Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

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

Nr. 3695 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 26 mei 2023

Overeenkomstig de bestaande afspraken ontvangt u hierbij 8 fiches die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissie voorstellen (BNC).

Fiche: Herziening EU farmaceutische wetgeving (Kamerstuk 36 365, nr. 2)

Fiche: Verordening en richtlijnen wijziging Europees crisisraamwerk voor banken (CMDI review) (Kamerstuk 22 112, nr. 3691)

Fiche: Wijziging Verordening Europees kader voor cyberbeveiligingscertificering (Cyber Security Act) (Kamerstuk 22 112, nr. 3692)

Fiche: Verordeningen aanvullende beschermingscertificaten (ABC's) (Kamerstuk 22 112, nr. 3693)

Fiche: Mededeling Cybersecurity Skills Academie (Kamerstuk 22 112, nr. 3694)

Fiche: Cybersolidariteitsverordening

Fiche: Raadsaanbeveling uitbreiding EU-maatregelen resistentie tegen antimicrobiële stoffen (Kamerstuk 22 112, nr. 3696)

Fiche: Raadsaanbevelingen digitaal onderwijs en digitale vaardigheden (Kamerstuk 22 112, nr. 3697)

De Minister van Buitenlandse Zaken,
W.B. Hoekstra

kst-22112-3695
ISSN 0921 - 7371
's-Gravenhage 2023

Fiche: Cybersolidariteitsverordening

1. Algemene gegevens

a) *Titel voorstel*
VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD tot vaststelling van maatregelen ter versterking van de solidariteit en de capaciteit in de Unie om voor te bereiden en te reageren op cybersecurity dreigingen en incidenten
b) *Datum ontvangst Commissiedocument*
18 april 2023
c) *Nr. Commissiedocument*
COM(2023)209
d) *EUR-Lex*
https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=COM:2023:209:FIN
e) *Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing*
Niet opgesteld.
f) *Behandelingstraject Raad*
Raad voor Vervoer, Telecommunicatie en Energie (Telecomraad)
g) *Eerstverantwoordelijk ministerie*
Ministerie van Justitie en Veiligheid
h) *Rechtsbasis*
Artikel 173, derde lid, VWEU en artikel 332, eerste lid, onder a, VWEU
i) *Besluitvormingsprocedure Raad*
Gekwalificeerde meerderheid
j) *Rol Europees Parlement*
Medebeslissing

2. Essentie voorstel

a) Inhoud voorstel

Op 18 april 2023 heeft de Europese Commissie (hierna: «de Commissie») het voorstel voor een Cybersolidariteitsverordening (hierna: het voorstel) gepubliceerd. Tegelijkertijd presenteerde de Commissie ook een mededeling inzake een Cyber Skills Academie en een voorstel voor een wijziging van de Cyberbeveiligingsverordening (*Cyber Security Act*), waarover separaat BNC-fiches worden opgesteld en die gelijktijdig aan uw Kamer worden verzonden.[1]

Het voorstel voor de Cybersolidariteitsverordening is een reactie op Raadsconclusies van 23 mei 2022, waarin de Commissie wordt aangespoord om een nieuw noodhulpfonds voor de respons op cybersecurityincidenten te presenteren, en het implementeert de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk waarin het opzetten van een Europees Cyberschild wordt aangekondigd.[2, 3] Ook bouwt het voorstel volgens de Commissie voort op de eerste stappen die al zijn ontwikkeld in nauwe samenwerking met de belangrijkste stakeholders en ondersteund door het Digitale Europa Programma (hierna: «DEP»). Tot slot werd de Cybersolidariteitsverordening reeds aangekondigd in het EU-beleid op het gebied van cyberdefensie van 10 november 2022.[4]

---

[1] COM (2023) 207, COM (2023) 208.
[2] Raadsconclusies EU Cyber Posture 23 mei, 2022 (9364/22).
[3] COM (2020) 18.
[4] JOIN (2022) 49 final.

De doelstellingen van het voorstel zijn drieledig. Allereerst ziet het voorstel op het versterken van de gemeenschappelijke EU-detectie en het situationeel bewustzijn van cyberdreigingen en -incidenten. De tweede doelstelling ziet op het versterken van de paraatheid van kritieke entiteiten in de hele EU en het versterken van solidariteit door gemeenschappelijke responscapaciteiten te ontwikkelen tegen significante of grootschalige cybersecurityincidenten. Ten derde wil de Commissie met dit voorstel de weerbaarheid van de Unie vergroten en bijdragen aan een doeltreffende respons door significante of grootschalige incidenten te evalueren en te beoordelen. Deze doelstellingen moeten worden verwezenlijkt door middel van: het opzetten van een zogenoemd Europees Cyberschild, het inrichten van een Europees Cybernoodmechanisme en het opstellen van een Europees Evaluatiemechanisme voor Cyberincidenten. De eerste twee genoemde acties zullen (deels) worden ondersteund door de DEP-gelden.

