EUROPESE
COMMISSIE

Straatsburg, 18.4.2023
COM(2023) 209 final

2023/0109 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

tot vaststelling van maatregelen ter versterking van de solidariteit en de capaciteit in de Unie om cyberdreigingen en -incidenten op te sporen, zich erop voor te bereiden en erop te reageren

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

• Motivering en doel van het voorstel

Deze toelichting hoort bij het voorstel voor een verordening cybersolidariteit. Nu de onderlinge verbondenheid en afhankelijkheid van onze overheidsdiensten, bedrijven en burgers, over sectoren en grenzen heen, groter is dan ooit tevoren, zijn het gebruik en de afhankelijkheid van informatie- en communicatietechnologieën fundamentele aspecten geworden van alle sectoren van de economische activiteit. Door deze grotere verbreiding van digitale technologieën neemt de blootstelling aan cyberbeveiligingsincidenten en de mogelijke gevolgen daarvan toe. Tegelijkertijd worden de lidstaten geconfronteerd met toenemende cyberbeveiligingsrisico's en een algemeen complex dreigingslandschap, met een duidelijk risico dat cyberbeveiligingsincidenten snel van de ene lidstaat naar de andere overslaan.

Bovendien worden cyberoperaties steeds meer geïntegreerd in hybride en oorlogsstrategieën, met aanzienlijke gevolgen voor het doelwit. Met name de militaire agressie van Rusland tegen Oekraïne werd voorafgegaan door en gaat gepaard met een strategie van vijandige cyberoperaties, wat een gamechanger is voor de perceptie en beoordeling van de collectieve paraatheid van de EU betreffende crisisbeheersing op het gebied van cyberbeveiliging en een oproep tot dringende actie. De dreiging van een mogelijk grootschalig incident met aanzienlijke verstoringen van en schade aan kritieke infrastructuur vereist een grotere paraatheid op alle niveaus van de cyberbeveiligingsomgeving van de EU. Deze dreiging gaat verder dan de militaire agressie van Rusland tegen Oekraïne en omvat voortdurende cyberdreigingen van statelijke en niet-statelijke actoren, die waarschijnlijk zullen aanhouden gezien het grote aantal staatsgebonden criminele en hacktivistische actoren die betrokken zijn bij de huidige geopolitieke spanningen. De afgelopen jaren is het aantal cyberaanvallen drastisch toegenomen, waaronder aanvallen op toeleveringsketens ("supplychainaanvallen") met het oog op cyberspionage, het gebruik van gijzelsoftware of verstoring. In 2020 trof de supplychainaanval SolarWinds meer dan 18 000 organisaties wereldwijd, waaronder overheidsinstanties en grote bedrijven. Significante cyberbeveiligingsincidenten kunnen zo ontwrichtend zijn dat een of meer getroffen lidstaten er alleen niet tegen opgewassen zijn. Daarom is meer solidariteit op het niveau van de Unie nodig om cyberdreigingen en -incidenten beter op te sporen en om er beter op voorbereid te zijn en op te kunnen reageren.

Wat de opsporing van cyberdreigingen en -incidenten betreft, is er dringend behoefte aan meer informatie-uitwisseling en betere collectieve capaciteiten om cyberdreigingen veel sneller te kunnen opsporen voordat ze grootschalige schade en kosten kunnen veroorzaken[1]. Hoewel veel cyberdreigingen en -incidenten een potentiële grensoverschrijdende dimensie hebben door de interconnectie van digitale infrastructuur, blijft de uitwisseling van relevante

[1] Volgens een rapport van het Ponemon Institute en IBM Security duurde het in 2022 gemiddeld 207 dagen om een inbreuk vast te stellen, en nog eens 70 dagen om het probleem in te dammen. Tegelijkertijd kosten datalekken die meer dan 200 dagen duurden in 2022 gemiddeld 4,86 miljoen euro, tegenover 3,74 miljoen euro als zij minder dan 200 dagen duurden. ("Cost of a data breach 2022", https://www.ibm.com/reports/data-breach)

informatie tussen de lidstaten beperkt. Het opzetten van een netwerk van landsgrensoverschrijdende centra voor beveiligingsoperaties (SOC's) om de opsporings- en responscapaciteit te verbeteren, moet dit probleem helpen aanpakken.

Wat de paraatheid voor en respons op cyberbeveiligingsincidenten betreft, is er momenteel beperkte steun op het niveau van de Unie en solidariteit tussen de lidstaten. In de conclusies van de Raad van oktober 2021 werd benadrukt dat deze lacunes moeten worden opgevuld door de Commissie op te roepen een voorstel voor een nieuw cyberbeveiligingsnoodfonds in te dienen[2].

Met deze verordening wordt ook uitvoering gegeven aan de in december 2020 aangenomen EU-strategie inzake cyberbeveiliging[3], waarin de oprichting van een Europees cyberschild wordt aangekondigd en waarmee de capaciteit voor het opsporen van cyberdreigingen en het uitwisselen van informatie in de Europese Unie wordt versterkt via een federatie van nationale en landsgrensoverschrijdende SOC's.

Deze verordening bouwt voort op de eerste stappen die reeds in nauwe samenwerking met de belangrijkste belanghebbenden zijn ontwikkeld en door het programma Digitaal Europa worden ondersteund. Wat SOC's betreft, is in het kader van het werkprogramma cyberbeveiliging 2021-2022 van het programma Digitaal Europa met name een oproep gedaan tot het indienen van blijken van belangstelling voor de gezamenlijke aanschaf van instrumenten en infrastructuur voor de oprichting van landsgrensoverschrijdende SOC's, alsook een oproep tot het indienen van voorstellen voor subsidies om de capaciteitsopbouw van SOC's ten dienste van publieke en particuliere organisaties mogelijk te maken. Wat paraatheid voor en respons op incidenten betreft, heeft de Commissie een kortetermijnprogramma opgezet om de lidstaten te ondersteunen, door middel van aanvullende financiering die aan het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) is toegewezen, teneinde de paraatheid voor en de capaciteit om te reageren op grote cyberbeveiligingsincidenten onmiddellijk te versterken. Beide acties zijn voorbereid in nauwe samenwerking met de lidstaten. In deze verordening worden tekortkomingen aangepakt en inzichten uit die acties geïntegreerd.

Ten slotte wordt met dit voorstel tegemoetgekomen aan de toezegging in overeenstemming met de op 10 november aangenomen gezamenlijke mededeling over cyberdefensie[4] om een voorstel voor een EU-initiatief voor cybersolidariteit op te stellen met de volgende doelstellingen: de gemeenschappelijke capaciteiten van de EU op het gebied van opsporing, situationeel bewustzijn en respons versterken, geleidelijk een cyberbeveiligingsreserve op EU-niveau opbouwen met diensten van betrouwbare particuliere aanbieders en het testen van kritieke entiteiten ondersteunen.

---

2 Conclusies van de Raad over de ontwikkeling van de cyberstrategie van de Europese Unie, goedgekeurd door de Raad tijdens zijn zitting van 23 mei 2022 (9364/22)

3 Gezamenlijke mededeling aan het Europees Parlement en de Raad, De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk JOIN(2020) 18 final.

4 Gezamenlijke mededeling aan het Europees Parlement en de Raad, Het EU-beleid op het gebied van cyberdefensie, JOIN(2022) 49 final.

Tegen deze achtergrond stelt de Commissie de huidige verordening cybersolidariteit voor om de solidariteit op het niveau van de Unie te versterken teneinde cyberdreigingen en -incidenten beter op te sporen en om er beter op voorbereid te zijn en op te kunnen reageren door middel van de volgende specifieke doelstellingen:

- de gemeenschappelijke capaciteiten van de EU op het gebied van opsporing en situationeel bewustzijn van cyberdreigingen en -incidenten versterken en aldus bijdragen tot de Europese technologische soevereiniteit op het gebied van cyberbeveiliging;
- de paraatheid van kritieke entiteiten in de hele EU vergroten en de solidariteit versterken door gemeenschappelijke capaciteit op het gebied van de respons op significante of grootschalige cyberbeveiligingsincidenten te ontwikkelen, onder meer door steun voor respons op incidenten beschikbaar te stellen aan derde landen die geassocieerd zijn met het programma Digitaal Europa;
- de weerbaarheid van de Unie vergroten en bijdragen tot een doeltreffende respons door significante of grootschalige incidenten te evalueren en te beoordelen, en daaruit lering te trekken en, in voorkomend geval, aanbevelingen te doen.

Deze doelstellingen worden nagestreefd door middel van de volgende acties:

- De uitrol van een pan-Europese infrastructuur van SOC's (Europees cyberschild) om gemeenschappelijke capaciteiten op het gebied van opsporing en situationeel bewustzijn op te bouwen en te versterken.
- De instelling van een cybernoodmechanisme om de lidstaten te ondersteunen bij de voorbereiding en respons op, en bij het onmiddellijke herstel van, significante en grootschalige cyberbeveiligingsincidenten. Steun voor respons op incidenten wordt ook beschikbaar gesteld aan Europese instellingen, organen en instanties van de Unie.
- De instelling van een Europees evaluatiemechanisme voor cyberbeveiligingsincidenten om specifieke significante of grootschalige incidenten te evalueren en te beoordelen.

Het Europees cyberschild en het cybernoodmechanisme zullen worden ondersteund door financiering uit het programma Digitaal Europa, dat met dit wetgevingsinstrument zal worden gewijzigd om de bovengenoemde acties vast te stellen, financiële steun te verlenen voor de ontwikkeling ervan en de voorwaarden voor het ontvangen van de financiële steun te verduidelijken.

•Verenigbaarheid met bestaande bepalingen op het beleidsterrein

Het EU-kader omvat verschillende reeds bestaande of op Unieniveau voorgestelde wetgevingen om kwetsbaarheden te verminderen, de weerbaarheid van kritieke entiteiten tegen cyberbeveiligingsrisico's te vergroten en het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en -crises te ondersteunen, met name de richtlijn betreffende

maatregelen voor een hoog gezamenlijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (NIS2)[5], de cyberbeveiligingsverordening[6], de richtlijn over aanvallen op informatiesystemen[7] en Aanbeveling (EU) 2017/1584 van de Commissie inzake een gecoördineerde respons op grootschalige cyberbeveiligingsincidenten en -crises[8].

De in het kader van de verordening cybersolidariteit voorgestelde acties hebben betrekking op situationeel bewustzijn, informatie-uitwisseling en steun voor paraatheid voor en respons op cyberbeveiligingsincidenten. Deze acties zijn verenigbaar met en ondersteunen de doelstellingen van het bestaande regelgevingskader op het niveau van de Unie, met name in het kader van Richtlijn (EU) 2022/2555 ("de NIS2-richtlijn"). De verordening cybersolidariteit zal met name voortbouwen op en steun verlenen aan de bestaande kaders voor operationele samenwerking en crisisbeheersing op het gebied van cyberbeveiliging, in het bijzonder het Europees Netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe) en het netwerk van Computer Security Incident Response Teams (CSIRT's).

De platforms van landsgrensoverschrijdende SOC's zouden een nieuwe capaciteit moeten vormen die een aanvulling vormt op het CSIRT-netwerk door gegevens over cyberdreigingen van publieke en private entiteiten te bundelen en te delen, de waarde van die gegevens te vergroten door middel van deskundige analyses en geavanceerde instrumenten, en bij te dragen tot de ontwikkeling van de capaciteiten en de technologische soevereiniteit van de Unie.

Ten slotte is dit voorstel verenigbaar met de aanbeveling van de Raad betreffende een Uniebrede gecoördineerde aanpak om de weerbaarheid van kritieke infrastructuur te versterken[9], waarin de lidstaten wordt verzocht dringende en doeltreffende maatregelen te nemen en loyaal, efficiënt, solidair en gecoördineerd met elkaar, de Commissie en andere relevante overheidsinstanties alsook de betrokken entiteiten samen te werken om kritieke infrastructuur die wordt gebruikt om essentiële diensten op de interne markt te verlenen weerbaarder te maken.

---

5 Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn).

6 Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening)

7 Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad.

8 Voorstel voor een regeling van het Europees Parlement en de Raad betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020, COM(2022) 454 final.

9 Aanbeveling van de Raad van 8 december 2022 betreffende een Uniebrede gecoördineerde aanpak om de weerbaarheid van kritieke infrastructuur te versterken (Voor de EER relevante tekst) 2023/C 20/01.

- **Verenigbaarheid met andere beleidsterreinen van de Unie**

Het voorstel is verenigbaar met andere crisismechanismen en -protocollen, zoals de geïntegreerde regeling politieke crisisrespons (IPCR). De verordening cybersolidariteit zal deze kaders en protocollen voor crisisbeheersing aanvullen door specifieke steun te verlenen voor de paraatheid voor en de respons op cyberbeveiligingsincidenten. Het voorstel zal ook verenigbaar zijn met het externe optreden van de EU in reactie op grootschalige incidenten in het kader van het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB), onder meer via het EU-instrumentarium voor cyberdiplomatie. Het voorstel vormt een aanvulling op acties die worden uitgevoerd in het kader van artikel 42, lid 7, van het Verdrag betreffende de Europese Unie of in situaties als omschreven in artikel 222 van het Verdrag betreffende de werking van de Europese Unie.

Het vormt ook een aanvulling op het in december 2013 ingestelde Uniemechanisme voor civiele bescherming[10] dat is aangevuld met nieuwe wetgeving die in mei 2021 is aangenomen[11] en die de pijlers preventie, paraatheid en respons van het Uniemechanisme voor civiele bescherming versterkt, de EU extra capaciteit geeft om te reageren op nieuwe risico's in Europa en de wereld, en de rescEU-voorraad vergroot.

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

- **Rechtsgrondslag**

De rechtsgrondslag voor dit voorstel is artikel 173, lid 3, en artikel 322, lid 1, punt a), van het Verdrag betreffende de werking van de Europese Unie (VWEU). In artikel 173 van het VWEU is bepaald dat de Unie en de lidstaten ervoor moeten zorgen dat de omstandigheden nodig voor het concurrentievermogen van de industrie van de Unie aanwezig zijn. Deze verordening heeft tot doel de concurrentiepositie van de industrie en de dienstensector in Europa in de gedigitaliseerde economie te versterken en hun digitale transformatie te ondersteunen door het niveau van cyberbeveiliging in de digitale eengemaakte markt te verhogen. Zij is er met name op gericht burgers, bedrijven en in kritieke en zeer kritieke sectoren actieve entiteiten weerbaarder te maken tegen de toenemende cyberdreigingen, die verwoestende maatschappelijke en economische gevolgen kunnen hebben.

Het voorstel is ook gebaseerd op artikel 322, lid 1, punt a), VWEU, want het bevat specifieke regels inzake overdracht die afwijken van het jaarperiodiciteitsbeginsel van Verordening (EU,

---

[10] Besluit nr. 1313/2013/EU van het Europees Parlement en de Raad van 17 december 2013 betreffende een Uniemechanisme voor civiele bescherming (Voor de EER relevante tekst).

[11] Verordening (EU) 2021/836 van het Europees Parlement en de Raad van 20 mei 2021 tot wijziging van Besluit nr. 1313/2013/EU betreffende een Uniemechanisme voor civiele bescherming (Voor de EER relevante tekst).

Euratom) 2018/1046 van het Europees Parlement en de Raad (het "Financieel Reglement")[12]. Met het oog op goed financieel beheer en gezien de onvoorspelbare, uitzonderlijke en specifieke aard van het cyberbeveiligingslandschap en cyberdreigingen, zou het cybernoodmechanisme een zekere mate van flexibiliteit moeten genieten wat begrotingsbeheer betreft, met name door toe te staan dat ongebruikte vastleggings- en betalingskredieten voor acties ter verwezenlijking van de in de verordening beschreven doelstellingen automatisch worden overgedragen naar het volgende begrotingsjaar. Aangezien deze nieuwe regel problemen oplevert met het Financieel Reglement, zou deze kwestie kunnen worden behandeld in het kader van de lopende onderhandelingen over de herziening van het Financieel Reglement.

- **Subsidiariteit (bij niet-exclusieve bevoegdheid)**

De sterke landsgrensoverschrijdende aard van cyberdreigingen en het toenemende aantal risico's en incidenten, die overloopeffecten hebben over grenzen, sectoren en producten heen, maken dat de doelstellingen van het huidige optreden niet doeltreffend door de lidstaten alleen kunnen worden verwezenlijkt en dat de realisatie ervan gemeenschappelijke actie en solidariteit op het niveau van de Unie vereist.

De ervaring met de bestrijding van cyberdreigingen die voortkomen uit de oorlog tegen Oekraïne en de lessen die zijn getrokken uit een cyberbeveiligingsoefening onder het Franse voorzitterschap (EU CyCLES) hebben aangetoond dat concrete mechanismen voor wederzijdse ondersteuning, met name samenwerking met de particuliere sector, zouden moeten worden ontwikkeld om solidariteit op EU-niveau tot stand te brengen. Tegen deze achtergrond wordt de Commissie in de conclusies van de Raad van 23 mei 2022 over de ontwikkeling van de cyberstrategie van de Europese Unie verzocht een voorstel in te dienen voor een nieuw cyberbeveiligingsnoodfonds.

Ondersteuning en acties op het niveau van de Unie om cyberdreigingen beter op te sporen en de paraatheid en responscapaciteit te vergroten, bieden een meerwaarde omdat zo dubbel werk in de Unie en de lidstaten wordt voorkomen. Het zou leiden tot een betere benutting van de bestaande middelen en tot meer coördinatie en uitwisseling van informatie over geleerde lessen. Het cybernoodmechanisme voorziet ook in het verlenen van steun uit de EU-cyberbeveiligingsreserve aan met het programma Digitaal Europa geassocieerde derde landen.

De steun die wordt verleend via de verschillende initiatieven die op het niveau van de Unie moeten worden opgezet en gefinancierd, zal de nationale capaciteiten op het gebied van opsporing, situationeel bewustzijn en paraatheid voor en respons op cyberdreigingen en -incidenten aanvullen en niet overlappen.

[12] Verordening (EU, Euratom) 2018/1046 van het Europees Parlement en de Raad van 18 juli 2018 tot vaststelling van de financiële regels van toepassing op de algemene begroting van de Unie (PB L 193 van 30.7.2018, blz. 1).

• Evenredigheid

De acties gaan niet verder dan wat nodig is om de algemene en specifieke doelstellingen van de verordening te verwezenlijken. De acties in deze verordening doen geen afbreuk aan de verantwoordelijkheden van de lidstaten voor de nationale veiligheid, de openbare veiligheid en het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten. Zij doen evenmin afbreuk aan de wettelijke verplichtingen van in kritieke en zeer kritieke sectoren actieve entiteiten om cyberbeveiligingsmaatregelen vast te stellen overeenkomstig de NIS 2-richtlijn.

De acties die onder deze verordening vallen, vormen een aanvulling op die inspanningen en maatregelen doordat zij de totstandbrenging van infrastructuur voor een betere opsporing en analyse van dreigingen ondersteunen en steun verlenen voor paraatheids- en responsacties in geval van significante of grootschalige incidenten.

• Keuze van het instrument

Het voorstel heeft de vorm van een verordening van het Europees Parlement en de Raad. Dit is het meest geschikte rechtsinstrument, aangezien alleen een verordening, met haar rechtstreeks toepasselijke wettelijke bepalingen, de mate van uniformiteit kan bieden die nodig is voor de instelling en werking van een Europees cyberschild en cybernoodmechanisme, door te voorzien in steun vanuit het programma Digitaal Europa voor de instelling ervan alsook in duidelijke voorwaarden voor het gebruik en de toewijzing van deze steun.

