AMENDEMENTEN 001-001
ingediend door de Commissie industrie, onderzoek en energie

Verslag
Lina Gálvez Muñoz **A9-0426/2023**
Verordening cybersolidariteit

Voorstel voor een verordening (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Amendement 1

AMENDEMENTEN VAN HET EUROPEES PARLEMENT*

op het voorstel van de Commissie

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*, en tot wijziging van Verordening (EU) 2021/694*

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),

---

* Amendementen: nieuwe of vervangende tekst staat in vet cursief, schrappingen zijn met het symbool ▌ aangegeven.

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 ***en de democratie, maar hebben zij tegelijkertijd mogelijke kwetsbaarheden met zich meegebracht***.

(2) De omvang, frequentie en impact van cyberbeveiligingsincidenten nemen ***overal in de Unie en wereldwijd*** toe ***wat methode en gevolgen betreft***, 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 ***in heel de Unie*** aanzienlijke verstoringen of schade aan ***economieën en democratieën en*** 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 ***en*** criminele ▌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 en evolueren, niet beperkt zijn tot een specifiek geografisch gebied en zich gelijktijdig of onmiddellijk over vele landen verspreiden. ***Er is derhalve behoefte aan nauwe en gecoördineerde samenwerking tussen de overheidssector, de particuliere sector, universiteiten, het maatschappelijk middenveld en de media. Daarnaast moet de respons van de Unie worden gecoördineerd met de internationale instellingen en betrouwbare en gelijkgestemde internationale partners. Betrouwbare en gelijkgestemde internationale partners zijn landen die de waarden van de Unie delen, te weten democratie, inzet voor de mensenrechten, effectief multilateralisme, en op regels gebaseerde orde, in overeenstemming met de kaders en overeenkomsten op het gebied van internationale samenwerking. Om samenwerking met betrouwbare en gelijkgestemde internationale partners en bescherming tegen systeemrivalen te waarborgen, moet het in derde landen gevestigde entiteiten die geen partijen bij de***

---

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

Overeenkomst inzake overheidsopdrachten zijn niet worden toegestaan om deel te nemen aan aanbestedingen uit hoofde van deze verordening.

(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[1], is het noodzakelijk om burgers, bedrijven***, met name micro-, kleine en middelgrote ondernemingen, met inbegrip van startende ondernemingen,*** en entiteiten die kritieke infrastructuur exploiteren***, waaronder lokale en regionale overheden,*** 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 ***en capaciteitsopbouw voor het ontwikkelen van cyberbeveiligingsvaardigheden*** 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.

(3 bis) Cyberaanvallen zijn vaak gericht tegen plaatselijke, regionale en/of nationale overheidsdiensten en infrastructurele voorzieningen. Lokale overheden behoren vanwege hun ontoereikende financiële middelen en personeel tot de meest kwetsbare doelwitten van cyberaanvallen. Het is dus bijzonder belangrijk plaatselijke beleidsmakers ervan te doordringen dat het essentieel is de digitale veerkracht te vergroten, aan capaciteitsopbouw te doen om de gevolgen van cyberaanvallen te verminderen, en gebruik te maken van de mogelijkheden die deze verordening biedt.

(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[2], Aanbeveling (EU) 2017/1584 van de Commissie[3], Richtlijn 2013/40/EU van het Europees Parlement en de Raad[4] en Verordening (EU) 2019/881 van het Europees Parlement en de Raad[5]. Daarnaast wordt de lidstaten

---

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

2 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).

3 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).

4 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)*.

5 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

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, er beter op voorbereid te zijn, ▌ ***er*** beter op te kunnen reageren ***en ervan te kunnen herstellen***. De lidstaten hebben de Commissie ook verzocht om in de conclusies van de Raad over een EU-cyberstrategie[1] 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[2] 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-***netwerk*** 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 ***ter voorkoming van en*** om te reageren op, significante en grootschalige cyberbeveiligingsincidenten te verbeteren. Daarom zou een ***pan-Europees netwerk*** 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***, en de capaciteiten van de Unie op het gebied van de opsporing van dreigingen en de uitwisseling van informatie te verbeteren***; 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.

---

tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15).

[1] 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).

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

(8) Om deze doelstellingen te bereiken, is het ook noodzakelijk Verordening (EU) 2021/694 van het Europees Parlement en de Raad[1] 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) 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.