Het Europese Cyberschild is een EU-netwerk van beveiligingsoperaties centra, in het voorstel *Security Operations Centers/SOCs* genoemd, dat zal worden opgericht om in de Unie geavanceerde capaciteiten te ontwikkelen voor het opsporen, analyseren en verwerken van gegevens over cyberdreigingen en -incidenten. Het Europees Cyberschild zal bestaan uit zogenoemde nationale SOCs, waarvoor iedere lidstaat ten minste één publiek orgaan moet aanwijzen, en grensoverschrijdende SOCs.[5, 6] Nationale SOCs worden aangespoord binnen twee jaar deel uit te maken van een grensoverschrijdende SOC. Binnen dit consortium dienen de nationale SOCs informatie uit te wisselen.[7] Grensoverschrijdende SOCs moeten relevante informatie met betrekking tot een (mogelijk) grootschalig cybersecurityincident verstrekken aan het EU-Cyber Crisis Liaison Organisation Netwerk (EU-CyCLONE), het *Computer Security Incident Response Teams Netwerk* (CSIRT-Netwerk) en de Commissie.[8, 9] De Commissie kan middels uitvoeringshandelingen onder meer de voorwaarden voor de interoperabiliteit tussen de grensoverschrijdende SOCs specificeren, de procedurele regelingen voor het delen van informatie bepalen, en technische vereisten voor de lidstaten vaststellen.[10] Ook krijgt het Europese Cybersecurity Competentie Centrum (ECCC) een rol toebedeeld bij de implementatie van acties ten aanzien van

---

[5] De Commissie omschrijft deze nationale SOCs als referentiepunt en toegangspoort naar andere publieke en private organisaties op nationaal niveau ten behoeve van het verzamelen en analyseren van informatie over cybersecuritydreigingen en -incidenten en om bij te dragen aan een grensoverschrijdende SOC. Het dient uitgerust te zijn met geavanceerde technologieën die in staat zijn informatie die relevant is voor cybersecuritydreigingen en -incidenten te detecteren, samen te voegen en te analyseren.

[6] Een grensoverschrijdend SOC wordt omschreven als een gecoördineerd platform dat bestaat uit een netwerk van nationale SOCs van ten minste drie lidstaten die gezamenlijk een hostingconsortium vormen. Hierbinnen zal informatie uit zowel publieke als private bronnen worden uitgewisseld, zullen geavanceerde capaciteiten worden gedeeld en zal er gezamenlijk gewerkt worden aan het ontwikkelen van cyberdetectie, -analyse -preventie en beschermingsmogelijkheden.

[7] Zoals informatie met betrekking tot cyberdreigingen, «bijna-missers», kwetsbaarheden, technieken en procedures, indicatoren voor compromitteren, tactieken van vijandige actoren, specifieke informatie over bedreigende actoren, cybersecuritywaarschuwingen en aanbevelingen met betrekking tot de configuratie van cyberbeveiligingstools om cyberaanvallen te detecteren.

[8] 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.

[9] Zoals bedoeld in artikel 12 van de NIB-richtlijn: Het CSIRTs-Netwerk is opgericht om bij te dragen tot het opbouwen van vertrouwen tussen de lidstaten en om snelle en doeltreffende operationele samenwerking te bevorderen, wordt een netwerk van nationale CSIRT's ingesteld. Het CSIRT-netwerk bestaat uit vertegenwoordigers van de CSIRT's van de lidstaten en CERT-EU.

[10] Met betrekking tot een hoog niveau van gegevensbeveiliging en fysieke beveiliging van de infrastructuur van het Europese Cyberschild.

het Europese Cyberschild, bijvoorbeeld bij de ondersteuning van grensoverschrijdende SOCs.[11]

Verder wil de Commissie het Europees Cybernoodmechanisme oprichten. Het Cybernoodmechanisme zal acties ten aanzien van paraatheid, respons en wederzijdse bijstand ondersteunen. Met betrekking tot paraatheid, zal het Cybernoodmechanisme gecoördineerd testen van entiteiten uit hoog-kritieke sectoren ondersteunen. Ook beoogt de Commissie onder het Cybernoodmechanisme een Europese Cybersecurity Reserve (hierna: «Reserve») op te richten, bestaande uit incidentresponsdiensten van vertrouwde private aanbieders. De ondersteuning die door de Reserve aan de lidstaten zal worden geleverd zal ook beschikbaar gesteld worden aan Europese instellingen, organen, bureaus en agentschappen van de Unie (EU-IBAs) en derde landen die zijn aangesloten op het DEP.[12] De Commissie stelt voor de algehele verantwoordelijkheid voor de uitvoering van de Reserve te dragen, waaronder de prioritering en doorontwikkeling van de Reserve. Ook kan de Commissie de operationalisering en administratie van de Reserve toevertrouwen aan het Europese Agentschap voor Netwerk- en Informatiebeveiliging (ENISA). Door middel van uitvoeringshandelingen kan de Commissie de toewijzing (aansturing) en het type en aantal van responsdiensten van de Reserve specificeren.

Het Europees Evaluatiemechanisme voor Cyberincidenten (*European Cybersecurity Incident Review Mechanism*) zal door ENISA opgesteld worden om dreigingen, kwetsbaarheden en risico beperkende acties met betrekking tot een specifiek grootschalig cyber incident te beoordelen. Deze beoordelingen zullen door ENISA gedeeld worden met het CSIRT-Netwerk, EU-CyCLONe en de Commissie.

