Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

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

Nr. 3182 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 27 augustus 2021

Overeenkomstig de bestaande afspraken ontvangt u hierbij 4 fiches die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissie voorstellen (BNC).

Fiche: Mededeling Eerste lessen Covid-19 pandemie (Kamerstuk 22 112, nr. 3181)
Fiche: Aanbeveling opbouw Joint Cyber Unit
Fiche: Mededeling «Europees Strategisch Kader voor gezondheid en veiligheid op het werk 2021–2027» (Kamerstuk 22 112, nr. 3183)
Fiche: Verordening voor Europese groene obligaties (Kamerstuk 22 112, nr. 3184)

De Minister van Buitenlandse Zaken,
S.A.M. Kaag

kst-22112-3182
ISSN 0921 - 7371
's-Gravenhage 2021

Fiche: Aanbeveling opbouw Joint Cyber Unit

1. Algemene gegevens

a) *Titel voorstel*
AANBEVELING VAN DE COMMISSIE van 23 juni 2021 betreffende de opbouw van een gezamenlijke cybereenheid
b) *Datum ontvangst Commissiedocument*
juni 2021
c) *Nr. Commissiedocument*
COM(2021) 4520
d) *EUR-lex*
https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32021H1086&qid=1625473547638
e) *Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing*
Niet opgesteld
f) *Behandelingstraject Raad*
Raad Algemene Zaken
g) *Eerstverantwoordelijk ministerie*
Ministerie van Justitie en Veiligheid

2. Essentie voorstel

Op 23 juni 2021 heeft de Commissie de aanbeveling inzake het opzetten van een *Joint Cyber Unit* (hierna: «JCU») gepubliceerd. Gelijktijdig met de publicatie van de aanbeveling inzake de JCU heeft de Commissie ook mededelingen gepubliceerd over de voortgang van de implementatie van de EU-strategie inzake cyberbeveiliging en over de voortgang van de implementatie van de EU veiligheidsunie[1]. Deze aanbeveling is eind 2020 aangekondigd als speerpunt van de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk[2], die de Commissie op 16 december 2020, samen met een voorstel tot herziening van de richtlijn inzake de beveiliging van netwerk- en informatiesystemen (NIB-richtlijn) en een richtlijn voor de veerkracht van kritische entiteiten (CER), heeft gepubliceerd en waarvoor BNC-fiches zijn opgesteld die op 12 februari 2021 aan uw Kamer zijn aangeboden. De Commissie constateert dat er nog geen gemeenschappelijk EU-platform bestaat waar informatie, afkomstig uit verschillende cybersecuritygemeenschappen (hierna «gemeenschappen)[3], efficiënt en veilig kan worden uitgewisseld en waar operationele capaciteiten kunnen worden gecoördineerd en gemobiliseerd. Deze aanbeveling strekt tot het opzetten van een JCU, dat geen nieuwe instantie zal worden, maar een virtueel en fysiek platform zal betreffen voor het versterken van de samenwerking tussen de in de aanbeveling geïdentificeerde operationele[4] en ondersteunende[5] deelnemers. De focus ligt daarbij op technische en operationele samenwerking inzake grootschalige cyberincidenten en

---

[1] Communication report on implementation of the EU's cybersecurity strategy for the digital decade and joint communication on the second progress report on the implementation of the EU security union. Over deze mededelingen worden geen BNC-fiches opgesteld.
[2] COM (2020) 18 & Kamerstuk 22 112, nr. 3052.
[3] Samenwerkende civiele, rechtshandhavings-, diplomatie- en defensiegroepen die zowel de lidstaten als de relevante EU-instellingen, -organen en -agentschappen (EU IOA's) vertegenwoordigen, die informatie uitwisselen om gedeelde doelen, belangen en missies met betrekking tot cyberbeveiliging na te streven.
[4] Operationele deelnemers zijn ENISA, Europol, CERT-EU, de Commissie, de Europese Dienst voor extern optreden (EDEO), inclusief het EU-Inlichtingen- en Situatiecentrum (INTCEN), het EU Computer Security Incident Response Teams (CSIRT's) Netwerk (CSIRT-netwerk) en EU-CyCLONE.
[5] Ondersteunende deelnemers zijn de voorzitter van de NIB-samenwerkingsgroep, voorzitter van de Raadswerkgroep Cyber, het Europees Defensieagentschap («EDA») en een afgevaardigde van relevante PESCO-projecten.