(9 bis) Gelet op de geopolitieke ontwikkelingen en de toenemende cyberdreigingen (PPE 52) en om de continuïteit en de verdere ontwikkeling van de in deze verordening vastgelegde maatregelen na 2027 te waarborgen, met name het Europees cyberschild en het Europees cybernoodmechanisme, moet in het meerjarig financieel kader voor de periode 2028-2034 een specifiek begrotingsonderdeel worden gecreëerd. De lidstaten moeten trachten zich te verplichten alle maatregelen te ondersteunen die nodig zijn om cyberdreigingen en -incidenten overal in de Unie te verminderen, en de solidariteit te versterken.

(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 ***Verordening (EU, Euratom) 2018/1046 van het Europees Parlement en de Raad***[2] 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

---

1 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).

2 ***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, tot wijziging van Verordeningen (EU) nr. 1296/2013, (EU) nr. 1301/2013, (EU) nr. 1303/2013, (EU) nr. 1304/2013, (EU) nr. 1309/2013, (EU) nr. 1316/2013, (EU) nr. 223/2014, (EU) nr. 283/2014 en Besluit nr. 541/2014/EU en tot intrekking van Verordening (EU, Euratom) nr. 966/2012 (PB L 193 van 30.7.2018, blz. 1, ELI: http://data.europa.eu/eli/reg/2018/1046/oj).***

van de Uniebegroting zoals vastgesteld in Verordening (EU, Euratom) 2020/2092 van het Europees Parlement en de Raad[1].

(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 ***Verordening (EU, Euratom) 2018/1046*** vastgestelde middelen, zodat de capaciteit van het cybernoodmechanisme om de lidstaten te ondersteunen bij de doeltreffende bestrijding van cyberdreigingen, wordt gemaximaliseerd.

(11 bis) Het cybernoodmechanisme en de EU-cyberbeveiligingsreserve die bij deze verordening worden vastgesteld, zijn nieuwe initiatieven en maakten geen deel uit van de vaststelling van het meerjarig financieel kader voor 2021-2027; de financiering voor deze initiatieven is bedoeld om de verlaging van de financiering voor andere prioriteiten in het programma Digitaal Europa zo min mogelijk te beperken. Het bedrag van de financiële middelen dat bestemd is voor de EU-cyberbeveiligingsreserve moet derhalve worden verlaagd en mag hoofdzakelijk afkomstig zijn uit niet-toegewezen marges binnen de maxima van het meerjarig financieel kader of beschikbaar worden gesteld via de niet-thematische speciale instrumenten van het meerjarig financieel kader. Reservering of herbestemming van middelen uit bestaande programma's moet tot een absoluut minimum worden beperkt teneinde bestaande programma's, met name Erasmus+, te beschermen tegen negatieve effecten en ervoor te zorgen dat de voor die programma's vastgestelde doelstellingen kunnen worden verwezenlijkt.

(12) Om cyberdreigingen en -incidenten doeltreffender te voorkomen***,*** te beoordelen***,*** er doeltreffender op te reageren ***en er beter van te herstellen***, 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. ***Een proactieve aanpak om mogelijke cyberdreigingen aan het licht te brengen, te beperken en te voorkomen, omvat toegenomen geavanceerde opsporingscapaciteiten die nodig zijn om een einde te maken aan geavanceerde aanhoudende dreigingen. Inlichtingen over dreigingen is informatie die wordt verzameld, geanalyseerd en geïnterpreteerd om potentiële dreigingen en risico's te begrijpen. Door grote hoeveelheden gegevens te analyseren en daar verbanden tussen te leggen, komen patronen en trends naar voren, alsook indicatoren voor aantasting die kwaadwillige activiteiten of kwetsbaarheden aan het licht kunnen brengen***. Er moet een ***netwerk*** 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

[1] ***Verordening (EU, Euratom) 2020/2092 van het Europees Parlement en de Raad van 16 december 2020 betreffende een algemeen conditionaliteitsregime ter bescherming van de Uniebegroting (PB L 433I van 22.12.2020, blz. 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).***

-analyse, de capaciteit voor de opsporing en het beheer van cyberdreigingen en -incidenten te verbeteren en realtime situationeel bewustzijn te bieden. ***Een nationale SOC heeft betrekking op een gecentraliseerde capaciteit die verantwoordelijk is voor het continu vergaren van inlichtingen en informatie over cyberdreigingen en het verbeteren van de cyberbeveiligingsstrategie van entiteiten die onder nationale jurisdictie vallen door cyberdreigingen te voorkomen, op te sporen en te analyseren***. 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[1], aan te vullen en te ondersteunen.