Ten slotte bevat het voorstel wijzigingen van de DEP-verordening ten behoeve van het certificeren van vertrouwde private partijen.

b) Impact assessment Commissie

Vanwege het urgente karakter van het voorstel heeft er geen impact assessment plaatsgevonden. Het kabinet wil echter benadrukken dat het voorstander is van het uitvoeren van impact assessments om zodoende het beleid en de regels van de EU zo doeltreffende en efficiënt mogelijk te maken.

Verder zullen de voorgestelde initiatieven uit het voorstel worden ondersteund door het DEP en de verordening beoogt hierop geen significante administratieve of milieueffecten met zich mee te brengen anders dan wat reeds is beoordeeld in de impact assessment van de DEP-verordening.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

Het Cyber Security Beeld Nederland (hierna ook: «CSBN») geeft jaarlijks een overzicht van de digitale dreigingen en weerbaarheid van Nederland.[13] Het CSBN 2022 erkent onder meer dat de digitale dreiging

---

[11] Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra, (EU) 2021/887.

[12] IJsland, Noorwegen en Liechtenstein nemen momenteel als derde (niet-EU) landen deel aan DEP. Kandidaat-landen zijn Turkije en Servië. Ook hebben Israël, Moldavië en Oekraïne interesse getoond in het DEP-programma.

[13] Bijlage bij Kamerstuk 26 643, nr. 891.

toeneemt en dat de digitale ruimte nauw verbonden is met geopolitiek en gebruikt wordt door staten voor hun belangenbehartiging. Staten voeren bijvoorbeeld digitale aanvallen uit om te spioneren of om te kunnen saboteren.

Het CSBN is een belangrijk fundament voor de probleemanalyse waarop de Nederlandse Cybersecuritystrategie (NLCS) is gebaseerd.[14] Verdeeld over vier pijlers wordt in de NLCS de kabinetsbrede inzet voor het realiseren van een digitaal veilige samenleving uiteengezet. Naast acties en samenwerking op nationaal niveau, wordt in de NLCS benadrukt dat internationale samenwerking in EU- en NAVO-verband en daarbuiten essentieel is gezien het grensoverschrijdende karakter van cyberdreigingen. Het kabinet zet zich daarom actief in bij de verschillende Europese gremia en samenwerkingsverbanden die tot doel hebben de digitale weerbaarheid in de EU te vergroten.[15]

Pijler I van de NLCS ziet toe op de digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties. Hierbij stelt het kabinet zich het doel om beter zicht op mogelijke dreigingen en incidenten te krijgen en organisaties goed te beschermen tegen digitale risico's, onder meer middels het implementatietraject van de herziening van de Europese Netwerk- en Informatiebeveiligingsrichtlijn (NIS2). Ook wordt onder deze pijler het doel gesteld het vermogen van organisaties om te reageren, herstellen en leren van cyberincidenten te vergroten; een belangrijk actiepunt hiervoor is de lancering van het geactualiseerde Landelijk Crisisplan Digitaal.[16] In pijler II van de NLCS wordt het belang van veilige en innovatieve digitale producten en diensten benadrukt, waarin het kabinet zich tot doel stelt in samenwerking met private partijen bij te dragen aan de ontwikkeling en aanname van Europese cybersecuritycertificeringschema's voor ICT-producten, diensten en processen. Dit komt momenteel onder meer tot uiting middels de Nederlandse inzet in de onderhandelingen omtrent de verordening cyberweerbaarheid.[17] Daarbij ziet Pijler III van de NLCS op het tegengaan van digitale dreigingen van staten en criminelen, onder meer door het zicht op digitale dreigingen te vergroten door een effectieve uitwisseling van inlichtingen en informatie met internationale partners.

Op 15 november jl. heeft het DEP een tender gepubliceerd voor het opzetten van grensoverschrijdende SOCs.[18] Deze tender is het project waarop de Commissie beoogt voort te bouwen door middel van het voorstel voor een Europees Cyberschild. Nederland heeft gereageerd op deze tender en maakt deel uit van het consortium onder leiding van Spanje waarin geanalyseerde dreigingsinformatie gedeeld wordt met overige deelnemende lidstaten. De uitvoering van deze tender is nog niet beoordeeld en geëvalueerd.

b) Beoordeling + inzet ten aanzien van dit voorstel

Het kabinet verwelkomt en onderschrijft, in lijn met de NLCS, de doelstelling van het voorstel waar het gaat om het vergroten van de digitale weerbaarheid van de EU en het belang van het hebben van een zo actueel mogelijk situationeel beeld van cyberrisico's. Ook ziet het kabinet

---

[14] Kamerstuk 26 643, nr. 925.

[15] Onder meer via het CSIRTs-Netwerk en EU-CyCLONe, de Netwerk- en Informatiebeveiliging (NIB) Samenwerkingsgroep, de Raadswerkgroep Cyber, de European Government CERT Group (ECG) en het Europees Justitieel Cybercrime Netwerk (EJCN).

[16] Kamerstukken 26 643 en 30 821, nr. 955.

[17] Cyber Resilience Act (CRA), COM(2022) 454.

