Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 3584 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 december 2022

Overeenkomstig de bestaande afspraken ontvangt u hierbij 5 fiches die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissie voorstellen (BNC).

Fiche: Verordening dataverzameling en -deling kortetermijnverhuur accommodatie (Kamerstuk 22 112, nr. 3581)

Fiche: Verordening aanscherping typegoedkeuring voor personenauto's, bestelwagens, vrachtwagens en bussen (Euro 7) (Kamerstuk 22 112, nr. 3582)

Fiche: Mededeling meststoffen (Kamerstuk 22 112, nr. 3583)

Fiche: Mededeling EU-Beleid Cyber Defensie

Fiche: Mededeling Actieplan Militaire Mobiliteit 2.0 (Kamerstuk 22 112, nr. 3585)

De Minister van Buitenlandse Zaken,
W.B. Hoekstra

kst-22112-3584
ISSN 0921 - 7371
's-Gravenhage 2022

Fiche: Mededeling EU-Beleid Cyber Defensie

1. Algemene gegevens

a) *Titel voorstel*
Gezamenlijke Mededeling aan het Europees Parlement en de Raad: Het EU-beleid op het gebied van cyberdefensie
b) *Datum ontvangst Commissiedocument*
10 november 2022
c) *Nr. Commissiedocument*
JOIN(2022) 49 final
d) *EUR-Lex*
https://eur-lex.Europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022JC0049&qid=1668607061632
e) *Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing*
Niet opgesteld
f) *Behandelingstraject Raad*
Raad Buitenlandse Zaken
g) *Eerstverantwoordelijk ministerie*
Ministerie van Defensie

2. Essentie voorstel

De oorlog in Oekraïne benadrukt het belang van gedegen cyber weerbaarheid in Europa en legt de verwevenheid van civiele en militaire, digitale en fysieke infrastructuur bloot. De Europese Commissie (hierna: de Commissie) en de Hoge Vertegenwoordiger (HV) willen middels deze mededeling de samenwerking tussen militaire en civiele cybergemeenschappen in de EU vergroten en benadrukken het belang van samenwerking met de private sector. Ook worden lidstaten opgeroepen met spoed meer te investeren in hun (actieve) cyberdefensievermogen. Het EU-beleid op het gebied van cyberdefensie werd aangekondigd in het Strategisch Kompas[1] met als doel om strijdkrachten, burgers en EU-crisismanagementmissies en operaties te beschermen tegen cyberaanvallen.

De mededeling rust op vier pilaren. Ten eerste beoogt het de samenwerking te bevorderen tussen nationale en Europese defensieactoren binnen het cyberdomein. Daarbinnen worden de acties onderscheiden in cyberdefensie acties en civiele ondersteuningsacties. Hier worden suggesties gedaan voor nieuwe samenwerkingsverbanden om actoren binnen cyberdefensie bij elkaar te brengen. Zo wordt voorgesteld om de gezamenlijke informatiepositie en het situationeel bewustzijn binnen de defensiegemeenschap te versterken door middel van de oprichting van een EU Coördinatiecentrum voor cyberdefensie (EUCDCC), door de verdere ontwikkeling en versterking van een EU-conferentie van cybercommandanten en door de oprichting van een operationeel netwerk «MICNET» bestaande uit militaire computercrisisteams (*milCERTs)*.

Ook bevat de tekst voorstellen om EU militaire structuren beter in contact te brengen met Europese civiele netwerken, zoals de EU-conferentie van cybercommandanten met CyCLONe[2], en EU-NAVO samenwerking te verbeteren, door samenwerking tussen het NATO *Computer Incident*

---

[1] ST 7371/22, «Een strategisch kompas voor veiligheid en defensie – Voor een Europese Unie die haar burgers, warden en belangen beschermt en bijdraagt aan de internationale vrede en veiligheid».
[2] Cyber Crisis Liaison Organisation Network (CyCLONe), het Europees netwerk van verbindingsorganisaties voor grootschalige cyberincidenten en -crises.