3. EVALUATIE, RAADPLEGING VAN BELANGHEBBENDEN EN EFFECTBEOORDELING

• Raadpleging van belanghebbenden

De acties van deze verordening zullen worden ondersteund door het programma Digitaal Europa, waarover breed overleg is gepleegd. Daarnaast zullen zij voortbouwen op de eerste stappen die in nauwe samenwerking met de belangrijkste belanghebbenden zijn voorbereid. Wat SOC's betreft, heeft de Commissie een conceptnota opgesteld over de ontwikkeling van platforms van landsgrensoverschrijdende SOC's alsook een oproep tot het indienen van blijken van belangstelling in nauwe samenwerking met de lidstaten in het kader van het Europees Kenniscentrum voor cyberbeveiliging (ECCC). In dit verband is een onderzoek naar de capaciteiten van nationale SOC's uitgevoerd en zijn gemeenschappelijke benaderingen en technische vereisten besproken in de technische werkgroep van het ECCC, waarin vertegenwoordigers van de lidstaten zitting hebben. Daarnaast vonden uitwisselingen plaats met het bedrijfsleven, met name via de door Enisa en de Europese organisatie voor cyberbeveiliging (ECSO) opgerichte deskundigengroep inzake SOC's.

Ten tweede heeft de Commissie, wat paraatheid voor en respons op incidenten betreft, een kortetermijnprogramma opgezet om de lidstaten te ondersteunen, door middel van aanvullende financiering uit het programma Digitaal Europa die aan Enisa is toegewezen, teneinde de paraatheid voor en de capaciteit om te reageren op grote cyberbeveiligingsincidenten onmiddellijk te versterken. De tijdens de uitvoering van dit kortetermijnprogramma verzamelde feedback van de lidstaten en het bedrijfsleven biedt reeds waardevolle inzichten die zijn meegenomen bij de voorbereiding van de voorgestelde verordening om de vastgestelde tekortkomingen aan te pakken. Dit was een eerste stap in overeenstemming met de conclusies van de Raad over de cyberstrategie, waarin de Commissie werd verzocht een voorstel voor een nieuw cyberbeveiligingsnoodfonds in te dienen.

Daarnaast heeft op 16 februari 2023 op basis van een discussienota een workshop met deskundigen van de lidstaten over het cybernoodmechanisme plaatsgevonden. Alle lidstaten hebben aan deze workshop deelgenomen en elf lidstaten hebben schriftelijke bijdragen ingediend.

- **Effectbeoordeling**

Gezien de urgentie van het voorstel heeft geen effectbeoordeling plaatsgevonden. De acties van deze verordening zullen worden ondersteund door het programma Digitaal Europa en zijn in overeenstemming met de acties die zijn vastgesteld in de verordening tot oprichting van het programma Digitaal Europa, waarvoor een specifieke effectbeoordeling is uitgevoerd. Deze verordening zal geen andere significante administratieve of milieueffecten met zich meebrengen dan die welke in de effectbeoordeling van de verordening tot oprichting van het programma Digitaal Europa reeds zijn beoordeeld.

Voorts wordt voortgebouwd op de eerste acties die in nauwe samenwerking met de belangrijkste belanghebbenden zijn ontwikkeld, zoals hierboven uiteengezet, en wordt gevolg gegeven aan de oproep van de lidstaten aan de Commissie om tegen het einde van het derde kwartaal van 2022 een voorstel voor een nieuw cyberbeveiligingsnoodfonds in te dienen.

Wat situationeel bewustzijn en opsporing in het kader van het Europees cyberschild betreft, is in het kader van het werkprogramma cyberbeveiliging 2021-2022 van het programma Digitaal Europa met name een oproep gedaan tot het indienen van blijken van belangstelling voor de gezamenlijke aanschaf van instrumenten en infrastructuur voor de oprichting van landsgrensoverschrijdende SOC's, alsook een oproep tot het indienen van voorstellen voor subsidies om de capaciteitsopbouw van SOC's ten dienste van publieke en particuliere organisaties mogelijk te maken.

Wat paraatheid voor en respons op incidenten betreft, heeft de Commissie, zoals hierboven vermeld, een door Enisa uitgevoerd kortetermijnprogramma opgezet ter ondersteuning van de lidstaten vanuit het programma Digitaal Europa. Bij de diensten in kwestie gaat het onder meer om paraatheidsacties, zoals penetratietests van kritieke entiteiten om kwetsbaarheden aan het licht te brengen. Het programma biedt ook meer mogelijkheden om de lidstaten bij te staan in geval van een ernstig incident dat kritieke entiteiten treft. De uitvoering van dit

kortetermijnprogramma door Enisa is aan de gang en heeft reeds relevante inzichten opgeleverd waarmee bij de opstelling van deze verordening rekening is gehouden.

- **Grondrechten**

Door bij te dragen tot de beveiliging van digitale informatie zal dit voorstel bijdragen tot de bescherming van het recht op vrijheid en veiligheid overeenkomstig artikel 6 van het Handvest van de grondrechten van de Europese Unie en tot het recht op eerbiediging van privéleven, familie-en gezinsleven overeenkomstig artikel 7 van het Handvest van de grondrechten van de Europese Unie. Door bedrijven te beschermen tegen economisch schadelijke cyberaanvallen zal het voorstel ook bijdragen tot de vrijheid van ondernemerschap overeenkomstig artikel 16 van het Handvest van de grondrechten van de Europese Unie en tot het recht op eigendom overeenkomstig artikel 17 van het Handvest van de grondrechten van de Europese Unie. Ten slotte zal het voorstel, door de integriteit van kritieke infrastructuur bij cyberaanvallen te beschermen, bijdragen tot het recht op toegang tot preventieve gezondheidszorg en op medische verzorging overeenkomstig artikel 35 van het Handvest van de grondrechten van de Europese Unie en tot het recht op toegang tot diensten van algemeen economisch belang overeenkomstig artikel 36 van het Handvest van de grondrechten van de Europese Unie.

4. GEVOLGEN VOOR DE BEGROTING

De acties van deze verordening zullen worden ondersteund door financiering in het kader van de strategische doelstelling “Cyberbeveiliging” van het programma Digitaal Europa.

De totale begroting omvat een verhoging van 100 miljoen euro – een bedrag waarvan in deze verordening wordt voorgesteld om het over te hevelen van andere strategische doelstellingen van het programma Digitaal Europa. Dit brengt het nieuwe totaalbedrag dat beschikbaar is voor acties op het gebied van cyberbeveiliging in het kader van het programma Digitaal Europa op 842,8 miljoen euro.

Een deel van de extra 100 miljoen euro zal het door het ECCC beheerde budget voor de uitvoering van acties op het gebied van SOC’s en de paraatheid in het kader van hun werkprogramma(’s) verhogen. Bovendien zal de aanvullende financiering dienen ter ondersteuning van de oprichting van de EU-cyberbeveiligingsreserve.

Deze vormt een aanvulling op het budget dat reeds is voorzien voor soortgelijke acties in het belangrijkste werkprogramma en het werkprogramma cyberbeveiliging van het programma Digitaal Europa voor de periode 2023-2027, waardoor het totale bedrag voor de periode 2023-2027 op 551 miljoen euro zou kunnen uitkomen, terwijl 115 miljoen reeds in de vorm van proefprojecten in de periode 2021-2022 is besteed. Inclusief de bijdragen van de lidstaten zou het totale budget kunnen oplopen tot 1,109 miljard euro.

Een overzicht van de betrokken kosten is opgenomen in het financieel memorandum bij dit voorstel.

5. OVERIGE ELEMENTEN

• Uitvoeringsplanning en regelingen betreffende controle, evaluatie en rapportage

De Commissie zal de uitvoering, toepassing en naleving van deze nieuwe bepalingen controleren om de doeltreffendheid ervan te beoordelen. De Commissie legt het Europees Parlement en de Raad uiterlijk vier jaar na de datum van toepassing van deze verordening een verslag over de evaluatie en de toetsing ervan voor.

• Artikelsgewijze toelichting

Algemene doelstellingen, onderwerp en definities (hoofdstuk I)

Hoofdstuk I bevat de doelstellingen van de verordening om de solidariteit op het niveau van de Unie te versterken met het oog op een betere opsporing van, en een betere voorbereiding en respons op, cyberdreigingen en -incidenten, en met name om de gemeenschappelijke opsporing en het situationeel bewustzijn van cyberdreigingen en -incidenten in de Unie te versterken, de paraatheid van in kritieke en zeer kritieke sectoren actieve entiteiten in de gehele Unie te vergroten en de solidariteit te versterken door gemeenschappelijke capaciteiten op het gebied van de respons op significante of grootschalige cyberbeveiligingsincidenten te ontwikkelen en de weerbaarheid van de Unie te vergroten door significante of grootschalige incidenten te evalueren en te beoordelen. In dit hoofdstuk worden ook de acties beschreven waarmee deze doelstellingen zullen worden verwezenlijkt: de uitrol van een Europees cyberschild, de instelling van een cybernoodmechanisme en de instelling van een evaluatiemechanisme voor cyberbeveiligingsincidenten. Het bevat ook de definities die in het instrument worden gebruikt.

Het Europees cyberschild (hoofdstuk II)

In hoofdstuk II wordt het Europees cyberschild vastgesteld en worden de verschillende elementen en de voorwaarden voor deelname uiteengezet. Om te beginnen wordt de algemene doelstelling van het Europees cyberschild beschreven, namelijk de ontwikkeling van geavanceerde capaciteiten voor de Unie om gegevens over cyberdreigingen en -incidenten in de Unie op te sporen, te analyseren en te verwerken, alsook de specifieke operationele doelstellingen. Er wordt gespecificeerd dat de EU-financiering voor het Europees cyberschild zal worden uitgevoerd overeenkomstig de verordening tot oprichting van het programma Digitaal Europa.

Voorts wordt in dit hoofdstuk het soort entiteiten beschreven dat het Europees cyberschild zal vormen. Het schild zal bestaan uit nationale centra voor beveiligingsoperaties (“nationale SOC’s”) en landsgrensoverschrijdende centra voor beveiligingsoperaties (“landsgrensoverschrijdende SOC’s”). Elke deelnemende lidstaat wijst een nationaal SOC aan. Dit fungeert als referentiepunt en toegangspoort tot andere publieke en private

organisaties op nationaal niveau voor het verzamelen en analyseren van informatie over cyberdreigingen en -incidenten en het bijdragen aan een landsgrensoverschrijdend SOC. Na een oproep tot het indienen van blijken van belangstelling kan het ECCC een nationaal SOC selecteren om samen met het ECCC deel te nemen aan een gezamenlijke aanbesteding van instrumenten en infrastructuur en om een subsidie te ontvangen voor het gebruik van de instrumenten en infrastructuur. Indien een nationaal SOC steun van de Unie ontvangt, verbindt het zich ertoe binnen twee jaar een aanvraag tot deelname aan een landsgrensoverschrijdende SOC in te dienen.

Landsgrensoverschrijdende SOC's bestaan uit een consortium van ten minste drie lidstaten, vertegenwoordigd door nationale SOC's, die zich ertoe verbinden samen te werken om hun activiteiten op het gebied van opsporing en controle van cyberdreigingen en -incidenten te coördineren. Na een eerste oproep tot het indienen van blijken van belangstelling kan het ECCC een onderbrengend consortium selecteren om samen met het ECCC deel te nemen aan een gezamenlijke aanbesteding van instrumenten en infrastructuur en om een subsidie voor het gebruik van de instrumenten en infrastructuur te ontvangen. De leden van het onderbrengend consortium sluiten een schriftelijke consortiumovereenkomst waarin hun interne regelingen zijn vastgelegd. In dit hoofdstuk worden vervolgens de vereisten beschreven voor het delen van informatie tussen de deelnemers aan een landsgrensoverschrijdend SOC, en voor het delen van informatie tussen een landsgrensoverschrijdend SOC en andere landsgrensoverschrijdende SOC's, alsook met relevante EU-entiteiten. Nationale SOC's die aan een landsgrensoverschrijdend SOC deelnemen, delen relevante informatie over cyberdreigingen met elkaar. De details, met inbegrip van de toezegging om aanzienlijke hoeveelheden gegevens te delen en de voorwaarden daarvoor, zouden in een consortiumovereenkomst moeten worden vastgelegd. Landsgrensoverschrijdende SOC's zorgen voor een hoog niveau van onderlinge interoperabiliteit. Landsgrensoverschrijdende SOC's zouden ook samenwerkingsovereenkomsten moeten sluiten met andere landsgrensoverschrijdende SOC's, waarin de beginselen voor informatie-uitwisseling worden gespecificeerd. Wanneer landsgrensoverschrijdende SOC's informatie verkrijgen over een mogelijk of lopend grootschalig cyberbeveiligingsincident, verstrekken zij relevante informatie aan EU-CyCLONe, het CSIRT-netwerk en de Commissie, met het oog op hun respectieve taken op het gebied van crisisbeheersing overeenkomstig Richtlijn (EU) 2022/2555. In hoofdstuk II worden tot slot de beveiligingsvoorwaarden voor deelname aan het Europees cyberschild gespecificeerd.

Cybernoodmechanisme (hoofdstuk III)

Bij hoofdstuk III wordt het cybernoodmechanisme ingesteld om de Unie weerbaarder te maken tegen grote cyberdreigingen en om in een geest van solidariteit de kortetermijngevolgen van significante en grootschalige cyberbeveiligingsincidenten of -crises te beperken en zich daarop voor te bereiden. Acties ter uitvoering van het cybernoodmechanisme worden ondersteund met financiering uit het programma Digitaal Europa. Het mechanisme voorziet in acties ter ondersteuning van de paraatheid, met inbegrip van gecoördineerde tests van in zeer kritieke sectoren actieve entiteiten, de respons op en het

onmiddellijke herstel van significante of grootschalige cyberbeveiligingsincidenten of het beperken van significante cyberdreigingen, en wederzijdse-bijstandsacties.

De paraatheidsacties in het kader van het cybernoodmechanisme omvatten het gecoördineerd testen van de paraatheid van in zeer kritieke sectoren actieve entiteiten. De Commissie zou, na raadpleging van Enisa en de NIS-samenwerkingsgroep, regelmatig relevante sectoren of subsectoren van de in bijlage I bij Richtlijn (EU) 2022/2555 vermelde zeer kritieke sectoren moeten vaststellen, waaruit entiteiten aan de gecoördineerde paraatheidstests op EU-niveau kunnen worden onderworpen.

Voor de uitvoering van de voorgestelde responsacties bij incidenten wordt bij deze verordening een EU-cyberbeveiligingsreserve ingesteld, bestaande uit incidentresponsdiensten van betrouwbare aanbieders, geselecteerd volgens de in deze verordening vastgestelde criteria. Tot de gebruikers van de diensten van de EU-cyberbeveiligingsreserve behoren de cybercrisisbeheerautoriteiten en CSIRT's van de lidstaten en de instellingen, organen en instanties van de Unie. De Commissie draagt de algemene verantwoordelijkheid voor de uitvoering van de EU-cyberbeveiligingsreserve en kan Enisa geheel of gedeeltelijk belasten met de werking en het beheer van de EU-cyberbeveiligingsreserve.

Om steun uit de EU-cyberbeveiligingsreserve te ontvangen, zouden de gebruikers zelf maatregelen moeten nemen om de gevolgen van het incident waarvoor om steun wordt verzocht, te beperken. De verzoeken om steun uit de EU-cyberbeveiligingsreserve zouden de nodige relevante informatie moeten bevatten over het incident en de maatregelen die de gebruikers reeds hebben genomen. In dit hoofdstuk worden ook de uitvoeringsmodaliteiten beschreven, met inbegrip van de beoordeling van verzoeken aan de EU-cyberbeveiligingsreserve.

De verordening voorziet ook in de aanbestedingsbeginselen en selectiecriteria met betrekking tot betrouwbare aanbieders van de EU-cyberbeveiligingsreserve.

Derde landen kunnen om steun uit de EU-cyberbeveiligingsreserve verzoeken indien de associatieovereenkomsten die zijn gesloten met betrekking tot hun deelname aan het programma Digitaal Europa daarin voorzien. In dit hoofdstuk worden nadere voorwaarden voor en modaliteiten van een dergelijke deelname beschreven.

Evaluatiemechanisme voor cyberbeveiligingsincidenten (hoofdstuk IV)

Op verzoek van de Commissie, EU-CyCLONe of het CSIRT-netwerk moet Enisa dreigingen, kwetsbaarheden en mitigerende maatregelen met betrekking tot een specifiek significant of grootschalig cyberbeveiligingsincident evalueren en beoordelen. Enisa moet de evaluatie en beoordeling in de vorm van een evaluatieverslag over het incident verstrekken aan het CSIRT-netwerk, EU-CyCLONe en de Commissie om hen te ondersteunen bij het uitvoeren van hun taken. Als het incident betrekking heeft op een derde land, moet de Commissie het verslag delen met de hoge vertegenwoordiger. Het verslag zou geleerde lessen moeten

bevatten en, in voorkomend geval, aanbevelingen om de cyberstrategie van de Unie te verbeteren.

Slotbepalingen (hoofdstuk V)

Hoofdstuk V bevat wijzigingen van de verordening tot oprichting van het programma Digitaal Europa en een verplichting voor de Commissie om met het oog op de evaluatie en herziening van de verordening regelmatig verslagen op te stellen en deze aan het Europees Parlement en de Raad voor te leggen. De Commissie is bevoegd om uitvoeringshandelingen vast te stellen overeenkomstig de in artikel 21 bedoelde onderzoeksprocedure teneinde: de voorwaarden voor deze interoperabiliteit tussen landsgrensoverschrijdende SOC's te specificeren; de procedurele regelingen vast te stellen voor de uitwisseling tussen landsgrensoverschrijdende SOC's en entiteiten van de Unie van informatie in verband met een mogelijk of lopend grootschalig cyberbeveiligingsincident; technische voorschriften vast te stellen om een hoog niveau van gegevensbeveiliging en fysieke beveiliging van de infrastructuur te waarborgen en de veiligheidsbelangen van de Unie te beschermen wanneer informatie wordt gedeeld met entiteiten die geen overheidsinstanties van de lidstaten zijn; de soorten en het aantal responsdiensten die nodig zijn voor de EU-cyberbeveiligingsreserve te specificeren; en de nadere regelingen voor de toewijzing van de ondersteunende diensten van de EU-cyberbeveiligingsreserve te specificeren.

2023/0109 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

tot vaststelling van maatregelen ter versterking van de solidariteit en de capaciteit in de Unie om cyberdreigingen en -incidenten op te sporen, zich erop voor te bereiden en erop te reageren

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 173, lid 3, en artikel 322, lid 1, punt a),

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van de Rekenkamer[1]

Gezien het advies van het Europees Economisch en Sociaal Comité[2],

Gezien het advies van het Comité van de Regio's[3],

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) Nu de onderlinge verbondenheid en afhankelijkheid van onze overheidsdiensten, bedrijven en burgers, over sectoren en grenzen heen, groter is dan ooit tevoren, zijn het gebruik en de afhankelijkheid van informatie- en communicatietechnologieën fundamentele aspecten geworden van alle sectoren van de economische activiteit.

(2) De omvang, frequentie en impact van cyberbeveiligingsincidenten nemen toe, met inbegrip van aanvallen op toeleveringsketens ('supplychainaanvallen") met het oog op cyberspionage, gijzelsoftware of verstoring. Zij vormen een grote bedreiging voor het functioneren van netwerk- en informatiesystemen. Gelet op het snel veranderende dreigingslandschap vereist de dreiging van mogelijke grootschalige incidenten die aanzienlijke verstoringen of schade aan kritieke infrastructuur veroorzaken, een grotere paraatheid op alle niveaus van het cyberbeveiligingskader van de Unie. Deze dreiging gaat verder dan de militaire agressie van Rusland tegen Oekraïne en zal waarschijnlijk aanhouden gezien het grote aantal staatsgebonden criminele en hacktivistische actoren die betrokken zijn bij de huidige geopolitieke spanningen. Dergelijke incidenten kunnen de verlening van openbare diensten en de uitoefening van economische activiteiten, ook in kritieke of zeer kritieke sectoren, belemmeren, aanzienlijke financiële verliezen veroorzaken, het vertrouwen van de gebruikers ondermijnen, grote schade toebrengen aan de economie van de Unie, en zelfs gevolgen voor de gezondheid of levensbedreigende gevolgen hebben. Bovendien zijn cyberbeveiligingsincidenten onvoorspelbaar, aangezien zij vaak zeer snel ontstaan

[1] PB C […], […], blz. […].
[2] PB C , , blz. .
[3] PB C , , blz. .

en evolueren, niet beperkt zijn tot een specifiek geografisch gebied en zich gelijktijdig of onmiddellijk over vele landen verspreiden.