[18] Tender «Capacity Building of Security Operation Centres», tender ID: DIGITAL-ECCC-2022-CYBER-03-SOC.

het belang van het bevorderen van samenwerking binnen de EU voor wat betreft de respons op (grootschalige) incidenten en staat het positief ten opzichte van de noodzaak om te investeren in onze wederzijdse bijstand. Het kabinet zal in de beoordeling van (de verdere uitwerking en implementatie van) de verschillende elementen uit dit voorstel telkens goed kijken naar hoe, wanneer en door wie deze doelstellingen het beste kunnen worden bereikt. Dit ook met het oog op de vele initiatieven en wetgeving op het gebied van cybersecurity die recentelijk door de Commissie zijn geïnitieerd. In deze context zal het kabinet bovendien oog houden voor de belasting van (nationale) partijen die de implementatie van (nieuwe) EU-initiatieven en wetgeving met zich meebrengt. Verder streeft het kabinet met betrekking tot de verschillende elementen uit dit voorstel naar complementariteit, goede samenhang en het voorkomen van duplicatie met bestaande netwerken en initiatieven binnen de EU, zoals EU-CyCLONe, het ECCC, het (wederzijdse bijstandsmechanisme binnen het) CSIRT-Netwerk en het PESCO-project *Cyber Rapid Response Teams*. Ook zal nadrukkelijk aandacht worden besteed aan de verhouding met de verdragsrechtelijke bepaling over de uitsluitende verantwoordelijkheid van lidstaten op het gebied van bescherming van nationale veiligheid (artikel 4, lid 2, VEU).

Met betrekking tot het voorstel van de Commissie voor het Europese Cyberschild kijkt het kabinet, ook met het oog op de betrokkenheid van Nederland bij het reeds lopende project zoals beschreven onder punt 3a met belangstelling naar de verdere uitwerking hiervan. Het kabinet ontvangt graag nadere toelichting van de Commissie over onder meer de rol en functie van de nationale SOCs, de dwarsverbanden met en betrokkenheid en verantwoordelijkheid van nationale CSIRTs, en de rol van de private sector.[19] Zo ontvangt het kabinet graag verduidelijking over welke informatie, wanneer, met welk doel en op welke juridische basis informatie verplicht uitgewisseld en geanalyseerd dient te worden tussen lidstaten onderling en met de Commissie. Hierbij merkt het kabinet op dat het delen van informatie ten aanzien van cybersecurityincidenten kan raken aan de uitsluitende verantwoordelijkheid van lidstaten ten aanzien van nationale veiligheid. In die context kijkt het kabinet kritisch naar het voorgestelde verplichtende karakter van informatiedeling. Lidstaten moeten zelf kunnen beslissen over het delen van informatie die raakt aan nationale veiligheid.[20] Daarnaast onderstreept het kabinet het belang van samenhang en complementariteit en het voorkomen van duplicatie met reeds bestaande netwerken, zoals het CSIRT-Netwerk, en is het belangrijk dat geleerde lessen en afgesproken randvoorwaarden uit reeds in ontwikkeling zijnde initiatieven worden meegenomen in de verdere uitwerking.[21]

Het kabinet ziet het testen van (kritieke) entiteiten als een maatregel die een positief effect kan hebben op de cyberweerbaarheid van de EU.[22] Het is hierbij echter onder meer belangrijk dat rollen en verantwoordelijkheden eerst verder worden uitgewerkt met het oog op de uitvoering en het belang van de betrokkenheid van lidstaten. Zo heeft het kabinet onder meer vragen over het soort testen, de selectie van kritieke entiteiten en raakvlakken met nationale verantwoordelijkheden waar het bijvoorbeeld

---

[19] Ook ten opzichte van de wettelijke taken van nationale CSIRTs zoals vastgelegd in de NIS2.

[20] De uitsluitende verantwoordelijkheid van de lidstaten op het gebied van bescherming van nationale veiligheid komt voort uit het VWEU art. 4 lid 2.

[21] Een voorbeeld van een relevant initiatief is de oproep tot het indienen van blijken van belangstelling voor grensoverschrijdende SOCs: Cyberbeveiliging: EU start eerste fase van de uitrol van Europese infrastructuur voor grensoverschrijdende veiligheidsoperaties | Shaping Europe's digital future (europa.eu).

[22] Zie hiervoor o.a. Kamerstuk 26 643, nr. 614.

gaat over de (implementatie van de) NIS2 en de vertrouwelijkheid van informatie over kritieke entiteiten die raakt aan nationale veiligheid.

Het kabinet ondersteunt het doel van de Europese Cybersecurity Reserve. Het kabinet acht het echter van essentieel belang dat het opstellen van voorwaarden ten aanzien van de inzet van de Reserve nadrukkelijk lidstaat-gedreven is en dat lidstaten worden betrokken bij de aansturing en doorontwikkeling van de Reserve gelet op mogelijke politieke implicaties, zeker ook met betrekking tot de inzet van de Reserve richting derde landen en de inzet van experts werkend voor private partijen uit derde landen. Daarbij is het belangrijk dat lidstaten zelf zeggenschap houden over het eventueel ontvangen van ondersteunende diensten van de Europese Cybersecurity Reserve, gezien de mogelijke gevoeligheid van betrokken gegevens of instanties en gezien de inzet van dergelijke diensten raakt aan de uitsluitende verantwoordelijkheid van de lidstaten op het terrein van de bescherming van nationale veiligheid. Verder moet oog worden gehouden voor het feit dat een dergelijke Reserve een beroep zal doen op experts uit de al schaarse cybersecuritycapaciteit binnen de Unie. Het kabinet zet dan ook in op een efficiënt, transparant en inclusief aansturingsmodel dat ontworpen is om in het geval van crisis snel besluiten te kunnen nemen.