Response Capability Technical Centre (NCIRC TC) en CERT-EU. Tot slot beschrijft het voorstel een op te richten EU initiatief voor cybersolidariteit, waarvoor de Commissie een – mogelijk wetgevend – voorstel voorbereidt om de uitrol van een EU-infrastructuur van operationele beveiligingscentra (SOC's) te bevorderen. Het EU initiatief voor cybersolidariteit zou volgens de Commissie kunnen resulteren in wettelijke wijzigingen in het programma Digitaal Europa (DEP). Wat deze wettelijke wijzigingen in zullen houden is nog niet helder. Het EU initiatief voor cybersolidariteit zou verder ook kunnen ondersteunen in het geleidelijk opzetten van een cyberreserve op EU-niveau met diensten van vertrouwde particuliere aanbieders, de verdere uitwerking van het concept van snelle reactie teams bij cyberincidenten (gebaseerd op een lopend PESCO[3] project CRRT) en een project voor gezamenlijke EU-brede cyberweerbaarheidsoefeningen (*CyDef-X*).

Ten tweede stelt de mededeling zich ten doel om het digitale ecosysteem beter te beschermen. Om bredere weerbaarheid te bevorderen, wordt onder meer voorgesteld om (niet-bindende) aanbevelingen voor cyberveiligheid standaarden voor de defensiesector te ontwikkelen. Ook zullen aanbevelingen voor interoperabiliteit vereisten en risico-scenario's voor kritieke infrastructuur worden ontwikkeld en wordt civiel-militaire samenwerking gestimuleerd voor de ontwikkeling van geharmoniseerde standaarden voor *dual-use* producten.

Ten derde roept de mededeling op tot investeringen in cyberdefensie capaciteiten. De mededeling benoemt verschillende manieren om richting te geven aan strategische investeringen zoals via een routekaart voor kritieke technologieën voor veiligheid en defensie («de routekaart»), prioritering in capaciteitsontwikkeling en strategische assessments. Er wordt een oproep gedaan aan de lidstaten om in dit verband beter gebruik te maken van bestaande kaders voor samenwerking (o.a. CARD, PESCO, EDF). Tot slot is de Commissie voornemens om in 2023 een academie voor cybervaardigheden op te richten. Dit initiatief is bedoeld om de tekorten in de cybersecurity-arbeidsmarkt te reduceren door diverse initiatieven op het gebied van trainingen, bij- en omscholingen en digitale vaardigheden bijeen te brengen.

Ten vierde beogen de Commissie en HV om nieuwe partnerschappen aan te gaan of bestaande partnerschappen te versterken. De mededeling spreekt ook over de ambitie om de EU-NAVO relatie op het gebied van cybersecurity te verdiepen op basis van complementariteit en interoperabiliteit, onder andere door het uitwisselen van personeel. Ook is er aandacht voor gelijkgestemde partners, specifiek de Verenigde Staten en Oekraïne. Als laatste is er aandacht voor partnerlanden in den brede, met het oog op veiligheid- en defensiesamenwerking via de Europese Vredesfaciliteit (EPF).

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

Nederland heeft in de Defensienota 2022 aangegeven grote ambities te hebben op het gebied van EU veiligheid en defensiebeleid, onderbouwd door grote investeringen in mensen en middelen. Nederland was dan ook voorstander van het in maart 2022 aangenomen EU Strategisch Kompas. Versterking van de Europese weerbaarheid, inclusief op cyberterrein, maakt hier onderdeel van uit. In de Defensienota 2022[4] wordt, onder de

[3] Permanent Structured Cooperation.
[4] Kamerstuk 36 124, nr. 1.

actielijn informatiegestuurd werken en optreden, ingezet op het uitbreiden van cybercapaciteiten, digitaal innoverend vermogen, nieuwe technologieën, meer Europese samenwerking en het verhogen van de *cyber-readiness* van Defensie.

