Raad van de
Europese Unie

Brussel, 19 november 2018
(OR. en)

14413/18

CYBER 285
CSDP/PSDC 669
COPS 444
POLMIL 214
EUMC 193
RELEX 978
JAI 1154
TELECOM 415
CSC 328
CIS 13
COSI 290

RESULTAAT BESPREKINGEN

van:	het secretariaat-generaal van de Raad
d.d.:	19 november 2018
aan:	de delegaties
Betreft:	EU-beleidskader voor cyberdefensie (update 2018)

Voor de delegaties gaat hierbij het EU-beleidskader voor cyberdefensie (update 2018), dat de Raad op 19 november 2018 tijdens zijn 3652e zitting heeft aangenomen.

BIJLAGE

EU-BELEIDSKADER VOOR CYBERDEFENSIE

(als bijgewerkt in 2018)

Werkingssfeer en doelstellingen

Als antwoord op de veranderende uitdagingen op het gebied van veiligheid moeten de EU en haar lidstaten de cyberweerbaarheid versterken en krachtige cyberbeveiligings- en defensievermogens ontwikkelen.

Het EU-beleidskader voor cyberdefensie (CDPF) ondersteunt de ontwikkeling van cyberdefensievermogens door de EU-lidstaten en de versterking van de cyberbescherming van de beveiligings- en defensie-infrastructuur van de EU, zonder afbreuk te doen aan de nationale wetgeving van de lidstaten en de EU-wetgeving, noch, indien die is bepaald, aan de reikwijdte van cyberdefensie.

Cyberspace is het vijfde activiteitsgebied, naast de gebieden land, zee, lucht en ruimte: de succesvolle uitvoering van EU-missies en operaties is in toenemende mate afhankelijk van de ononderbroken toegang tot een veilige cyberspace, en daarom zijn robuuste en veerkrachtige operationele cybervermogens nodig.

Het doel van het bijgewerkte CDPF is het verder ontwikkelen van het EU-cyberdefensiebeleid door rekening te houden met relevante ontwikkelingen in andere betrokken fora en beleidsdomeinen, en met de uitvoering van het CDPF sinds 2014. In het CDPF worden prioritaire gebieden voor cyberdefensie geformuleerd en de taken van de verschillende Europese actoren nader belicht, met volledige inachtneming van de verantwoordelijkheden en bevoegdheden van actoren van de Unie en de lidstaten, en van het institutionele kader van de EU en haar besluitvormingsautonomie.

Context

In de conclusies van de Europese Raad van december 2013 over het GVDB, alsmede in de Raadsconclusies van november 2013 over het GVDB werd verzocht om de ontwikkeling van een EU-beleidskader voor cyberdefensie, op basis van een voorstel van de hoge vertegenwoordiger, in samenwerking met de Europese Commissie en het Europees Defensieagentschap (EDA). Het EU-beleidskader voor cyberdefensie is door de Raad op 18 november 2014[1] vastgesteld en sindsdien heeft de uitvoering ervan geleid tot concrete resultaten die hebben bijgedragen tot een aanzienlijke versterking van de cyberdefensievermogens van de lidstaten. In het kader van het jaarverslag van 2017 over de uitvoering van het beleidskader voor cyberdefensie[2], en rekening houdend met EU-initiatieven op het gebied van veiligheid en defensie, met name de gecoördineerde jaarlijkse evaluatie inzake defensie (CARD), de permanente gestructureerde samenwerking (PESCO), het Europees Defensiefonds (EDF), en het pact inzake het civiele GVDB, evenals de herziening van 2018 van het vermogensontwikkelingsplan (CDP) en het programma voor de ontwikkeling van civiele vermogens (CCDP), vroegen de lidstaten het EU-beleidskader voor cyberdefensie bij te werken.

Cyberbeveiliging vormt een prioritair element van de integrale strategie voor het buitenlands en veiligheidsbeleid van de EU en van het ambitieniveau van de EU[3]. In de integrale strategie wordt benadrukt dat de vermogens om de EU en haar burgers te beschermen en om op externe crises te reageren, moeten worden versterkt. De integrale strategie onderstreept dat de EU als veiligheidsgemeenschap moet worden versterkt. In dit verband zouden inspanningen op het gebied van veiligheid en defensie ook de strategische rol van de Unie moeten vergroten, evenals haar capaciteit om zelfstandig op te treden waar en indien nodig, en te handelen met partners overal waar mogelijk. Deze doelstellingen vereisen meer samenwerking bij vermogensontwikkeling, waarbij de doeltreffendheid en de interoperabiliteit van de daaruit resulterende civiele en militaire vermogens wordt bevorderd.

---

1 Raadsdocument 15585/14 van 18.11.2014.
2 Raadsdocument 15870/17 van 19.12.2017.
3 Conclusies van de Raad over de uitvoering van de integrale EU-strategie op het gebied van veiligheid en defensie, 14.11.2016

Het gemeenschappelijk pakket voorstellen voor de uitvoering van de gezamenlijke verklaring, ondertekend door de voorzitter van de Europese Raad, de voorzitter van de Europese Commissie en de secretaris-generaal van de Noord-Atlantische Verdragsorganisatie op 8 juli 2016 in Warschau[4], omvat concrete acties om de samenwerking tussen de EU en de NAVO op het gebied van cyberbeveiliging en -defensie uit te breiden, onder meer in het kader van missies en operaties, alsook met betrekking tot de ontwikkeling van cyberdefensievermogens, tot onderzoek en technologie, opleiding, onderwijs en oefeningen ter zake, en tot de integratie van cyberaangelegenheden in crisisbeheersing. Deze samenwerking vindt plaats met volledige inachtneming van de beginselen openheid, transparantie, inclusiviteit en wederkerigheid, en van de besluitvormingsautonomie van de EU. Een technische regeling tussen het computer-crisisresponsteam van de EU (CERT-EU) en de responscapaciteit voor computerincidenten van de NAVO (NCIRC), ondertekend in februari 2016, vergemakkelijkt de uitwisseling van technische informatie om de preventie en detectie van, en de respons op cyberincidenten in beide organisaties te verbeteren.