Ten aanzien van het voornemen om vertrouwde private aanbieders te certificeren heeft het kabinet, in lijn met de NLCS, een positieve houding. Hierbij kijkt het kabinet met belangstelling naar de verdere uitwerking van de selectiecriteria van deze private aanbieders en is het belangrijk dat lidstaten hier ook inspraak in hebben, onder meer met het oog op de raakvlakken met bescherming van de nationale veiligheid. Daarnaast acht het kabinet het van belang dat een certificeringssysteem zoveel mogelijk aansluit bij bestaande, vergelijkbare certificeringssystematiek. Dit zal verder toegelicht worden in het BNC-Fiche omtrent het wijzigingsvoorstel van de Cyberbeveiligingsverordening.

Ten aanzien van het Europees Evaluatiemechanisme voor cybersecurity incidenten onderstreept het kabinet het belang van het leren waar het gaat om incidenten, conform de aanbeveling uit het WRR-rapport.[23] Het kabinet kijkt daarom met belangstelling naar de verdere uitwerking van het Europees Evaluatiemechanisme, waarbij het kabinet onder meer het belang van betrokkenheid van lidstaten en de onafhankelijkheid van dergelijke evaluaties onderstreept.

Gelet op de rollen die ENISA wordt gegeven in het voorstel en de taken die ENISA mede op basis van de huidige wetgeving thans heeft, zal het kabinet nadere toelichting vragen ten aanzien van de ondersteunende rol van ENISA ten behoeve van onder andere het Europees Evaluatiemechanisme en het Europese Cyberschild.[24]

De Commissie voorziet een actieve rol voor het ECCC bij de implementatie van de Cybersolidariteitsverordening. Zo wordt het ECCC inhoudelijk betrokken bij de opzet en implementatie van de grensoverschrijdende SOCs. Daarnaast zal het ECCC ook de implementatie en opvolging overzien van budgetten die via het DEP voor cybersecurity beschikbaar worden gemaakt, zoals voor het Europees Cybernoodmechanisme en de Europese Cybersecurity Reserve. Het kabinet heeft vragen over de rol die het ECCC heeft kunnen spelen bij de totstandkoming van dit voorstel. Daarnaast merkt het kabinet op dat het ECCC is opgericht om

[23] Kamerstukken 26 643 en 30 821, nr. 673.
[24] Met betrekking tot een hoog niveau van gegevensbeveiliging en fysieke beveiliging van de infrastructuur van het Europese Cyberschild.

EU-subsidies op het gebied van cybersecurity (met name via het DEP) te kanaliseren en te implementeren, met het oog op langetermijn innovatie-doelstellingen zoals verwoord in haar Strategische Agenda. Doordat de Commissie middels deze verordening een beroep doet op een groot deel van de beschikbare DEP-middelen, heeft het kabinet vragen over hoe dit raakt aan (het behalen van) de strategische doelstellingen op de lange termijn en daarmee de slagkracht van het ECCC. Daarbij bevindt het ECCC zich nog in haar oprichtingsfase en is er nog geen sprake van volledige operationele capaciteit of financiële autonomie. Het kabinet acht het daarom van belang dat oog wordt gehouden voor de afhankelijkheidsrelatie tussen enerzijds de ontwikkelingssnelheid van het ECCC en anderzijds de actieve rol die het ECCC krijgt toebedeeld bij de implementatie van het voorstel. Tijdens de verdere uitwerking van het voorstel zal het kabinet bovengenoemde zorgen opbrengen.

c) Eerste inschatting van krachtenveld

In algemene zin onderschrijven alle EU-lidstaten het belang van het waarborgen van de digitale weerbaarheid in de EU. In die context zullen veel lidstaten naar verwachting in beginsel de doelstellingen van de Cybersolidariteitsverordening ondersteunen, namelijk het versterken van de solidariteit en capaciteit ten aanzien van cybersecuritydreigingen en -incidenten. De verwachting is echter wel dat een meerderheid van de lidstaten meerdere elementen uit de Cybersolidariteitsverordening kritisch zal ontvangen. Veel lidstaten zullen, net als Nederland, bijvoorbeeld kritisch zijn op plannen van de Commissie die zien op de financiële verantwoording en de rol van lidstaten waar het gaat om de (inzet van de) Cyberreserve.

De positie van het Europees Parlement (EP) ten aanzien van dit voorstel is nog niet bekend. Het voorstel zal behandeld worden in de Commissie industrie, onderzoek en energie (ITRE). Parlementslid Lina Gálvez Muñoz (S&D) is aangewezen als Rapporteur.