(13) ***Om aan het cyberschild deel te nemen, moet elke*** lidstaat een overheidsinstantie op nationaal niveau aanwijzen die belast is met de coördinatie van de activiteiten voor het opsporen van cyberdreigingen in die lidstaat. ***De lidstaten worden aangemoedigd de capaciteit van de nationale SOC's te integreren in de bestaande structuur en het bestaande beheerskader voor cyberbeveiliging en geen extra beheerslagen te creëren, alsook om deze af te stemmen op de bestaande wetgevingshandeling, waaronder Richtlijn (EU) 2022/2555***. Deze nationale SOC's moeten fungeren als referentiepunt en toegangspoort op nationaal niveau voor deelname ***van private en publieke entiteiten, met name hun nationale SOC's,*** 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. ***De nationale SOC's moet de samenwerking en informatie-uitwisseling tussen publieke en private entiteiten verbeteren om de huidige verkokering bij de communicatie te doorbreken. Hiertoe kunnen zij gegevensuitwisselingsmodellen ontwikkelen en moeten zij het delen van informatie in een betrouwbare en veilige omgeving faciliteren en aanmoedigen. Nauwe en gecoördineerde samenwerking tussen publieke en private entiteiten is essentieel om de weerbaarheid van de Unie op het gebied van cyberbeveiliging te versterken.***

(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, ***waaronder het verzamelen en delen van gegevens en informatie over mogelijk kwaadwillig hacken, recent ontstane kwaadwillige dreigingen en exploits die nog niet tot cyberincidenten hebben geleid, en analyse-inspanningen, met betrekking tot 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

[1] 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).

van opsporings-, analyse- en preventiecapaciteiten in een betrouwbare ***en veilige*** omgeving***, met de ondersteuning van Enisa, inzake kwesties die verband houden met de operationele samenwerking tussen de lidstaten***. ***Landsgrensoverschrijdende SOC's*** moeten ***het delen van informatie in een betrouwbare en veilige omgeving vergemakkelijken en bevorderen en 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 ***geïntegreerd wordt in de bestaande cyberbeveiligingsinfrastructuur, met name*** het CSIRT-netwerk door gegevens over cyberdreigingen van publieke en private entiteiten***, in het bijzonder hun SOC's,*** 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 technologische soevereiniteit***, de open strategische autonomie, het concurrentievermogen en de weerbaarheid*** van de Unie***, en aan de ontwikkeling van een solide cyberbeveiligingsecosysteem, ook in de samenwerking met betrouwbare en gelijkgestemde internationale partners***.

(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) ***teneinde het doorbreken van de bestaande verkokering bij de communicatie te vergemakkelijken***. ***Hiertoe kunnen de landsgrensoverschrijdende SOC's ook de creatie van gegevensuitwisselingsmodellen in de hele Unie ondersteunen.*** 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***, met inbegrip van het verzamelen en delen van gegevens en informatie over mogelijk kwaadwillig hacken, recent ontstane kwaadwillige dreigingen en exploits die nog niet tot cyberincidenten hebben geleid, en analyse-inspanningen***. 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[1] 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 ***van de Raad***[2]. 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 ***in overeenstemming met Richtlijn (EU) 2022/2555***. 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 ***en veilige*** omgeving mogelijk te maken, moeten entiteiten die deelnemen aan het Europees cyberschild worden uitgerust met geavanceerde en zeer veilige instrumenten, apparatuur en infrastructuur ***en gekwalificeerd personeel***. 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***, de open strategische autonomie, het concurrentievermogen en de weerbaarheid*** van de Unie, ***en een solide cyberbeveiligingsomgeving van de EU*** 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. ***Artificiële intelligentie werkt het beste in combinatie met menselijke analyses. Derhalve blijven geschoolde arbeidskrachten van essentieel belang voor het bundelen van hoogwaardige gegevens.*** Dit moet worden vergemakkelijkt door het Europees

---

1 ***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 (***PB L 347 van 20.12.2013, blz. 924),
ELI: http://data.europa.eu/eli/dec/2013/1313/oj***).***

2 ***Uitvoeringsbesluit (EU) 2018/1993 van de Raad van 11 december 2018 inzake de geïntegreerde EU-regeling politieke crisisrespons (*****PB L 320 van 17.12.2018, blz. 28,***
ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

cyberschild te verbinden met de pan-Europese high-performance computing-infrastructuur die is opgericht bij Verordening (EU) 2021/1173 van de Raad[1].