Er zij aan herinnerd dat verschillende EU-maatregelen bijdragen tot de doelstellingen van het cyberdefensiebeleid als vervat in dit document, en dat dit kader ook rekening houdt met de desbetreffende regelgeving, het beleid ter zake en de technologische ondersteuning op civiel gebied. In juli 2016 bijvoorbeeld hebben het Europees Parlement en de Raad de richtlijn netwerk- en informatiebeveiliging[5] (NIB) vastgesteld, waardoor de algehele paraatheid van de lidstaten ten aanzien van cyberdreigingen zal worden vergroot en de samenwerking in de gehele EU zal worden bevorderd. Deze richtlijn bevat maatregelen die moeten leiden tot een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, teneinde de werking van de interne markt te verbeteren. De termijn voor de omzetting van de richtlijn liep af op 9 mei 2018.

---

4 Conclusies van de Raad over de uitvoering van de gezamenlijke verklaring van de voorzitter van de Europese Raad, de voorzitter van de Europese Commissie en de secretaris-generaal van de Noord-Atlantische Verdragsorganisatie (6 december 2016, 15283/16; 5 december 2017, 14802/17)

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

Het voorstel van september 2017 voor een EU- cyberbeveiligingsverordening omvat het nieuwe mandaat van het Agentschap van de EU voor cyberveiligheid (Enisa) en de oprichting van een EU-breed certificeringskader. Eenmaal operationeel zou het certificeringskader voor hoge normen voor ICT-processen, -producten of -diensten moeten zorgen, concurrentievoordeel moeten opleveren en het vertrouwen van consumenten en aanbesteders moeten vergroten. In september 2017 heeft de Commissie ook een nieuwe stap gezet bij het voorbereiden van de EU op grootschalige grensoverschrijdende cyberbeveiligingsincidenten ("blauwdruk"), en nu werkt zij samen met de lidstaten en andere instellingen, organen en instanties aan de ontwikkeling van een Europese samenwerking inzake cyberbeveiligingscrises, waarbij wordt gezorgd voor de praktische operationalisering en de documentatie van alle betrokken actoren, processen en procedures in de context van bestaande EU-mechanismen voor crisis- en rampenbeheersing, met name de geïntegreerde regeling politieke crisisrespons.

In de conclusies van de Raad over het versterken van de Europese cyberbeveiliging van november 2016 werd het gemeenschappelijk doel vermeld om bij te dragen tot de strategische autonomie van de EU, zoals bedoeld in de conclusies van de Raad van november 2016 over de integrale strategie voor het buitenlands en veiligheidsbeleid van de Europese Unie, inclusief in de cyberspace. De Europese Raad heeft dit bericht in juni 2018 bevestigd en tevens onderstreept dat de vermogens ter bestrijding van buiten de EU afkomstige cyberdreigingen moeten worden versterkt.

In 2017 heeft de Raad een kader vastgesteld voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten (het "instrumentarium voor cyberdiplomatie")[6]. Het kader moet de samenwerking bevorderen, het beperken van bedreigingen vergemakkelijken en het gedrag van potentiële agressors op lange termijn beïnvloeden. Het kader maakt gebruik van de GBVB-maatregelen, met inbegrip van beperkende maatregelen, om kwaadwillige cyberactiviteiten te voorkomen en daarop te reageren. Personen die kwaadwillige cyberactiviteiten verrichten, moeten daarvoor ter verantwoording worden geroepen, en de EU-lidstaten worden aangemoedigd om hun vermogen om op een gecoördineerde manier, in overeenstemming met het instrumentarium voor cyberdiplomatie, te reageren op kwaadwillige cyberactiviteiten, verder te ontwikkelen. Staten mogen geen ICT-activiteiten uitvoeren of doelbewust steunen die in strijd zijn met hun verplichtingen uit hoofde van het internationaal recht, en zij mogen niet doelbewust toestaan dat hun grondgebied wordt gebruikt voor internationaal onrechtmatige handelingen waarbij gebruik wordt gemaakt van informatie- en communicatietechnologie.

In september 2017 hebben de Commissie en de HV/VV een gezamenlijke mededeling[7] over cyber opgesteld om de risico's als gevolg van het nieuwe dreigingslandschap te beperken. Hierin geldt cyberdefensie als een van de belangrijkste gebieden voor actie, en het CDPF is een van de pijlers van de concrete uitvoering ervan[8].

In de conclusies van de Raad van november 2017 over cyberkwesties worden de groeiende connecties tussen cyberbeveiliging en -defensie erkend, en wordt opgeroepen tot intensivering van de samenwerking op het gebied van cyberdefensie, mede door het stimuleren van samenwerking tussen civiele en militaire gemeenschappen die zich bezighouden met de respons op incidenten. Er wordt tevens in beklemtoond dat een cyberincident of -crisis van bijzonder ernstige aard voldoende reden kan zijn voor een lidstaat om een beroep te doen op de solidariteitsclausule van de EU en/of de clausule inzake wederzijdse bijstand.

---

6 Conclusies van de Raad over een kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten ("Instrumentarium voor cyberdiplomatie"), 9916/17, 7 juni 2017

7 Gezamenlijke mededeling aan het Europees Parlement en de Raad: "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU" (13 september 2017, JOIN (2017) 450 final)).

8 Conclusies van de Raad over de gezamenlijke mededeling aan het Europees Parlement en de Raad: "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU" (20 november 2017, 14435/17).

Op 11 december 2017 ging de permanente gestructureerde samenwerking (PESCO) van start. Dit ambitieuze, bindende en inclusieve samenwerkingskader is vastgesteld tussen 25 lidstaten en omvat een verbintenis tot intensivering van de inspanningen bij de samenwerking op het gebied van cyberdefensie, alsmede daarmee verband houdende PESCO-projecten. De eerste reeks PESCO-projecten die de aan de PESCO deelnemende lidstaten in 2017 hebben vastgesteld, omvat twee projecten met betrekking tot cyberdefensie: "snellereactieteams bij cyberincidenten en wederzijdse bijstand op het gebied van cyberbeveiliging" en "platform voor het delen van informatie over cyberdreigingen en respons op incidenten". Er zijn nog reeksen PESCO-projecten gepland. PESCO zal cyberdefensievermogens ontwikkelen en derhalve de samenwerking tussen de deelnemende lidstaten versterken en de interoperabiliteit vergroten.