4. Beoordeling bevoegdheid, subsidiariteit en proportionaliteit

a) Bevoegdheid

Het oordeel van het kabinet is positief. Het voorstel is gebaseerd op artikel 173, derde lid, VWEU en artikel 332, eerste lid, onder a, VWEU. Artikel 173, derde lid, VWEU geeft de EU de bevoegdheid tot het vaststellen van specifieke maatregelen ter ondersteuning van de activiteiten die in de lidstaten worden ondernomen, om onder meer een gunstig klimaat voor het ontplooien van initiatieven en voor de ontwikkeling van ondernemingen in de gehele Unie, met name van het midden- en kleinbedrijf, te bevorderen, een gunstig klimaat voor de samenwerking tussen ondernemingen te bevorderen; een betere benutting van het industriële potentieel van het beleid inzake innovatie, onderzoek en technologische ontwikkeling te stimuleren. Artikel 322, eerste lid, onder a, VWEU geeft de EU de bevoegdheid om financiële regels en de wijze waarop rekening en verantwoording wordt gedaan, vast te stellen.

Het kabinet verzoekt verdere toelichting van de Commissie over hoe de bevoegdheden en bepalingen omtrent de inzet van de Cyber Reserve, het testen van kritieke entiteiten, het verplichtende karakter van informatie-deling tussen nationale SOCs en met de Commissie, en de uitwerking van deze plannen zich precies verhouden tot de uitsluitende verantwoordelijkheid van de lidstaten op het gebied van nationale veiligheid, in overeenstemming met artikel 4, tweede lid, VEU.

Op het terrein van industrie is sprake van een aanvullende bevoegdheid tussen de EU en de lidstaten (artikel 6, onder b, VWEU). Op het terrein van de ruimte van veiligheid, vrijheid en rechtvaardigheid is er sprake van een gedeelde bevoegdheid tussen de EU en de lidstaten op basis van artikel 4, tweede lid, onder j, VWEU.

b) Subsidiariteit

De subsidiariteit is niet van toepassing voor zover het gaat om het vaststellen van financiële regels voor de opstelling en uitvoering van de EU-begroting, gezien het feit dat deze bevoegdheid enkel door de EU kan worden uitgeoefend. Met betrekking tot de overige bepalingen, is het oordeel van het kabinet positief. Het voorstel heeft tot doel om de gemeenschappelijke EU-detectie en het bewustzijn van cyberbedreigingen en incidenten te versterken, de paraatheid van kritieke entiteiten in de EU en responscapaciteiten te versterken en de weerbaarheid van de Unie te vergroten door grootschalige incidenten te evalueren. Gezien het inherent grensoverschrijdende karakter van cyberdreigingen en incidenten kan dit onvoldoende door de lidstaten op centraal, regionaal of lokaal niveau worden verwezenlijkt en is het wenselijk dat gemeenschappelijk optreden op Unie-niveau plaatsvindt. Ondersteuning op EU-niveau zorgt voor een verhoogde digitale weerbaarheid van en binnen de Unie. Bovendien zorgt optreden op EU-niveau voor beter gebruik van bestaande maatregelen en betere coördinatie en samenwerking tussen de lidstaten. Om die redenen is optreden op het niveau van de EU gerechtvaardigd.

c) Proportionaliteit

Het oordeel van het kabinet ten aanzien van de proportionaliteit is positief met kanttekening. Het kabinet onderschrijft de doelen van het voorstel om de gemeenschappelijk EU-detectie en bewustzijn van cyberbedreigingen en incidenten te versterken, de paraatheid van kritieke entiteiten in de EU en responscapaciteiten te versterken en de weerbaarheid van de Unie vergroten door grootschalige incidenten te evalueren. Het opzetten van een Europees Cyberschild, het inrichten van een Cybernoodmechanisme en het opstellen van een Europees Evaluatiemechanisme voor Cyberincidenten zijn geschikt om de doelstellingen van de verordening te bereiken, omdat deze zaken detectiecapaciteiten zullen versterken, lidstaten zullen ondersteunen in snelle reacties en lidstaten in staat zullen stellen om incidenten te analyseren voor toekomstige lessen.

Wel ziet het kabinet risico's dat de Cybersolidariteitsverordening mogelijk verder gaat dan noodzakelijk op onderdelen van de verordening. Het kabinet twijfelt of het neerleggen van de verplichte procedurele voorwaarden en regelingen omtrent informatiedeling tussen grensoverschrijdende SOCs noodzakelijk is om de doelstelling van het optreden te bereiken. Het kabinet verzoekt daarom in ieder geval verdere toelichting van de Commissie welke procedurele voorwaarden en regelingen worden bedoeld.

Ook heeft het kabinet twijfels bij de noodzaak van aanwijzing van de types en het aantal ondersteunende diensten voor de EU Cybersecurity Reserve en het opstellen van specifieke regels over het alloceren van de ondersteunende diensten. Dit gaat volgens het kabinet verder dan noodzakelijk om de doelstelling van het optreden te bereiken voor zover het ook betrekking heeft op nationale situaties, omdat het ook de aanwijzing en allocatie van ondersteunende diensten zou regelen met betrekking tot geheel nationale cybersecurity-incidenten terwijl dit niet noodzakelijk is voor het bereiken van de doelstelling. Het kabinet zal zich daarom inzetten

voor het beperken van het alloceren van ondersteunende diensten tot specifiek grensoverschrijdende cybersecurity-incidenten.