(3) De concurrentiepositie van de industrie en de dienstensector in de Unie in de gedigitaliseerde economie moet worden versterkt en de digitale transformatie ervan moet worden ondersteund door het niveau van cyberbeveiliging in de digitale eengemaakte markt te verhogen. Zoals aanbevolen in drie verschillende voorstellen van de Conferentie over de toekomst van Europa[4], is het noodzakelijk om burgers, bedrijven en entiteiten die kritieke infrastructuur exploiteren weerbaarder te maken tegen de toenemende cyberbedreigingen, die verwoestende maatschappelijke en economische gevolgen kunnen hebben. Daarom is er behoefte aan investeringen in infrastructuur en diensten ter ondersteuning van een snellere opsporing van en respons op cyberdreigingen en -incidenten, en hebben de lidstaten bijstand nodig om zich beter voor te bereiden en beter te kunnen reageren op significante en grootschalige cyberbeveiligingsincidenten. De Unie zou ook haar capaciteit op deze gebieden moeten vergroten, met name wat betreft het verzamelen en analyseren van gegevens over cyberdreigingen en -incidenten.

(4) De Unie heeft reeds een aantal maatregelen genomen om kritieke infrastructuur en entiteiten minder kwetsbaar te maken voor en weerbaarder te maken tegen cyberbeveiligingsrisico's, met name Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad[5], Aanbeveling (EU) 2017/1584 van de Commissie[6], Richtlijn 2013/40/EU van het Europees Parlement en de Raad[7] en Verordening (EU) 2019/881 van het Europees Parlement en de Raad[8]. Daarnaast wordt de lidstaten in de aanbeveling van de Raad betreffende een Uniebrede gecoördineerde aanpak om de weerbaarheid van kritieke infrastructuur te versterken, verzocht dringende en doeltreffende maatregelen te nemen en loyaal, efficiënt, solidair en gecoördineerd met elkaar, de Commissie en andere relevante overheidsinstanties alsook de betrokken entiteiten samen te werken om kritieke infrastructuur die wordt gebruikt om essentiële diensten op de interne markt te verlenen weerbaarder te maken.

(5) De toenemende cyberbeveiligingsrisico's en een algemeen complex dreigingslandschap, met een duidelijk risico dat cyberbeveiligingsincidenten snel overslaan van de ene lidstaat naar de andere en van een derde land naar de Unie, vereisen versterkte solidariteit op het niveau van de Unie om cyberdreigingen en -incidenten beter op te sporen en om er beter op voorbereid te zijn en beter op te kunnen reageren. De lidstaten hebben de Commissie ook verzocht om in de conclusies

---

4 https://futureu.europa.eu/nl/

5 Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (PB L 333 van 27.12.2022).

6 Aanbeveling (EU) 2017/1584 van de Commissie van 13 september 2017 inzake een gecoördineerde respons op grootschalige cyberbeveiligingsincidenten en -crises (PB L 239 van 19.9.2017, blz. 36).

7 Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad (J L 218 van 14.8.2013, blz. 8).

8 Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15).

van de Raad over een EU-cyberstrategie[9] een voorstel voor een nieuw cyberbeveiligingsnoodfonds in te dienen.

(6) In de op 10 november 2022 aangenomen gezamenlijke mededeling over het EU-beleid op het gebied van cyberdefensie[10] werd een EU-initiatief voor cybersolidariteit aangekondigd met de volgende doelstellingen: versterken van de gemeenschappelijke capaciteiten van de EU op het gebied van opsporing, situationeel bewustzijn en respons door de uitrol van een EU-infrastructuur van centra voor beveiligingsoperaties (’sOC’s”) te bevorderen, de geleidelijke opbouw van een cyberbeveiligingsreserve op EU-niveau met diensten van betrouwbare particuliere aanbieders te ondersteunen en kritieke entiteiten op basis van EU-risicobeoordelingen op mogelijke kwetsbaarheden te testen.

(7) Het is noodzakelijk de opsporing en het situationeel bewustzijn van cyberdreigingen en -incidenten in de hele Unie te versterken en de solidariteit te versterken door de paraatheid van de lidstaten en de Unie voor, alsook hun vermogen om te reageren op, significante en grootschalige cyberbeveiligingsincidenten te verbeteren. Daarom zou een pan-Europese infrastructuur van SOC’s (Europees cyberschild) moeten worden uitgerold om gemeenschappelijke capaciteiten op het gebied van opsporing en situationeel bewustzijn op te bouwen en te versterken; er zou een cybernoodmechanisme moeten worden ingesteld om de lidstaten te ondersteunen bij de voorbereiding en respons op, en bij het onmiddellijke herstel van, significante en grootschalige cyberbeveiligingsincidenten; er zou een evaluatiemechanisme voor cyberbeveiligingsincidenten moeten worden ingesteld om specifieke significante of grootschalige incidenten te evalueren en te beoordelen. Deze acties laten de artikelen 107 en 108 van het Verdrag betreffende de werking van de Europese Unie (“VWEU”) onverlet.

(8) Om deze doelstellingen te bereiken, is het ook noodzakelijk Verordening (EU) 2021/694 van het Europees Parlement en de Raad[11] op bepaalde gebieden te wijzigen. Deze verordening zou met name Verordening (EU) 2021/694 wijzigen wat betreft de toevoeging van nieuwe operationele doelstellingen in verband met het Europees cyberschild en het cybernoodmechanisme in het kader van specifieke doelstelling 3 van het programma Digitaal Europa, dat erop gericht is de weerbaarheid, integriteit en betrouwbaarheid van de digitale eengemaakte markt te waarborgen, de capaciteit om cyberaanvallen en -dreigingen te monitoren en erop te reageren te versterken, en de landsgrensoverschrijdende samenwerking op het gebied van cyberbeveiliging te versterken. Dit zal worden aangevuld met de specifieke voorwaarden waaronder financiële steun voor deze acties kan worden verleend en de governance- en coördinatiemechanismen die nodig zijn om de beoogde doelstellingen te verwezenlijken, moeten worden vastgesteld. Andere wijzigingen van Verordening (EU) 2021/694 moeten beschrijvingen van voorgestelde acties in het kader van de nieuwe operationele doelstellingen omvatten, evenals meetbare indicatoren om de uitvoering van deze nieuwe operationele doelstellingen te monitoren.

---

9 Conclusies van de Raad over de ontwikkeling van de cyberstrategie van de Europese Unie, goedgekeurd door de Raad tijdens zijn zitting van 23 mei 2022 (9364/22).

10 Gezamenlijke mededeling aan het Europees Parlement en de Raad, Het EU-beleid op het gebied van cyberdefensie, JOIN(2022) 49 final.

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

(9) De financiering van acties in het kader van deze verordening moet worden voorzien in Verordening (EU) 2021/694, die de relevante basishandeling moet blijven voor deze acties die zijn vastgelegd in specifieke doelstelling 3 van het programma Digitaal Europa. Specifieke voorwaarden voor deelname aan elke actie zullen worden vastgesteld in de desbetreffende werkprogramma's, overeenkomstig de toepasselijke bepaling van Verordening (EU) 2021/694.

(10) De horizontale financiële regels die het Europees Parlement en de Raad op grond van artikel 322 VWEU hebben vastgesteld, zijn op deze verordening van toepassing. Deze regels zijn vastgelegd in het Financieel Reglement en bepalen met name de procedure voor het opstellen en uitvoeren van de begroting van de Unie, en zij voorzien in controles op de verantwoordelijkheid van financiële actoren. De op grond van artikel 322 VWEU vastgestelde regels omvatten ook een algemeen conditionaliteitsregime ter bescherming van de Uniebegroting zoals vastgesteld in Verordening (EU, Euratom) 2020/2092 van het Europees Parlement en de Raad.

(11) Met het oog op een goed financieel beheer moeten specifieke regels worden vastgesteld voor de overdracht van ongebruikte vastleggings- en betalingskredieten. Met inachtneming van het beginsel dat de begroting van de Unie jaarlijks wordt vastgesteld, zou deze verordening, vanwege de onvoorspelbare, uitzonderlijke en specifieke aard van het cyberbeveiligingslandschap, moeten voorzien in mogelijkheden om ongebruikte middelen over te dragen naast de in het Financieel Reglement vastgestelde middelen, zodat de capaciteit van het cybernoodmechanisme om de lidstaten te ondersteunen bij de doeltreffende bestrijding van cyberdreigingen, wordt gemaximaliseerd.

(12) Om cyberdreigingen en -incidenten doeltreffender te voorkomen en te beoordelen en er doeltreffender op te reageren, is het noodzakelijk meer kennis te ontwikkelen over de bedreigingen voor kritieke activa en infrastructuur op het grondgebied van de Unie, met inbegrip van de geografische spreiding, interconnectie en mogelijke gevolgen ervan in geval van cyberaanvallen die deze infrastructuur treffen. Er moet een grootschalige EU-infrastructuur van SOC's worden uitgerold ("het Europees cyberschild"), bestaande uit verscheidene interoperabele landsgrensoverschrijdende platforms, die elk verscheidene nationale SOC's groeperen. Die infrastructuur moet de belangen en behoeften van de lidstaten en de Unie op het gebied van cyberbeveiliging dienen, door gebruik te maken van de modernste technologie voor geavanceerde instrumenten voor gegevensverzameling en -analyse, de capaciteit voor de opsporing en het beheer van cyberdreigingen en -incidenten te verbeteren en realtime situationeel bewustzijn te bieden. Die infrastructuur moet dienen om de opsporing van cyberdreigingen en -incidenten te verbeteren en aldus de entiteiten en netwerken van de Unie die verantwoordelijk zijn voor crisisbeheersing in de Unie, met name het Europees Netwerk van verbindingsorganisaties voor cybercrises ("EU-CyCLONe"), zoals gedefinieerd in Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad[12], aan te vullen en te ondersteunen.

(13) Elke lidstaat moet een overheidsinstantie op nationaal niveau aanwijzen die belast is met de coördinatie van de activiteiten voor het opsporen van cyberdreigingen in die

[12] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PB L 333 van 27.12.2022, blz. 80).

lidstaat. Deze nationale SOC's moeten fungeren als referentiepunt en toegangspoort op nationaal niveau voor deelname aan het Europees cyberschild en moeten ervoor zorgen dat informatie over cyberdreigingen van publieke en private entiteiten op doeltreffende en gestroomlijnde wijze op nationaal niveau wordt gedeeld en verzameld.

(14) Als onderdeel van het Europees cyberschild moet een aantal landsgrensoverschrijdende centra voor cyberbeveiligingsoperaties ("landsgrensoverschrijdende SOC's") worden opgericht. Deze moeten de nationale SOC's van ten minste drie lidstaten samenbrengen, om ten volle voordeel te halen uit de landsgrensoverschrijdende opsporing van dreigingen alsook uit informatie-uitwisseling en -beheer. De algemene doelstelling van landsgrensoverschrijdende SOC's moet zijn: het versterken van de capaciteit voor het analyseren, voorkomen en opsporen van cyberdreigingen en het ondersteunen van de productie van hoogwaardige inlichtingen over cyberdreigingen, met name door het delen van gegevens uit diverse publieke of private bronnen, alsook door het delen en gezamenlijk gebruiken van geavanceerde instrumenten, en het gezamenlijk ontwikkelen van opsporings-, analyse- en preventiecapaciteiten in een betrouwbare omgeving. Zij moeten nieuwe aanvullende capaciteit bieden, voortbouwend en als aanvulling op bestaande SOC's en Computer Security Incident Response Teams (CSIRT's) en andere relevante actoren.

(15) Op nationaal niveau worden de monitoring, opsporing en analyse van cyberdreigingen doorgaans verzorgd door SOC's van publieke en private entiteiten, in combinatie met CSIRT's. Daarnaast wisselen CSIRT's informatie uit in het kader van het CSIRT-netwerk, overeenkomstig Richtlijn (EU) 2022/2555. De landsgrensoverschrijdende SOC's moeten een nieuwe capaciteit vormen die een aanvulling vormt op het CSIRT-netwerk door gegevens over cyberdreigingen van publieke en private entiteiten te bundelen en te delen, de waarde van die gegevens te vergroten door middel van deskundige analyses en gezamenlijk verworven infrastructuren en geavanceerde instrumenten, en bij te dragen tot de ontwikkeling van de capaciteiten en de technologische soevereiniteit van de Unie.

(16) De landsgrensoverschrijdende SOC's moeten fungeren als centraal punt dat het mogelijk maakt relevante gegevens en informatie over cyberdreigingen breed te bundelen en dreigingsinformatie te verspreiden onder een grote en diverse groep actoren (bv. computercrisisresponsteams ("CERT's"), CSIRT's, centra voor informatie-uitwisseling en -analyse ("ISAC's"), exploitanten van kritieke infrastructuur). De informatie die tussen deelnemers aan een landsgrensoverschrijdend SOC wordt uitgewisseld, kan onder meer bestaan uit gegevens afkomstig van netwerken en sensoren, informatiebronnen over dreigingen, indicatoren voor aantasting en gecontextualiseerde informatie over incidenten, dreigingen en kwetsbaarheden. Daarnaast moeten landsgrensoverschrijdende SOC's ook samenwerkingsovereenkomsten sluiten met andere landsgrensoverschrijdende SOC's.

(17) Een gedeeld situationeel bewustzijn onder de betrokken autoriteiten is een absolute voorwaarde voor paraatheid en coördinatie in de hele Unie met betrekking tot significante en grootschalige cyberbeveiligingsincidenten. Bij Richtlijn (EU) 2022/2555 wordt EU-CyCLONe opgericht om het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en -crises op operationeel niveau te ondersteunen en om ervoor te zorgen dat relevante informatie regelmatig tussen de lidstaten en de instellingen, organen en instanties van de Unie wordt uitgewisseld. In Aanbeveling (EU) 2017/1584 inzake een gecoördineerde respons op grootschalige

cyberbeveiligingsincidenten en -crises wordt ingegaan op de rol van alle relevante actoren. In richtlijn (EU) 2022/2555 wordt ook herinnerd aan de verantwoordelijkheden van de Commissie in het bij Besluit 1313/2013/EU van het Europees Parlement en de Raad ingestelde Uniemechanisme voor civiele bescherming, alsmede voor het verstrekken van analytische verslagen voor de geïntegreerde regeling politieke crisisrespons (IPCR) in het kader van Uitvoeringsbesluit (EU) 2018/1993. In situaties waarin landsgrensoverschrijdende SOC's informatie verkrijgen over een mogelijk of lopend grootschalig cyberbeveiligingsincident, moeten zij daarom relevante informatie verstrekken aan EU-CyCLONe, het CSIRT-netwerk en de Commissie. Afhankelijk van de situatie kan de te delen informatie met name bestaan uit technische informatie, informatie over de aard en de motieven van de aanvaller of potentiële aanvaller, en niet-technische informatie op hoger niveau over een mogelijk of lopend grootschalig cyberbeveiligingsincident. In dit verband moet terdege rekening worden gehouden met het "need-to-know" -beginsel en met de mogelijk gevoelige aard van de gedeelde informatie.

(18) Entiteiten die deelnemen aan het Europees cyberschild moeten zorgen voor een hoog niveau van interoperabiliteit, onder meer, in voorkomend geval, wat betreft gegevensformaten, taxonomie, instrumenten voor gegevensverwerking en -analyse, en beveiligde communicatiekanalen, een minimumniveau van beveiliging van de applicatielaag, een dashboard voor situationeel bewustzijn en indicatoren. Bij de vaststelling van een gemeenschappelijke taxonomie en de ontwikkeling van een model voor situatieverslagen om de technische oorzaak en gevolgen van cyberbeveiligingsincidenten te beschrijven, moet rekening worden gehouden met de lopende werkzaamheden inzake de melding van incidenten in het kader van de uitvoering van Richtlijn (EU) 2022/2555.

(19) Om de grootschalige uitwisseling van gegevens over cyberdreigingen uit verschillende bronnen in een betrouwbare omgeving mogelijk te maken, moeten entiteiten die deelnemen aan het Europees cyberschild worden uitgerust met geavanceerde en zeer veilige instrumenten, apparatuur en infrastructuur. Dit moet het mogelijk maken de collectieve opsporingscapaciteit en de tijdige waarschuwingen aan autoriteiten en relevante entiteiten te verbeteren, met name door gebruik te maken van de nieuwste technologieën op het gebied van artificiële intelligentie (AI) en gegevensanalyse.

(20) Door gegevens te verzamelen , te delen en uit te wisselen, moet het Europees cyberschild de technologische soevereiniteit van de Unie versterken. De bundeling van hoogwaardige samengestelde gegevens moet ook bijdragen tot de ontwikkeling van geavanceerde technologieën op het gebied van artificiële intelligentie (AI) en gegevensanalyse. Dit moet worden vergemakkelijkt door het Europees cyberschild te verbinden met de pan-Europese high-performance computing-infrastructuur die is opgericht bij Verordening (EU) 2021/1173 van de Raad[13].

(21) Hoewel het Europees cyberschild een civiel project is, zou de cyberdefensiegemeenschap kunnen profiteren van sterkere capaciteiten op het gebied van civiele opsporing en situationeel bewustzijn die zijn ontwikkeld voor de bescherming van kritieke infrastructuur. Landsgrensoverschrijdende SOC's moeten, met steun van de Commissie en het Europees Kenniscentrum voor cyberbeveiliging

[13] Verordening (EU) 2021/1173 van de Raad van 13 juli 2021 tot oprichting van de Gemeenschappelijke Onderneming Europese high-performance computing en tot intrekking van Verordening (EU) 2018/1488 (PB L 256 van 19.7.2021, blz. 3).

("ECCC"), en in samenwerking met de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid (de "hoge vertegenwoordiger"), geleidelijk specifieke protocollen en normen ontwikkelen om samenwerking met de cyberdefensiegemeenschap mogelijk te maken, met inbegrip van doorlichting en beveiligingsvoorwaarden. De ontwikkeling van het Europees cyberschild moet gepaard gaan met een reflectie die het mogelijk maakt om in de toekomst samen te werken met netwerken en platforms die verantwoordelijk zijn voor informatie-uitwisseling in de cyberdefensiegemeenschap, in nauwe samenwerking met de hoge vertegenwoordiger.

(22) De uitwisseling van informatie tussen deelnemers aan het Europees cyberschild moet in overeenstemming zijn met de bestaande wettelijke voorschriften en in het bijzonder met de uniale en nationale wetgeving inzake gegevensbescherming, alsook met de mededingingsregels van de Unie die van toepassing zijn op de uitwisseling van informatie. De ontvanger van de informatie moet, voor zover de verwerking van persoonsgegevens noodzakelijk is, technische en organisatorische maatregelen nemen om de rechten en vrijheden van de betrokkenen te beschermen, moet de gegevens vernietigen zodra zij niet langer nodig zijn voor het aangegeven doel, en moet de instantie die de gegevens ter beschikking stelt ervan in kennis stellen dat de gegevens zijn vernietigd.

(23) Onverminderd artikel 346 VWEU moet de uitwisseling van informatie die op grond van uniale of nationale regelgeving vertrouwelijk is, beperkt blijven tot informatie die relevant is voor en in verhouding staat tot het doel van die uitwisseling. Bij de uitwisseling van dergelijke informatie moet de vertrouwelijkheid van de informatie worden gewaarborgd en moeten de veiligheids- en commerciële belangen van de betrokken entiteiten worden beschermd, met volledige inachtneming van handels- en bedrijfsgeheimen.

(24) Gezien de toenemende risico's en het groeiende aantal cyberbeveiligingsincidenten waarmee de lidstaten te maken krijgen, moet een instrument voor crisisondersteuning worden opgezet om de Unie weerbaarder te maken tegen significante en grootschalige cyberbeveiligingsincidenten en moeten de acties van de lidstaten worden aangevuld met financiële noodsteun voor paraatheid, respons en onmiddellijk herstel van essentiële diensten. Dat instrument moet het mogelijk maken om in welbepaalde omstandigheden en onder duidelijke voorwaarden snel bijstand te verlenen en om het gebruik van de middelen zorgvuldig te monitoren en te evalueren. Hoewel de primaire verantwoordelijkheid voor de preventie van, en voor de voorbereiding en respons op, cyberbeveiligingsincidenten en -crises bij de lidstaten ligt, bevordert het cybernoodmechanisme de solidariteit tussen de lidstaten overeenkomstig artikel 3, lid 3, van het Verdrag betreffende de Europese Unie ("VEU").