In het bijgewerkte CDP van de EU, dat door het bestuur van het EDA in juni 2018 is goedgekeurd, wordt cyberdefensie een kernelement genoemd en de noodzaak van defensieve cyberoperaties in een operationele context erkend, op basis van een geavanceerd huidig en predictief situationeel bewustzijn met betrekking tot de cyberspace, onder meer het vermogen om grote hoeveelheden data en inlichtingen van talrijke bronnen te combineren ter ondersteuning van snelle besluitvorming en een grotere automatisering van het proces van dataverzameling, analyse en besluitondersteuning. Het CDP 2018 bepaalt prioriteiten inzake cyberdefensievermogens op de volgende gebieden: samenwerking en synergieën met relevante actoren op alle terreinen van cyberdefensie en cyberbeveiliging; activiteiten op het gebied van cyberdefensieonderzoek en -technologie; kaders voor systeemtechniek voor cyberoperaties; onderwijs, opleiding, oefeningen en evaluatie (ETEE); de aanpak van uitdagingen op het gebied van cyberdefensie in de lucht, de ruimte, te land en ter zee.

Ten slotte is het de afgelopen jaren duidelijk geworden dat de internationale gemeenschap conflicten moet voorkomen, moet samenwerken en de cyberspace moet stabiliseren. De EU streeft, in nauwe samenwerking met andere internationale organisaties, met name de VN, de OVSE en het Regionaal Forum van de Asean, naar een strategisch kader voor conflictpreventie, samenwerking en stabiliteit in de cyberspace, met inbegrip van i) de toepassing van het internationaal recht, met name het integrale Handvest van de VN, in de cyberspace; ii) de eerbiediging van universele niet-bindende normen, regels en beginselen voor verantwoordelijk staatsgedrag; iii) de ontwikkeling en uitvoering van regionale vertrouwenwekkende maatregelen. Het beleidskader voor cyberdefensie zou dit streven ook moeten ondersteunen.

Prioriteiten

In het bijgewerkte CDPF zijn zes prioritaire gebieden vastgesteld. Het beleidskader is in eerste instantie gericht op de ontwikkeling van cyberdefensievermogens, alsmede op de bescherming van de GVDB-communicatie- en informatienetwerken van de EU. Andere prioritaire gebieden omvatten: opleiding en oefeningen, onderzoek en technologie, civiel-militaire samenwerking en internationale samenwerking. Wat opleiding betreft, ligt de nadruk op het opwaarderen van de opleiding van de lidstaten op het gebied van cyberdefensie en van de opleiding van de GVDB-commandoketen met betrekking tot cyberbewustzijn. De cyberdimensie dient ook een passende plaats te krijgen in oefeningen teneinde het reactievermogen van de EU op cyber- en hybride crisissen te versterken door de besluitvormingsprocedures en de beschikbaarheid van informatie te verbeteren. De cyberspace is een zich snel ontwikkelend domein en nieuw technologische ontwikkelingen moeten worden ondersteund, zowel in het civiele als in het militaire domein. Civiel-militaire samenwerking op cybergebied is van cruciaal belang om een coherente respons op cyberdreigingen te garanderen. Tot slot, maar daarom niet minder belangrijk, kan intensievere samenwerking met internationale partners bijdragen tot het verbeteren van de cyberbeveiliging in de EU en daarbuiten, en tot het bevorderen van de beginselen en de waarden van de EU.

Dit kader geeft een overzicht van de voorstellen en de mogelijkheden voor coördinatie tussen de betrokken EU-instellingen, -organen en -instanties. Het brengt ook de belangrijke rol van de particuliere sector voor de ontwikkeling van cyberbeveiligings- en cyberdefensietechnologieën onder de aandacht.

Bovendien ondersteunt het beleidskader voor cyberdefensie voort de integratie van cyberdefensie in de mechanismen voor crisisbeheersing van de Unie, waarbij met het oog op het aanpakken van de gevolgen van een cybercrisis, de betrokken bepalingen van het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie[9] van toepassing kunnen zijn.

1. Ondersteunen van de ontwikkeling van cyberdefensievermogens door de lidstaten

Bij de ontwikkeling van cyberdefensievermogens en -technologieën moeten alle aspecten van vermogensontwikkeling aan bod komen, waaronder doctrine, leiderschap, organisatie, personeel, opleiding, industrie, technologie, infrastructuur, logistiek en interoperabiliteit. Daartoe moeten de lidstaten meer inspanningen leveren teneinde effectieve cyberdefensievermogens tot stand te brengen. De EDEO, de Commissie en het EDA moeten samenwerken en die inspanningen ondersteunen.

De zwakke punten van de informatie-infrastructuren die de GVDB-missies en -operaties ondersteunen, moeten permanent worden geëvalueerd; daarnaast is ook bijna realtime inzicht in de doeltreffendheid van de bescherming vereist. Vanuit operationeel oogpunt zal het handhaven van de beschikbaarheid, de integriteit en de vertrouwelijkheid van GVDB-communicatie- en -informatienetwerken een van de belangrijkste aandachtsgebieden van cyberdefensie-activiteiten zijn, tenzij anderszins is bepaald in het mandaat van de operaties of missies. Voorts zal de EDEO in samenwerking met de lidstaten de cybervermogens verder integreren in GVDB-missies en operaties.

Actoren van kwaadwillige cyberactiviteiten moeten ter verantwoording worden geroepen voor hun daden. Het is van belang dat de EU-lidstaten, met de steun van de EDEO, wederzijdse samenwerking als antwoord op kwaadwillige cyberactiviteiten bevorderen. Het instrumentarium voor cyberdiplomatie is ontwikkeld om een dergelijke respons op basis van wederzijdse samenwerking tot stand te helpen brengen. De EDEO en het EDA zullen regelmatig oefeningen op basis van het instrumentarium voor cyberdiplomatie organiseren waar de EU-lidstaten een en ander in de praktijk kunnen brengen.