-crises.[6] Ten tijde van grootschalige ICT-incidenten ziet de Commissie graag dat alle relevante EU-actoren voorbereid zijn om gecoördineerd te reageren en kunnen rekenen op solidariteit binnen de EU in de vorm van gecoördineerde bijstand. ENISA[7] zal een belangrijke rol krijgen om het opzetten van de JCU te ondersteunen door onder meer te fungeren als secretariaat, en bij te dragen aan de operationalisering. De JCU kent de volgende doelstellingen: zorgen voor een gecoördineerde reactie binnen de EU op grootschalige cyberdreigingen, -incidenten en -crises; verbeteren van het situationeel bewustzijn; en het verbeteren van gezamenlijke paraatheid. Ten behoeve van eerstgenoemde doelstelling stelt de Commissie onder meer de oprichting en de gecoördineerde inzet van *EU Cybersecurity Rapid Reaction Teams* voor. Deze teams zullen in de eerste plaats een beroep doen op de capaciteiten van lidstaten, ondersteund door ENISA, CERT-EU[8] en Europol[9]. Het situationeel bewustzijn en de gezamenlijke paraatheid wil de Commissie onder meer verbeteren door de ontwikkeling van een geïntegreerd verslag van de cybersecuritysituatie in de EU en van een EU-plan voor incident- en crisisrespons dat geacht wordt voort te bouwen op door lidstaten krachtens artikel 7, derde lid, van het voorstel tot herziening van de NIB-richtlijn op te stellen nationale plannen daarvoor[10]. Ook zal de JCU deelnemers in staat moeten stellen afspraken te maken met de private sector op het terrein van informatiedeling en operationele samenwerking. Daarnaast is er ook een rol voor de JCU voorzien om samenwerking te bevorderen en ondersteuning te bieden aan de inzet van diplomatieke maatregelen in reactie op cyberactiviteiten. Voor de JCU wordt een gefaseerde aanpak gepresenteerd met verschillende mijlpalen. Tevens wordt voorgesteld om gebruik te maken van MoU's[11] tussen deelnemers voor de samenwerking binnen de JCU. Ten behoeve van de totstandkoming en verdere ontwikkeling van de JCU wordt een werkgroep gestart[12].

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

De uitwerking van de Nederlandse cyberbeveiligingsaanpak is vastgelegd in de Nederlandse Cyber Security Agenda (NCSA), waarin het weerbaar maken van Nederland tegen digitale dreigingen op geïntegreerde wijze wordt geadresseerd.[13] Nederland is als open en internationaal georiënteerde economie gebaat bij een stabiel, veilig en vrij toegankelijk cyberdomein. Het kabinet zet zich hier samen met haar internationale partners voor in, waarbij de kansen die digitalisering onze economie en samenleving biedt volop worden benut, dreigingen het hoofd wordt geboden, cybercriminaliteit wordt bestreden en fundamentele rechten en waarden worden beschermd.

---

[6] De definitie van deze incidenten is als volgt: «grootschalig incident»: incident als gedefinieerd in artikel 4, punt 7, van Richtlijn (EU) 2016/1148 «met aanzienlijke gevolgen in ten minste twee lidstaten».

[7] Europees agentschap voor cybersecurity.

[8] Het *Computer Emergency Respons Team* voor EU-instellingen, organen en agentschappen.

[9] Europees agentschap voor rechtshandhaving.