(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 ("ECCC"), en in samenwerking met de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid (de "hoge vertegenwoordiger"), geleidelijk specifieke ***toegangsvoorwaarden en*** protocollen en normen ontwikkelen om samenwerking met de cyberdefensiegemeenschap mogelijk te maken, met inbegrip van doorlichting en beveiligingsvoorwaarden***, rekening houdend met het civiele karakter van instellingen en de bestemming van financiering, zodat alleen gebruik wordt gemaakt van middelen die beschikbaar zijn gesteld aan de defensiegemeenschap***. 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 ***en met de volledige eerbiediging van rechten en vrijheden***.

(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 ***het Unierecht*** of ***het nationale recht*** 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 ***en doeltreffend*** bijstand te verlenen en om het

[1] 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, ***ELI: http://data.europa.eu/eli/reg/2021/1173/oj***).

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[1] 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[2], de geïntegreerde EU-regeling politieke crisisrespons (IPCR)[3], 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***, Enisa*** 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

---

1 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.

2 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).

3 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.

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, 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[1]. 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.

---

[1] 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.

(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.

(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***, en tegelijkertijd de weerbaarheid van de Unie vergroten, waaronder de deelname van Europese aanbieders van beheerde beveiligingsdiensten die kmo's zijn, en ervoor zorgen dat er een cyberbeveiligingsomgeving wordt gecreëerd, in het bijzonder micro-ondernemingen, kmo's met inbegrip van startende ondernemingen, middels investeringen in onderzoek en innovatie (O&I) voor het ontwikkelen van geavanceerde technologieën, zoals in verband met de cloud en artificiële intelligentie. Betrouwbare aanbieders, waaronder kmo's, moeten met elkaar kunnen samenwerken om aan de bovenstaande criteria te voldoen.*** 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. ***De cyberbeveiligingsreserve moet derhalve investeringen in onderzoek en innovatie stimuleren om de ontwikkeling van deze technologieën te bevorderen. In voorkomend geval kunnen er gemeenschappelijke oefeningen met betrouwbare aanbieders en potentiële gebruikers van de cyberbeveiligingsreserve worden gehouden om te waarborgen dat de reserve wanneer nodig doeltreffend werkt.*** 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. ***De Commissie moet de betrokkenheid van en intensieve uitwisselingen met de lidstaten waarborgen om overlapping met vergelijkbare initiatieven te voorkomen, ook binnen de Noord-Atlantische Verdragsorganisatie (NAVO).***

(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. ***De deelname van kleinere aanbieders die op regionaal en lokaal niveau actief zijn, moet worden aangemoedigd.***

(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. ***Om de aanvullende taken naar aanleiding van dit voorschrift te kunnen vervullen, moet aan Enisa passende, aanvullende financiering ter beschikking worden gesteld.***

(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.

(37 bis) Derde landen kunnen uit hoofde van deze verordening toegang krijgen tot middelen en ondersteuning, door een beroep te doen op de steun voor respons op incidenten van de EU-beveiligingsreserve. Bovendien zijn er mogelijk aanbieders van incidentresponsdiensten uit derde landen, waaronder met het programma Digitaal Europa geassocieerde derde landen of andere internationale partnerlanden en NAVO-leden, nodig om specifieke diensten te leveren aan de EU-cyberbeveiligingsreserve. In afwijking van Verordening (EU, Euratom) 2018/1046, moet het in derde landen gevestigde entiteiten die geen partijen bij de Overeenkomst inzake overheidsopdrachten zijn en die niet zijn onderworpen aan een screening in de zin van Verordening (EU) 2019/452 van het Europees Parlement en de Raad[1] en, in voorkomend geval, aan beperkende maatregelen, niet worden toegestaan om deel te nemen, teneinde de technologische soevereiniteit, de open strategische autonomie, het concurrentievermogen en de weerbaarheid van de Unie te versterken, en de strategische activa, belangen of veiligheid van de Unie te beschermen, rekening houdend met de doelstellingen van deze verordening. De externe dimensie van deze verordening moet in overeenstemming zijn met het bepaalde in de associatieovereenkomst in het kader van het programma Digitaal Europa. De deelname van derde landen moet onderworpen zijn aan publieke controle, met de deelname van de wetgevende autoriteiten, om te waarborgen dat burgers aan het proces kunnen deelnemen.