(25) Het cybernoodmechanisme moet steun verlenen aan de lidstaten ter aanvulling van hun eigen maatregelen en middelen, en andere bestaande steunmogelijkheden in geval van respons op en onmiddellijk herstel van significante en grootschalige cyberbeveiligingsincidenten, zoals de diensten die het Agentschap van de Europese Unie voor cyberbeveiliging ("Enisa") overeenkomstig zijn mandaat verleent, de gecoördineerde respons en de bijstand van het CSIRT-netwerk, de mitigatiesteun van EU-CyCLONe, alsook wederzijdse bijstand tussen de lidstaten, onder meer in het kader van artikel 42, lid 7, VEU, de snellereactieteams bij cyberbeveiligingsincidenten

van de PESCO[14] en de snellereactieteams bij hybride dreigingen. Het moet voorzien in de noodzaak ervoor te zorgen dat er gespecialiseerde middelen beschikbaar zijn om de paraatheid voor en de respons op cyberbeveiligingsincidenten in de hele Unie en in derde landen te ondersteunen.

(26) Dit instrument doet geen afbreuk aan procedures en kaders voor de coördinatie van crisisrespons op het niveau van de Unie, met name het Uniemechanisme voor civiele bescherming[15], de geïntegreerde EU-regeling politieke crisisrespons (IPCR[16,]) en Richtlijn (EU) 2022/2555. Het kan bijdragen tot of een aanvulling vormen op acties die worden uitgevoerd in het kader van artikel 42, lid 7, VEU of in situaties als omschreven in artikel 222 VWEU. Het gebruik van dit instrument moet in voorkomend geval ook worden gecoördineerd met de uitvoering van de maatregelen van het instrumentarium voor cyberdiplomatie.

(27) De in het kader van deze verordening verleende bijstand moet de acties van de lidstaten op nationaal niveau ondersteunen en aanvullen. Daartoe moet worden gezorgd voor nauwe samenwerking en overleg tussen de Commissie en de getroffen lidstaat. Bij een verzoek om steun in het kader van het cybernoodmechanisme moet de lidstaat relevante informatie verstrekken die de noodzaak van de steun rechtvaardigt.

(28) Krachtens Richtlijn (EU) 2022/2555 moeten de lidstaten een of meer cybercrisisbeheerautoriteiten aanwijzen of oprichten en ervoor zorgen dat deze over voldoende middelen beschikken om hun taken doeltreffend en efficiënt uit te voeren. Ook moeten de lidstaten capaciteiten, middelen en procedures vaststellen die in geval van een crisis kunnen worden ingezet, en moeten zij een nationaal plan voor respons op grootschalige cyberbeveiligingsincidenten en -crises aannemen waarin de doelstellingen van en regelingen voor het beheer van grootschalige cyberbeveiligingsincidenten en -crises zijn uiteengezet. De lidstaten moeten ook een of meer CSIRT's oprichten die belast zijn met de behandeling van incidenten volgens een welomschreven proces en die ten minste de sectoren, subsectoren en soorten entiteiten bestrijken die onder het toepassingsgebied van die richtlijn vallen, en moeten ervoor zorgen dat zij over voldoende middelen beschikken om hun taken doeltreffend uit te voeren. Deze verordening doet geen afbreuk aan de rol van de Commissie om ervoor te zorgen dat de lidstaten de verplichtingen van Richtlijn (EU) 2022/2555 nakomen. Het cybernoodmechanisme moet bijstand verlenen voor acties die gericht zijn op het verbeteren van de paraatheid en voor responsacties bij incidenten om de gevolgen van significante en grootschalige cyberbeveiligingsincidenten te beperken, onmiddellijk herstel te ondersteunen en/of de werking van essentiële diensten te herstellen.

(29) Om een consistente aanpak te bevorderen en de veiligheid in de hele Unie en haar interne markt te verbeteren, moet als onderdeel van de paraatheidsacties steun worden verleend voor het op gecoördineerde wijze testen en beoordelen van de cyberbeveiliging van entiteiten die actief zijn in sectoren die in Richtlijn (EU) 2022/2555 als zeer kritieke sectoren zijn aangemerkt. Daartoe moet de Commissie,

---

14 Besluit (GBVB) 2017/2315 van de Raad van 11 december 2017 tot instelling van de permanente gestructureerde samenwerking (PESCO) en tot opstelling van de lijst van deelnemende lidstaten.

15 Besluit nr. 1313/2013/EU van het Europees Parlement en de Raad van 17 december 2013 betreffende een Uniemechanisme voor civiele bescherming (PB L 347 van 20.12.2013, blz. 924).

16 Geïntegreerde regelingen politieke crisisrespons (IPCR) en in overeenstemming met Aanbeveling (EU) 2017/1584 van de Commissie van 13 september 2017 inzake een gecoördineerde respons op grootschalige cyberbeveiligingsincidenten en -crises.

met de steun van Enisa en in samenwerking met de bij Richtlijn (EU) 2022/2555 opgerichte NIS-samenwerkingsgroep, regelmatig relevante sectoren of subsectoren vaststellen die in aanmerking moeten komen om financiële steun te ontvangen voor gecoördineerde tests op het niveau van de Unie. De sectoren of subsectoren moeten worden gekozen uit bijlage I bij Richtlijn (EU) 2022/2555 ("zeer kritieke sectoren"). De gecoördineerde tests moeten gebaseerd zijn op gemeenschappelijke risicoscenario's en -methoden. Bij de selectie van sectoren en de ontwikkeling van risicoscenario's moet rekening worden gehouden met relevante Uniebrede risicobeoordelingen en risicoscenario's, met inbegrip van de noodzaak om dubbel werk te voorkomen, zoals de risicobeoordeling en risicoscenario's waarom wordt verzocht in de conclusies van de Raad over de ontwikkeling van de cyberstrategie van de Europese Unie en die door de Commissie, de hoge vertegenwoordiger en de NIS-samenwerkingsgroep moeten worden uitgevoerd, in coördinatie met de betrokken civiele en militaire organen en instanties en gevestigde netwerken, waaronder EU-CyCLONe, alsmede de risicobeoordeling van communicatienetwerken en -infrastructuur waarom is verzocht in het kader van de gezamenlijke ministeriële oproep van Nevers en die wordt uitgevoerd door de NIS-samenwerkingsgroep, met de steun van de Commissie en Enisa, en in samenwerking met het Orgaan van Europese regulerende instanties voor elektronische communicatie (Berec), de gecoördineerde risicobeoordelingen die moeten worden uitgevoerd krachtens artikel 22 van Richtlijn (EU) 2022/2555 en het testen van de digitale operationele weerbaarheid als bedoeld in Verordening (EU) 2022/2554 van het Europees Parlement en de Raad[17]. Bij de selectie van sectoren moet ook rekening worden gehouden met de aanbeveling van de Raad betreffende een Uniebrede gecoördineerde aanpak om de weerbaarheid van kritieke infrastructuur te versterken.

(30) Daarnaast moet het cybernoodmechanisme steun bieden voor andere paraatheidsacties en de paraatheid ondersteunen in andere sectoren die niet vallen onder de gecoördineerde tests van in zeer kritieke sectoren actieve entiteiten. Deze acties kunnen verschillende soorten nationale paraatheidsactiviteiten omvatten.

(31) Het cybernoodmechanisme moet ook steun verlenen voor responsacties bij incidenten om de gevolgen van significante en grootschalige cyberbeveiligingsincidenten te beperken, onmiddellijk herstel te ondersteunen of de werking van essentiële diensten te herstellen. In voorkomend geval moet het het UCPM aanvullen om te zorgen voor een alomvattende aanpak van de gevolgen van cyberbeveiligingsincidenten voor de burgers.

(32) Het cybernoodmechanisme moet de door de lidstaten verleende bijstand aan een lidstaat die is getroffen door een significant of grootschalig cyberbeveiligingsincident steunen, onder meer via het in artikel 15 van Richtlijn (EU) 2022/2555 bedoelde CSIRT-netwerk. De lidstaten die bijstand verlenen, moeten kunnen verzoeken om dekking van de kosten in verband met het uitzenden van deskundigenteams in het kader van wederzijdse bijstand. De subsidiabele kosten kunnen de reis- en verblijfkosten en de dagvergoedingen van cyberbeveiligingsdeskundigen omvatten.

[17] Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011

(33) Er moet geleidelijk een cyberbeveiligingsreserve op Unieniveau worden opgezet, bestaande uit diensten van particuliere aanbieders van beheerde beveiligingsdiensten ter ondersteuning van responsacties en acties gericht op onmiddellijk herstel in geval van significante of grootschalige cyberbeveiligingsincidenten. De EU-cyberbeveiligingsreserve moet de beschikbaarheid en paraatheid van de diensten waarborgen. De diensten van de EU-cyberbeveiligingsreserve moeten dienen om de nationale autoriteiten te ondersteunen bij het verlenen van bijstand aan getroffen in kritieke of zeer kritieke sectoren actieve entiteiten, als aanvulling op hun eigen acties op nationaal niveau. Bij een verzoek om steun uit de EU-cyberbeveiligingsreserve moeten de lidstaten specificeren welke steun op nationaal niveau aan de getroffen entiteit is verleend, waarmee rekening moet worden gehouden bij de beoordeling van het verzoek van de lidstaat. De diensten van de EU-cyberbeveiligingsreserve kunnen ook dienen ter ondersteuning van instellingen, organen en instanties van de Unie, onder vergelijkbare voorwaarden.

(34) Met het oog op de selectie van particuliere aanbieders die diensten verlenen in het kader van de EU-cyberbeveiligingsreserve moet een reeks minimumcriteria worden vastgesteld die moeten worden opgenomen in de aanbesteding voor de selectie van deze dienstverleners teneinde ervoor te zorgen dat wordt voldaan aan de behoeften van de autoriteiten van de lidstaten en de in kritieke of zeer kritieke sectoren actieve entiteiten.

(35) Om de oprichting van de EU-cyberbeveiligingsreserve te ondersteunen, zou de Commissie kunnen overwegen Enisa te verzoeken een potentiële certificeringsregeling overeenkomstig Verordening (EU) 2019/881 op te stellen voor beheerde beveiligingsdiensten op de gebieden die onder het cybernoodmechanisme vallen.

(36) Om de doelstellingen van deze verordening te ondersteunen, namelijk het bevorderen van gedeeld situationeel bewustzijn, het vergroten van de weerbaarheid van de Unie en het mogelijk maken van een doeltreffende respons op significante en grootschalige cyberbeveiligingsincidenten, moeten EU-CyCLONe, het CSIRT-netwerk of de Commissie Enisa kunnen verzoeken om dreigingen, kwetsbaarheden en mitigatiemaatregelen met betrekking tot een specifiek significant of grootschalig cyberbeveiligingsincident te evalueren en te beoordelen. Na de voltooiing van een evaluatie en beoordeling van een incident moet Enisa in samenwerking met relevante belanghebbenden, waaronder vertegenwoordigers van de particuliere sector, de lidstaten, de Commissie en andere relevante instellingen, organen en instanties van de EU een evaluatieverslag over het incident opstellen. Wat de particuliere sector betreft, ontwikkelt Enisa kanalen voor de uitwisseling van informatie met gespecialiseerde aanbieders, waaronder aanbieders van beheerde beveiligingsoplossingen en verkopers, om bij te dragen tot de opdracht van Enisa om in de hele Unie een hoog gemeenschappelijk niveau van cyberbeveiliging te bereiken. Voortbouwend op de samenwerking met belanghebbenden, met inbegrip van de particuliere sector, moet het evaluatieverslag over specifieke incidenten gericht zijn op het beoordelen van de oorzaken en gevolgen van een incident alsook de maatregelen om het incident te beperken nadat het zich heeft voorgedaan. Bijzondere aandacht dient uit te gaan naar de inbreng van, en de lessen die worden gedeeld door, de aanbieders van beheerde beveiligingsdiensten die voldoen aan de voorwaarden hoogste professionele integriteit, onpartijdigheid en vereiste technische deskundigheid, zoals in deze verordening vereist. Het verslag moet worden ingediend bij en als input dienen voor de werkzaamheden van EU-CyCLONe, het CSIRT-netwerk en de Commissie. Als het

incident betrekking heeft op een derde land, zal de Commissie het verslag ook delen met de hoge vertegenwoordiger.

(37) Gezien de onvoorspelbare aard van cyberaanvallen en het feit dat deze vaak niet beperkt zijn tot een specifiek geografisch gebied en een groot risico op overloopeffecten inhouden, draagt de versterking van de weerbaarheid van buurlanden en hun capaciteit om doeltreffend te reageren op significante en grootschalige cyberbeveiligingsincidenten bij tot de bescherming van de Unie als geheel. Daarom kunnen met het programma Digitaal Europa geassocieerde derde landen steun ontvangen uit de EU-cyberbeveiligingsreserve indien daarin is voorzien in de desbetreffende associatieovereenkomst met het programma Digitaal Europa. De financiering voor geassocieerde derde landen moet door de Unie worden ondersteund in het kader van relevante partnerschappen en financieringsinstrumenten voor die landen. De steun moet betrekking hebben op diensten op het gebied van respons op en onmiddellijk herstel van significante of grootschalige cyberbeveiligingsincidenten. De in deze verordening vastgestelde voorwaarden voor de EU-cyberbeveiligingsreserve en betrouwbare aanbieders moeten gelden wanneer steun wordt verleend aan de met het programma Digitaal Europa geassocieerde derde landen.

(38) Om eenvormige voorwaarden voor de uitvoering van deze verordening te waarborgen, moeten aan de Commissie uitvoeringsbevoegdheden worden toegekend om de voorwaarden voor de interoperabiliteit tussen landsgrensoverschrijdende SOC's te specificeren; de procedurele regelingen vast te stellen voor de uitwisseling van informatie in verband met een mogelijk of lopend grootschalig cyberbeveiligingsincident tussen landsgrensoverschrijdende SOC's en entiteiten van de Unie; technische voorschriften vast te stellen om de beveiliging van het Europees cyberschild te waarborgen; de soorten en het aantal responsdiensten die nodig zijn voor de EU-cyberbeveiligingsreserve te specificeren; en de nadere regelingen voor de toewijzing van de ondersteunende diensten van de EU-cyberbeveiligingsreserve te specificeren. Die bevoegdheden moeten worden uitgeoefend in overeenstemming met Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad.

(39) De doelstelling van deze verordening kan beter op het niveau van de Unie dan door de lidstaten worden verwezenlijkt. De Unie kan derhalve maatregelen nemen overeenkomstig de in artikel 5 van het Verdrag betreffende de Europese Unie neergelegde beginselen van subsidiariteit en evenredigheid. Deze verordening gaat niet verder dan wat nodig is om dat doel te bereiken.

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

Hoofdstuk I

ALGEMENE DOELSTELLINGEN, ONDERWERP EN DEFINITIES

Artikel 1

Onderwerp en doelstellingen

1. Bij deze verordening worden maatregelen vastgesteld ter versterking van de capaciteit in de Unie om cyberdreigingen en -incidenten op te sporen, zich erop voor te bereiden en erop te reageren, met name door middel van de volgende acties:

a) de uitrol van een pan-Europese infrastructuur van centra voor beveiligingsoperaties ("Europees cyberschild") om gemeenschappelijke capaciteiten op het gebied van opsporing en situationeel bewustzijn op te bouwen en te versterken;

b) de instelling van een cybernoodmechanisme om de lidstaten te ondersteunen bij de voorbereiding en respons op, en bij het onmiddellijke herstel van, significante en grootschalige cyberbeveiligingsincidenten;

c) de instelling van een Europees evaluatiemechanisme voor cyberbeveiligingsincidenten om significante of grootschalige incidenten te evalueren en te beoordelen.

2. Met deze verordening wordt beoogd de solidariteit op het niveau van de Unie te versterken door middel van de volgende specifieke doelstellingen:

a) de gemeenschappelijke capaciteiten van de Unie op het gebied van opsporing en situationeel bewustzijn van cyberdreigingen en -incidenten versterken, waardoor de concurrentiepositie van de industrie en de dienstensector in de Unie in de digitale economie kan worden versterkt en kan worden bijgedragen tot de technologische soevereiniteit van de Unie op het gebied van cyberbeveiliging;

b) de paraatheid van in kritieke en zeer kritieke sectoren actieve entiteiten in de hele Unie vergroten en de solidariteit versterken door gemeenschappelijke capaciteit op het gebied van de respons op significante of grootschalige cyberbeveiligingsincidenten te ontwikkelen, onder meer door steun van de Unie voor respons op cyberbeveiligingsincidenten beschikbaar te stellen aan derde landen die geassocieerd zijn met het programma Digitaal Europa;

c) de weerbaarheid van de Unie vergroten en bijdragen tot een doeltreffende respons door significante of grootschalige incidenten te evalueren en te beoordelen, en daaruit lering te trekken en, in voorkomend geval, aanbevelingen te doen.

3. Deze verordening doet geen afbreuk aan de primaire verantwoordelijkheid van de lidstaten voor de nationale veiligheid, de openbare veiligheid en het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.

Artikel 2

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

(1) **'landsgrensoverschrijdend centrum voor beveiligingsoperaties" ("landsgrensoverschrijdend SOC")**: een meerlandenplatform dat nationale SOC's uit ten minste drie lidstaten die een onderbrengend consortium vormen, samenbrengt in een gecoördineerde netwerkstructuur, en dat bedoeld is om cyberdreigingen en -

incidenten te voorkomen en de productie van hoogwaardige inlichtingen te ondersteunen, met name door het uitwisselen van gegevens uit diverse publieke en private bronnen, het delen van geavanceerde instrumenten en het gezamenlijk ontwikkelen van capaciteit op het gebied van de opsporing, analyse en preventie van alsook de bescherming tegen cyberdreigingen en -incidenten in een betrouwbare omgeving**;**

(2) "**overheidsinstantie**": een publiekrechtelijke instelling zoals gedefinieerd in artikel 2, lid 1, punt 4), van Richtlijn 2014/24/EU van het Europees Parlement en de Raad[18];

(3) "**onderbrengend consortium**": een consortium bestaande uit deelnemende staten, vertegenwoordigd door nationale SOC's, die zijn overeengekomen om instrumenten en infrastructuur voor en de exploitatie van een landsgrensoverschrijdend SOC op te zetten en bij te dragen aan de verwerving ervan;

(4) "**entiteit**": een entiteit zoals gedefinieerd in artikel 6, punt 38, van Richtlijn (EU) 2022/2555*;*

(5) "**in kritieke of zeer kritieke sectoren actieve entiteiten**": de soorten entiteiten die zijn opgenomen in bijlage I en bijlage II bij Richtlijn (EU) 2022/2555;

(6) "**cyberdreiging**": een cyberdreiging zoals gedefinieerd in artikel 2, punt 8, van Verordening (EU) 2019/881;

(7) "**significant cyberbeveiligingsincident**": een cyberbeveiligingsincident dat voldoet aan de criteria van artikel 23, lid 3, van Richtlijn (EU) 2022/2555;

(8) "**grootschalig cyberbeveiligingsincident**": een incident zoals gedefinieerd in artikel 6, punt 7, van Richtlijn (EU) 2022/2555;

(9) "**paraatheid**": een staat van gereedheid en vermogen om te zorgen voor een doeltreffende snelle respons op een significant of grootschalig cyberbeveiligingsincident, die het resultaat is van vooraf genomen risicobeoordelings- en risicocontrolemaatregelen;

(10) "**respons**": actie in het geval van een significant of grootschalig cyberbeveiligingsincident, of tijdens of na een dergelijk incident, om de onmiddellijke nadelige gevolgen alsook de nadelige kortetermijngevolgen ervan aan te pakken;

(11) "**betrouwbare aanbieders**": aanbieders van beheerde beveiligingsdiensten zoals gedefinieerd in artikel 6, punt 40, van Richtlijn (EU) 2022/2555, geselecteerd overeenkomstig artikel 16 van deze verordening.