[10] Verzameling van rollen, modaliteiten en procedures die leiden tot voltooiing van het EU-kader voor respons op cybercrises als beschreven in de aanbeveling inzake een gecoördineerde respons op grootschalige cyberincidenten- en crises (C2017/1584)

[11] Memoranda van overeenstemming.

[12] De aanbeveling beoogt de volgende deelnemers aan de werkgroep: een vertegenwoordiger van de Commissie, van de Hoge Vertegenwoordiger en een vertegenwoordiger namens alle lidstaten.

[13] Kamerbrief van 20 april 2018, Kamerstuk 26 643, nr. 536.

Het versterken van de digitale weerbaarheid is een prioriteit voor het kabinet. Het Cybersecuritybeeld Nederland 2021[14] laat zien dat de digitale risico's onverminderd groot zijn. Gezien het inherente grensoverschrijdende karakter van cyberbeveiliging en cyberdreiging is Europese en internationale samenwerking voor het kabinet van groot belang. Het kabinet zet zich daarom actief in bij de verschillende Europese gremia[15] die tot doel hebben de digitale weerbaarheid in de EU te vergroten. Ook op nationaal niveau is er de afgelopen jaren aandacht besteed aan het verbeteren van de samenwerking en informatie-uitwisseling tussen verschillende betrokken overheidsorganisaties, waartoe bijvoorbeeld de Cyber Info/Intel Cel[16] en het diplomatiek responskader voor cyberincidenten zijn opgericht. Daarnaast heeft het kabinet prioriteit gegeven aan het vergroten van de paraatheid van organisaties om te reageren op grootschalige cyberincidenten, onder meer door het organiseren van een grootschalige cyberoefening[17] en de publicatie van het Nationaal Crisisplan Digitaal[18].

b) Beoordeling + inzet ten aanzien van dit voorstel

Het kabinet onderschrijft de noodzaak tot versterking van de samenwerking tussen verschillende gemeenschappen binnen de EU, met het oog op de toegenomen digitalisering en het permanente karakter van digitale dreigingen[19]. Het kabinet verwelkomt de ambitie van de aanbeveling om de paraatheid en het situationeel bewustzijn van de EU-instellingen, -organen, en -agentschappen (EU IOA's) en lidstaten te versterken, door onder meer informatie-uitwisseling over cyberdreigingen en -incidenten te verbeteren, en om de coördinatie van de respons op grootschalige ICT-incidenten te versterken. Het kabinet kijkt met belangstelling uit naar de verdere uitwerking van een JCU met het oog op deze doelstellingen.
Goede samenhang en aansluiting van de JCU met bestaande netwerken en initiatieven binnen de EU, zoals het CSIRT Netwerk[20], EU-CyCLONe[21], de NIB-Samenwerkingsgroep[22], de Raadswerkgroep Cyber, de *Joint Cybercrime Taskforce* [23] en EU INTCEN[24] is essentieel voor het slagen van de JCU. Het kabinet zal daarbij bewaken dat duplicatie met bestaande structuren waarbinnen reeds samenwerking plaatsvindt wordt voorkomen. Ook zal verduidelijking gevraagd worden aan de Commissie