---

[9] De artikelen 222 VWEU en 42, lid 7, VEU, met inachtneming van artikel 17 VEU.

Overwegende dat, indien en voor zover omschreven, de reikwijdte van cyberdefensie in het nationale recht van de lidstaten en in het Unierecht breed en divers is, moet een gemeenschappelijk algeheel inzicht betreffende de reikwijdte van cyberdefensie worden ontwikkeld.

Aangezien militaire GVDB-operaties steunen op door de lidstaten verstrekte C4-infrastructuur (commando, controle, communicatie, computers), is een bepaalde mate van strategische convergentie nodig bij het plannen van cyberdefensiebehoeften voor de informatie-infrastructuur.

Voortbouwend op de werkzaamheden van het cyberdefensie-projectteam van het EDA voor de ontwikkeling van cyberdefensievermogens, zullen het EDA en de lidstaten:

- een beroep doen op het CDP en andere instrumenten zoals CARD ter facilitering en ondersteuning van samenwerking tussen de lidstaten, met het oog op een hogere mate van convergentie bij het plannen van cyberdefensiebehoeften van de lidstaten op strategisch niveau, met name wat betreft monitoring, situationeel bewustzijn, preventie, opsporing en bescherming, informatiedeling, forensisch onderzoek en capaciteit voor malwareanalyse, geleerde lessen, schadebeperking, dynamische herstelcapaciteit, opslag van gedistribueerde gegevens en gegevensback-ups;
- hun steun verlenen aan huidige en toekomstige cyberdefensiegerelateerde "pooling and sharing"-projecten voor militaire operaties (bijvoorbeeld bij forensisch onderzoek, interoperabiliteitsontwikkeling, normering);
- een standaardpakket van doelstellingen en behoeften ontwikkelen, dat op basis van bestaande, in de gehele EU opgedane ervaring het door de lidstaten te bereiken minimumniveau van cyberbeveiliging en vertrouwen bepaalt.

De EDEO en het EDA zullen:

- uitwisselingen tussen de lidstaten faciliteren betreffende nationale cyberdefensiedoctrines, alsmede betreffende cyberdefensiegerichte programma's voor rekrutering, behoud en reserves.

Het EDA zal:

- de verschillende reikwijdten van de militaire behoeften inzake cyberdefensie in het nationale recht en de beste praktijken van de lidstaten onderzoeken. Belangrijkste doelstelling van het onderzoek is een bedrijfsarchitectuur voor cyberdefensie te ontwikkelen, die de reikwijdte, de functionaliteiten en de behoeften moet omvatten welke door de lidstaten op dit gebied worden gebruikt op basis van het nationale recht en het Unierecht.

De lidstaten zullen, op vrijwillige basis:

- de samenwerking tussen hun militaire CERT's verbeteren, met het oog op een betere voorkoming en behandeling van incidenten;
- gebruik maken van de PESCO om de samenwerking inzake cyberdefensie verder te intensiveren, ook wat betreft nieuwe projecten;
- gebruik maken van het Europees Defensiefonds teneinde gezamenlijk cyberdefensie-vermogens te ontwikkelen;
- een gemeenschappelijk inzicht ontwikkelen betreffende de toepassing van de clausule inzake wederzijdse bijstand op cybergebied, waarbij tegelijk de flexibiliteit ervan bewaard blijft;
- basisbehoeften inzake cyberdefensie voor informatie-infrastructuur ontwikkelen;
- voor zover de verbetering van cyberdefensievermogens afhangt van deskundigheid op het gebied van civiele netwerk- en informatiebeveiliging, gebruik maken van de deskundigheid van Enisa, van de in de NIS-samenwerkingsgroep verenigde autoriteiten van de lidstaten, en andere mogelijke entiteiten op EU-niveau met deskundigheid inzake civiele cyberbeveiliging.

De lidstaten, de EDEO/de Militaire Staf van de EU, de EVDA en het EDA zullen:

- het ontwikkelen van opleiding op cyberdefensiegebied in overweging nemen, met het oog op EU-gevechtsgroepcertificering.

De Commissie zal, in samenwerking met de lidstaten:

- cyberdefensie in aanmerking nemen in de werkprogramma's van het industrieel ontwikkelingsprogramma voor de Europese defensie en het Europees Defensiefonds.

2. Verbeteren van de bescherming van door EU-entiteiten gebruikte GVDB-communicatie- en informatiesystemen

Zonder afbreuk te doen aan de rol van het computercrisisresponsteam voor de instellingen, organen en instanties van de Europese Unie (CERT-EU) als centrale EU-coördinatiestructuur voor cyberincidentenrespons voor alle instellingen, organen en instanties van de Unie, zal de EDEO binnen het bestek van de toepasselijke voorschriften betreffende de begroting van de Unie een passend en autonoom inzicht verwerven in beveiligings- en netwerkdefensie-aangelegenheden en zijn eigen IT-beveiligingscapaciteit ontwikkelen. Er zal naar worden gestreefd de bestendigheid van GVDB-netwerken van de EDEO te verbeteren, met aandacht voor preventie, opsporing, incidentenrespons, situationeel bewustzijn, informatie-uitwisseling en mechanismen voor vroegtijdige waarschuwing.

De bescherming van communicatie- en informatiesystemen van de EDEO en de ontwikkeling van IT-beveiligingscapaciteiten worden geleid door het directoraat-generaal Begroting en Administratie (BA) van de EDEO. Aanvullende specifieke middelen en ondersteuning zullen tevens worden verstrekt door de Militaire Staf van de EU (EUMS), het directoraat Crisisbeheersing en Planning (CMPD) en het civiel plannings- en uitvoeringsvermogen (CPCC). Deze IT-beveiligingscapaciteit zal voor zowel gerubriceerde als niet-gerubriceerde systemen worden aangewend en een integrerend deel uitmaken van de bestaande operationele entiteiten.

Ook moeten de beveiligingsvoorschriften van de informatiesystemen die tijdens de uitvoering van GVDB-missies en -operaties door verschillende institutionele actoren van de EU ter beschikking worden gesteld, worden gestroomlijnd. In dit verband kan een gemeenschappelijke commandostructuur in overweging worden genomen teneinde de voor het GVDB gebruikte netwerken bestendiger te maken.

