de lange termijn resultaten kan boeken.

overwegen **een reeks vrijwillige verbintenissen voor de ontwikkeling van nationale cyberdefensievermogens uit te werken**, ook wat betreft multinationale vermogens die verder gaan dan de bestaande cyberdefensieprojecten in het kader van Pesco[41]. In het kader van de gecoördineerde jaarlijkse evaluatie inzake defensie (CARD) kan met de lidstaten een dialoog over de cyberdefensievereisten en de nationale doelstellingen voor de ontwikkeling van cyberdefensievermogens worden opgezet en kan de uitvoering van de verbintenissen worden beoordeeld. De Commissie ondersteunt en cofinanciert via het Europees Defensiefonds (EDF) de ontwikkeling van en het onderzoek naar cyberdefensievermogens over het volledige spectrum, onder meer voor actieve defensievermogens. De Commissie heeft de investeringen in cyberdefensie via het EDF al opgevoerd. Dit moet leiden tot de ontwikkeling van Europese gemeenschappelijke en/of interoperabele instrumenten voor operaties in cyberspace en incidentenbeheer, defensieoperaties en preventieve maatregelen voor informatieoorlogvoering, en tot sterkere weerbaarheid van de communicatie- en informatiesystemen. Het EDF richt zich op gebieden als cybersituationeel bewustzijn, threat hunting in realtime en responsieve operationele vermogens, vermogens voor cyberoperaties en cyberopleidingen en -oefeningen[42]. Om ervoor te zorgen dat de lidstaten in staat zijn gezamenlijke cyberoperaties uit te voeren, zullen de responsieve operationele vermogens en de vermogens voor cyberoperaties de komende jaren in het kader van het EDF worden ondersteund. Tot slot worden de lidstaten aangemoedigd actief deel te nemen aan de diverse samenwerkingskaders en gebruik te maken van alle instrumenten die op EU-niveau zijn opgezet, zoals het projectteam cyberdefensie van het EDA[43].

De lopende herziening van de in 2018 vastgestelde EU-prioriteiten inzake vermogensontwikkeling[44] biedt een goede gelegenheid om geactualiseerde prioriteiten voor coöperatieve en gezamenlijke ontwikkeling vast te stellen, waardoor een versterking van de coöperatieve vermogensontwikkeling mogelijk wordt gemaakt. Bij de herziening van de specifieke prioriteit op het gebied van cyberdefensie moet rekening worden gehouden met de resultaten van de CARD 2022 en met de bevindingen van de in mei 2022 aan de lidstaten voorgelegde analyse van lacunes. Daarna zal de CARD een regelmatig kader bieden om de voortgang van de uitvoering van deze geactualiseerde prioriteit op nationaal niveau te evalueren en nieuwe opties te onderzoeken voor de gezamenlijke ontwikkeling van cyberdefensievermogens met de lidstaten. De geactualiseerde EU-prioriteiten inzake vermogensontwikkeling zullen een belangrijke referentie zijn voor Pesco-projecten op het gebied van cyberdefensie.

In dit verband zal de militaire staf van de EU op basis van een opdracht van het Militair Comité van de EU, in nauwe samenwerking met de lidstaten, zorgen voor de ontwikkeling van het uitvoeringsplan voor cyberoperaties. Daarmee wordt een overzicht gegeven van de stand van

[41] Snellereactieteams bij cyberincidenten en wederzijdse bijstand op het gebied van cyberbeveiliging (CRRT), het coördinatiecentrum voor het cyber- en informatiedomein (CIDCC), het platform voor het delen van informatie over cyberdreigingen en respons op incidenten (CTIRISP), Cyber Ranges Federation (CRF) en de EU-cyberacademie en innovatiehub (EU CAIH).

[42] In het kader van het industrieel ontwikkelingsprogramma voor de Europese defensie (EDIDP) zijn zes projecten gefinancierd (Pandora, Discretion, Cyber4de, Ecysap, Smotanet en Hermes) met een budget van 39 miljoen EUR. In het kader van EDF 2021 zal bijna 40 miljoen EUR worden besteed aan drie samenwerkingsprojecten voor O&O op het gebied van cyberdefensie die voor financiering zijn geselecteerd (Acting, AInception, EU-Guardian).

[43] Het projectteam cyberdefensie biedt de lidstaten een forum om cyberdefensieaangelegenheden met militaire implicaties te bespreken.

[44] CDP-facsheet EDA (28.6.2018): CDP-factsheet

zaken met betrekking tot de uitvoering van de cyberdefensievermogens en worden de lidstaten geholpen om hun inspanningen en activiteiten beter op elkaar af te stemmen. Deze activiteiten zijn gebaseerd op het EU-concept inzake cyberdefensie voor door de EU geleide militaire operaties en missies die aansluiten bij de prioriteiten van het vermogensontwikkelingsplan (CDP).