---

[14] Cybersecuritybeeld Nederland 2021, Kamerstuk 26 643, nr. 767.
[15] Onder meer via het EU Computer Security Incident Response Teams Netwerk, het Cyber Crisis Liaison Officers Netwerk (CyCLONe), de Netwerk- en Informatiebeveiliging (NIB) Samenwerkingsgroep, en de Raadswerkgroep Cyber.
[16] Binnen deze cel werken AIVD, MIVD, NCSC, OM en Politie samen ten behoeve van het versterken van een landelijk situationeel beeld ten aanzien van cyberdreigingen en -incidenten, het op basis daarvan door partijen in relatie tot die dreigingen en incidenten beter kunnen uitoefenen van hun wettelijke taken, het meer en sneller bieden van handelingsperspectief aan andere belanghebbende organisaties inzake cyberdreigingen, en het hierdoor vergroten van de digitale slagkracht van genoemde organisaties en versterken van de veiligheid in het digitale domein. De CIIC is bij Convenant opgericht (Stcrt. 2020, nr. 30702).
[17] ISIDOOR 2021.
[18] Bijlage bij Kamerstuk 30 821, nr. 102
[19] Zie ook het BNC Fiche Herziening richtlijn netwerk- en informatiebeveiliging (NIB-richtlijn): Kamerstuk 22 112, nr. 3053.
[20] Bedoeld in artikel 12 van de NIB-richtlijn.
[21] EU CyCLONe heeft tot doel snelle coördinatie van cybercrisisbeheer mogelijk te maken in het geval van een grootschalig grensoverschrijdend cyberincident of -crisis in de EU door tijdige informatie-uitwisseling en situationeel bewustzijn tussen bevoegde autoriteiten te bieden.
[22] Bedoeld in artikel 11 van de NIB-richtlijn.
[23] J-CAT heeft tot doel het helpen van het bestrijden van cybercrime binnen en buiten de EU. J-CAT bestaat uit een team van cyber liaison officers van verschillende lidstaten en niet-EU-partners, gebaseerd bij het hoofdkwartier van Europol en gecomplementeerd met Europol EC3 medewerkers.
[24] EU Intelligence and Situation Centre (EU INTCEN).

of de samenwerking op het platform primair tussen lidstaten en EU IOA's plaatsvindt of juist met name tussen de bovengenoemde netwerken (CSIRT-Netwerk, etc.) en organisaties zoals ENISA en Europol, dit onder meer met het oog op het sluiten van MoU's. Daarnaast acht het kabinet het van belang dat de JCU ten dienste staat van de behoeften en mogelijkheden van lidstaten, en uitoefening van taken en bevoegdheden van betrokken autoriteiten van lidstaten onverlet laat. Ook zal het kabinet ten aanzien van enkele onderdelen van de aanbeveling, zoals de activiteiten ter ondersteuning van diplomatieke reactie op cyberaanvallen en de inzet van EU *Cybersecurity Rapid Reaction Teams*, eerst vragen om een verdere uitwerking daarvan – zoals coördinatie van de inzet van laatstbedoelde teams – met name ook om te kunnen bepalen of die onderdelen op gespannen voet zouden kunnen komen te staan met de uitsluitende verantwoordelijkheid van lidstaten op het gebied van bescherming van nationale veiligheid (artikel 4, tweede lid, VEU). Voor het door lidstaten laten opstellen en inbrengen van een nationaal cybersecurity incident- en crisisresponsplan, ten behoeve van EU-plan voor incident- en crisisrespons, merkt het kabinet nu al op dat dit op gespannen voet staat met genoemde uitsluitende verantwoordelijkheid voor zover dit geacht wordt een verplicht karakter te hebben. Van belang is namelijk dat lidstaten zelf bepalen welke elementen zij met het oog op de bescherming van de nationale veiligheid deel willen laten uitmaken van nationale crisisplannen en daarbij niet, zoals is vermeld in artikel 7 van het voorstel tot herziening van de NIB-richtlijn waaraan de Commissie hier ook aan refereert, verplichte elementen worden voorgeschreven[25].