Het Cybersecurity Beeld Nederland (CSBN2022) erkent dat de digitale ruimte nauw verbonden is met geopolitiek en gebruikt wordt door staten voor hun strategische belangenbehartiging op onder andere militair en economisch gebied. Staten voeren digitale aanvallen uit om te spioneren of om te kunnen saboteren. De dreiging van cyberaanvallen uit onder andere Rusland en China is groter dan ooit. De Tijdelijke Wet cyberoperaties speelt hier op in door de inlichtingendiensten AIVD en MIVD meer mogelijkheden te geven om in te grijpen. Naar aanleiding van de bevindingen van de Evaluatie Commissie WIV (2021) zal later een uitgebreide herziening van de Wet op de Inlichtingen- en Veiligheidsdiensten plaatsvinden. Gezien de urgentie kiest het kabinet ervoor zaken al eerder te regelen met deze tijdelijke wet.

Daarnaast schetst de Nederlandse Cybersecuritystrategie (NLCS)[5], waarvoor het (CSBN2022) als uitgangspunt ter formulering van de probleemstellingen dient, de bredere Nederlandse inzet op het realiseren van een digitaal veilige samenleving. De NLCS benadrukt ook het belang van veilige en innovatieve digitale producten en diensten. Dit komt momenteel tot uiting via de implementatietrajecten van de Netwerk en Informatie Beveiligingsrichtlijn (NIB2) en de onderhandelingen omtrent de verordening cyberweerbaarheid (CRA). De CRA[6] beoogt hardware- en software producten met digitale elementen te voorzien van horizontale robuuste cybersecurity voorwaarden. Producten die exclusief zijn ontwikkeld voor de nationale veiligheid, militaire doeleinden of om gerubriceerde informatie te verwerken vallen buiten de reikwijdte. De NIB2-richtlijn heeft als doel om de weerbaarheid in het digitale domein van vitale aanbieders en de vitale infrastructuur binnen de EU naar een hoger gemeenschappelijk niveau brengen. Ook stelt de NLCS als doel om (internationaal) digitale dreigingen van criminelen en staten tegen te gaan, bij voorkeur in samenwerking en door coalities met EU- en NAVO-partners. Daarnaast zet het kabinet zich binnen de EU in voor intensieve diplomatieke samenwerking in het kader van cyberweerbaarheid (*Cyber Diplomacy Toolbox*). Zo kan de EU gezamenlijke restrictieve maatregelen in de vorm van een inreisverbod en bevriezen van financiële tegoeden opleggen aan kwaadwillende hackers, waardoor zij voortaan persoonlijke gevolgen ondervinden van hun gedrag. NL maakt zich momenteel in EU verband hard voor de doorontwikkeling c.q. uitbreiding van het instrumentarium van de Toolbox.

b) Beoordeling + inzet ten aanzien van dit voorstel

Het kabinet verwelkomt de mededeling van de Commissie en de HV die moet bijdragen aan betere bescherming van de EU en haar lidstaten tegen cyberaanvallen. Dit is des te meer zo omdat cyberdreigingen steeds complexer worden en groeien in reikwijdte, frequentie en verfijning. Het versterken van samenwerking tussen de EU en de lidstaten op het gebied van capaciteitsontwikkeling, kennisdeling en kennisontwikkeling in het cyberdomein bevordert een gedeeld omgevingsbewustzijn en dreigingsbeeld. Dit faciliteert de ontwikkeling van gedeelde handelingsperspectieven en verhoogt de slagkracht van de EU en de lidstaten. Zelfstandige Europese capaciteiten zijn benodigd om een krachtig en volwaardige partner te zijn in de trans-Atlantische relatie. Gelet op de focus op

[5] Kamerstuk 26 643, nr. 925.
[6] Kamerstuk 22 112, nr. 3552.

civiel-militaire samenwerking in het voorstel, benadrukt het kabinet het belang van goede samenhang met en aansluiting bij bestaande initiatieven en het voorkomen van duplicatie tussen NAVO-EU initiatieven en tussen het militaire en civiele terrein. Het kabinet zal vragen om verduidelijking ten aanzien van een aantal genoemde initiatieven. Dit betreft met name de inkadering, respectievelijke rollen en verantwoordelijkheden van de betrokken partijen, en de financiering ervan.