Versterking van de onderzoeksactiviteiten op het gebied van belangrijke technologieën voor cyberdefensie

Om geavanceerde cyberdefensievermogens in stand te kunnen houden, moet gelijke tred worden gehouden met de technologische ontwikkelingen en de toepassingen daarvan in defensiegerelateerde systemen, met name wat betreft opkomende en disruptieve technologieën (EDT's, zoals artificiële intelligentie, encryptie en kwantumcomputing)[45]. De EU moet met name investeren in post-kwantumcryptografie om de beveiliging van haar defensiesystemen in stand te houden. Gezien de snelle ontwikkeling van de technologie moeten de gezamenlijke inspanningen op het gebied van onderzoek en technologische ontwikkeling worden toegespitst op het bereiken van een voldoende hoog niveau van technologische paraatheid, zodat de resultaten ervan sneller in de bestaande en toekomstige vermogens kunnen worden geïntegreerd.

De Commissie financiert in het kader van het EDF technologische innovatie op defensiegebied en ondersteunt de ontwikkeling van opkomende, disruptieve en geavanceerde technologieën, onder meer voor cyberdefensie. Tot 8 % van de EDF-begroting wordt uitgetrokken voor thema's die betrekking hebben op disruptieve technologieën voor defensie, waaronder een aantal dat verband houdt met cyberdefensie. In het kader van het EDF wordt de komende jaren bijzondere aandacht besteed aan onderzoeksacties en -projecten die gericht zijn op nieuwe technologieën die zijn ontwikkeld om opkomende en veranderende dreigingen het hoofd te bieden en om de weerbaarheid, cyberbeveiliging en de integratie daarvan in defensievermogens te versterken.

Overeenkomstig het EDT-actieplan[46] zal het EDA de lidstaten jaarlijks inlichten over het landschap van opkomende technologieën, waaronder technologieën die toepasbaar zijn op het gebied van cyberdefensie. Verder zal het EDA de Europese strategische evaluatie van EDT's ontwikkelen om de lidstaten te ondersteunen bij het opvolgen van strategische langetermijnrichtsnoeren en het in kaart brengen van synergieën en samenwerkingsmogelijkheden. Het Europees Kenniscentrum voor cyberbeveiliging (ECCC) zal een strategische agenda opstellen voor investeringen op gebieden die belangrijk zijn voor cyberbeveiliging. Die agenda zal weer als leidraad dienen bij het opstellen van toekomstige werkprogramma's in het kader van Digitaal Europa en Horizon Europa met betrekking tot cyberbeveiliging en ter ondersteuning van onderzoek, innovatie en marktintroductie. Om synergieën te bevorderen, zullen het ECCC en het EDA ook een werkregeling ontwikkelen om de uitwisseling van informatie tussen elkaars personeel over de prioriteiten inzake civiele technologie, technologie voor tweeërlei gebruik en defensietechnologie te faciliteren.

[45] Zoals genoemd in de strategische onderzoeksagenda voor cyberdefensie en in de overkoepelende strategische onderzoeksagenda (OSRA).

[46] "Emerging Disruptive Technologies (EDT's): A capability-driven Action Plan" is op 16 december 2021 goedgekeurd door het EDA-bestuur in de samenstelling directeuren onderzoek en technologie.

Werken aan de voor cyberdefensie benodigde technologie

Verdere maatregelen en coördinatie zijn nodig om ervoor te zorgen dat de snelle technologische ontwikkelingen op cybergebied vlot door de defensiesector worden opgepakt. Dit houdt in dat meer moet worden gedaan om kritieke technologieën voor cyberdefensie en cyberbeveiliging in kaart te brengen en die technologieën prioriteit te geven. Dat is noodzakelijk om de technologische afhankelijkheid van de EU terug te dringen en om te kunnen beoordelen of deze afhankelijkheden met de huidige prioriteiten en financieringsinstrumenten voldoende kunnen worden aangepakt.

Daartoe zal de Commissie samen met het EDA en de lidstaten in 2023 een **technologieroutekaart voor kritieke cybertechnologieën** voorstellen op basis van overleg, waar nuttig ook met de industrie. De technologieroutekaart zal cybertechnologieën identificeren die belangrijk zijn voor de technologische soevereiniteit van de EU. De routekaart zal zowel cyberdefensie als cyberbeveiliging bestrijken, technologische ontwikkelingen en strategische afhankelijkheden in kaart brengen en in maatregelen voorzien om deze afhankelijkheden terug te dringen. De routekaart voor cybertechnologie zal als basis dienen voor de strategische prioriteiten van de financieringsinstrumenten van de EU. Er zal worden voorgesteld om ten volle gebruik te maken van de programma's voor onderzoek en ontwikkeling op civiel en defensiegebied, de programma's voor vermogensontwikkeling en financieringsinstrumenten, overeenkomstig de onderscheiden governanceregels daarvan. In de routekaart zullen ook methoden worden voorgesteld om de ontwikkeling van onderzoek voor tweeërlei gebruik, technologische ontwikkeling en innovatie op het gebied van cyberbeveiliging en cyberdefensie in de EU en de lidstaten aan te moedigen.