Het kabinet acht het positief dat de JCU geen nieuwe op zichzelf staande instantie zal zijn en verwelkomt het opzetten van een fysiek en virtueel platform om informatie-uitwisseling en andere samenwerking tussen de JCU-deelnemers te versterken teneinde daarmee de digitale weerbaarheid binnen de EU te vergroten. Een hoog niveau van (cyber)beveiliging van het virtuele en fysieke platform zelf is een absolute voorwaarde voor het functioneren van een JCU. Het kabinet zal in elk geval inzetten op een samenwerking binnen de JCU tussen lidstaten en EU-IOA's die gebaseerd is op gelijkwaardigheid waarbij – op vrijwillige basis – organisaties samenkomen om bijvoorbeeld informatie, kennis en expertise uit te wisselen om zo onder meer te werken aan een beter situationeel beeld, met als doel om binnen de EU grootschalige cyberincidenten en -crises te voorkomen, te ontmoedigen en te verhelpen. Hierbij is van belang dat voldoende tijd wordt besteed aan het definiëren van rollen en taken van verschillende deelnemers, het opbouwen van onderling vertrouwen, en het creëren van een gedeeld en gedragen beeld van de JCU zijn toegevoegde waarde. Het kabinet steunt het uitgangspunt om te streven naar versterkte informatie-uitwisseling, maar merkt hierbij op dat vervolggesprekken met alle betrokkenen nodig zijn over uitwerking van randvoorwaarden voor effectieve en efficiënte informatie-uitwisseling zoals de technische randvoorwaarden, de beperkingen vanwege wettelijke kaders en het garanderen van de vertrouwelijkheid van informatie. De rol van de gemeenschap van inlichtingen- en veiligheidsdiensten verdient hierbij in het bijzonder ook nadere aandacht. Het kabinet hecht aan een gedegen en gefaseerd proces inzake het ontwikkelen van de JCU. Hierbij zal het kabinet uitdragen dat prioriteit moet worden gegeven aan het uitwerken van gemeenschappelijke doelen en het opbouwen van vertrouwen en veilige informatie-uitwisseling tussen deelnemers.

[25] Zie ook BNC Fiche Herziening richtlijn netwerk- en informatiebeveiliging (NIB-richtlijn): Kamerstuk 22 112, nr. 3053.

Inzake de deelname door lidstaten aan voorziene activiteiten ten behoeve van de coördinatie van respons en de opvolging daarvan door lidstaten, is het voor het kabinet, net als bij de andere doelstellingen van de aanbeveling, van belang dat deze op basis van vrijwilligheid plaatsvinden en dat bedoelde activiteiten strekken tot ondersteuning van de lidstaten en EU-instellingen. Ten aanzien van het instellen en actief zijn van *EU Cybersecurity Rapid Reaction Teams* [26] behoeft het kabinet eerst meer uitleg over de praktische uitwerking hiervan en de toegevoegde waarde ten opzichte van bijvoorbeeld de *Cyber Rapid Response Teams* in het kader van Permanente Gestructureerde Samenwerking (PESCO)[27], bestaande afspraken in het CSIRT Netwerk voor bijstand bij de aanpak van incidenten en afspraken binnen het opsporings- en handhavingsdomein[28]. Daarnaast verwelkomt het kabinet de geschetste bijdrage van een JCU aan coalitievorming ten behoeve van diplomatieke reacties op cyberaanvallen. Gelet op de voorgestelde rol van ENISA ten aanzien van de JCU, zal het kabinet kritisch zijn op taken die verder gaan dan de taken die ENISA mede op basis van de huidige wetgeving thans heeft.[29] Het kabinet zal daarbij in het bijzonder ook vragen om nadere toelichting ten aanzien van de ondersteunende rol van ENISA ten behoeve van diplomatieke reactie op cyberaanvallen, waaronder de *Cyberdiplomatie Toolbox*.

De aanbeveling om MoU's tussen deelnemers te sluiten om samenwerking via de JCU te bewerkstelligen, beoordeelt het kabinet op zich als positief. Wel ontvangt het kabinet graag eerst meer duidelijkheid van de Commissie over in elk geval de inhoud, het proces van totstandbrenging en de daartoe al dan niet voorziene coördinatie.