Ten aanzien van de samenwerking tussen nationale en EU cyberdefensie actoren onderschrijft het kabinet het belang om waar mogelijk en wenselijk civiel-militaire samenwerking te verbeteren. Daarbij moet op het terrein van nationale veiligheid en defensie altijd oog worden gehouden voor de bijzondere nationale bevoegdheden en taken. Voor wat betreft de betrokkenheid van civiele organisaties met (civiel-militaire) samenwerking op EU-niveau, zal het kabinet er op letten dat deze onderdelen geen afbreuk doen aan de uitsluitende verantwoordelijkheid van lidstaten. Specifiek in het cyberdomein, waar snel handelen noodzakelijk is en met gerubriceerde informatie wordt omgegaan, ziet het kabinet grote toegevoegde waarde in Europese samenwerking, maar is het van belang bij alle samenwerkingsverbanden zorgvuldig alle waarborgen, zoals een aanwezige juridische grondslag en een duidelijke beschrijving van rollen en bevoegdheden van betrokken actoren, in acht te nemen. Dit geldt des te meer bij (beoogde) betrokkenheid van civiele partijen. Voor wat betreft het voorstel van een EU Coördinatiecentrum voor Cyberdefensie (EUCDCC) ziet het kabinet veel mogelijkheden om een gedeeld dreigingsbeeld te ontwikkelen en zo gezamenlijke slagkracht te vergroten. De EU is geschikt om hier een faciliterende rol in nemen. Wel acht het kabinet het van belang dat duplicatie in de voorgestelde samenwerking met civiele structuren wordt vermeden. Ook spreken de Commissie en HV over het opzetten van een onafhankelijk actief informatietechnologiesensorsysteem binnen het EUCDCC om een 24/7 operationeel beeld van cyberspace mogelijk te maken ter ondersteuning van militaire GVDB-missies en -operaties. Hoewel de EU-instellingen zorg moeten dragen voor de eigen informatiebeveiliging, wil het kabinet ervoor waken dat de EU zonder juridische grondslag eigen sensoren gaat opstellen om CTI te verzamelen. In de mededeling staan meerdere voornemens voor het oprichten van instrumenten zoals het EUDCC, SOCs, MICNET etc. die strekken tot vergaande verzameling van kennis afkomstig uit het militaire en civiele domein via cybermiddelen, en tot het delen tussen deze actoren van deze kennis. Hoewel het kabinet zich actief ten doel stelt om vaker internationaal inlichtingen te delen, zal het aandacht vragen voor een toereikende juridische grondslag voor bovengenoemde initiatieven, evenals voor de bescherming van persoonsgegevens. Voor wat betreft de verdere uitwerking van heet EU Cybersolidariteitsinitiatief ontvangt het kabinet graag meer informatie van de Commissie, onder andere met betrekking tot de benodigde middelen.

Het kabinet ziet meerwaarde in de interactie tussen het EU-conferentie van cybercommandanten met het CyCLONe netwerk om wederzijds begrip te vergroten en *best practices* te delen. Het kabinet vraagt wel nader inzicht van de Commissie te krijgen in de voor- en nadelen van een dergelijke koppeling. Voor het voorgestelde CyDef-X project acht het kabinet synergie met het civiele domein van belang. Het kabinet ziet toegevoegde waarde in directe lijnen tussen MIL CERTS, zeker met het oog op de defensiegemeenschap en bij CSDP-missies en -operaties. Nederland heeft in november jl. getekend voor deelname aan dit project. Het project zal een netwerkomgeving opleveren waarbinnen de MilCERTs van alle deelnemende landen Cyber Threat Intel (CTI) kunnen delen, security maatregelen kunnen uitwisselen en beter kunnen reageren op cyberdreigingen. Het is daarbij van belang dat er goed gecoördineerd