In deze context zal de Commissie[47] in 2023 samen met het ECCC en het EDA een beoordeling geven van technologieën die al zijn aangemerkt als cruciaal voor cyberdefensie. Zij zal, eventueel met steun van het waarnemingscentrum voor kritieke technologieën, bestaande afhankelijkheden verder in kaart brengen en identificeren[48]. Daarbij zal rekening worden gehouden met het werk dat wordt gedaan in het kader van het jaarlijkse monitoringdocument[49] van het EDA en de strategische evaluatie[50] van de Europese EDT's. Verder zou het ECCC een specifiek beleidsondersteunend project kunnen opzetten dat kan worden meegenomen in het proces van technologische routekaarten en dat belanghebbenden uit de civiele en de militaire sector samenbrengt.

In het kader van de activiteiten van het actieplan voor synergieën, de routekaart en de analyse van lacunes worden al verschillende acties ondernomen om de synergieën te versterken, zodat het volledige potentieel van technologieën voor tweeërlei gebruik, ook op cybergebied, beter kan worden benut.

Daarnaast worden de lidstaten aangemoedigd om ten volle gebruik te maken van de al bestaande initiatieven ter ondersteuning van onderzoek en technologische ontwikkeling. Op

[47] Met inbegrip van het JRC.
[48] Het waarnemingscentrum voor kritieke technologieën is aangekondigd in het actieplan voor synergieën tussen de civiele, defensie- en ruimtevaartindustrieën.
[49] Eerste fase van het EDT-actieplan 2021 van het EDA.
[50] Tweede fase van het EDT-actieplan 2021 van het EDA.

defensiegebied zijn dat de technologiegroepen voor defensievermogens van het EDA[51] en de bijbehorende technologische bouwstenen van de OSRA[52], het ad-hoc-kader van het EDA[53], het EDF en de Pesco. Wat civiele technologieën en technologieën voor tweeërlei gebruik betreft, kunnen het ECCC en het netwerk projecten beheren die zowel een defensiedimensie als een civiele dimensie hebben, hetgeen ook is vastgesteld in de rechtsgrondslag ervan[54]. Zoals in het actieplan voor synergieën en de routekaart is aangekondigd, zal de Commissie ook streven naar versterking van de synergieën tussen de activiteiten van het ECCC en het EDF op het gebied van cyberbeveiliging en cyberdefensie, in overeenstemming met de governanceregels van het EDF.

3.2. Een flexibele, concurrerende en innovatieve Europese defensie-industrie

De EU heeft een sterke, flexibele, concurrerende en innovatieve Europese defensie-industrie nodig, die in staat is een volledig spectrum van geavanceerde defensievermogens, waaronder cyberdefensievermogens, tot stand te brengen. Wat cyberdefensie betreft, is de defensie-industrie van de EU momenteel voor geavanceerde oplossingen echter in aanzienlijke mate afhankelijk van de civiele sector en van externe markten. Hoewel de technologische vooruitgang op civiel gebied snel verloopt en de markt voor civiele informatie- en cyberbeveiligingsproducten rap groeit, zijn er specifieke militaire vereisten waaraan kant-en-klare civiele producten niet voldoen. Belangrijke onderdelen van hardware en software die momenteel voor cyberdefensie worden gebruikt, worden in de EU niet geproduceerd, waardoor industriële en technologische afhankelijkheden ontstaan. De EU is evenmin sterk vertegenwoordigd in de mondiale cyberbeveiligings- en cyberdefensie-industrie. De sterk gefragmenteerde **EDTIB** beperkt het vermogen van de EU om haar concurrentiepositie te verbeteren aanzienlijk[55], aangezien de meeste cyberbeveiligingsbedrijven klein of middelgroot zijn[56]. Een technologisch soevereine industriële capaciteit is cruciaal voor het vermogen van de EU om op te treden.

---

[51] Technologiegroepen voor defensievermogens ("CapTech's") bieden deskundigen van de lidstaten een netwerkforum en een flexibel kader voor samenwerkingsprojecten. Meer informatie over de CapTech's die betrekking hebben op cyberzaken (cyber, informatie, componenten) is te vinden op: https://eda.europa.eu/what-we-do/research-technology/capability-technology-areas-(captechs).