Tot slot stelt het kabinet vast dat er in de op te richten inter-institutionele werkgroep een juiste balans moet zijn tussen afvaardigingen van lidstaten en EU-IOA's. Voorts zal het kabinet zich ervoor inzetten dat lidstaten in het gehele proces van verdere uitwerking en het operationeel maken van de JCU sterk vertegenwoordigd zijn.

c) Eerste inschatting van krachtenveld

Naar verwachting zal een meerderheid van de EU-lidstaten de algehele doelstelling om informatie-uitwisseling en verdere samenwerking tussen verschillende gemeenschappen te bevorderen steunen. De verwachting is wel dat diverse lidstaten, net als Nederland, aandacht zullen vragen voor de rol en mate van invloed van lidstaten in zowel het totstandkomingsproces van de JCU als de activiteiten binnen de JCU zelf, alsook bij onderdelen van de aanbeveling die op gespannen voet (zouden kunnen komen te) staan met de uitsluitende verantwoordelijkheid van lidstaten op het terrein van nationale veiligheid.
Het Europees Parlement lijkt in beginsel positief te staan tegenover de oprichting van JCU zoals beschreven in de resolutie[30] n.a.v. de publicatie van de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk.

---

[26] Door ENISA, CERT-EU en Europol ondersteund team van erkende deskundigen op het gebied van cyberbeveiliging, die vooral afkomstig zijn van de CSIRT's van de lidstaten, dat voorbereid is om deelnemers die worden getroffen door grootschalige incidenten en crises op afstand bij te staan

[27] Onder de vlag van *Permanent Structured Cooperation* (PESCO) werken 25 Europese lidstaten intensief samen aan verschillende projecten op veiligheids- en defensiegebied.

[28] Zie o.a. het EU Law Enforcement Emergency Response Protocol – het crisisresponsprotocol van EU-rechtshandhavingsinstanties.

[29] Zoals vastgelegd in artikel 7 van de Cybersecurity Act (Verordening (EU) 2019/881) voor ENISA.

[30] P9_TA(2021)0286.

4. Grondhouding ten aanzien van bevoegdheid, subsidiariteit, proportionaliteit, financiële gevolgen en gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

a) Bevoegdheid

De grondhouding van het kabinet ten aanzien van de bevoegdheid is positief. De aanbeveling heeft betrekking op de terreinen van de ruimte van vrijheid, veiligheid en recht en de interne markt. Op deze terreinen heeft de EU een met de lidstaten gedeelde bevoegdheid (artikel 4, tweede lid, onderdelen a en j, VWEU). Op grond van artikel 292 VWEU is de Commissie bevoegd om aanbevelingen vast te stellen op de gebieden waarvoor de EU bevoegd is. De Commissie is zodoende bevoegd deze aanbeveling vast te stellen. De bevoegdheid van de EU wordt echter niet zonder meer onderschreven voor het onderdeel van de aanbeveling dat betrekking heeft op het door lidstaten laten opstellen en inbrengen van een nationaal cybersecurity incident- en crisisresponsplan, ten behoeve van een EU-plan voor incident- en crisisrespons, voor zover dit onderdeel geacht wordt een verplicht karakter te hebben omdat dit onderdeel op gespannen voet staat met de uitsluitende verantwoordelijkheid van de lidstaten op het gebied van nationale veiligheid (artikel 4, tweede lid, VEU). Zie voor een nadere toelichting hierop paragraaf 3b, tweede alinea, van dit fiche.

b) Subsidiariteit

Het kabinet heeft een positieve grondhouding ten opzichte van de subsidiariteit van de aanbeveling. Gezien het inherent grensoverschrijdende karakter van cyberdreigingen en -incidenten is het naar het oordeel van het kabinet wenselijk dat waar aangewezen, samenwerking tussen lidstaten en EU IOA's plaatsvindt, teneinde hen op die wijze beter in staat te stellen om onder meer grootschalige incidenten te voorkomen en respons in geval van dergelijke incidenten te bevorderen, en daarmee de digitale weerbaarheid binnen de EU verder te versterken. Deze aanbeveling strekt tot het vergroten van die samenwerking binnen de EU ten behoeve van onder meer coördinatie op respons, in aanvulling op al aanwezige samenwerkingsgremia. Naar het oordeel van het kabinet kan dit doel het beste worden verwezenlijkt door optreden op EU-niveau.