[18] Richtlijn 2014/24/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende het plaatsen van overheidsopdrachten en tot intrekking van Richtlijn 2004/18/EG (PB L 94 van 28.3.2014, blz. 65).

Hoofdstuk II

HET EUROPEES CYBERSCHILD

Artikel 3

Oprichting van het Europees cyberschild

1. Er wordt een onderling verbonden pan-Europese infrastructuur van centra voor beveiligingsoperaties ("Europees cyberschild") opgezet om voor de Unie geavanceerde capaciteiten op het gebied van het opsporen en analyseren van cyberdreigingen en -incidenten in de Unie en het verwerken van gegevens daarover te ontwikkelen. Het cyberschild bestaat uit alle nationale centra voor beveiligingsoperaties ("nationale SOC's") en landsgrensoverschrijdende centra voor beveiligingsoperaties ("landsgrensoverschrijdende SOC's").

De acties ter uitvoering van het Europees cyberschild worden ondersteund door financiering uit het programma Digitaal Europa en uitgevoerd overeenkomstig Verordening (EU) nr. 2021/694 en met name specifieke doelstelling 3 daarvan.

2. Het Europees cyberschild:

a) bundelt en deelt gegevens over cyberdreigingen en -incidenten uit verschillende bronnen via landsgrensoverschrijdende SOC's;

b) produceert hoogwaardige, bruikbare informatie en inlichtingen over cyberdreigingen door gebruik te maken van geavanceerde instrumenten, met name artificiële intelligentie en technologieën voor gegevensanalyse;

c) draagt bij tot een betere bescherming tegen en respons op cyberdreigingen;

d) draagt bij tot een snellere opsporing van cyberdreigingen en situationeel bewustzijn in de hele Unie;

e) levert diensten en activiteiten voor de cyberbeveiligingsgemeenschap in de Unie, waaronder het bijdragen aan de ontwikkeling van geavanceerde instrumenten voor artificiële intelligentie en gegevensanalyse.

Het cyberschild wordt ontwikkeld in samenwerking met de bij Verordening (EU) 2021/1173 opgerichte pan-Europese high-performance computing-infrastructuur.

Artikel 4

Nationale centra voor beveiligingsoperaties

1. Om deel te nemen aan het Europees Cyberschild wijst elke lidstaat ten minste één nationaal SOC aan. Het nationale SOC is een overheidsinstantie.

Het kan fungeren als referentiepunt en toegangspoort tot andere publieke en private organisaties op nationaal niveau voor het verzamelen en analyseren van informatie over cyberdreigingen en -incidenten en voor het bijdragen tot een landsgrensoverschrijdend SOC. Het wordt uitgerust met geavanceerde technologieën waarmee gegevens over cyberdreigingen en -incidenten kunnen worden opgespoord, samengevoegd en geanalyseerd.

2. Na een oproep tot het indienen van blijken van belangstelling worden de nationale SOC's door het Europees Kenniscentrum voor cyberbeveiliging ("ECCC") geselecteerd om samen met het ECCC deel te nemen aan een gezamenlijke aanbesteding van instrumenten en infrastructuur. Het ECCC kan aan de geselecteerde nationale SOC's subsidies toekennen om de werking van die instrumenten en infrastructuur te financieren. De financiële bijdrage van de Unie dekt tot 50 % van de verwervingskosten van de instrumenten en infrastructuur en tot 50 % van de exploitatiekosten; de resterende kosten komen voor rekening van de lidstaat. Alvorens de procedure voor de verwerving van de instrumenten en infrastructuur in gang te zetten, sluiten het ECCC en het nationale SOC een onderbrengings- en gebruiksovereenkomst waarin het gebruik van de instrumenten en infrastructuur wordt geregeld.

3. Een overeenkomstig lid 2 geselecteerd nationaal SOC verbindt zich ertoe een aanvraag tot deelname aan een landsgrensoverschrijdend SOC in te dienen binnen twee jaar na de datum waarop de instrumenten en infrastructuur zijn verworven of, indien dit eerder is, waarop het een subsidie ontvangt. Indien een nationaal SOC tegen die tijd niet deelneemt aan een landsgrensoverschrijdend SOC, komt het niet in aanmerking voor aanvullende steun van de Unie uit hoofde van deze verordening.

Artikel 5

Grensoverschrijdende centra voor beveiligingsoperaties

1. Een onderbrengend consortium bestaande uit ten minste drie lidstaten, vertegenwoordigd door nationale SOC's, die zich ertoe verbinden samen te werken om hun activiteiten op het gebied van het opsporen en monitoren van cyberdreigingen en -incidenten te coördineren, komt in aanmerking om deel te nemen aan acties voor de oprichting van een landsgrensoverschrijdend SOC.

2. Na een oproep tot het indienen van blijken van belangstelling selecteert het ECCC een onderbrengend consortium om samen met het ECCC deel te nemen aan een gezamenlijke aanbesteding van instrumenten en infrastructuur. Het ECCC kan het onderbrengend consortium een subsidie toekennen om de werking van de instrumenten en infrastructuur te financieren. De financiële bijdrage van de Unie dekt tot 75 % van de verwervingskosten van de instrumenten en infrastructuur en tot 50 % van de exploitatiekosten; de resterende kosten komen voor rekening van het onderbrengend consortium. Alvorens de procedure voor de verwerving van de instrumenten en infrastructuur in gang te zetten, sluiten het ECCC en het onderbrengend consortium een onderbrengings- en gebruiksovereenkomst waarin het gebruik van de instrumenten en infrastructuur wordt geregeld.

3. De leden van het onderbrengend consortium sluiten een schriftelijke consortiumovereenkomst waarin hun interne regelingen voor de uitvoering van de onderbrengings- en gebruiksovereenkomst zijn vastgelegd.

4. Een landsgrensoverschrijdend SOC wordt voor juridische doeleinden vertegenwoordigd door een nationaal SOC dat optreedt als coördinerend SOC, of door het onderbrengend consortium indien dit rechtspersoonlijkheid bezit. Het coördinerend SOC is verantwoordelijk

voor de naleving van de voorschriften van de onderbrengings- en gebruiksovereenkomst en van deze verordening.

Artikel 6

Samenwerking en informatie-uitwisseling binnen en tussen landsgrensoverschrijdende SOC's

1. De leden van een onderbrengend consortium wisselen onderling relevante informatie uit binnen het landsgrensoverschrijdende SOC, met inbegrip van informatie over cyberdreigingen, bijna-incidenten, kwetsbaarheden, technieken en procedures, indicatoren voor aantasting, vijandige tactieken, dreigingsactorspecifieke informatie, cyberbeveiligingswaarschuwingen en aanbevelingen betreffende de configuratie van cyberbeveiligingsinstrumenten om cyberaanvallen te detecteren, wanneer dat uitwisselen van informatie:

a) bedoeld is om incidenten te voorkomen, te detecteren, erop te reageren of ervan te herstellen of de gevolgen ervan te beperken;

b) het niveau van de cyberbeveiliging verhoogt, met name door de bewustwording met betrekking tot cyberdreigingen te vergroten, het vermogen van dergelijke dreigingen om zich te verspreiden te beperken of te belemmeren, een reeks verdedigingscapaciteiten, het herstel en de openbaarmaking van kwetsbaarheden, het opsporen van dreigingen, beheersings- en preventietechnieken, beperkingsstrategieën of respons- en herstelfasen te ondersteunen of gezamenlijk onderzoek naar dreigingen door publieke en particuliere entiteiten te bevorderen.

2. In de in artikel 5, lid 3, bedoelde schriftelijke consortiumovereenkomst wordt het volgende vastgesteld:

a) een verbintenis om een aanzienlijke hoeveelheid gegevens als bedoeld in lid 1 uit te wisselen en de voorwaarden waaronder die informatie wordt uitgewisseld;

b) een governancekader dat de uitwisseling van informatie door alle deelnemers stimuleert;

c) doelstellingen voor de bijdrage aan de ontwikkeling van geavanceerde AI-instrumenten en instrumenten voor gegevensanalyse.

3. Om de uitwisseling van informatie tussen landsgrensoverschrijdende SOC's te bevorderen, zorgen de landsgrensoverschrijdende SOC's voor een hoog niveau van onderlinge interoperabiliteit. Om de interoperabiliteit tussen de landsgrensoverschrijdende SOC's te faciliteren, kan de Commissie door middel van uitvoeringshandelingen en na raadpleging van het ECCC de voorwaarden voor deze interoperabiliteit specificeren. Deze uitvoeringshandelingen worden vastgesteld volgens de in artikel 21, lid 2, van deze verordening bedoelde onderzoeksprocedure.

4. Landsgrensoverschrijdende SOC's sluiten samenwerkingsovereenkomsten met elkaar, waarin de beginselen voor informatie-uitwisseling tussen de landsgrensoverschrijdende platforms worden gespecificeerd.

Artikel 7

Samenwerking en informatie-uitwisseling met entiteiten van de Unie

1. Wanneer de landsgrensoverschrijdende SOC's informatie verkrijgen over een mogelijk of lopend grootschalig cyberbeveiligingsincident, verstrekken zij onverwijld relevante informatie aan EU-CyCLONe, het CSIRT-netwerk en de Commissie, gezien hun respectieve taken op het gebied van crisisbeheersing overeenkomstig Richtlijn (EU) 2022/2555.

2. De Commissie kan door middel van uitvoeringshandelingen de procedurele regelingen voor de in lid 1 bedoelde informatie-uitwisseling vaststellen. Deze uitvoeringshandelingen worden vastgesteld volgens de in artikel 21, lid 2, van deze verordening bedoelde onderzoeksprocedure.

Artikel 8

Beveiliging

1. De lidstaten die deelnemen aan het Europees cyberschild zorgen voor een hoog niveau van gegevensbeveiliging en fysieke beveiliging van de infrastructuur van het Europees cyberschild en zien erop toe dat de infrastructuur adequaat wordt beheerd en gecontroleerd zodat deze tegen dreigingen wordt beschermd en zodat de beveiliging van de infrastructuur en van de systemen, met inbegrip van de via de infrastructuur uitgewisselde gegevens, wordt gewaarborgd.

2. De lidstaten die deelnemen aan het Europees cyberschild zorgen ervoor dat de uitwisseling van informatie binnen het Europees cyberschild met entiteiten die geen overheidsinstanties van een lidstaat zijn, geen negatieve gevolgen heeft voor de veiligheidsbelangen van de Unie.

3. De Commissie kan uitvoeringshandelingen vaststellen waarin technische voorschriften worden vastgelegd waaraan de lidstaten moeten voldoen om hun verplichting uit hoofde van de leden 1 en 2 na te komen. Deze uitvoeringshandelingen worden vastgesteld volgens de in artikel 21, lid 2, van deze verordening bedoelde onderzoeksprocedure. Daarbij houdt de Commissie, gesteund door de hoge vertegenwoordiger, rekening met de relevante beveiligingsnormen op defensieniveau, teneinde de samenwerking met militaire actoren te vergemakkelijken.

Hoofdstuk III

CYBERNOODMECHANISME

Artikel 9

Instelling van het cybernoodmechanisme

1. Er wordt een cybernoodmechanisme ingesteld om de Unie weerbaarder te maken tegen grote cyberdreigingen en om in een geest van solidariteit de kortetermijngevolgen van significante en grootschalige cyberbeveiligingsincidenten of -crises te beperken en zich daarop voor te bereiden (het "mechanisme").

2. De acties ter uitvoering van het cybernoodmechanisme worden ondersteund door financiering uit het programma Digitaal Europa en worden uitgevoerd overeenkomstig Verordening (EU) 2021/694 en met name specifieke doelstelling 3 daarvan.

Artikel 10

Soorten acties

1. Het mechanisme ondersteunt de volgende soorten acties:

a) paraatheidsacties, met inbegrip van de gecoördineerde paraatheidstests van in zeer kritieke sectoren actieve entiteiten in de hele Unie;

b) responsacties, ter ondersteuning van de respons op en het onmiddellijke herstel van significante en grootschalige cyberbeveiligingsincidenten, die moeten worden uitgevoerd door betrouwbare aanbieders die deelnemen aan de bij artikel 12 ingestelde EU-cyberbeveiligingsreserve;

c) wederzijdse-bijstandsacties die bestaan uit het verlenen van bijstand door de nationale autoriteiten van een lidstaat aan een andere lidstaat, met name als bedoeld in artikel 11, lid 3, punt f), van Richtlijn (EU) 2022/2555.

Artikel 11

Gecoördineerde paraatheidstests van entiteiten

1. Teneinde de gecoördineerde paraatheidstests van de in artikel 10, lid 1, punt a), bedoelde entiteiten in de hele Unie te ondersteunen, stelt de Commissie, na raadpleging van de NIS-samenwerkingsgroep en Enisa, uit de in bijlage I bij Richtlijn (EU) 2022/2555 vermelde zeer kritieke sectoren de sectoren of subsectoren vast waaruit entiteiten aan de gecoördineerde paraatheidstests kunnen worden onderworpen, rekening houdend met bestaande en geplande gecoördineerde risicobeoordelingen en weerbaarheidstests op het niveau van de Unie.

2. De NIS-samenwerkingsgroep ontwikkelt in samenwerking met de Commissie, Enisa en de hoge vertegenwoordiger gemeenschappelijke risicoscenario's en -methoden voor de gecoördineerde tests.

Artikel 12

Instelling van de EU-cyberbeveiligingsreserve

1. Er wordt een EU-cyberbeveiligingsreserve ingesteld om de in lid 3 bedoelde gebruikers bij te staan bij de respons, of de ondersteuning van de respons, op significante of grootschalige cyberbeveiligingsincidenten en bij het onmiddellijke herstel van dergelijke incidenten.

2. De EU-cyberbeveiligingsreserve bestaat uit incidentresponsdiensten van betrouwbare aanbieders die zijn geselecteerd overeenkomstig de criteria van artikel 16. De reserve omvat vooraf vastgelegde diensten. De diensten kunnen in alle lidstaten worden geleverd.

3. Tot de gebruikers van de diensten van de EU-cyberbeveiligingsreserve behoren:

a) De cybercrisisbeheerautoriteiten en CSIRT's van de lidstaten als bedoeld in respectievelijk artikel 9, leden 1 en 2, en artikel 10 van Richtlijn (EU) 2022/2555;

b) instellingen, organen en instanties van de Unie.

4. De in lid 3, punt a), bedoelde gebruikers gebruiken de diensten van de EU-cyberbeveiligingsreserve voor de respons, of de ondersteuning van de respons, op en het onmiddellijke herstel van significante of grootschalige incidenten die in kritieke of zeer kritieke sectoren actieve entiteiten treffen.

5. De Commissie draagt de algemene verantwoordelijkheid voor de uitvoering van de EU-cyberbeveiligingsreserve. De Commissie bepaalt de prioriteiten en ontwikkeling van de EU-cyberbeveiligingsreserve in overeenstemming met de vereisten van de in lid 3 bedoelde gebruikers, houdt toezicht op de uitvoering ervan en zorgt voor complementariteit, consistentie, synergieën en koppelingen met andere ondersteunende acties in het kader van deze verordening en met andere acties en programma's van de Unie.

6. De Commissie kan de werking en het beheer van de EU-cyberbeveiligingsreserve geheel of gedeeltelijk toevertrouwen aan Enisa door middel van bijdrageovereenkomsten.

7. Om de Commissie te ondersteunen bij de instelling van de EU-cyberbeveiligingsreserve brengt Enisa, na raadpleging van de lidstaten en de Commissie, de benodigde diensten in kaart. Na raadpleging van de Commissie stelt Enisa een soortgelijk overzicht op om de behoeften vast te stellen van derde landen die in aanmerking komen voor steun uit de EU-cyberbeveiligingsreserve overeenkomstig artikel 17. Indien relevant raadpleegt de Commissie de hoge vertegenwoordiger.

8. De Commissie kan door middel van uitvoeringshandelingen de soorten en het aantal responsdiensten specificeren die voor de EU-cyberbeveiligingsreserve vereist zijn. Deze uitvoeringshandelingen worden vastgesteld volgens de in artikel 21, lid 2, bedoelde onderzoeksprocedure.

Artikel 13

Verzoeken om steun uit de EU-cyberbeveiligingsreserve

1. De in artikel 12, lid 3, bedoelde gebruikers kunnen om diensten van de EU-cyberbeveiligingsreserve verzoeken ter ondersteuning van de respons op en het onmiddellijke herstel van significante of grootschalige cyberbeveiligingsincidenten.

2. Om steun uit de EU-cyberbeveiligingsreserve te ontvangen, nemen de in artikel 12, lid 3, bedoelde gebruikers maatregelen om de gevolgen van het incident waarvoor om steun wordt verzocht te beperken, met inbegrip van het verlenen van directe technische bijstand en andere middelen om de respons op het incident en de inspanningen voor onmiddellijk herstel te ondersteunen.

3. Ondersteuningsverzoeken van de in artikel 12, lid 3, punt a), van deze verordening bedoelde gebruikers worden aan de Commissie en Enisa toegezonden via het centrale contactpunt dat door de lidstaat is aangewezen of ingesteld overeenkomstig artikel 8, lid 3, van Richtlijn (EU) 2022/2555.

4. De lidstaten stellen het CSIRT-netwerk en, in voorkomend geval, EU-CyCLONe in kennis van hun verzoeken om ondersteuning bij de respons op incidenten en bij het onmiddellijke herstel overeenkomstig dit artikel.

5. Verzoeken om ondersteuning bij de respons op incidenten en bij het onmiddellijke herstel omvatten:

a) de nodige informatie over de getroffen entiteit en de potentiële gevolgen van het incident en het geplande gebruik van de gevraagde steun, met inbegrip van een indicatie van de geraamde behoeften;

b) informatie over de maatregelen die zijn genomen om het incident waarvoor om steun wordt verzocht, te beperken, als bedoeld in lid 2;

c) informatie over andere vormen van steun die beschikbaar zijn voor de getroffen entiteit, met inbegrip van bestaande contractuele regelingen inzake incidentresponsdiensten en diensten op het gebied van onmiddellijk herstel, alsook verzekeringscontracten die een dergelijk soort incident kunnen dekken.

6. In samenwerking met de Commissie en de NIS-samenwerkingsgroep ontwikkelt Enisa een model om de indiening van verzoeken om steun uit de EU-cyberbeveiligingsreserve te vergemakkelijken.

7. Door middel van uitvoeringshandelingen kan de Commissie de nadere regelingen voor de toewijzing van de ondersteunende diensten van de EU-cyberbeveiligingsreserve nader specificeren. Deze uitvoeringshandelingen worden vastgesteld volgens de in artikel 21, lid 2, bedoelde onderzoeksprocedure.

Artikel 14

Uitvoering van de steun uit de EU-cyberbeveiligingsreserve

1. Verzoeken om steun uit de EU-cyberbeveiligingsreserve worden beoordeeld door de Commissie, met de steun van Enisa of zoals omschreven in bijdrageovereenkomsten uit hoofde van artikel 12, lid 6, en er wordt onverwijld een antwoord toegezonden aan de in artikel 12, lid 3, bedoelde gebruikers.

2. Bij de prioritering van verzoeken in geval van meerdere gelijktijdige verzoeken wordt in voorkomend geval rekening gehouden met de volgende criteria:

a) de ernst van het cyberbeveiligingsincident;

b) het soort getroffen entiteit, met een hogere prioriteit voor incidenten die essentiële entiteiten treffen als gedefinieerd in artikel 3, lid 1, van Richtlijn (EU) 2022/2555;

c) de mogelijke gevolgen voor de getroffen lidsta(a)t(en) of gebruikers;

d) de mogelijke landsgrensoverschrijdende aard van het incident en het risico op overloopeffecten naar andere lidstaten of gebruikers;

e) de door de gebruiker genomen maatregelen ter ondersteuning van de respons en inspanningen voor onmiddellijk herstel, als bedoeld in artikel 13, lid 2, en artikel 13, lid 5, punt b).