[52] De OSRA (overkoepelende strategische onderzoeksagenda) brengt relevante gebieden voor O&O op defensiegebied in kaart en beschrijft concrete samenwerkingsmogelijkheden. Er zijn 17 technologie-bouwstenen, met bijbehorende technologische routekaarten, die in verband staan met cybertechnologieën die gericht zijn op situationeel bewustzijn op het gebied van cyberdefensie, de bescherming van militaire communicatiesystemen, de verwerking van informatie uit heterogene bronnen, modellering en simulatie, kwantumcomputing en cryptografie, en het onderzoeken van synergieën tussen cyberoperaties en elektronische oorlogvoering. Artificiële intelligentie en big data spelen een belangrijke rol bij informatieverwerking.

[53] Het ad-hoc-kader van het EDA is vastgesteld bij Besluit (GBVB) 2015/1835 van de Raad. Momenteel worden in dit kader zes projecten met cybertechnologische elementen uitgevoerd, met een budget van ongeveer 20 miljoen EUR: ANQUOR, Cerere, EDA SOC 2, MASFAD II, PASEI II en ASSAI.

[54] Verordening (EU) 2021/887 van het Europees Parlement en de Raad van 20 mei 2021 tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra.

[55] Zoals aangegeven in de gezamenlijke mededeling over de analyse van de lacunes op het gebied van defensie-investeringen en de te volgen koers.

[56] Het totale aantal kleine en middelgrote ondernemingen in de EU die actief zijn in de meerlagige en vaak grensoverschrijdende toeleveringsketens voor defensie, wordt geraamd op 2 500. Deze bedrijven bedienen klanten op het gebied van defensie en 7,8 % van hun activiteiten houdt verband houdt met cyberactiviteiten.

De EU steunt de ontwikkeling van een sterke EDTIB met een reeks programma's en initiatieven. Het EDF financiert technologische innovatie voor defensie en ondersteunt de ontwikkeling van technologieën, hetgeen uiteindelijk leidt tot gezamenlijk ontwikkelde geavanceerde militaire vermogens en bijdraagt aan het concurrentievermogen van de defensie-industrie van de EU, terwijl Horizon Europa en het programma Digitaal Europa steun verlenen aan cyberbeveiligingsonderzoek en de ontwikkeling van technologieën voor tweeërlei gebruik, waaronder kwantumtechnologie, encryptie, beveiligde cloud en AI[57].

Verdere maatregelen in verband met kritieke technologieën voor cyberdefensie en industriële behoeften, zoals vastgesteld in de **technologie routekaart voor kritieke cybertechnologieën**, moeten worden uitgewerkt. Er moeten passende steunstromen worden vastgesteld: gemeenschappelijke aanbestedingsactiviteiten kunnen bijvoorbeeld worden gestimuleerd via het toekomstige Europese defensie-investeringsprogramma, en de toegang tot eigen vermogen en leningen kan worden gefaciliteerd via het Europees Investeringsfonds en de Europese Investeringsbank.

Om een sterke EDTIB op te bouwen, moeten synergieën tussen civiele ondernemingen en defensiebedrijven worden benut. Innovatieve maatregelen zoals voorgesteld in het kader van de EU-regeling voor defensie-innovatie (EUDIS), waaronder ondersteuning van kleine en middelgrote ondernemingen en technologieverkenning, kunnen een positief effect hebben op de defensie-industrie van de EU en de EDTIB.

De Commissie zal ook een sectorale dialoog op gang brengen met het oog op de ontwikkeling van de cyberdefensie-industrie van de EU, en daarbij zo nodig ook het EDA betrekken.

De Commissie en de hoge vertegenwoordiger stellen verschillende maatregelen voor om de bedrijfstak in staat te stellen op korte en lange termijn resultaten te boeken. Dit houdt op de onmiddellijke termijn in dat de industriële productiecapaciteit van de EU op defensiegebied nauwkeurig in kaart moet worden gebracht, zodat precies kan worden vastgesteld waar de lacunes zijn en op welke gebieden meer inspanningen nodig zijn.

De kritieke afhankelijkheden op cybergebied, zoals die op technologische routekaarten kunnen worden aangewezen, zouden ook kunnen worden teruggedrongen in het kader van het nieuwe Europese Soevereiniteitsfonds dat Commissievoorzitter Von der Leyen in haar toespraak over de Staat van de Unie van september 2022 heeft aangekondigd.

Het EU-kader voor de screening van buitenlandse directe investeringen zal verder worden ingezet om de risico's te beperken waarmee de aankoop van Europese technologieën of oplossingen gepaard kan gaan als het gaat om defensie en veiligheid. Lidstaten die nog geen nationale screeningmechanismen hebben opgezet, moeten dit onverwijld doen.