wordt met bestaande CTI platforms om inlichtingen-echo's[7] te voorkomen. Het kabinet steunt de uitwerking en uiteindelijke inbedding van lopende PESCO-projecten in de EU institutionele structuren, mits deze gepaard gaan met gedegen evaluaties met oog voor *lessons learned.* Dit betreft bijvoorbeeld het PESCO-project *Cyber Rapid Response Teams en Mutual Assistance in Cyber Security* (CRRT) en uitwerking van het PESCO-project *Cyber and Information Domain Coordination Centre* (CIDCC). Nederland onderschrijft de ambities van deze projecten en is dan ook deelnemer aan beide projecten. Het kabinet heeft nog wel vragen over de governance en financiering. Tot slot ziet het kabinet sterke meerwaarde in voorstellen om met elkaar te oefenen in het cyberdomein. Dat versterkt de professionaliteit en wederzijds vertrouwen. Wel benadrukt het kabinet om binnen de geldende juridische kaders de mogelijkheden voor oefenen in het cyberdomein goed in te kleden.

De nog in onderhandeling zijnde Cyber Resilience Act (CRA) en de recentelijk vastgestelde Netwerk en Informatie Beveiligingsrichtlijn (NIB-2) leggen de basis voor breed gedragen cybersecurity-basismaatregelen bij verschillende organisaties maar kennen een uitzondering voor Defensie. De HV, als hoofd van het Europees Defensieagentschap (EDA), wil, met behulp van de Commissie, (niet-bindende) aanbevelingen voor de defensieorganisaties van de lidstaten ontwikkelen. Voor wat betreft de beoogde aanbevelingen voor cybersecurity-standaarden en basismaatregelen voor de defensie cyber security sector, het ontwikkelen van *dual-use* producten en de ontwikkeling van aanbevelingen voor EU cyberdefensie interoperabiliteitsvereisten, ziet het kabinet sterke toegevoegde waarde, maar acht het kabinet het van belang om vrijwilligheid van de toepasselijkheid hiervan te behouden, dit vanwege de noodzakelijke geheimhouding over beveiligingsmaatregelen van Defensie. Voor het kabinet is het ook belangrijk om de samenhang van de mededeling met andere (bestaande of in onderhandeling zijnde) raamwerken te waarborgen. Het kabinet streeft er bijvoorbeeld naar zoveel mogelijk aan te sluiten bij bestaande initiatieven zoals *Federated Mission Networking*, een NAVO-initiatief waarin de normering voor cybersecurity is opgenomen. Cyber securitymaatregelen voor de defensiesector moeten bovendien, gezien de enorme dynamiek van het cyberdomein, in een grote mate van flexibiliteit in de uitvoering voorzien. Het cyberdomein is een cruciale *enabler* op militair strategisch gebied en kan bij gebrek aan maatregelen een risico vormen voor operationele effecten in andere domeinen (land, lucht, zee, ruimte of het cyberdomein zelf). Bezien vanuit de doelstellingen uit de NLCS kan het kabinet het voorstel rondom de nieuwe EU cybersecurity certificeringsschema's voor de cyber security industrie en private partijen steunen, wel zal het kabinet de Commissie vragen stellen over hoe wordt beoogd dit op te zetten.

Ten aanzien van investeringen in cyberdefensie capaciteiten steunt het kabinet het voorstel om bestaande EU-instrumenten, zoals het Europees Defensie Fonds (EDF), in te zetten om gerichte investeringen in digitale weerbaarheid te faciliteren. Dit ligt in lijn met de ambities zoals uitgesproken in de Defensienota 2022. Voor een strategisch autonoom Europa is een vitale defensiesector cruciaal. Het kabinet steunt ook de inzet op het ontwikkelen van vaardigheden en competenties in cybersecurity en cyberdefensie op de arbeidsmarkt door onder andere het om- en bijscholen van professionals. Dit versterkt de positie van de EU in de mondiale cyber-defensie-industrie. Deze focus op het versterken van de cybersecuritykennis- en innovatieketen en de cybersecurity-arbeidsmarkt is ook in lijn met de Nederlandse Cybersecuritystrategie. In het licht van