3. De diensten van de EU-cyberbeveiligingsreserve worden verleend in overeenstemming met specifieke overeenkomsten tussen de dienstverlener en de gebruiker aan wie de steun in het

kader van de EU-cyberbeveiligingsreserve wordt verleend. Deze overeenkomsten bevatten aansprakelijkheidsvoorwaarden.

4. De in lid 3 bedoelde overeenkomsten kunnen worden gebaseerd op modellen die Enisa na overleg met de lidstaten heeft opgesteld.

5. De Commissie en Enisa zijn niet contractueel aansprakelijk voor schade die aan derden is toegebracht door de diensten die in het kader van de uitvoering van de EU-cyberbeveiligingsreserve worden verleend.

6. Binnen een maand na het einde van de ondersteuningsactie dienen de gebruikers bij de Commissie en Enisa een samenvattend verslag in over de verleende dienst, de bereikte resultaten en de geleerde lessen. Indien de gebruiker afkomstig is uit een derde land als bedoeld in artikel 17, wordt dit verslag gedeeld met de hoge vertegenwoordiger.

7. De Commissie brengt regelmatig verslag uit aan de NIS-samenwerkingsgroep over het gebruik en de resultaten van de steun.

Artikel 15

Coördinatie met crisisbeheersingsmechanismen

1. In gevallen waarin significante of grootschalige cyberbeveiligingsincidenten voortkomen uit of resulteren in rampen zoals gedefinieerd in Besluit 1313/2013/EU[19], vormt de steun uit hoofde van deze verordening voor de respons op dergelijke incidenten een aanvulling op acties in het kader van en onverminderd Besluit 1313/2013/EU.

2. In het geval van een grootschalig, landsgrensoverschrijdend cyberbeveiligingsincident waarbij geïntegreerde regelingen politieke crisisrespons (IPCR) in werking treden, wordt de steun uit hoofde van deze verordening voor de respons op een dergelijk incident behandeld overeenkomstig de relevante protocollen en procedures in het kader van de IPCR.

3. In overleg met de hoge vertegenwoordiger kan de steun in het kader van het cybernoodmechanisme een aanvulling vormen op de bijstand die wordt verleend in het kader van het gemeenschappelijk buitenlands en veiligheidsbeleid en het gemeenschappelijk veiligheids- en defensiebeleid, onder meer via de snellereactieteams bij cyberbeveiligingsincidenten. Deze steun kan ook een aanvulling vormen op of bijdragen aan bijstand die een lidstaat aan een andere lidstaat verleent in het kader van artikel 42, lid 7, van het Verdrag betreffende de Europese Unie.

4. Steun in het kader van het cybernoodmechanisme kan deel uitmaken van de gezamenlijke respons van de Unie en de lidstaten in situaties als bedoeld in artikel 222 van het Verdrag betreffende de werking van de Europese Unie.

Artikel 16

Betrouwbare aanbieders

1. Bij aanbestedingsprocedures voor de oprichting van de EU-cyberbeveiligingsreserve handelt de aanbestedende dienst in overeenstemming met de beginselen van Verordening (EU, Euratom) 2018/1046 en met de volgende beginselen:

[19] Besluit nr. 1313/2013/EU van het Europees Parlement en de Raad van 17 december 2013 betreffende een Uniemechanisme voor civiele bescherming (PB L 347 van 20.12.2013, blz. 924).

a) ervoor zorgen dat de EU-cyberbeveiligingsreserve diensten omvat die in alle lidstaten kunnen worden verleend, met name rekening houdend met nationale vereisten voor het verlenen van dergelijke diensten, met inbegrip van certificering of accreditatie;

b) de bescherming van de wezenlijke veiligheidsbelangen van de Unie en haar lidstaten waarborgen.

c) ervoor zorgen dat de EU-cyberbeveiligingsreserve EU-meerwaarde oplevert door bij te dragen tot de verwezenlijking van de doelstellingen van artikel 3 van Verordening (EU) 2021/694, met inbegrip van het bevorderen van de ontwikkeling van cyberbeveiligingsvaardigheden in de EU.

2. Bij de aanbesteding van diensten voor de EU-cyberbeveiligingsreserve neemt de aanbestedende dienst in de aanbestedingsdocumenten de volgende selectiecriteria op:

a) de aanbieder toont aan dat zijn personeel de hoogste mate van professionele integriteit, onafhankelijkheid en verantwoordelijkheid bezit en de vereiste technische bekwaamheid heeft om de activiteiten op hun specifieke gebied uit te voeren, en zorgt voor de permanentie/continuïteit van de deskundigheid en de vereiste technische middelen;

b) de aanbieder, zijn dochterondernemingen en onderaannemers beschikken over een kader voor de bescherming van gevoelige informatie met betrekking tot de dienst, en met name bewijsmateriaal, bevindingen en verslagen, en houden zich aan de beveiligingsvoorschriften van de Unie inzake de bescherming van gerubriceerde EU-gegevens;

c) de aanbieder levert voldoende bewijs dat zijn bestuursstructuur transparant is, zijn onpartijdigheid en de kwaliteit van zijn diensten niet in het gedrang brengt of geen belangenconflicten veroorzaakt;

d) de aanbieder beschikt over een passende veiligheidsmachtiging, ten minste voor het personeel dat de dienst gaat verlenen;

e) de aanbieder beschikt over het relevante beveiligingsniveau voor zijn IT-systemen;

f) de aanbieder beschikt over de technische hardware en software die nodig zijn om de gevraagde dienst te ondersteunen;

g) de aanbieder kan aantonen dat hij ervaring heeft met het verlenen van soortgelijke diensten aan relevante nationale autoriteiten of in kritieke of zeer kritieke sectoren actieve entiteiten;

h) de aanbieder is in staat de dienst binnen een korte termijn te verlenen in de lidstaat of lidstaten waar hij de dienst kan verlenen;

i) de aanbieder is in staat de dienst te verlenen in de plaatselijke taal van de lidstaat of lidstaten waar hij de dienst kan verlenen;

j) zodra een EU-certificeringsregeling voor beheerde beveiligingsdiensten overeenkomstig Verordening (EU) 2019/881 van kracht is, wordt de aanbieder overeenkomstig die regeling gecertificeerd.

Artikel 17

Steun aan derde landen

1. Derde landen kunnen om steun uit de EU-cyberbeveiligingsreserve verzoeken indien de associatieovereenkomsten die zijn gesloten met betrekking tot hun deelname aan het programma Digitaal Europa daarin voorzien.

2. Steun uit de EU-cyberbeveiligingsreserve is in overeenstemming met deze verordening en voldoet aan alle specifieke voorwaarden die in de in lid 1 bedoelde associatieovereenkomsten zijn vastgesteld.

3. Tot de gebruikers uit geassocieerde derde landen die in aanmerking komen om diensten uit de EU-cyberbeveiligingsreserve te ontvangen, behoren bevoegde autoriteiten zoals CSIRT's en cybercrisisbeheerautoriteiten.

4. Elk derde land dat in aanmerking komt voor steun uit de EU-cyberbeveiligingsreserve wijst een autoriteit aan die voor de toepassing van deze verordening als centraal contactpunt fungeert.

5. Voordat derde landen steun uit de EU-cyberbeveiligingsreserve ontvangen, verstrekken zij de Commissie en de hoge vertegenwoordiger informatie over hun cyberweerbaarheid en risicobeheercapaciteiten, met inbegrip van ten minste informatie over nationale maatregelen ter voorbereiding op significante of grootschalige cyberbeveiligingsincidenten, alsook informatie over verantwoordelijke nationale entiteiten, met inbegrip van CSIRT's of gelijkwaardige entiteiten, hun capaciteiten en de daaraan toegewezen middelen. Wanneer in de bepalingen van de artikelen 13 en 14 van deze verordening wordt verwezen naar de lidstaten, zijn zij van toepassing op derde landen als bedoeld in lid 1.

6. De Commissie coördineert met de hoge vertegenwoordiger de ontvangen verzoeken en de uitvoering van de steun aan derde landen uit de EU-cyberbeveiligingsreserve.

Hoofdstuk IV

EVALUATIEMECHANISME VOOR CYBERBEVEILIGINGSINCIDENTEN

Artikel 18

Evaluatiemechanisme voor cyberbeveiligingsincidenten

1. Op verzoek van de Commissie, EU-CyCLONe of het CSIRT-netwerk evalueert en beoordeelt Enisa dreigingen, kwetsbaarheden en mitigerende maatregelen met betrekking tot een specifiek significant of grootschalig cyberbeveiligingsincident. Na de voltooiing van een evaluatie en beoordeling van een incident verstrekt Enisa een evaluatieverslag over het incident aan het CSIRT-netwerk, EU-CyCLONe en de Commissie om hen te ondersteunen bij de uitvoering van hun taken, met name met het oog op de in de artikelen 15 en 16 van Richtlijn (EU) 2022/2555 vastgestelde taken. Indien relevant deelt de Commissie het verslag met de hoge vertegenwoordiger.

2. Om het in lid 1 bedoelde evaluatieverslag over het incident op te stellen, werkt Enisa samen met alle relevante belanghebbenden, waaronder vertegenwoordigers van de lidstaten, de Commissie, andere relevante EU-instellingen, -organen en -instanties, aanbieders van beheerde beveiligingsdiensten en gebruikers van cyberbeveiligingsdiensten. In voorkomend

geval werkt Enisa ook samen met entiteiten die getroffen zijn door significante of grootschalige cyberbeveiligingsincidenten. Ter ondersteuning van de evaluatie kan Enisa ook andere soorten belanghebbenden raadplegen. De geraadpleegde vertegenwoordigers maken elk mogelijk belangenconflict bekend.

3. Het verslag omvat een evaluatie en analyse van het specifieke significante of grootschalige cyberbeveiligingsincident, met inbegrip van de belangrijkste oorzaken, kwetsbaarheden en geleerde lessen. Het beschermt vertrouwelijke informatie overeenkomstig het Unierecht of het nationale recht inzake de bescherming van gevoelige of gerubriceerde informatie.

4. In voorkomend geval worden in het verslag aanbevelingen gedaan om de cyberstrategie van de Unie te verbeteren.

5. Indien mogelijk wordt een versie van het verslag openbaar gemaakt. Deze versie bevat uitsluitend openbare informatie.

Hoofdstuk V

SLOTBEPALINGEN

Artikel 19

Wijzigingen van Verordening (EU) 2021/694

Verordening (EU) 2021/694 wordt als volgt gewijzigd:

(1) Artikel 6 wordt als volgt gewijzigd:

a) lid 1 wordt als volgt gewijzigd:

(1) het volgende punt a bis) wordt ingevoegd:

"a bis) ondersteunen van de ontwikkeling van een EU-cyberschild, met inbegrip van de ontwikkeling, uitrol en exploitatie van nationale en landsgrensoverschrijdende SOC-platforms die bijdragen tot het situationeel bewustzijn in de Unie en tot de versterking van de inlichtingencapaciteit van de Unie op het gebied van cyberdreigingen";

(2) het volgende punt g) wordt toegevoegd:

"g) instellen en beheren van een cybernoodmechanisme om de lidstaten te ondersteunen bij de voorbereiding en respons op significante cyberbeveiligingsincidenten, in aanvulling op de nationale middelen en capaciteiten en andere vormen van steun die op het niveau van de Unie beschikbaar zijn, met inbegrip van de instelling van een EU-cyberbeveiligingsreserve";

a) Lid 2 wordt vervangen door:

"2. De acties in het kader van specifieke doelstelling 3 worden voornamelijk uitgevoerd via het Europees Kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het Netwerk van nationale coördinatiecentra, overeenkomstig Verordening (EU) 2021/887 van het Europees Parlement en de Raad[20], met uitzondering van acties ter uitvoering van de EU-cyberbeveiligingsreserve, die door de Commissie en Enisa worden uitgevoerd.**";**

(2) Artikel 9 wordt als volgt gewijzigd:

a) in lid 2 worden de punten b), c) en d) vervangen door:

"b) 1 776 956 000 EUR voor specifieke doelstelling 2 – Artificiële intelligentie;

c) 1 629 566 000 EUR voor specifieke doelstelling 3 – Cyberbeveiliging en vertrouwen;

d) 482 347 000 EUR voor specifieke doelstelling 4 – Geavanceerde digitale vaardigheden";

b) het volgende lid 8 wordt toegevoegd:

"8. In afwijking van artikel 12, lid 4, van Verordening (EU, Euratom) 2018/1046 worden ongebruikte vastleggings- en betalingskredieten voor acties ter verwezenlijking van de in artikel 6, lid 1, punt g), van deze verordening genoemde doelstellingen automatisch overgedragen en kunnen deze tot en met 31 december van het volgende begrotingsjaar worden vastgelegd en betaald.";

(3) In artikel 14 wordt lid 2 vervangen door:

"2. In het kader van het programma kan financiering worden verstrekt in een van de in het Financieel Reglement opgenomen vormen, inclusief door met name aanbestedingen als primaire vorm of subsidies en prijzen.

Als voor het verwezenlijken van de doelstelling van een actie de aanbesteding van innovatieve goederen en diensten vereist is, kunnen subsidies uitsluitend worden toegekend aan begunstigden die aanbestedende diensten of aanbestedende instanties zijn als gedefinieerd in de Richtlijnen 2014/24/EU[27] en 2014/25/EU[28] van het Europees Parlement en de Raad.

Als de levering van nog niet op grote commerciële basis beschikbare innovatieve goederen of diensten noodzakelijk is voor het bereiken van de doelstellingen van een actie, kan de aanbestedende dienst of de aanbestedende instantie de gunning van meerdere contracten binnen dezelfde aanbestedingsprocedure toestaan.

[20] Verordening (EU) 2021/887 van het Europees Parlement en de Raad van 20 mei 2021 tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra (PB L 202 van 8.6.2021, blz. 1-31).

Om naar behoren gemotiveerde redenen van openbare veiligheid kan de aanbestedende dienst of de aanbestedende instantie eisen dat de plaats van uitvoering van het contract op het grondgebied van de Unie gelegen is.

Bij de uitvoering van aanbestedingsprocedures voor de bij artikel 12 van Verordening (EU) 2023/XX ingestelde EU-cyberbeveiligingsreserve kunnen de Commissie en Enisa optreden als aankoopcentrale voor aanbestedingen namens of in naam van met het programma geassocieerde derde landen overeenkomstig artikel 10. De Commissie en Enisa kunnen ook als groothandelaar optreden door goederen en diensten, met inbegrip van verhuurde zaken, aan te kopen, in voorraad te houden en aan die derde landen door te verkopen of te schenken. In afwijking van artikel 169, lid 3, van Verordening (EU) XXX/XXXX [FR herschikking] volstaat het verzoek van één derde land om de Commissie of Enisa te machtigen om op te treden.

Bij de uitvoering van aanbestedingsprocedures voor de bij artikel 12 van Verordening (EU) 2023/XX ingestelde EU-cyberbeveiligingsreserve kunnen de Commissie en Enisa optreden als aankoopcentrale voor aanbestedingen namens of in naam van instellingen, organen en instanties van de Unie. De Commissie en Enisa kunnen ook als groothandelaar optreden door goederen en diensten, met inbegrip van verhuurde zaken, aan te kopen, in voorraad te houden en aan instellingen, organen en instanties van de Unie door te verkopen of te schenken. In afwijking van artikel 169, lid 3, van Verordening (EU) XXX/XXXX [FR Herschikking] volstaat het verzoek van één instelling, orgaan of instantie van de Unie om de Commissie of Enisa te machtigen om op te treden.

Het programma kan eveneens financiering verstrekken in de vorm van financieringsinstrumenten in het kader van blendingverrichtingen."

(4) Het volgende artikel 16 bis wordt toegevoegd:

In het geval van acties ter uitvoering van het bij artikel 3 van Verordening (EU) 2023/XX ingestelde Europees cyberschild zijn de toepasselijke regels die van de artikelen 4 en 5 van Verordening (EU) 2023/XX. In geval van strijdigheid tussen de bepalingen van deze verordening en de artikelen 4 en 5 van Verordening (EU) 2023/XX hebben deze laatste voorrang en zijn zij van toepassing op die specifieke acties.

(5) Artikel 19 wordt vervangen door:

"Subsidies krachtens het programma worden toegekend en beheerd in overeenstemming met titel VIII van het Financieel Reglement en mogen tot 100 % van de subsidiabele kosten dekken, onverminderd het medefinancieringsbeginsel dat is vastgelegd in artikel 190 van het Financieel Reglement. Dergelijke subsidies worden toegekend en beheerd zoals gespecificeerd voor elke specifieke doelstelling.

Zonder oproep tot het indienen van voorstellen kan het ECCC steun in de vorm van subsidies rechtstreeks toekennen aan de nationale SOC's als bedoeld in artikel 4 van Verordening XXXX en het onderbrengend consortium als bedoeld in artikel 5 van

Verordening XXXX, overeenkomstig artikel 195, lid 1, punt d), van het Financieel Reglement.

Steun in de vorm van subsidies voor het cybernoodmechanisme als bedoeld in artikel 10 van Verordening XXXX kan door het ECCC rechtstreeks aan de lidstaten worden toegekend zonder oproep tot het indienen van voorstellen, overeenkomstig artikel 195, lid 1, punt d), van het Financieel Reglement.

Voor de in artikel 10, lid 1, punt c), van Verordening 202X/XXXX gespecificeerde acties stelt het ECCC de Commissie en Enisa in kennis van verzoeken van lidstaten om rechtstreekse subsidies zonder oproep tot het indienen van voorstellen.

Voor de ondersteuning van wederzijdse bijstand bij de respons op een significant of grootschalig cyberbeveiligingsincident zoals gedefinieerd in artikel 10, punt c), van Verordening XXXX, en overeenkomstig artikel 193, lid 2, tweede alinea, punt a), van het Financieel Reglement, kunnen in naar behoren gemotiveerde gevallen de kosten als subsidiabel worden beschouwd, zelfs als zij vóór de indiening van de subsidieaanvraag zijn gemaakt.”;

(6) De bijlagen I en II worden gewijzigd overeenkomstig de bijlage bij deze verordening.

Artikel 20

Evaluatie

Uiterlijk [vier jaar na de datum van toepassing van deze verordening] dient de Commissie bij het Europees Parlement en de Raad een verslag in over de evaluatie en toetsing van deze verordening.

Artikel 21

Comitéprocedure

1. De Commissie wordt bijgestaan door het bij Verordening (EU) 2021/694 ingestelde Coördinatiecomité voor het programma Digitaal Europa. Dat comité is een comité in de zin van Verordening (EU) nr. 182/2011.
2. Wanneer naar dit lid wordt verwezen, is artikel 5 van Verordening (EU) nr. 182/2011 van toepassing.

Artikel 22

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Straatsburg,

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*

FINANCIEEL MEMORANDUM

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

1.2. Betrokken beleidsterrein(en)

1.3. Het voorstel/initiatief betreft:

1.4. Doelstelling(en)

1.4.1. Algemene doelstelling(en)

1.4.2. Specifieke doelstelling(en)

1.4.3. Verwachte resulta(a)t(en) en gevolg(en)

1.4.4. Prestatie-indicatoren

1.5. Motivering van het voorstel/initiatief

1.5.1. Behoefte(n) waarin op korte of lange termijn moet worden voorzien, met een gedetailleerd tijdschema voor de uitrol van het initiatief

1.5.2. Toegevoegde waarde van de deelname van de Unie (deze kan het resultaat zijn van verschillende factoren, bijvoorbeeld coördinatiewinst, rechtszekerheid, grotere doeltreffendheid of complementariteit). Voor de toepassing van dit punt wordt onder "toegevoegde waarde van de deelname van de Unie" verstaan de waarde die een optreden van de Unie oplevert bovenop de waarde die door een optreden van alleen de lidstaat zou zijn gecreëerd.