3.3. Personen werkzaam op het gebied van cyberdefensie in de EU

Europa wordt geconfronteerd met een reëel en alarmerend tekort aan cybervaardigheden: de Europese organisatie voor cyberbeveiliging (ECSO) schat dat er nu, in 2022, in totaal al een half miljoen professionals nodig zijn. Het tekort aan vaardigheden belemmert het vermogen van de EU om nieuwe technologieën te ontwikkelen en onze kritieke infrastructuur te

[57] Het programma Horizon Europa beoogt ervoor te zorgen dat synergieën met het Europees Defensiefonds ten goede zullen komen aan civiel en defensieonderzoek, hoewel de activiteiten uit hoofde van het kaderprogramma uitsluitend op civiele toepassingen gericht zullen zijn.

verdedigen. De felle concurrentie om vaardigheden en de aantrekkelijke salarissen die de particuliere sector aanbiedt, verergeren de problemen die overheidsinstanties zoals de ministeries van Defensie en de strijdkrachten ondervinden om cybertalenten aan te trekken en vast te houden.

In het kader van het Europees Jaar van de Vaardigheden 2023 zal de **Commissie een initiatief opzetten voor de oprichting van een academie voor cybervaardigheden**. Dit zal fungeren als een overkoepelend initiatief om meer professionals op te leiden op het gebied van cyberbeveiliging. De academie zal de verschillende initiatieven op het gebied van cybervaardigheden samenbrengen en zorgen voor coördinatie, integratie en gemeenschappelijke communicatie daaromtrent. De academie voor cybervaardigheden zal worden opgezet rond verschillende actiepijlers, zoals financiering, gemeenschapsondersteuning, opleiding en certificering, betrokkenheid van belanghebbenden en kennisontwikkeling, en zal ook het cyberdefensiepersoneel ten goede kunnen komen. De Europese Veiligheids- en Defensieacademie (EVDA) zal onderzoeken hoe beste praktijken en verdere synergieën tussen het militaire en het civiele domein met betrekking tot opleiding en de ontwikkeling van cyberspace-specifieke militaire vaardigheden gemakkelijker kunnen worden uitgewisseld.

Op basis van een EU-analyse van de opleidingsvereisten en opleidingsbehoeften zullen de EVDA, het EDA en de lidstaten zorgen voor verdere ontwikkeling en organisatie van opleidingsactiviteiten en oefeningen op het gebied van cyberdefensie voor EU-instellingen, GVDB-operaties en -missies en ambtenaren van de lidstaten. Ook zal worden onderzocht of de verdere **ontwikkeling van het EVDA-platform voor onderwijs, opleiding, oefening en evaluatie op het gebied van cyberbeveiliging (ETEE)** meer opleidingscapaciteit zou kunnen genereren. Daarbij moeten ook opleidingscursussen voor specifieke operationele en meerdere domeinen omvattende operaties aan bod komen. Met name moet er worden gestreefd naar synergieën met het Pesco-project EU-cyberacademie en innovatiehub (EU CAIH)[58].

De lidstaten worden aangemoedigd specifieke onderwijsprogramma's op het gebied van cyberdefensie te ontwikkelen, zodat hogeronderwijsinstellingen en academische instellingen (zowel civiele als militaire) gemeenschappelijke curricula voor cyberdefensie kunnen ontwikkelen en opzetten, beste praktijken kunnen uitwisselen, partnerschappen en gemeenschappelijke projecten kunnen opzetten en uitwisselingen van opleiders en stagiairs kunnen vergemakkelijken. Om interoperabiliteit en een gemeenschappelijke cultuur in de hele EU te waarborgen, zal de EVDA via het ETEE de uitwisseling tussen de lidstaten bevorderen.

De lidstaten zouden de samenwerking tussen actoren op het gebied van opleiding en onderwijs moeten versterken door zowel civiele als militaire aspecten op technisch, operationeel, strategisch en juridisch gebied te combineren en de basis te leggen voor gemeenschappelijke, gestandaardiseerde opleidingsprogramma's op verschillende niveaus ten behoeve van de gemeenschappen op civiel, diplomatiek, rechtshandhavings- en cyberdefensiegebied. Om het competentieniveau en de vaardigheden van het personeel in militaire GVDB-missies en -operaties te verbeteren, zouden daarnaast de lidstaten moeten samenwerken met Europese particuliere aanbieders van opleidingen en met academische instellingen.