Met het oog op een betere coördinatie en een betere bescherming en grotere bestendigheid van de GVDB-communicatie- en informatiesystemen en -netwerken is in 2017 bij de EDEO een interne raad van bestuur voor cyberaspecten (Cyber Governance Board), onder het gezag van de secretaris-generaal van de EDEO ingesteld.

Het EDEO/BA zal:

- de IT-beveiligingscapaciteit in de EDEO versterken op basis van bestaande technische vermogens en procedures, met aandacht voor preventie, opsporing, incidentenrespons, situationeel bewustzijn, informatie-uitwisseling en mechanismen voor vroegtijdige waarschuwing. De samenwerkingsstrategie met het CERT-EU en bestaande EU-cyberbeveiligingsvermogens zal verder worden verbeterd.

Het EDEO/BA zal, samen met de EUMS, het MPCC, het CMPD en het CPCC:

- coherente IT-beveiligingsmaatregelen en -richtsnoeren opstellen, waarbij ook rekening wordt gehouden met technische eisen voor cyberdefensie in een GVDB-context voor structuren, missies en operaties, en binnen de EU bestaande samenwerkingskaders en beleidsmaatregelen in aanmerking worden genomen teneinde te komen tot convergentie in de regels, het beleid en de organisatie.

De EDEO/de gezamenlijke capaciteit op het gebied van inlichtingenanalyse (SIAC) zal:

- voortbouwend op bestaande structuren, zijn capaciteit voor het beoordelen van cyberdreigingen en het inwinnen van inlichtingen versterken om nieuwe cyberrisico's in kaart te brengen, en regelmatig risicobeoordelingen verrichten op basis van de strategische dreigingsevaluatie en van de incidentengegevens in bijna realtime die tussen de betrokken EU-structuren worden gecoördineerd en op verschillende rubriceringsniveaus toegankelijk worden gemaakt.

De EDEO/de SIAC en het CERT-EU zullen:

- het delen van informatie in realtime over cyberdreigingen bevorderen tussen de lidstaten en de betrokken EU-entiteiten. Daartoe zullen er tussen de betrokken nationale en Europese instanties informatiedelingsmechanismen en maatregelen voor het opbouwen van vertrouwen worden ontwikkeld aan de hand van een vrijwillige aanpak die voortbouwt op bestaande samenwerking.

De EDEO/de EUMS en het MPCC zullen:

- voortwerken aan het ontwikkelen van een cyberdefensieconcept voor militaire missies en operaties in het kader van het GVDB en dit integreren in de planning op strategisch niveau;
- in samenwerking met de operationele hoofdkwartieren een generieke operationele standaardprocedure inzake cyberaspecten ontwikkelen.

De EDEO/het CPCC en het CMPD zullen:

- voortwerken aan het ontwikkelen van een cyberdefensieconcept voor civiele missies in het kader van het GVDB en dit integreren in de strategische planning;
- de cyberdefensievermogens van civiele missies in het kader van het GVDB versterken, waarbij op bestaande infrastructuur zal worden voortgebouwd en de standaardisering en harmonisatie van de bij GVDB-missies en -operaties gebruikte technologieën zal worden bevorderd en, in voorkomend geval, profijt zal worden getrokken van de deskundigheid van het CERT-EU, Enisa en het EDA;
- bij de versterking van het civiele GVDB nader bekijken of civiele missies in het kader van het GVDB de gastlanden mogelijkerwijs bijstand inzake cyberbeveiliging kunnen verlenen.

De EDEO zal:

- voortwerken aan het ontwikkelen van gemeenschappelijke behoeften voor militaire en civiele missies en operaties in het kader van het GVDB;
- de coördinatie van cyberdefensie verbeteren ter verwezenlijking van doelstellingen in verband met de bescherming van netwerken die worden gebruikt door het GVDB ondersteunende institutionele actoren van de EU, en daarbij gebruik maken van bestaande, in de gehele EU opgedane ervaringen;
- middelenbehoeften en andere relevante beleidsbeslissingen regelmatig opnieuw bezien op basis van de veranderende dreigingsomgeving, in overleg met de lidstaten en andere EU-instellingen.

3. Bevorderen van civiel-militaire samenwerking

De cyberspace is een zich snel ontwikkelend domein: technologische ontwikkelingen moeten worden geschraagd door beveiligingssystemen, zowel op civiel als op militair gebied. Er moet in de mate van het mogelijke worden voorzien in coördinatie tussen het civiel en het militair domein in gevallen waarin soortgelijke technologische ontwikkelingen oplossingen voor civiele en militaire toepassingen opleveren. In andere gevallen zijn militaire vermogens en wapensystemen zo specifiek dat er geen uitwisseling met civiele technologieën mogelijk is. Zonder afbreuk te doen aan de interne organisatie en wetgeving van de lidstaten kan civiel-militaire samenwerking op cybergebied worden overwogen voor onder meer de uitwisseling van beste praktijken, de uitwisseling van informatie, mechanismen voor vroegtijdige waarschuwing, risicobeoordelingen in het kader van incidentenrespons en bewustmaking, alsmede voor opleiding en oefeningen.

Een betere civiele cyberbeveiliging is een belangrijk element dat bijdraagt tot een in het algemeen robuustere netwerk- en informatiebeveiliging. De richtlijn inzake netwerk- en informatiebeveiliging (NIB) zorgt voor grotere paraatheid op nationaal niveau en intensievere samenwerking op Unieniveau tussen de lidstaten op zowel strategisch als operationeel niveau. Bij deze samenwerking zijn zowel nationale instanties die toezicht houden op het cyberbeveiligingsbeleid als nationale CERT's en het CERT-EU betrokken. De samenwerking tussen civiele en militaire CERT's moet worden versterkt, terdege rekening houdend met deze ontwikkelingen. De nieuwe cyber-beveiligingsverordening van de EU strekt ertoe de weerbaarheid van Europa tegen cyberaanvallen te verbeteren en te voorzien in een kader voor cyberbeveiligingscertificering van producten en diensten, waardoor het vertrouwen in de civiele digitale omgeving wordt versterkt.