[7] Meermaals gedeelde inlichtingen die ten onrechte worden toegeschreven aan verschillende bronnen en zo artificieel de inlichtingenwaarde van de informatie versterken.

de NLCS steunt het kabinet de oprichting van een *EU Cyber Skills Academy*, waarbij duplicatie tussen bijvoorbeeld het werk van ENISA en het *European Cyber Defence College* moet worden voorkomen.

Tot slot kan het kabinet zich vinden in de brede partnerschappen die worden toegelicht in de laatste pijler. Nederlandse veiligheid is ingebed in de NAVO en de EU. Om onnodige duplicatie te voorkomen en in te zetten op complementariteit en interoperabiliteit, is goede internationale en bondgenootschappelijke afstemming vereist. Samenwerking met de NAVO hoort dus ook nauwkeurig toegelicht en uitgewerkt terug te komen in het voorstel. Ook mag het belang van het strategische partnerschap met de Verenigde Staten niet worden onderschat, dit geldt ook voor andere partners zoals het Verenigd Koninkrijk, Noorwegen, Canada en Australië. Het kabinet steunt initiatieven op het gebied van capaciteitsontwikkeling voor partnerlanden. Dit sluit aan bij de ontwikkelingssamenwerkingsagenda. Cyberveiligheid elders in de wereld draagt bij aan de cyberveiligheid in Nederland en de EU.

c) Eerste inschatting van krachtenveld

Er is op dit moment nog beperkt zicht op het Brusselse krachtenveld over de verschillende onderdelen van het voorstel van de Commissie. Wel is er momenteel een sterk momentum voor meer Europese defensiesamenwerking. De grote lijnen van het voorstel worden dan ook met enthousiasme verwelkomd door lidstaten die meerwaarde zien in internationale samenwerking binnen cyberdefensie. Uit eerste discussies blijkt dat veel lidstaten initiatieven ten behoeve van betere samenwerking tussen het civiele en militaire domein toejuichen. Meerdere landen vragen naar de juridische basis van de voorgestelde initiatieven en hebben zorgen over duplicatie van initiatieven en activiteiten. In bredere zin zijn meerdere Lidstaten beducht voor de groeiende rol van de Commissie op defensievlak, met het oog op het behoud van de exclusieve nationale bevoegdheden op dit terrein. Concreet bouwen enkele voorstellen voort op succesvolle, lopende PESCO-projecten waarvan het aanneembaar is dat de deelnemende lidstaten deze voorstellen zullen steunen, zoals in het geval van de *Cyber Rapid Response Teams* (CRRT) (zeven deelnemende landen) en de Cyber and Information *Domain Coordination Centre* (CIDCC) (vier deelnemende landen). Vragen van lidstaten zien voornamelijk op de voorgestelde samenwerking van het civiele en militaire domein, het voorgestelde cybersolidariteitsmechanisme en de samenhang tussen het nieuwe EU Cyberdefensie Coördinatiecentrum en andere (bestaande) initiatieven om cybersecurity te versterken.

4. Grondhouding ten aanzien van bevoegdheid, subsidiariteit, proportionaliteit, financiële gevolgen en gevolgen op het gebied van regeldruk en administratieve lasten

a) Bevoegdheid

De grondhouding van het kabinet ten aanzien van de bevoegdheid is positief. De mededeling heeft betrekking op het terrein van het EU Gemeenschappelijk Veiligheids- en Defensiebeleid (GVDB). Het GVDB valt onder het Gemeenschappelijk Buitenlands en Veiligheidsbeleid (GBVB). Op het terrein van het GBVB zijn de lidstaten bevoegd om extern naast de Unie op te treden (artikel 2, lid 4, VWEU). Voor zover de EU een positie heeft ingenomen, dienen de lidstaten deze te respecteren.