[58] https://www.pesco.europa.eu/project/eu-cyber-academia-and-innovation-hub-eu-caih/

De samenwerking inzake opleidingsnormen en certificering op het gebied van cyberdefensie tussen de lidstaten, de EU-IOA's, internationale partners en andere actoren, ook in de particuliere sector en de academische wereld, zou bovendien moeten worden bevorderd. De EVDA zal, voortbouwend op bestaande civiele initiatieven zoals het door Enisa ontwikkelde Europees kader voor vaardigheden op het gebied van cyberbeveiliging (ECSF), een regeling voor de certificering van vaardigheden op het gebied van cyberdefensie ontwikkelen. De Commissie wil ook benaderingen overwegen voor het certificeren van cybervaardigheden die op de markt en in de academische wereld beschikbaar zijn, en tegelijkertijd via de academie voor cybervaardigheden synergieën tussen deze benaderingen stimuleren en lacunes opvullen, met name met gerichte EU-financiering.

Maatregelen op het gebied van cyberdefensie

- De strategische evaluatie van de EDT's ontwikkelen ter ondersteuning van strategische investeringsbeslissingen voor de lange termijn.
- Een technologieroutekaart voor kritieke cybertechnologieën voor de EU ontwikkelen, die met betrekking tot kritieke technologieën voor cyberdefensie en cyberbeveiliging de mate van afhankelijkheid beoordeelt.
- Voorstellen doen om afhankelijkheid terug te dringen, door gebruik te maken van alle EU-instrumenten, waaronder het programma Digitaal Europa, Horizon Europa en het EDF, en anticiperen op technologische ontwikkelingen om de technologische soevereiniteit te versterken en het handelend vermogen te waarborgen.
- De ontwikkeling van een certificeringskader voor cyberdefensievaardigheden ondersteunen.
- EU-oefeningen op het gebied van cyberdefensie ontwikkelen en onderzoeken hoe het ETEE-cyberplatform van de EVDA verder kan worden ontwikkeld om meer opleidingscapaciteit te genereren.

Civiele ondersteunende maatregelen

- Een EU-academie voor cybervaardigheden oprichten, rekening houdend met de specifieke vaardigheden die nodig zijn voor verschillende beroepsprofielen en sectoren, ook op defensiegebied.
- Benaderingen analyseren voor het certificeren van cybervaardigheden, en er daarbij naar streven synergieën te bevorderen en lacunes op te vullen, onder meer met EU-financiering.

4. Partnerschappen aangaan om gemeenschappelijke uitdagingen aan te pakken

Partners hebben baat bij een EU die in cyberspace van meer slagvaardigheid en veerkracht getuigt en via relevante EU-instrumentarium bijstand en capaciteitsopbouw kan bieden op het gebied van cyberdefensie. De EU zal ernaar streven op maat gesneden partnerschappen op het gebied van cyberdefensie tot stand te brengen waar deze beide partijen ten goede komen. Partnerschappen op het gebied van cyberdefensie zullen ook aan bod komen in het kader van de deelname van de partnerlanden aan militaire GVDB-missies en -operaties.

In voorkomend geval zal bij deze activiteiten worden voortgebouwd op bestaande cyberdialogen en veiligheids- en defensiedialogen. De hoge vertegenwoordiger zal ook streven

naar synergieën tussen het **informele EU-netwerk voor cyberdiplomatie en het netwerk van defensieattachés in de delegaties van de EU.**

4.1. Samenwerking met de NAVO

Het strategische partnerschap van de EU met de NAVO blijft essentieel voor de Euro-Atlantische veiligheid, zoals is benadrukt in het strategisch kompas en het strategisch concept van de NAVO van 2022[59]. De EU blijft zich ten volle committeren aan versterking van dit essentiële partnerschap, ook op het gebied van cyberdefensie. Er moeten verdere stappen worden gezet voor de ontwikkeling van gedeelde oplossingen voor gemeenschappelijke dreigingen en problemen. Overeenkomstig de gezamenlijke verklaringen van Warschau en Brussel betreffende samenwerking tussen de EU en de NAVO[60] en op basis van de beginselen van transparantie, wederkerigheid en inclusiviteit, openheid en de beslissingsautonomie van beide organisaties behoren cyberbeveiliging en cyberdefensie tot de belangrijkste prioriteitsgebieden voor samenwerking voor de EU.

Op basis van wederkerigheid zal de EU in gesprek blijven met de NAVO over het militaire conceptuele kader voor de integratie van cyberdefensieaspecten in de planning en uitvoering van militaire GVDB-missies en -operaties. De EU zal streven naar een zo groot mogelijke compatibiliteit met de NAVO-concepten en -doctrine inzake cyberdefensie.

Wat de grote vraag naar cyberdefensievermogens betreft, zal de EU synergieën en complementariteit met de NAVO bevorderen over organisatorische en nationale grenzen heen. De EU zal als partner met de NAVO samenwerken om de technische en procedurele interoperabiliteit van de cyberdefensievermogens te versterken, met inbegrip van de ontwikkeling van vermogens overeenkomstig het FMN-initiatief. Dit zal de weg effenen voor de mogelijke wederzijds ondersteunende ontwikkeling en inzet van cyberdefensievermogens. Bijzondere aandacht moet worden geschonken aan de interoperabiliteit van normen, die bijdraagt aan de cyberweerbaarheid en de interoperabiliteit van de militaire communicatie- en informatiesystemen, door waar nodig de industrie erbij te betrekken.