c) Proportionaliteit

De grondhouding van het kabinet ten aanzien van de proportionaliteit is positief, met name ook omdat naar het oordeel van het kabinet de aanbeveling zelf, met uitzondering van het onderdeel betreffende het door lidstaten opstellen en inbrengen van nationale cybersecurity incident- en responsplannen, ertoe strekt dat deelname aan de voorgenomen activiteiten binnen de JCU, evenals de opvolging door lidstaten naar aanleiding van die activiteiten binnen de JCU, vrijwillig zal zijn. De aanbeveling gaat daarmee niet verder dan noodzakelijk. De aanbeveling heeft zoals aangegeven tot doel te zorgen voor een gecoördineerde reactie binnen de EU op grootschalige cyberincidenten en -crises, het verbeteren van het situationeel bewustzijn, en het garanderen van de gezamenlijke paraatheid. Het hierin aanbevolen optreden is o.a. dankzij de verbeterde informatiepositie als gevolg van bredere informatiedeling, geschikt om de cybersecurity van de EU en haar lidstaten volgens het kabinet naar een hoger niveau brengen. Wel merkt het kabinet op dat ten aanzien van een groot aantal van de cybersecurityincidenten thans in de praktijk samenwerking tussen lidstaten al plaatsvindt binnen de eerdergenoemde reeds bestaande netwerken. Het kabinet ziet daarom met name meerwaarde in samenwerking bij casussen waar samenwerking tussen

deze netwerken of anderszins tussen lidstaten en EU-instellingen op dit moment nog onvoldoende tot stand komt.

d) Financiële gevolgen

De Commissie geeft in haar aanbeveling aan dat de JCU voornamelijk gefinancierd zal worden vanuit het programma Digitaal Europa. Specifiek zullen de benodigde investeringen voor het opzetten van het fysieke en virtuele platform, en het opbouwen en onderhouden van veilige communicatiekanalen, trainingscapaciteiten, en het ontwikkelen en implementeren van detectie capaciteiten uit het programma Digitaal Europa komen. Daarnaast refereert de Commissie aan het Europees Defensie Fonds dat ondersteunend kan zijn bij het versterken van de paraatheid van nationale (defensie) autoriteiten in lidstaten door het financieren bij onderzoek naar of ontwikkeling van sleutel cyber (defensie) technologieën en capaciteiten. Het kabinet is van mening dat de benodigde EU-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.

Mogelijkerwijs zijn er in de toekomst budgettaire gevolgen voor Nederland die voortvloeien uit activiteiten van Nederlandse overheidsorganisaties in de context van de JCU. Eventuele budgettaire gevolgen voor de nationale begroting zullen worden ingepast op de begroting van de beleidsverantwoordelijke departementen, conform de regels inzake budgetdiscipline.

e) Gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

De aanbeveling zelf bevat geen voorstellen voor nieuwe wettelijke maatregelen met gevolgen op regeldruk en administratieve lasten, voor de overheid, bedrijfsleven of burgers. Mocht er, volgend op deze aanbeveling, nieuwe ontwerp-regelgeving bekend worden, dan zal daarvoor worden bezien of en in hoeverre dit gevolgen heeft voor de regeldruk, administratieve lasten en concurrentiekracht.

De aanbeveling om een JCU op te zetten kent relevante geopolitieke implicaties. Activiteiten binnen de JCU ten behoeve van een gecoördineerde respons op grootschalige cyberincidenten zouden ook betrekking kunnen hebben op cyberaanvallen afkomstig van zowel statelijke actoren als niet-statelijke actoren. De uitkomst daarvan zou kunnen resulteren in een groter vermogen van lidstaten afzonderlijk en de EU als geheel tot afschrikking van cyberaanvallen en efficiënte andere reacties daarop. Dit draagt bij aan de weerbaarheid van de EU en het vermogen van de EU om haar veiligheidsbelangen te waarborgen. Bovendien heeft het invloed op het vermogen van de EU om de internationale slagkracht te vergroten.