5. Financiële consequenties, gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

a) Consequenties EU-begroting

Het budget voor de strategische doelstelling «Cybersecurity» van het Digital Europe Programma (DEP) wordt met deze verordening verhoogd met 100 miljoen euro. Deze middelen zijn afkomstig uit herschikkingen uit andere strategische doelstellingen van het DEP. Het is nog onduidelijk wat de totale financiële kosten of consequenties van het voorstel van de Commissie zijn. Het kabinet zal daarover om verduidelijking vragen tijdens de behandeling van dit voorstel.

Het grootste deel van het budget voor de verschillende acties uit de verordening komt vanuit het DEP WP 2023–2024, waar de middelen reeds geoormerkt waren voor vergelijkbare acties. In die zin ligt het voorstel dus in lijn met eerder gemaakte afspraken. Tegelijkertijd hebben verschillende lidstaten zich via het ECCC kritisch uitgesproken over de beperkte consultatie van het ECCC bij de totstandkoming van het DEP WP 2023–2024. Dientengevolge liggen de voorgestelde acties niet direct in lijn met de Strategische Agenda van het ECCC.

Het is nog onduidelijk uit welke DEP-budgetten de ophoging van 100 miljoen euro gefinancierd wordt en welke andere strategische doelstellingen hierdoor benadeeld worden. Het kabinet zal hier verduidelijking over vragen. Het kabinet 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.

b) Financiële consequenties (incl. personele) voor rijksoverheid en/of medeoverheden

De totale voorziene begroting wordt door de Commissie geschat op zo'n 1,109 miljard euro. Hierin zijn ook contributies van lidstaten meegerekend. Hoe deze begroting precies is opgebouwd en wat de omvang is van de bijdragen van lidstaten, is echter onduidelijk. Hier hoopt het kabinet tijdens de verdere uitwerking van het voorstel meer duidelijkheid over te krijgen van de Commissie. Lidstaten worden in het voorstel bijvoorbeeld geacht om 50 procent van de kosten te dekken voor het opstellen van de nationale SOCs en een deel van de kosten voor het SOC-consortium te dekken.
De budgettaire gevolgen voor de nationale begroting worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline.

c) Financiële consequenties en gevolgen voor regeldruk voor bedrijfsleven en burger

Het voorstel lijkt geen financiële consequenties te hebben voor de burger. Ten aanzien van het voornemen om vertrouwde private aanbieders te certificeren heeft het kabinet de opvatting dat dit positieve gevolgen kan hebben voor het Nederlandse bedrijfsleven. De certificering van private aanbieders zal de inzet van private partijen aanmoedigen. Deze certificering is vrijwillig, cybersecuritybedrijven kunnen zelf de afweging maken of het certificaat van toegevoegde waarde is en tot certificatie over gaan. Vanwege de invoering van de certificeringssystematiek zullen voor het

bedrijfsleven regeldrukkosten ontstaan, maar op dit moment kan de hoogte daarvan nog niet worden vastgesteld aangezien de selectiecriteria door de Commissie nog nader moeten worden uitgewerkt.

Zoals in de beoordeling benoemd kijkt het kabinet met belangstelling naar de verdere uitwerking van de selectiecriteria van deze private aanbieders en is het belangrijk dat lidstaten hier ook inspraak in hebben met het oog op de raakvlakken met bescherming van de nationale veiligheid. Daarnaast acht het kabinet het van belang dat een certificeringssysteem zoveel mogelijk aansluit bij bestaande, vergelijkbare certificeringssystematiek zodat er geen verdere druk uitgeoefend zal worden op het bedrijfsleven. Dit zal verder toegelicht worden in het BNC-Fiche omtrent het wijzigingsvoorstel van de Cyberbeveiligingsverordening.

d) Gevolgen voor concurrentiekracht en geopolitieke aspecten

Het kabinet verwacht dat de voorgestelde maatregel een positief maar beperkt effect zal hebben op het Europese concurrentievermogen. Zo kan het certificeren van private aanbieders ten behoeve van de Cyberreserve naar verwachting op de middellange termijn een toename in de digitale veiligheid van in de EU geproduceerde diensten teweegbrengen.

Het voorstel draagt bij aan de digitale weerbaarheid van de EU en Nederland door de gemeenschappelijke EU-detectie en het bewustzijn van cyberbedreigingen en incidenten te versterken, de paraatheid van kritieke entiteiten in de EU en responscapaciteiten te versterken en door grootschalige incidenten te evalueren. Door het vergroten van de digitale weerbaarheid heeft het voorstel ook een positief effect op de open strategische autonomie van de EU.

6. Implicaties juridisch

a) Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid (inclusief toepassing van de lex silencio positivo)

De verordening is rechtstreeks toepasselijk op de lidstaten.

b) Gedelegeerde en/of uitvoeringshandelingen, incl. NL-beoordeling daarvan

Het voorstel bevat bevoegdheden voor de Commissie om uitvoeringshandelingen vast te stellen in de artikelen 6(3), 7(2), 8(3), 12(8), en 13(7). Dit betreffen bevoegdheden om de voorwaarden voor de interoperabiliteit tussen de grensoverschrijdende SOCs te specificeren, de procedurele regelingen voor het delen van informatie door grensoverschrijdende SOCs te bepalen, en technische vereisten voor de lidstaten vast te stellen, het type en aantal responsdiensten te specificeren die nodig zijn voor het EU Cybersecurity Reserve en de nadere regelingen voor toewijzing van de responsdiensten te specificeren.