1.5.3. Nuttige ervaring die bij soortgelijke activiteiten in het verleden is opgedaan

1.5.4. Verenigbaarheid met het meerjarig financieel kader en eventuele synergie met andere passende instrumenten

1.5.5. Beoordeling van de verschillende beschikbare financieringsopties, waaronder mogelijkheden voor herschikking

1.6. Duur en financiële gevolgen van het voorstel/initiatief

1.7. Wijze(n) van uitvoering van de begroting

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

2.2. Beheers- en controlesyste(e)m(en)

2.2.1. Rechtvaardiging van de voorgestelde beheersvorm(en), uitvoeringsmechanisme(n) voor financiering, betalingsvoorwaarden en controlestrategie

2.2.2. Informatie over de geïdentificeerde risico's en het (de) systeem (systemen) voor interne controle dat is (die zijn) opgezet om die risico's te beperken

2.2.3. Raming en motivering van de kosteneffectiviteit van de controles (verhouding van de controlekosten tot de waarde van de desbetreffende financiële middelen) en evaluatie van het verwachte foutenrisico (bij betaling en bij afsluiting)

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubriek(en) van het meerjarig financieel kader en betrokken begrotingsonderde(e)l(en) voor uitgaven

3.2. Geraamde financiële gevolgen van het voorstel inzake kredieten

3.2.1. Samenvatting van de geraamde gevolgen voor de beleidskredieten

3.2.2. Geraamde output, gefinancierd met beleidskredieten

3.2.3. Samenvatting van de geraamde gevolgen voor de administratieve kredieten

3.2.3.1. Geraamde personeelsbehoeften

3.2.4. Verenigbaarheid met het huidige meerjarig financieel kader

3.2.5. Bijdragen van derden

3.3. Geraamde gevolgen voor de ontvangsten

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

Verordening van het Europees Parlement en de Raad tot vaststelling van maatregelen ter versterking van de solidariteit en de capaciteit in de Unie om cyberdreigingen en -incidenten op te sporen, zich erop voor te bereiden en erop te reageren

1.2. Betrokken beleidsterrein(en)

Een Europa dat klaar is voor het digitale tijdperk

Europese strategische investeringen

Activiteit: De digitale toekomst van Europa vormgeven.

1.3. Het voorstel/initiatief betreft:

☒ **een nieuwe actie**

☐ **een nieuwe actie na een proefproject/voorbereidende actie**[33]

☐ **de verlenging van een bestaande actie**

☐ **de samenvoeging of ombuiging van een of meer acties naar een andere/een nieuwe actie**

1.4. Doelstelling(en)

1.4.1. Algemene doelstelling(en)

De verordening cybersolidariteit zal de solidariteit op het niveau van de Unie versterken teneinde cyberdreigingen en -incidenten beter op te sporen en om er beter op voorbereid te zijn en op te kunnen reageren. De verordening heeft tot doel:

a) de gemeenschappelijke capaciteiten van de EU op het gebied van opsporing en situationeel bewustzijn van cyberdreigingen en -incidenten versterken;

b) de paraatheid van kritieke entiteiten in de hele EU vergroten en de solidariteit versterken door gemeenschappelijke capaciteit op het gebied van de respons op significante of grootschalige cyberbeveiligingsincidenten te ontwikkelen, onder meer door steun voor respons op incidenten beschikbaar te stellen aan derde landen die geassocieerd zijn met het programma Digitaal Europa;

c) de weerbaarheid van de Unie te vergroten en bij te dragen tot een doeltreffende respons door significante of grootschalige incidenten te evalueren en te beoordelen, en daaruit lering te trekken en, in voorkomend geval, aanbevelingen te doen.

1.4.2. Specifieke doelstelling(en)

De doelstellingen van de verordening cybersolidariteit zullen worden bereikt door:

a) de uitrol van een pan-Europese infrastructuur van centra voor beveiligingsoperaties (Europees cyberschild) om gemeenschappelijke

[33] In de zin van artikel 58, lid 2, punt a) of b), van het Financieel Reglement.

capaciteiten op het gebied van opsporing en situationeel bewustzijn op te bouwen en te versterken.

b) de instelling van een cybernoodmechanisme om de lidstaten te ondersteunen bij de voorbereiding en respons op, en het onmiddellijke herstel van, significante en grootschalige cyberbeveiligingsincidenten. Steun voor respons op incidenten wordt ook beschikbaar gesteld aan Europese instellingen, organen en instanties van de Unie.

Deze acties zullen worden ondersteund door financiering uit het programma Digitaal Europa, dat met dit wetgevingsinstrument zal worden gewijzigd om de bovengenoemde acties vast te stellen, financiële steun te verlenen voor de ontwikkeling ervan en de voorwaarden voor het ontvangen van de financiële steun te verduidelijken.

c) de instelling van een Europees evaluatiemechanisme voor cyberbeveiligingsincidenten om significante of grootschalige incidenten te evalueren en te beoordelen.

1.4.3. Verwachte resulta(a)t(en) en gevolg(en)

Vermeld de gevolgen die het voorstel/initiatief zou moeten hebben voor de begunstigden/doelgroepen.

Het voorstel zou aanzienlijke voordelen opleveren voor de verschillende belanghebbenden. Het Europees cyberschild zal het vermogen van de lidstaten om cyberdreigingen op te sporen, verbeteren. Het cybernoodmechanisme zal de acties van de lidstaten aanvullen met noodhulp voor paraatheid, respons en onmiddellijk herstel/herstel van de werking van essentiële diensten.

Deze acties zullen de concurrentiepositie van de industrie en het bedrijfsleven in Europa in de hele gedigitaliseerde economie versterken en de digitale transformatie ervan ondersteunen door het niveau van cyberbeveiliging in de digitale eengemaakte markt te verhogen. Het is er met name op gericht burgers, bedrijven en in kritieke of zeer kritieke sectoren actieve entiteiten weerbaarder te maken tegen de toenemende cyberdreigingen, die verwoestende maatschappelijke en economische gevolgen kunnen hebben. Het zal dit doen door te investeren in instrumenten die een snellere opsporing van en respons op cyberdreigingen en -incidenten ondersteunen, en zal de lidstaten helpen zich beter voor te bereiden en beter te reageren op significante en grootschalige cyberbeveiligingsincidenten. Dit moet er ook toe bijdragen dat Europa meer capaciteit krijgt op deze gebieden, met name wat betreft het verzamelen en analyseren van gegevens over cyberdreigingen en -incidenten.

1.4.4. Prestatie-indicatoren

Vermeld de indicatoren voor de monitoring van de voortgang en de beoordeling van de resultaten

Om de solidariteit op het niveau van de Unie te bevorderen, kan rekening worden gehouden met verschillende indicatoren:

(1) Het aantal gezamenlijk verworven infrastructuurvoorzieningen en/of instrumenten inzake cyberbeveiliging

(2) Het aantal acties ter ondersteuning van de paraatheid voor en de respons op cyberbeveiligingsincidenten in het kader van het cybernoodmechanisme.

1.5. Motivering van het voorstel/initiatief

1.5.1. Behoefte(n) waarin op korte of lange termijn moet worden voorzien, met een gedetailleerd tijdschema voor de uitrol van het initiatief

De verordening moet kort na de vaststelling ervan volledig van toepassing zijn, d.w.z. op de twintigste dag na die van de bekendmaking ervan in het Publicatieblad van de Europese Unie.

1.5.2. Toegevoegde waarde van de deelname van de Unie (deze kan het resultaat zijn van verschillende factoren, bijvoorbeeld coördinatiewinst, rechtszekerheid, grotere doeltreffendheid of complementariteit). Voor de toepassing van dit punt wordt onder "toegevoegde waarde van de deelname van de Unie" verstaan de waarde die een optreden van de Unie oplevert bovenop de waarde die door een optreden van alleen de lidstaat zou zijn gecreëerd.

De sterke landsgrensoverschrijdende aard van cyberdreigingen in het algemeen en het toenemende aantal risico's en incidenten, die overloopeffecten hebben over grenzen, sectoren en producten heen, maken dat de doelstellingen van het huidige optreden niet doeltreffend door de lidstaten alleen kunnen worden verwezenlijkt en dat de realisatie ervan gemeenschappelijke actie en solidariteit op het niveau van de Unie vereist. De ervaring met de bestrijding van cyberdreigingen die voortkomen uit de oorlog tegen Oekraïne en de lessen die zijn getrokken uit een cyberbeveiligingsoefening onder het Franse voorzitterschap (EU CyCLES) hebben aangetoond dat concrete mechanismen voor wederzijdse ondersteuning, met name samenwerking met de particuliere sector, zouden moeten worden ontwikkeld om solidariteit op EU-niveau tot stand te brengen. Tegen deze achtergrond wordt de Commissie in de conclusies van de Raad van 23 mei 2022 over de ontwikkeling van de cyberstrategie van de Europese Unie verzocht een voorstel in te dienen voor een nieuw cyberbeveiligingsnoodfonds. Ondersteuning en acties op het niveau van de Unie om cyberdreigingen beter op te sporen en de paraatheid en responscapaciteit te vergroten, bieden een meerwaarde omdat zo dubbel werk in de Unie en de lidstaten wordt voorkomen. Het zou leiden tot een betere benutting van de bestaande middelen en tot meer coördinatie en uitwisseling van informatie over geleerde lessen.

1.5.3. Nuttige ervaring die bij soortgelijke activiteiten in het verleden is opgedaan

Wat situationeel bewustzijn en opsporing in het kader van het Europees cyberschild betreft, is in het kader van het werkprogramma cyberbeveiliging 2021-2022 van het programma Digitaal Europa een oproep gedaan tot het indienen van blijken van belangstelling voor de gezamenlijke aanschaf van instrumenten en infrastructuur voor de oprichting van landsgrensoverschrijdende SOC's, alsook een oproep tot het indienen van voorstellen voor subsidies om de capaciteitsopbouw van SOC's ten dienste van publieke en particuliere organisaties mogelijk te maken.

Wat paraatheid voor en respons op incidenten betreft, heeft de Commissie een kortetermijnprogramma opgezet om de lidstaten te ondersteunen, door middel van aanvullende financiering die aan Enisa is toegewezen, teneinde de paraatheid voor en de capaciteit om te reageren op grote cyberbeveiligingsincidenten onmiddellijk te versterken. Bij de diensten in kwestie gaat het onder meer om paraatheidsacties, zoals penetratietests van kritieke entiteiten om kwetsbaarheden aan het licht te brengen. Het programma biedt ook meer mogelijkheden om de lidstaten bij te staan in geval van een ernstig incident dat kritieke entiteiten treft. De uitvoering van dit kortetermijnprogramma door Enisa is aan de gang en heeft reeds relevante,

waardevolle inzichten opgeleverd waarmee bij de opstelling van deze verordening rekening is gehouden

1.5.4. Verenigbaarheid met het meerjarig financieel kader en eventuele synergie met andere passende instrumenten

De verordening cybersolidariteit zal voortbouwen op acties die momenteel door de Unie en de lidstaten worden ondersteund om het situationeel bewustzijn en de opsporing van cyberdreigingen te verbeteren, en om te reageren op grootschalige en landsgrensoverschrijdende cyberbeveiligingsincidenten. Daarnaast is het instrument verenigbaar met andere kaders voor crisisbeheersing, waaronder de geïntegreerde regeling politieke crisisrespons (IPCR), het gemeenschappelijk veiligheids- en defensiebeleid (GVDB), met inbegrip van snellereactieteams bij cyberincidenten, en de bijstand die een lidstaat aan een andere lidstaat verleent in het kader van artikel 42, lid 7, van het Verdrag betreffende de Europese Unie. Het nieuwe voorstel zou ook structuren aanvullen en ondersteunen die zijn ontwikkeld in het kader van andere cyberbeveiligingsinstrumenten, zoals Richtlijn (EU) 2022/2555 (NIS2-richtlijn) of Verordening 2019/881 (de cyberbeveiligingsverordening).

1.5.5. Beoordeling van de verschillende beschikbare financieringsopties, waaronder mogelijkheden voor herschikking

Het beheer van de aan Enisa toegewezen actiegebieden sluit aan bij het bestaande mandaat en de algemene taken. Voor deze actiegebieden kunnen specifieke profielen of nieuwe opdrachten nodig zijn, maar deze kunnen worden opgevangen door de bestaande middelen van Enisa en kunnen worden opgelost door middel van hertoewijzing of koppeling van verschillende opdrachten. Enisa voert momenteel een kortetermijnprogramma uit dat in 2022 door de Commissie is opgezet om de paraatheid voor en de capaciteit om te reageren op grote cyberincidenten onmiddellijk te versterken. De betrokken diensten omvatten mogelijkheden om lidstaten bij te staan in geval van een ernstig incident dat kritieke entiteiten treft. De uitvoering van dit kortetermijnprogramma door Enisa is aan de gang en heeft reeds relevante, waardevolle inzichten opgeleverd waarmee bij de opstelling van deze verordening rekening is gehouden. De aan het kortetermijnprogramma toegewezen middelen kunnen ook in het kader van deze verordening worden gebruikt.

1.6. Duur en financiële gevolgen van het voorstel/initiatief

☒ **beperkte geldigheidsduur**

– ☒ van kracht vanaf de datum van vaststelling van het voorstel voor een verordening van het Europees Parlement en de Raad betreffende de versterking van de solidariteit en de capaciteit in de Unie om cyberdreigingen en -incidenten op te sporen, zich erop voor te bereiden en erop te reageren ("de verordening cybersolidariteit");

– ☒ financiële gevolgen vanaf 2023 tot en met 2027 voor vastleggingskredieten en vanaf 2023 tot en met 2031 voor betalingskredieten[34].

☐ **onbeperkte geldigheidsduur**

– uitvoering met een opstartperiode vanaf JJJJ tot en met JJJJ,

– gevolgd door een volledige uitvoering.

1.7. Wijze(n) van uitvoering van de begroting[35]

☒ **Direct beheer** door de Commissie

– ☒ door haar diensten, waaronder het personeel in de delegaties van de Unie;

– ☐ door de uitvoerende agentschappen.

☐ **Gedeeld beheer** met de lidstaten

☒ **Indirect beheer** door begrotingsuitvoeringstaken te delegeren aan:

– ☐ derde landen of de door hen aangewezen organen;

– ☐ internationale organisaties en hun agentschappen (geef aan welke);

– ☐ de EIB en het Europees Investeringsfonds;

– ☒ de in de artikelen 70 en 71 van het Financieel Reglement bedoelde organen;

– ☐ publiekrechtelijke organen;

– ☐ privaatrechtelijke organen met een openbare dienstverleningstaak, voor zover zij zijn voorzien van voldoende financiële garanties;

– ☐ privaatrechtelijke organen van een lidstaat waaraan de uitvoering van een publiek-privaat partnerschap is toevertrouwd en die zijn voorzien van voldoende financiële garanties;

– ☐ organen of personen aan wie de uitvoering van specifieke maatregelen op het gebied van het GBVB in het kader van titel V van het VEU is toevertrouwd en die worden genoemd in de betrokken basishandeling.

– *Verstrek, indien meer dan een beheersvorm is aangekruist, extra informatie onder "Opmerkingen".*

Opmerkingen

De acties in verband met het Europees cyberschild zullen door het ECCC worden uitgevoerd. Totdat het ECCC over de capaciteit beschikt om zijn eigen begroting uit te voeren, zal de

[34] De acties in de verordening moeten worden ondersteund door het volgende meerjarig financieel kader.

[35] Nadere gegevens over de wijzen van uitvoering van de begroting en verwijzingen naar het Financieel Reglement zijn beschikbaar op BUDGpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx

Europese Commissie de acties in direct beheer uitvoeren namens het ECCC. Het ECCC kan entiteiten selecteren op basis van oproepen tot het indienen van blijken van belangstelling om deel te nemen aan de gezamenlijke aanschaf van instrumenten. Het ECCC kan subsidies toekennen voor de exploitatie van deze instrumenten.

Bovendien kan het ECCC subsidies toekennen voor paraatheidsacties in het kader van het cybernoodmechanisme.

De Commissie draagt de algemene verantwoordelijkheid voor de uitvoering van de EU-cyberbeveiligingsreserve. De Commissie kan door middel van bijdrageovereenkomsten de exploitatie en het beheer van de EU-cyberbeveiligingsreserve geheel of gedeeltelijk aan Enisa toevertrouwen. De in deze verordening aan Enisa toegewezen acties zijn in overeenstemming met zijn bestaande mandaat. Deze acties omvatten: i) ondersteuning van de NIS-samenwerkingsgroep bij de ontwikkeling van paraatheidsacties op basis van risicobeoordelingen; ii) ondersteuning van de Commissie bij de instelling en het toezicht op de uitvoering van de EU-cyberbeveiligingsreserve, met inbegrip van het ontvangen en verwerken van verzoeken om steun; iii) ontwikkeling van modellen ter vergemakkelijking van de indiening van verzoeken om steun en specifieke overeenkomsten die moeten worden gesloten tussen de dienstverlener en de gebruiker waaraan de steun in het kader van de EU-cyberbeveiligingsreserve wordt verleend; (iv) evaluatie en beoordeling van dreigingen, kwetsbaarheden en mitigatiemaatregelen met betrekking tot specifieke significante of grootschalige cyberbeveiligingsincidenten en opstelling van verslagen daarover.

Al deze opdrachten worden geraamd op ongeveer 7 vte's uit de bestaande middelen van Enisa, waarbij reeds wordt voortgebouwd op de expertise en voorbereidende werkzaamheden die Enisa momenteel verricht in het kader van het proefproject voor noodhulp voor paraatheid voor en respons op incidenten.

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

Vermeld de frequentie en voorwaarden.

De Commissie zal de uitvoering, toepassing en naleving van deze nieuwe bepalingen controleren om de doeltreffendheid ervan te beoordelen. De Commissie legt het Europees Parlement en de Raad uiterlijk vier jaar na de datum van toepassing van deze verordening een verslag over de evaluatie en de toetsing ervan voor.

2.2. Beheers- en controlesyste(e)m(en)

2.2.1. Rechtvaardiging van de voorgestelde beheersvorm(en), uitvoeringsmechanisme(n) voor financiering, betalingsvoorwaarden en controlestrategie

Met de verordening wordt een kader geïntroduceerd voor de uitvoering van EU-financiering met het oog op het vergroten van de weerbaarheid op het gebied van cyberbeveiliging door middel van acties ter verbetering van de capaciteiten op het gebied van opsporing, respons en herstel in geval van significante en grootschalige cyberbeveiligingsincidenten. De eenheden binnen DG CNECT die belast zijn met het beleidsterrein zullen de uitvoering van de richtlijn beheren.

Om de nieuwe taken te kunnen oppakken, moeten de diensten van de Commissie over voldoende middelen beschikken. Voor de handhaving van de nieuwe verordening zijn naar schatting 6 vte's (3 AD en 3 CA) nodig om de volgende taken uit te voeren:

- bepalen van paraatheidsacties op basis van risicobeoordelingen;
- ervoor zorgen dat platforms van landsgrensoverschrijdende SOC's interoperabel zijn;
- opstellen van mogelijke uitvoeringshandelingen (twee voor SOC's en twee voor het cybernoodmechanisme);
- beheren van de onderbrengings- en gebruiksovereenkomsten voor SOC's;
- oprichten en beheren van de EU-cyberbeveiligingsreserve, rechtstreeks of via een bijdrageovereenkomst met Enisa – in geval van een bijdrageovereenkomst met Enisa, uitwerken van de bijdrageovereenkomst voor de aan Enisa toegewezen taken en toezien op de uitvoering van die overeenkomst;
- deelnemen aan de door Enisa bijeengeroepen overleggroepen om significante en grootschalige cyberincidenten te evalueren en te beoordelen, en opstellen van de verslagen.

2.2.2. Informatie over de geïdentificeerde risico's en het (de) systeem (systemen) voor interne controle dat is (die zijn) opgezet om die risico's te beperken

Een voor het Europees cyberschild vastgesteld risico is dat de lidstaten onvoldoende relevante informatie over cyberdreigingen uitwisselen binnen de platforms van landsgrensoverschrijdende SOC's of tussen die platforms en andere relevante entiteiten op EU-niveau. Om deze risico's te beperken, wordt de financiering toegekend na een oproep tot het indienen van blijken van belangstelling waarbij de lidstaten zich ertoe verbinden een bepaalde hoeveelheid informatie met het EU-niveau te delen. Deze verbintenis wordt vervolgens geformaliseerd in een

onderbrengings- en gebruiksovereenkomst, waarin het ECCC de bevoegdheid krijgt om controles uit te voeren teneinde ervoor te zorgen dat de gezamenlijk aangeschafte instrumenten en infrastructuur overeenkomstig de overeenkomst worden gebruikt. Verbintenissen tot een hoog niveau van informatie-uitwisseling binnen de landsgrensoverschrijdende SOC's worden geformaliseerd in een consortiumovereenkomst.