Het EDA, het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa), het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) en het CERT-EU, samen met andere relevante EU-organen en -instanties, binnen hun respectieve mandaten en zonder overlappingen met de bevoegdheden van de lidstaten, alsmede de lidstaten worden aangemoedigd hun samenwerking verder te versterken op de volgende gebieden:

- het ontwikkelen van gemeenschappelijke competentieprofielen voor cyberbeveiliging en cyberdefensie, op basis van internationale beste praktijken en door de EU-instellingen, -organen en -instanties gebruikte certificering, mede rekening houdend met certificeringsnormen van de particuliere sector;
- het helpen ontwikkelen en aanpassen van in de openbare sector geldende organisatorische en technische normen inzake cyberbeveiliging en cyberdefensie voor gebruik in de defensie- en beveiligingssector. Waar nodig moet worden voortgebouwd op de lopende werkzaamheden van het Enisa en het EDA;
- het opzetten of verder ontwikkelen van operationele mechanismen en regelingen voor de uitwisseling van beste praktijken, met name inzake onderwijs, opleiding en oefeningen, alsmede op gebied van onderzoek en technologie en andere gebieden waarop in civiel-militaire synergieën is voorzien;
- gebruik maken van de bestaande ervaringen van de EU inzake preventie van cybercriminaliteit, onderzoek en forensische capaciteiten, en het intensievere gebruik ervan bij de ontwikkeling van cyberdefensievermogens.

De lidstaten zullen, op vrijwillige basis:

- de samenwerking tussen civiele en militaire CERT's tussen de lidstaten onderling versterken.

De EDEO, de Commissie en de lidstaten zullen:

- cyberdefensie integreren in de procedures voor crisis- en rampenbeheersing van de EU (via het blauwdrukproces).

4. Onderzoek en technologie

Exploitanten van infrastructuur en ICT-diensten (informatie- en communicatiediensten) voor civiele en defensiedoeleinden worden geconfronteerd met soortgelijke uitdagingen op het gebied van cyberbeveiliging, omdat de technologische en operationele vermogensbehoeften dezelfde zijn. Gemeenschappelijke O&T-behoeften en gemeenschappelijke systeemvereisten worden van tevoren gepland om de interoperabiliteit van systemen op lange termijn te verbeteren en de kosten voor het ontwikkelen van oplossingen te beperken. Er moeten schaalvoordelen worden verwezenlijkt om het steeds toenemende aantal dreigingen en zwakke punten het hoofd te kunnen bieden. Dit moet op zijn beurt het behoud en de groei van een concurrerende cyberdefensiesector in Europa vergemakkelijken.

De ontwikkeling van cyberdefensievermogens heeft een belangrijke O&T-dimensie. In het kader van de onderzoeksagenda voor cyberdefensie (CDRA) heeft het EDA een solide basis geleverd voor de prioritering van toekomstige O&T-financiering binnen het intergouvernementeel kader. De daaropvolgende strategische onderzoeksagenda die in de betrokken ad-hocwerkgroep van het EDA is ontwikkeld, voorziet in een weloverwogen prioritering van cybergerelateerde technologieën die nodig zijn op militair gebied, en brengt tegelijk mogelijkheden in kaart voor inspanningen inzake tweeërlei gebruik en investeringen, in een context van nationale, multinationale of EU-financiering.

Het is van essentieel belang technologische vermogens in Europa te ontwikkelen om dreigingen en zwakke punten te ondervangen. De industrie zal de belangrijkste aanjager van cyberdefensie-gerelateerde technologie en innovatie blijven. De aandacht moet onder meer gaan naar cryptografie, ingebedde systemen, opsporing van kwaadaardige software, simulatie- en visualisatietechnieken, bescherming van netwerk- en communicatiesystemen, identificatie- en authentificatietechnologie. Het is tevens van belang bij te dragen tot een concurrerende Europese industriële toeleveringsketen voor cyberbeveiliging door de deelname van kleine en middelgrote ondernemingen (kmo's) te ondersteunen.

Ons vermogen om baanbrekende innovatie te stimuleren aan de hand van zowel nationale als EU-instrumenten, zoals de Europese Innovatieraad, bepaalt mede of we kunnen waarborgen dat Europa zich inzake technologische capaciteiten op cybergebied kan blijven meten met internationale concurrenten.

Teneinde civiel-militaire samenwerking bij de ontwikkeling van cyberdefensievermogens te vergemakkelijken, de Europese technologische en industriële defensiebasis te versterken[10], en bij te dragen tot de strategische autonomie van de EU, ook op het gebied van cyberspace, waar en indien nodig, en met partners overal waar mogelijk**,**

Het EDA, de Commissie en de lidstaten zullen:

- streven naar synergieën van O&T in de militaire sector met civiele onderzoeks- en ontwikkelingsprogramma's, in het bijzonder die welke gericht zijn op baanbrekende innovaties, en de cyberbeveiligings- en cyberdefensiedimensie in aanmerking nemen bij de uitvoering van de voorbereidende actie inzake defensieonderzoek;
- onderzoekagenda's inzake cyberveiligheid (bv. de strategische onderzoeksagenda inzake cyberbeveiliging van het Europees Defensieagentschap), alsook de daaruit resulterende routekaarten en acties delen; daartoe zal een sectoroverschrijdende onderzoeksagenda inzake cyberdefensie worden ontwikkeld, in nauwe samenwerking met de Commissie en de lidstaten;
- bijdragen tot een betere integratie van cyberbeveiligings- en cyberdefensieaspecten in programma's die een beveiligings- en defensiedimensie voor tweeërlei gebruik hebben, zoals het ATM-onderzoeksproject voor het gemeenschappelijk Europees luchtruim (*Single European Sky Air Traffic Management Research* - Sesar).

[10] Mededeling "Naar een meer competitieve en efficiënte defensie- en veiligheidssector" (doc. COM (2013) 542).