Met het oog op een coherente opleiding van het cyberdefensiepersoneel van beide organisaties zal de EU waar nodig ook de samenwerking met de NAVO versterken op het gebied van de harmonisatie van opleidingsbehoeften en vereistenanalyse, door gezamenlijke curricula, cursussen en oefeningen te ontwikkelen. Op basis van de beginselen van wederkerigheid en non-discriminatie zal de EVDA haar opleidingen op het gebied van cyberdefensie openstellen voor NAVO-personeel en een platform opzetten om bekendheid te geven aan gemeenschappelijke cursussen. De EU zal ook de deelname van NAVO-personeel aan cyberoefeningen en crisisbeheeroefeningen met cyberelementen bevorderen.

De EU en de NAVO zullen zich ook inzetten voor een verdere verbetering van het wederzijdse situationeel bewustzijn en de mogelijkheden voor coördinatie verkennen, onder meer door de samenwerking tussen NCIRC en CERT-EU te versterken. Om de samenwerking op het gebied van de cyberaspecten en de implicaties van crisisbeheer en crisisrespons te bevorderen, zal de EU bijdragen tot overleg over militaire, civiele en gemeenschappelijke initiatieven en, in voorkomend geval, tot de ontwikkeling van potentiële synergieën tussen elkaars regelingen en

[59] https://www.nato.int/strategic-concept/
[60] Ondertekend in respectievelijk 2016 en 2018.

initiatieven voor crisisbeheer, ook in het geval van grootschalige incidenten. Om te zorgen voor wederzijdse complementariteit en onnodig dubbel werk te voorkomen, zal de EU streven naar nauwere samenwerking en informatie-uitwisseling met de NAVO inzake capaciteitsopbouw op het gebied van cyberdefensie in partnerlanden.

4.2. Samenwerking met gelijkgestemde partners

De hoge vertegenwoordiger zal cyberdefensievraagstukken systematischer opnemen in bestaande en toekomstige cyberdialogen en veiligheids- en defensiedialogen met partners. Aangezien cyberdefensieaspecten in bilaterale dialogen aan de orde zullen komen, zal er in toenemende mate ruimte zijn om cyberdefensievraagstukken in andere vormen van samenwerking met EU-partners op te nemen.

Binnen het strategische partnerschap van de EU met de **Verenigde Staten** zal de samenwerking op het gebied van veiligheid en defensie verder worden verdiept op een wijze die voor beide partijen voordeel biedt, onder meer door gestructureerde uitwisseling van informatie over het situationeel bewustzijn. De regelmatige cyberdialogen veiligheids- en defensiedialogen tussen de EU en de VS bevestigen de kracht van het sterke trans-Atlantische partnerschap. De hoge vertegenwoordiger zal waar nodig de relevante aspecten van cyberdefensie in deze dialogen aankaarten.

Samen met haar internationale partners zal de EU steun blijven verlenen aan **Oekraïne**, onder meer in het kader van een cyberdialoog. Gezien de ervaring van Oekraïne met het opbouwen van cyberweerbaarheid en cyberdefensievermogens zal de uitwisseling van beste praktijken op het gebied van cyberdefensie, met inbegrip van informatie over het dreigingslandschap en het situationeel bewustzijn alsmede relevante beleidsontwikkelingen van gemeenschappelijk belang, worden voortgezet en uitgebreid.

Gelijkgestemde partners spelen een belangrijke rol voor de instandhouding van een mondiale, open, stabiele en veilige cyberspace. Zij kunnen een aanvullende rol spelen met betrekking tot het vermogen van de EU om kwaadwillig gedrag in cyberspace te voorkomen, te ontmoedigen en te bestrijden en erop te reageren. De EU blijft openstaan voor brede, ambitieuze en wederzijds voordelige samenwerking met alle gelijkgestemde partners op het gebied van veiligheid en defensie, ook wat cyberdefensie betreft.