Een risico dat voor het cybernoodmechanisme is vastgesteld, is dat gebruikers die eraan deelnemen onvoldoende maatregelen nemen om de paraatheid bij cyberaanvallen te waarborgen. Om die reden zijn gebruikers verplicht dergelijke paraatheidsmaatregelen te nemen om steun uit de EU-cyberbeveiligingsreserve te kunnen ontvangen. Bij het indienen van verzoeken om steun bij de EU-cyberbeveiligingsreserve moeten gebruikers uitleggen welke maatregelen al zijn genomen om op het incident te reageren, waarmee rekening zal worden gehouden bij de beoordeling van de bij de EU-cyberbeveiligingsreserve ingediende verzoeken.

2.2.3. Raming en motivering van de kosteneffectiviteit van de controles (verhouding van de controlekosten tot de waarde van de desbetreffende financiële middelen) en evaluatie van het verwachte foutenrisico (bij betaling en bij afsluiting)

Aangezien de regels voor deelname aan het programma Digitaal Europa die van toepassing zijn op de steun in het kader van de verordening cybersolidariteit vergelijkbaar zijn met die welke de Commissie in haar werkprogramma's zal hanteren, en met een groep begunstigden met een soortgelijk risicoprofiel als dat van programma's onder direct beheer, kan worden verwacht dat het foutenpercentage vergelijkbaar zal zijn met het door de Commissie voor het programma Digitaal Europa beoogde niveau, d.w.z. dat er een redelijke zekerheid bestaat dat het foutenrisico gedurende de meerjarige uitgavenperiode op jaarbasis tussen de 2 en 5 % beweegt, met als einddoel tot een resterend foutenpercentage te komen dat zo dicht mogelijk bij 2 % ligt bij de sluiting van de meerjarenprogramma's, wanneer rekening is gehouden met het financiële effect van alle controles en corrigerende en herstelmaatregelen.

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

Vermeld de bestaande en geplande preventie- en beschermingsmaatregelen, bijvoorbeeld in het kader van de fraudebestrijdingsstrategie.

In het geval van het Europees Cyberschild zal het ECCC bevoegd zijn om op basis van toegang tot informatie en controles ter plaatse de gezamenlijk aangeschafte instrumenten en infrastructuur te controleren overeenkomstig de tussen het onderbrengend consortium en het ECCC te ondertekenen onderbrengings- en gebruiksovereenkomst.

De voor deze verordening vereiste aanvullende kredieten zullen onder de bestaande fraudepreventiemaatregelen vallen die van toepassing zijn op de instellingen, organen en instanties van de Unie.

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubriek(en) van het meerjarig financieel kader en betrokken begrotingsonderde(e)l(en) voor uitgaven

- Bestaande begrotingsonderdelen

in volgorde van de rubrieken van het meerjarig financieel kader en de begrotingsonderdelen.

Rubriek van het meerjarig financieel kader	Begrotingsonderdeel	Soort uitgave	Bijdrage			
	Nummer	GK / NGK[36].	van EVA-landen[37]	van kandidaat-lidstaten en potentiële kandidaat-lidstaten[38]	van andere derde landen	andere bestemmingsontvangsten
1	02 04 01 10 - Programma Digitaal Europa - Cyberbeveiliging	GK	JA	JA	NEE	NEE
1	02 04 01 11 - Programma Digitaal Europa - Europees Kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging	GK	JA	JA	NEE	NEE
1	02 04 03 - Programma Digitaal Europa - Artificiële intelligentie	GK	JA	JA	NEE	NEE
1	02 04 04 - Programma Digitaal Europa - Vaardigheden	GK	JA	JA	NEE	NEE
1	02 01 30 - Ondersteunende uitgaven voor het programma Digitaal Europa	NGK	JA	JA	NEE	NEE

[36] GK = gesplitste kredieten / NGK = niet-gesplitste kredieten.
[37] EVA: Europese Vrijhandelsassociatie.
[38] Kandidaat-lidstaten en, in voorkomend geval, potentiële kandidaat-lidstaten.

3.2. Geraamde financiële gevolgen van het voorstel inzake kredieten

3.2.1. Samenvatting van de geraamde gevolgen voor de beleidskredieten

– ☐ Voor het voorstel/initiatief zijn geen beleidskredieten nodig

– ☒ Voor het voorstel/initiatief zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven:

in miljoenen euro's (tot op drie decimalen)

Rubriek van het meerjarig financieel kader	Nummer	1 **Eengemaakte markt, innovatie en digitaal beleid**

Het voorstel zal het totale niveau van de vastleggingen in het kader van het programma Digitaal Europa niet verhogen. De bijdrage aan dit initiatief is namelijk een herverdeling van de vastleggingen van SO2 en SO4 om de begroting van SO3 en het ECCC te versterken. Elke verhoging van de vastleggingen in het kader van het programma Digitaal Europa als gevolg van een herziening van het MFK zou voor dit initiatief kunnen worden gebruikt.

DG CONNECT			Jaar **2025**	Jaar **2026**	Jaar **2027**	Jaar **2028+**	Vul zoveel jaren in als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)			**TOTAAL**
○ Beleidskredieten										
Begrotingsonderdeel[39] 02.040110 (herverdeling van 02.0403 en 02.0404)	Vastleggingen	1 bis)	15 000	15 000	6 000	p.m.				**36 000**
	Betalingen	2 bis)	15 000	15 000	6 000					**36 000**
Begrotingsonderdeel 02.040111.02 (herverdeling van 02.0403 en 02.0404)	Vastleggingen	(1b)	13 000	23 000	28 000	p.m.				**64 000**
	Betalingen	(2b)	8 450	18 200	25 250	12 100				**64 000**
Uit het budget van specifieke programma's gefinancierde administratieve kredieten[40]										
Begrotingsonderdeel 02.0130		(3)	0,150	0,150	0,150	p.m.				0,450

[39] Volgens de officiële begrotingsnomenclatuur.

[40] Technische en/of administratieve bijstand en uitgaven ter ondersteuning van de uitvoering van programma's en/of acties van de EU (vroegere "BA"-onderdelen), onderzoek onder contract, eigen onderzoek.

TOTAAL kredieten voor DG CONNECT	Vastleggingen	=1a+1b +3	**28 150**	**38 150**	**34 150**	**p.m.**				**100 450**
	Betalingen	=2a+2b +3	**23 600**	**33 350**	**31 400**	**12 100**				**100 450**

○ TOTAAL beleidskredieten	Vastleggingen	(4)	28 000	38 000	34 000	p.m.				**100 000**
	Betalingen	(5)	23 450	33 200	31 250	12 100				**100 000**
○ TOTAAL uit het budget van specifieke programma's gefinancierde administratieve kredieten		(6)	0,150	0,150	0,150	p.m.				**0,450**
TOTAAL kredieten onder RUBRIEK 1 van het meerjarig financieel kader	Vastleggingen	=4+ 6	**28 150**	**38 150**	**34 150**	**p.m.**				**100 450**
	Betalingen	=5+ 6	**23 600**	**33 350**	**31 400**	**12 100**				**100 450**

Als het voorstel/initiatief gevolgen heeft voor meerdere beleidsrubrieken, herhaal bovenstaand deel:

○ TOTAAL beleidskredieten (alle beleidsrubrieken)	Vastleggingen	(4)	28 000	38 000	34 000	p.m.				**100 000**
	Betalingen	(5)	23 450	33 200	31 250	12 100				**100 000**
TOTAAL uit het budget van specifieke programma's gefinancierde administratieve kredieten (alle beleidsrubrieken)		(6)	0,150	0,150	0,150					**0,450**
TOTAAL kredieten onder de RUBRIEKEN 1 tot en met 6 van het meerjarig financieel kader (Referentiebedrag)	Vastleggingen	=4+ 6	**28 150**	**38 150**	**34 150**	**p.m.**				**100 450**
	Betalingen	=5+ 6	**23 600**	**33 350**	**31 400**	**12 100**				**100 450**

Rubriek van het meerjarig financieel kader	**7**	"Administratieve uitgaven"

Dit deel moet worden ingevuld aan de hand van de "administratieve begrotingsgegevens", die eerst moeten worden opgenomen in de bijlage bij het financieel memorandum (bijlage 5 bij het besluit van de Commissie betreffende de interne uitvoeringsvoorschriften voor de afdeling "Commissie" van de algemene begroting van de Europese Unie), te uploaden in DECIDE met het oog op overleg tussen de diensten.

in miljoenen euro's (tot op drie decimalen)

		Jaar **2025**	Jaar **2026**	Jaar **2027**	Jaar **2028+**	Vul zoveel jaren in als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)			**TOTAAL**
DG: CONNECT									
○ Personele middelen		0,786	0,786	0,786	p.m.				**2 358**
○ Andere administratieve uitgaven		0,035	0,035	0,035	p.m.				**0,105**
TOTAAL DG CONNECT	Kredieten	**0,821**	**0,821**	**0,821**					**2 463**

TOTAAL kredieten onder RUBRIEK 7 van het meerjarig financieel kader	(Totaal vastleggingen = totaal betalingen)	**0,821**	**0,821**	**0,821**					**2 463**

in miljoenen euro's (tot op drie decimalen)

		Jaar **2025**	Jaar **2026**	Jaar **2027**	Jaar **2028+**	Vul zoveel jaren in als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)			**TOTAAL**
TOTAAL kredieten onder de RUBRIEKEN 1 tot en met 7 van het meerjarig financieel kader	Vastleggingen	**28 971**	**38 971**	**34 971**	**p.m.**				**102 913**
	Betalingen	**24 421**	**34 171**	**32 221**	**12 100**				**102 913**

3.2.2. Geraamde output, gefinancierd met beleidskredieten

Vastleggingskredieten, in miljoenen euro's (tot op drie decimalen)

Vermeld doelstellingen en outputs ⇩			Jaar **N**		Jaar **N+1**		Jaar **N+2**		Jaar **N+3**		Vul zoveel jaren in als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)						**TOTAAL**	
	OUTPUTS																	
	Soort [41]	Gem. kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Aantal	Kosten	Totaal aantal	Totale kosten
SPECIFIEKE DOELSTELLING NR. 1[42]...																		
- Output																		
- Output																		
- Output																		
Subtotaal voor specifieke doelstelling nr. 1																		
SPECIFIEKE DOELSTELLING NR. 2 ...																		
- Output																		
Subtotaal voor specifieke doelstelling nr. 2																		
TOTAAL																		

[41] Outputs zijn de te verstrekken producten en diensten (bv. aantal gefinancierde studentenuitwisselingen, aantal km aangelegde wegen enz.).

[42] Zoals beschreven in punt 1.4.2. "Specifieke doelstelling(en)…"

3.2.3. Samenvatting van de geraamde gevolgen voor de administratieve kredieten

– ☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig

– ☒ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader wordt beschreven:

in miljoenen euro's (tot op drie decimalen)

	Jaar 2025	Jaar r 2026	Jaar 2027	Jaar N+3	Vul zoveel jaren in als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)			**TOTAAL**
RUBRIEK 7 van het meerjarig financieel kader								
Personele middelen	0,786	0,786	0,786					**2 358**
Andere administratieve uitgaven	0,035	0,035	0,035					**0,105**
Subtotaal RUBRIEK 7 van het meerjarig financieel kader	**0,821**	**0,821**	**0,821**					**2 463**

Buiten RUBRIEK 7[43] van het meerjarig financieel kader								
Personele middelen								
Andere administratieve uitgaven	0,150	0,150	0,150					**0,450**
Subtotaal buiten RUBRIEK 7 van het meerjarig financieel kader	**0,150**	**0,150**	**0,150**					**0,450**

TOTAAL	**0,971**	**0,971**	**0,971**					**2 913**

De benodigde kredieten voor personeel en andere administratieve uitgaven zullen worden gefinancierd uit de kredieten van het DG die reeds voor het beheer van deze actie zijn toegewezen en/of binnen het DG zijn herverdeeld, eventueel aangevuld met middelen die in het kader van de jaarlijkse toewijzingsprocedure met inachtneming van de budgettaire beperkingen aan het beherende DG kunnen worden toegewezen.

[43] Technische en/of administratieve bijstand en uitgaven ter ondersteuning van de uitvoering van programma's en/of acties van de EU (vroegere "BA"-onderdelen), onderzoek onder contract, eigen onderzoek.

3.2.3.1. Geraamde personeelsbehoeften

– ☐ Voor het voorstel/initiatief zijn geen personele middelen nodig.

– ☒ Voor het voorstel/initiatief zijn personele middelen nodig, zoals hieronder nader wordt beschreven:

Raming in voltijdequivalenten

		Jaar **2025**	Jaar **2026**	Jaar 2027	Jaar **N+3**	Vul zoveel jaren in als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)		
O Posten opgenomen in de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen)								
20 01 02 01 (Hoofdkantoor en vertegenwoordigingen van de Commissie)		3	3	3				
20 01 02 03 (delegaties)								
01 01 01 01 (onderzoek onder contract)								
01 01 01 11 (eigen onderzoek)								
Ander begrotingsonderdeel (te vermelden)								
O Extern personeel (in voltijdequivalenten: vte)[44]								
20 02 01 (AC, END, INT van de "totale financiële middelen")		3	3	3				
20 02 03 (AC, AL, END, INT en JPD in de delegaties)								
XX 01 xx **yy zz** [45]	- zetel							
	- delegaties							
01 01 01 02 (AC, END, INT - onderzoek onder contract)								
01 01 01 12 (AC, END, INT - eigen onderzoek)								
Ander begrotingsonderdeel (te vermelden)								
TOTAAL		**6**	**6**	**6**				

XX is het beleidsterrein of de begrotingstitel.

Voor de benodigde personele middelen zal een beroep worden gedaan op het personeel van het DG dat reeds voor het beheer van deze actie is toegewezen en/of binnen het DG is herverdeeld, eventueel aangevuld met middelen die in het kader van de jaarlijkse toewijzingsprocedure met inachtneming van de budgettaire beperkingen aan het beherende DG kunnen worden toegewezen.

Beschrijving van de uit te voeren taken:

Ambtenaren en tijdelijk personeel	- bepalen van paraatheidsacties op basis van risicobeoordelingen (artikel 11); - opstellen van mogelijke uitvoeringshandelingen (twee voor SOC's en twee voor het cybernoodmechanisme); - beheren van de onderbrengings- en gebruiksovereenkomsten voor SOC's; - oprichten en beheren van de EU-cyberbeveiligingsreserve, rechtstreeks of via een bijdrageovereenkomst met Enisa.
Extern personeel	Onder toezicht van een ambtenaar, - bepalen van paraatheidsacties op basis van risicobeoordelingen (artikel 11); - opstellen van mogelijke uitvoeringshandelingen (twee voor SOC's en twee voor het cybernoodmechanisme); - beheren van de onderbrengings- en gebruiksovereenkomsten voor SOC's; - oprichten en beheren van de EU-cyberbeveiligingsreserve, rechtstreeks of via

[44] AC = Agent Contractuel (arbeidscontractant); AL = Agent Local (plaatselijk functionaris); END = Expert National Détaché (gedetacheerd nationaal deskundige); INT = Intérimaire (uitzendkracht); JPD = Junior Professional in Delegations (jonge deskundige in delegaties).

[45] Subplafond voor extern personeel uit beleidskredieten (vroegere "BA"-onderdelen).

	een bijdrageovereenkomst met Enisa.

3.2.4. *Verenigbaarheid met het huidige meerjarig financieel kader*

Het voorstel/initiatief:

– [X] kan volledig worden gefinancierd door middel van herschikking binnen de relevante rubriek van het meerjarig financieel kader (MFK).

Zet uiteen welke herprogrammering nodig is, onder vermelding van de betrokken begrotingsonderdelen en de desbetreffende bedragen. Verstrek een Excel-tabel in het geval van een omvangrijke herprogrammeringsexercitie.

	2023	2024	2025	2026	2027	totaal
SO1	16 232 897	20 528 765	17 406 899	16 223 464	10 022 366	80 414 391
SO2 initieel	226 316 819	295 067 000	195 649 000	221 809 000	246 608 000	1 185 449 819
Naar CYBER-initiatief			18 000 000	28 000 000	19 000 000	65 000 000
NIEUW SO2	**226 316 819**	**295 067 000**	**177 649 000**	**193 809 000**	**227 608 000**	**1 120 449 819**
SO3 DB 24	24 361 553	35 596 172	3 638 000	3 638 000	11 175 000	78 408 725
Van SO2-SO4			15 000 000	15 000 000	6 000 000	36 000 000
NIEUW SO3	**24 361 553**	**35 596 172**	**18 638 000**	**18 638 000**	**17 175 000**	**114 408 725**
ECCC initieel	176 222 303	208 374 879	104 228 130	90 704 986	84 851 497	664 381 795
Van SO2-SO4			13 000 000	23 000 000	28 000 000	64 000 000
NIEUW ECCC	**176 222 303**	**208 374 879**	**117 228 130**	**113 704 986**	**112 851 497**	**728 381 795**
SO4 initieel	66 902 708	64 892 032	56 577 977	70 477 245	72 107 201	330 957 163
Naar CYBER-initiatief			10 000 000	10 000 000	15 000 000	35 000 000
NIEUW SO4	**66 902 708**	**64 892 032**	**46 577 977**	**60 477 245**	**57 107 201**	**295 957 163**

– [ ] hiervoor moet een beroep worden gedaan op de niet-toegewezen marge in de desbetreffende rubriek van het MFK en/of op de speciale instrumenten zoals gedefinieerd in de MFK-verordening.

Zet uiteen wat nodig is, onder vermelding van de betrokken rubrieken en begrotingsonderdelen, de desbetreffende bedragen en de voorgestelde instrumenten.

– [ ] hiervoor is een herziening van het MFK nodig.

Zet uiteen wat nodig is, onder vermelding van de betrokken rubrieken en begrotingsonderdelen en de desbetreffende bedragen.

3.2.5. *Bijdragen van derden*

Het voorstel/initiatief:

– [X] voorziet niet in medefinanciering door derden

– [ ] voorziet in medefinanciering door derden, zoals hieronder wordt geraamd:

Kredieten in miljoenen euro's (tot op drie decimalen)

	Jaar **N**[46]	Jaar **N+1**	Jaar **N+2**	Jaar **N+3**	Vul zoveel jaren in als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)	Totaal

[46] Het jaar N is het jaar waarin met de uitvoering van het voorstel/initiatief wordt begonnen. Vervang "N" door het verwachte eerste jaar van uitvoering (bijvoorbeeld: 2021). Hetzelfde voor de volgende jaren.

Medefinancieringsbron								
TOTAAL medegefinancierde kredieten								

3.3. Geraamde gevolgen voor de ontvangsten

– ☒ Het voorstel/initiatief heeft geen financiële gevolgen voor de ontvangsten.

– ☐ Het voorstel/initiatief heeft de hieronder beschreven financiële gevolgen:

  – ☐ voor de eigen middelen

  – ☐ voor overige ontvangsten

  – Geef aan of de ontvangsten worden toegewezen aan begrotingsonderdelen voor uitgaven ☐

in miljoenen euro's (tot op drie decimalen)

Begrotingsonderdeel voor ontvangsten:	Voor het lopende begrotingsjaar beschikbare kredieten	Gevolgen van het voorstel/initiatief[47]						
		Jaar **N**	Jaar **N+1**	Jaar **N+2**	Jaar **N+3**	Vul zoveel jaren in als nodig om de duur van de gevolgen weer te geven (zie punt 1.6)		
Artikel …….								

Vermeld voor de toegewezen ontvangsten het (de) betrokken begrotingsonderde(e)l(en) voor uitgaven.

[…]

Andere opmerkingen (bv. over de methode/formule voor de berekening van de gevolgen voor de ontvangsten of andere informatie).

[…]

[47] Voor traditionele eigen middelen (douanerechten en suikerheffingen) moeten nettobedragen worden vermeld, d.w.z. na aftrek van 20 % aan inningskosten.