De Commissie zal:

- de oprichting overwegen van een Europees industrieel, technologisch en onderzoeks-kenniscentrum voor cyberbeveiliging met een netwerk van nationale coördinatiecentra ter ondersteuning van de technologische en industriële capaciteiten voor cyberbeveiliging en ter vergroting van het concurrentievermogen van de Europese cyberbeveiligingsindustrie, waarbij voor complementariteit wordt gezorgd en dubbel werk binnen het netwerk van kenniscentra voor cyberbeveiliging en met andere EU-agentschappen wordt vermeden; dit centrum dient onder meer de samenwerking tussen civiele en defensietechnologieën en -toepassingen te vergroten, en daarbij in volledige complementariteit nauw met het Europees Defensieagentschap samen te werken op het gebied van cyberdefensie;
- de ontwikkeling steunen van industriële ecosystemen en innovatieclusters die de gehele beveiligingswaardeketen bestrijken, en wel door een beroep te doen op academische kennis, innovatie door kleine en middelgrote ondernemingen, en industriële productie.

De Commissie zal in samenwerking met de lidstaten:

- cyberdefensiekwesties aan de orde stellen in de oproepen tot het indienen van voorstellen in het kader van de voorbereidende actie inzake defensieonderzoek;
- cyberdefensie in aanmerking nemen in de onderwerpen die in het Europees Defensiefonds aan de orde komen;
- de samenhang van het EU-beleid ondersteunen opdat technische en beleidsaspecten van EU-cyberbeveiliging centraal blijven staan in technologische innovatie, alsook in de gehele EU geharmoniseerd worden (analyse en beoordelingsvermogen inzake cyberdreigingen, "*security by design*"-initiatieven, afhankelijkheidsbeheer voor toegang tot technologie enz.);

5. Verbeteren van de mogelijkheden op het gebied van onderwijs, opleiding en oefeningen

Om beter voorbereid te zijn op cyberdreigingen en tot een gemeenschappelijke cyberdefensie-cultuur in de gehele EU te komen - waarvan ook EU-missies en -operaties profiteren - moeten de opleidingsmogelijkheden op het gebied van cyberdefensie worden verbeterd en opgewaardeerd. Het is van het grootste belang dat de onderwijs- en opleidingsbudgetten efficiënt worden aangewend en de hoogst mogelijke kwaliteit opleveren. Het bundelen en delen op Europees niveau van onderwijs en opleiding in cyberdefensie zal cruciaal zijn.

De Europese Veiligheids- en defensieacademie (EVDA), de EDEO, het EDA, de Commissie en de lidstaten zullen:

- op basis van de door het EDA verrichte analyse van de opleidingsbehoeften inzake cyberdefensie en op basis van de ervaringen met opleidingen van de EVDA inzake cyberbeveiliging , voorzien in opleiding en onderwijs in het kader van het GVDB voor verschillende doelgroepen, waaronder de EDEO, het personeel van GVDB-missies en -operaties en ambtenaren van de lidstaten, waarbij ook aandacht moet uitgaan naar het behoud van gekwalificeerd personeel op de korte, middellange en lange termijn;
- voorstellen een cyberdefensiedialoog over opleidingsnormen en certificering op te zetten met de lidstaten, EU-instellingen, derde landen en andere internationale organisaties, alsmede met de particuliere sector;
- samenwerken met Europese aanbieders van opleidingen uit de particuliere sector en met academische instellingen, teneinde de competenties en vaardigheden van personeel in GVDB-operaties en -missies te verbeteren.

De EVDA zal:

- de verdere ontwikkeling van het binnen de EVDA opgerichte platform voor onderwijs, opleiding, evaluatie en oefeningen (het ETEE-platform op cybergebied) ter hand nemen;
- synergieën creëren met de opleidingsprogramma's van andere betrokken partijen zoals het Enisa, Europol, het Agentschap van de Europese Unie voor opleiding op het gebied van rechtshandhaving (Cepol) en het Kenniscentrum voor coöperatieve cyberdefensie van de NAVO;
- nagaan of gezamenlijke opleidingsprogramma's inzake cyberdefensie van de EVDA en de NAVO kunnen worden opgezet die openstaan voor alle EU-lidstaten, teneinde een gedeelde cyberdefensiecultuur te bevorderen;

De Commissie zal:

- de opties nagaan om de door het digitale ETEE-platform op cybergebied in kaart gebrachte opleidings- en onderwijsmogelijkheden in de lidstaten te verbeteren;

Het EDA zal:

- in samenwerking met de EVDA EDA-opleidingen verder ontwikkelen om tegemoet te komen aan de behoeften van de lidstaten inzake onderwijs, opleiding en oefeningen op het gebied van cyberveiligheid;
- het ETEE-platform op cybergebied ondersteunen, onder meer door middel van de geleidelijke integratie van onderwijs-, opleidings-, evaluatie- en praktijkmodules op cybergebied die door het EDA zijn ontwikkeld;

De EDEO en de lidstaten zullen:

- zich houden aan de vastgestelde EVDA-certificeringsmechanismen voor opleidings-programma's, in nauw overleg met de bevoegde diensten van de instellingen, organen en agentschappen van de EU, een en ander op basis van bestaande normen en kennis; nagaan of cyberspecifieke modules kunnen worden ontwikkeld in het kader van het militair Erasmus-initiatief.

Militaire en civiele GVDB-actoren moeten betere mogelijkheden krijgen om te oefenen in cyber-defensie. Gezamenlijke oefeningen zijn een instrument om gemeenschappelijke kennis van en inzicht in cyberdefensie te ontwikkelen. Dit zal zorgen voor een grotere paraatheid van de nationale strijdkrachten om te opereren in een multinationale omgeving. Het houden van gezamenlijke cyberdefensie-oefeningen zal tevens interoperabiliteit en vertrouwen helpen opbouwen.