Het toekennen van deze bevoegdheden is bij sommige aspecten van het voorstel mogelijk, omdat het daar geen essentiële onderdelen van de basishandeling betreft. Dit is het geval bij de artikelen 6(3) en 8(3).

Het inzetten van de diensten van de Cyberreserve (artikel 12(8) en 13(7)) is echter een kwestie die belangrijke politieke keuzes vereist en derhalve een essentieel onderdeel is en als bevoegdheid niet kunnen worden overgedragen aan de Commissie. De specificering van de technische informatiedelingsverplichtingen binnen het Cyberschild (artikel 7(2) is mogelijk ook een essentieel onderdeel die politieke keuzes vereist. Met betrekking tot

artikel 7(2) van het voorstel lijkt dit mogelijk essentiële zaken te betreffen als de Commissie de reikwijdte van de informatiedeling door lidstaten zou kunnen beïnvloeden, aangezien dit een materieel effect zou hebben op de verplichtingen omtrent informatiedeling. Het kabinet zal de Commissie verzoeken verdere toelichting hierover te geven. De uitvoeringshandelingen over de allocatie en inventarisatie van de ondersteunende diensten evenals de inzet van dergelijke diensten, genoemd in artikel 12 en 13 van het voorstel, zullen een belangrijke materiële invloed hebben op de inzet van de EU Cybersecurity Reserve, wat derhalve een essentieel onderdeel betreft met politieke keuzes die door de Uniewetgever zelf gespecificeerd zou moeten worden.

Toekenning van de uitvoeringsbevoegdheden acht het kabinet wenselijk, ten aanzien van de eerdergenoemde bevoegdheden specifiek omtrent het stellen van de voorwaarden voor interoperabiliteit van grensoverschrijdende SOCs, vastgelegd in artikel 6(3) van het voorstel, en het specificeren van de technische informatiedelingsverplichtingen binnen het Cyberschild, vastgelegd in artikel 8(3). Het toekennen van deze uitvoeringsbevoegdheden is wenselijk, omdat het technische gedetailleerde zaken betreft die gezien de gewenste flexibiliteit en snelheid normaliter niet het beste via de normale wetgevingsprocedure kunnen worden geregeld. Met betrekking tot de overige uitvoeringsbevoegdheden, is het kabinet van oordeel dat het regelen hiervan in uitvoeringshandelingen ook wenselijk is ten behoeve van de flexibiliteit en snelheid in het kader van de technische details, maar dat dit mogelijk essentiële kwesties betreffen en dat deze maatregelen verder gaan dan noodzakelijk. Voor zover dit geregeld dient te worden, heeft het kabinet derhalve de voorkeur dat dit zoveel mogelijk al in de basishandeling wordt geregeld.

De keuze voor uitvoering in plaats van delegatie ligt hier voor de hand omdat het gaat om uitvoering van de verordening volgens eenvormige voorwaarden. De uitvoeringshandelingen worden vastgesteld volgens de onderzoeksprocedure als bedoeld in artikel 5 van verordening 182/2011. Toepassing van deze procedure is hier volgens het kabinet op zijn plaats omdat het gaat om de vaststelling van uitvoeringshandelingen van algemene strekking overeenkomstig artikel 2, tweede lid, en onder a van de Comitologieverordening.

c) Voorgestelde implementatietermijn (bij richtlijnen), dan wel voorgestelde datum inwerkingtreding (bij verordeningen en besluiten) met commentaar t.a.v. haalbaarheid

De verordening zal in werking treden op de twintigste dag na publicatie in het Publicatieblad van de Europese Unie. Specifieke termijnen zijn opgesteld voor de uitvoering van het Cyberschild. Een nationale SOC wordt bijvoorbeeld geacht zich binnen twee jaar aan te melden voor een grensoverschrijdende SOC om een beroep te kunnen maken op de vrijgemaakte gelden.

d) Wenselijkheid evaluatie-/horizonbepaling

Na vier jaar zal de Commissie een evaluatierapport delen met het Europese Parlement en de Raad. Het kabinet zit ook graag eerdere evaluaties tegemoet bijvoorbeeld met betrekking tot het Cyberschild voorstel en het Cybernoodmechanisme.

e) Constitutionele toets

N.v.t.

7. Implicaties voor uitvoering en/of handhaving

Het voorstel heeft verschillende implicaties voor de uitvoering en handhaving. Zo zal er, op basis van de uitwerking van het Cyberschild, een nationale SOC opgezet en bemenst moeten worden. Daarnaast kunnen er ten tijde van grootschalige incidenten medewerkers van vertrouwde private partijen ingezet worden binnen de overheid. Daarnaast is het van belang dat de gecertificeerde private partijen die onderdeel uit zullen maken van de Cybersecurity Reserve gehandhaafd moeten worden. Binnen het voorstel wordt de ECCC aangewezen om audits uit te voeren op de gezamenlijk aangeschafte tools en infrastructuren binnen de grensoverschrijdende SOCs.

8. Implicaties voor ontwikkelingslanden

Voor zover beoogd zijn er geen implicaties voor ontwikkelingslanden.