4.3. Partnerlanden steunen bij capaciteitsopbouw op het gebied van cyberdefensie

Door mondiale en regionale uitdagingen is de onderlinge afhankelijkheid tussen de EU en haar partners vergroot en is duidelijk geworden dat nauwere partnerschappen op het gebied van veiligheid en defensie een noodzaak zijn. Dit is met name relevant voor kandidaat-lidstaten van de EU. Gezien recente grootschalige cyberaanvallen is gebleken dat meer betrokkenheid en partnerschap van de EU op het gebied van cyberveiligheid en cyberdefensie noodzakelijk zijn. Daarbij kan worden voortgebouwd op bestaande programma's. Door de transnationale aard van cyberdreigingen zal het versterken van de cyberweerbaarheid van partnerlanden, met name die met minder cybermaturiteit, bijdragen tot een veiligere en betrouwbaardere cyberspace. Daardoor wordt de EU beter in staat cyberaanvallen te voorkomen, op te sporen en te ontmoedigen en zich ertegen te verdedigen. Om de cyberweerbaarheid van de partnerlanden te verbeteren, zal de EU de samenwerking op het gebied van veiligheid en defensie versterken, onder meer door middel van bestaande dialogen. Waar nodig en

wederzijds nuttig zal de EU haar partners, met name de kandidaat-lidstaten die zich aansluiten bij het gemeenschappelijk buitenlands en veiligheidsbeleid en het gemeenschappelijk veiligheids- en defensiebeleid van de EU, helpen bij de opbouw van hun capaciteit op het gebied van cyberdefensie. Met name in crisisbeheersituaties, kan dit ook het opleiden, adviseren, begeleiden en uitrusten van hun strijdkrachten en veiligheidstroepen omvatten. De lidstaten kunnen besluiten aan de partners operationele bijstand op het gebied van cyberdefensie te verlenen. Verder zal de EU haar partners helpen hun vermogen om bij te dragen aan militaire GVDB-missies en -operaties te versterken, aangezien dat een waardevolle bijdrage levert aan de wederzijdse inspanningen ter bevordering van vrede en veiligheid.

De Europese Vredesfaciliteit (EPF) zal steun blijven verlenen aan de inspanningen van de EU om de defensievermogens (met inbegrip van cyberdefensie) op te bouwen in de partnerlanden, met name de buurlanden van de EU. Dit vormt een aanvulling op de inspanningen op het gebied van crisisbeheer in het kader van het GVDB. In deze context zal de EU waar nodig cyberdefensiebijstand ook beter koppelen aan civiele capaciteitsopbouw op het gebied van cyberbeveiliging, met name via de EU-raad voor de opbouw van cybercapaciteit. Efficiënte coördinatie tussen de programma's en instrumenten van de EU (waaronder de EPF) en de lidstaten is noodzakelijk voor het welslagen van maatregelen voor cyberdefensie en capaciteitsopbouw op het gebied van cyberbeveiliging.

Bij de steunverlening aan partnerlanden ten behoeve van capaciteitsopbouw op het gebied van cyberdefensie zal de EU met andere donoren nauw samenwerken om situationeel bewustzijn en coördinatieplatforms te ontwikkelen. Daardoor kan betere ondersteuning op maat worden geboden, wordt de samenhang verzekerd en wordt dubbel werk voorkomen.

Maatregelen op het gebied van cyberdefensie

- De samenwerking tussen de EU en de NAVO inzake opleiding, onderwijs, situationeel bewustzijn en oefeningen op het gebied van cyberdefensie versterken.
- Cyberdefensiethema's opnemen in door de EU geleide cyberdialogen en veiligheids- en defensiedialogen met partnerlanden.
- Samenwerken met gelijkgezinde landen, onder meer in het kader van de ontwikkeling van cyberdefensievermogens en cyberweerbaarheid.
- De bijstand aan partners bij de ontwikkeling van cyberdefensievermogens opvoeren, onder meer via de Europese Vredesfaciliteit (EPF), met name in de buurlanden van de EU en ter ondersteuning van kandidaat-lidstaten van de EU.

Civiele ondersteunende maatregelen

- De samenwerking tussen de EU en de NAVO op het gebied van cyberbeveiliging versterken voor wat betreft situationeel bewustzijn, crisisrespons, de bescherming van kritieke infrastructuur, en normalisatie en certificering.

III. CONCLUSIE

De hoge vertegenwoordiger (ook als hoofd van het EDA) en de Commissie roepen de lidstaten op de relevante aspecten van dit beleid inzake cyberdefensie verder uit te werken. Zij zullen contact onderhouden met de lidstaten om praktische uitvoeringsmaatregelen vast te stellen. Samen met de lidstaten kan een uitvoeringsplan worden opgezet. De resultaten van de uitvoering van het EU-beleid inzake cyberdefensie zullen bijdragen tot de algemene doelstellingen van zowel de EU-strategie inzake cyberbeveiliging als het strategisch kompas.

Aan de Raad zal jaarlijks verslag worden uitgebracht om de voortgang van de uitvoering van het cyberdefensiebeleid te monitoren en te beoordelen. De lidstaten wordt gevraagd daaraan bij te dragen door verslag te doen van de voortgang van de uitvoeringsmaatregelen die nationaal en in samenwerkingsverband worden uitgevoerd.