De EDEO, het EDA, het CERT-EU en de lidstaten zullen bijzondere aandacht besteden aan het bevorderen van cyberdefensieaspecten in het GVDB en in andere oefeningen, en zullen daartoe:

- een cyberdefensiedimensie integreren in bestaande oefeningsscenario's voor *Milex* en *Multilayer*;
- regelmatig strategische/politieke oefeningen organiseren zoals *CYBRID 2017*, zulks in samenwerking met de door de EU geleide parallelle en gecoördineerde oefening van de EU (PACE) en technisch-operationele oefeningen zoals *DEFNET*;
- zo nodig een specifieke EU-cyberdefensie-oefening in het kader van het GVDB ontwikkelen en nagaan of coördinatie mogelijk is met pan-Europese cyberoefeningen zoals het door het Enisa georganiseerde CyberEurope;
- blijven deelnemen aan andere multinationale cyberdefensie-oefeningen, zoals *Locked Shields*;
- in overeenstemming met het EU-beleidskader voor oefeningen, relevante internationale partners, zoals de NAVO, uitnodigen;
- regelmatig oefeningen houden op basis van het instrumentarium voor cyberdiplomatie, in het kader waarvan EU-lidstaten hun vermogen kunnen oefenen om te reageren op kwaadwillige cyberactiviteiten.

6. Intensiveren van de samenwerking met relevante internationale partners

In het kader van internationale samenwerking moet er een dialoog komen met internationale partners, meer bepaald de NAVO en andere internationale organisaties, teneinde bij te dragen tot de ontwikkeling van effectieve cyberdefensievermogens. Er dient te worden gestreefd naar een grotere betrokkenheid bij de werkzaamheden in het kader van de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE) en de Verenigde Naties (VN), zodat werk kan worden gemaakt van een strategisch kader voor conflictpreventie, samenwerking en stabiliteit in de cyberspace.

Er is politieke wil in de EU om nader met de NAVO samen te werken aan cyberdefensie, teneinde robuuste en bestendige cyberdefensievermogens te ontwikkelen, zoals verlangd wordt in de gezamenlijke verklaring die op 8 juli 2016 te Warschau is ondertekend door de voorzitter van de Europese Raad, de voorzitter van de Europese Commissie en de secretaris-generaal van de Noord-Atlantische Verdragsorganisatie. Regelmatig overleg op personeelsniveau, cross-briefings en eventuele vergaderingen tussen de Politiek-militaire Groep en de bevoegde NAVO-comités zullen dubbel werk helpen voorkomen en mede zorgen voor samenhang en complementariteit van de werkzaamheden, conform het bovengenoemde samenwerkingskader.

De EDEO en het EDA zullen samen met de lidstaten de samenwerking inzake cyberdefensie tussen de EU en de NAVO verdiepen, met inachtneming van het institutionele kader en de besluitvormingsautonomie van beide organisaties, en zullen daartoe:

- de lopende werkzaamheden in het kader van de uitvoering van de gezamenlijke verklaring van de voorzitter van de Europese Raad, de voorzitter van de Europese Commissie en de secretaris-generaal van de Noord-Atlantische Verdragsorganisatie opvoeren;
- beste praktijken op het gebied van crisisbeheersing en van cyberdefensie in het kader van militaire en civiele missies en operaties uitwisselen;
- werk maken van samenhangende resultaten bij het vaststellen van vermogensbehoeften op het gebied van cyberdefensie in het geval van overlappingen, meer bepaald wat betreft de ontwikkeling van cyberdefensievermogens op lange termijn;
- intensiever gebruik maken van het EDA-kader voor samenwerking met het Kenniscentrum voor coöperatieve cyberdefensie van de NAVO, als eerste platform voor nauwere samenwerking bij multinationale cyberdefensieprojecten, op basis van adequate beoordelingen.

De EVDA, de EDEO en het EDA zullen:

- de samenwerking inzake concepten voor opleiding, onderwijs en oefeningen op het gebied van cyberdefensie verdiepen;
- zorgen voor wederzijdse deelname van het personeel aan oefeningen, conform het overeengekomen samenwerkingskader.

Het CERT-EU zal:

- de technische afspraken tussen het CERT-EU en de responscapaciteit voor computerincidenten van de NAVO (*NATO Computer Incident Response Capability* - NCIRC) verder uitwerken om het situationeel bewustzijn, de informatiedeling en de mechanismen voor vroegtijdige waarschuwing te verbeteren, alsmede dreigingen te ondervangen die gevolgen kunnen hebben voor beide organisaties.

Met betrekking tot andere internationale organisaties en relevante internationale partners van de EU, zullen de EDEO en de lidstaten, indien nodig:

- strategische ontwikkelingen volgen en overleg plegen met internationale partners (internationale organisaties en derde landen) over cyberdefensie-aangelegenheden;
- mogelijkheden verkennen voor samenwerking inzake cyberdefensie-aangelegenheden, onder meer met derde landen die aan GVDB-missies en -operaties deelnemen;
- zich in relevante internationale organisaties, zoals de VN, de OVSE en het Regionaal Forum van de ASEAN, sterk maken voor de toepassing van het vigerende internationaal recht, met name het gehele VN-Handvest, in de cyberspace, voor de uitwerking en uitvoering van universele niet-bindende normen van verantwoordelijk gedrag van staten, en voor regionale maatregelen tot vertrouwensopbouw tussen staten teneinde de transparantie te vergroten en het risico op verkeerde percepties van overheidsgedrag te verminderen.

De Commissie en de EDEO zullen:

- in voorkomend geval, de opbouw van cybercapaciteit ten behoeve van de partners van de EU steunen via het gewijzigde instrument voor bijdrage aan stabiliteit en vrede (IcSP).

Vervolg

Ten vervolge op de EDEO-coördinatie van het CDPF zullen de EDEO, het EDA en de Commissie jaarlijks aan de Politiek-militaire Groep, met deelname van de leden van de Horizontale Groep cybervraagstukken, en aan het Politiek en Veiligheidscomité een voortgangsverslag over de zes hierboven genoemde gebieden voorleggen waarin de uitvoering van het CDPF wordt geëvalueerd. Ook zal er een halfjaarlijkse mondelinge presentatie plaatsvinden.

Naarmate de cyberdreiging evolueert, moeten er nieuwe behoeften voor cyberdefensie worden vastgesteld, die vervolgens in het CDFP worden opgenomen. De volgende herziening van het CDPF moet uiterlijk medio 2022 worden voorgelegd en dient in nauw overleg met de lidstaten tot stand te komen.