b) Subsidiariteit

Het kabinet heeft een positieve grondhouding ten aanzien van de subsidiariteit van de mededeling. Het doel van de mededeling is om bij te dragen aan de versterking van de cyber defensie capaciteiten (digitale veiligheid en weerbaarheid) van de EU en haar lidstaten. Met het oog op het grensoverschrijdende karakter van het cyberdomein en de groeiende complexiteit, reikwijdte en frequentie van cyberdreigingen is een Europese aanpak op het gebied van cyber veiligheid en defensie gerechtvaardigd. Door middel van optreden op EU-niveau ontstaat er meer slagklacht om tegen cyberdreigingen op te treden dan door middel van optreden door afzonderlijke lidstaten (op centraal, regionaal of lokaal niveau). In aanvulling op en in samenhang met de al aanwezige samenwerkingsgremia en initiatieven, kan dit doel naar het oordeel van het kabinet het beste worden verwezenlijkt door optreden op EU-niveau.

c) Proportionaliteit

De grondhouding van het kabinet is positief. De mededeling heeft tot doel om bij te dragen aan de versterking van de cyberdefensie capaciteiten van de EU en de lidstaten. Het beleid in de mededeling en de acties die de Commissie en de HV voorstellen zijn over het algemeen geschikt om bij de lidstaten en de EU bij te dragen aan de versterking van de cyberdefensie capaciteiten. Dit geldt bijvoorbeeld voor het voorstel om EU Coördinatiecentrum voor cyberdefensie op te richten, de versterkte interactie tussen het EU-conferentie van cybercommandanten met het CyCLONe netwerk en de voorstellen om met elkaar te oefenen in het cyberdomein. Bovendien gaat het optreden niet verder dan noodzakelijk, omdat het optreden zich beperkt tot capaciteitsontwikkeling, kennisdeling en kennisontwikkeling en omdat er op verschillende terreinen aansluiting wordt gezocht bij al bestaande samenwerkingsgremia en initiatieven. Het kabinet merkt daarbij op dat ten aanzien van de voorgestelde civiel-militaire samenwerking op het gebied van EU-crisismanagement de samenwerking tussen lidstaten al plaatsvindt binnen al reeds bestaande netwerken. Het kabinet ziet daarom met name meerwaarde in civiel-militaire samenwerking die aansluit bij al bestaande structuren zoals het CSIRTs Network en CyCLONe.

d) Financiële gevolgen

Nederland is van mening dat de middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2021–2027 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting. Het voorstel bespreekt in algemene zin vier pijlers waarbinnen lidstaten cyberdefensie/ cyber-readiness kunnen versterken. Het kabinet steunt het voorstel om bestaande EU-instrumenten, zoals het Europees Defensie Fonds (EDF), in te zetten om gerichte investeringen in digitale weerbaarheid te faciliteren. Omdat er in deze fase nog geen sprake is van expliciete nationale ambities ten aanzien van dit voorstel zijn er (nog) geen financiële gevolgen voor Defensie te identificeren. Op het moment dat er wel nationale ambities worden geformuleerd zullen deze binnen de huidige vastgestelde financiële middelen moeten worden opgevangen. De budgettaire gevolgen worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline.

e) Gevolgen voor regeldruk en administratieve lasten en concurrentiekracht

Door strategische investeringen in technologieën en het stimuleren van de cybersecurity arbeidsmarkt wordt gewerkt aan een toekomstbestendig economisch (cyber-) ecosysteem. Daarnaast zijn investeringen in strategische technologieën van cruciaal belang in de mondiale strijd om technologisch leiderschap. Technologisch leiderschap stelt ons in staat onze economische en uiteindelijk ook politieke belangen beter te verdedigen en draagt zo bij aan het versterken van onze (economische) weerbaarheid. Zowel een verhoogde cyberweerbaarheid als technologisch leiderschap dragen bij aan de open strategische autonomie van de EU.