(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*.

---

* ***Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren (PB L 55 van 28.2.2011, blz. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).***

(38 bis) Gekwalificeerd personeel dat in staat is de benodigde cyberbeveiligingsdiensten op betrouwbare wijze te leveren en daarbij aan de hoogste normen te voldoen, is volstrekt noodzakelijk voor de doeltreffende uitvoering van het Europees cyberschild en het

---

[1] Verordening (EU) 2019/452 van het Europees Parlement en de Raad van 19 maart 2019 tot vaststelling van een kader voor de screening van buitenlandse directe investeringen in de Unie (PB L 79I van 21.3.2019, blz. 1), ELI: http://data.europa.eu/eli/reg/2019/452/oj.

cybernoodmechanisme. Het is derhalve zorgwekkend dat de Unie door een tekort aan gekwalificeerde vakkrachten kampt met een gebrek aan talent op een moment dat zij geconfronteerd wordt met een snel veranderend dreigingslandschap, zoals aangegeven in de mededeling van de Commissie van 18 april 2023 over de academie voor cyberbeveiligingsvaardigheden. Het is belangrijk om dit gebrek aan talent aan te pakken door de samenwerking en coördinatie tussen de verschillende belanghebbenden, waaronder de particuliere sector, universiteiten, de lidstaten, de Commissie en Enisa, te versterken en zodoende in heel de Unie meer synergieën creëren voor investeringen in onderwijs en opleiding, de ontwikkeling van publiek-private partnerschappen, de ondersteuning van initiatieven op het gebied van onderzoek en innovatie, de ontwikkeling en wederzijdse erkenning van gemeenschappelijke normen en de certificering van cyberbeveiligingsvaardigheden, onder meer door middel van het Europees kader voor cyberbeveiligingsvaardigheden. Dit moet ook de mobiliteit van cyberbeveiligingsprofessionals binnen de Unie vergemakkelijken. Met deze verordening moet ook worden gestreefd naar bevordering van de diversiteit in de cyberbeveiligingssector. Alle maatregelen ter versterking van de cyberbeveiligingsvaardigheden vereisen waarborgen om een "braindrain" en een risico voor arbeidsmobiliteit te voorkomen.

(38 ter) Er is behoefte aan versterking van specialistische, interdisciplinaire en algemene vaardigheden en kennis in heel de Unie, met name onder vrouwen, aangezien er op het gebied van cyberbeveiliging nog altijd sprake is van een genderkloof, met wereldwijd 20 % vrouwen in deze sector. Vrouwen moeten betrokken worden bij de opzet van de digitale toekomst en de governance daarvan.

(38 quater) Versterking van onderzoek en innovatie (O&I) op het gebied van cyberbeveiliging is bedoeld om de weerbaarheid en de open strategische autonomie van de Unie te vergroten. Zo is het ook belangrijk om synergieën tot stand te brengen met O&I-programma's en met bestaande instrumenten en instellingen, en om samenwerking en coördinatie tussen de verschillende belanghebbenden te versterken, waaronder de particuliere sector, het maatschappelijk middenveld, universiteiten, de lidstaten, de Commissie en Enisa;

(38 quinquies) Deze verordening moet bijdragen tot de toezeggingen als bedoeld in de Europese verklaring over digitale rechten en beginselen voor het digitale decennium in verband met de bescherming van de belangen van onze democratieën, bevolkingen, bedrijven en overheden tegen cyberbeveiligingsrisico's en cybercriminaliteit, waaronder datalekken en identiteitsdiefstal of -manipulatie. De toepassing van deze verordening moet ook helpen de uitvoering van andere wetgeving te verbeteren, bijvoorbeeld op het gebied van artificiële intelligentie, gegevensbescherming en gegevensregulering met betrekking tot cyberbeveiliging en cyberveerkracht.

(38 sexies) Versterking van de cyberbeveiligingscultuur, inclusief beveiliging, met inbegrip van de digitale omgeving, als een publiek goed, zal essentieel zijn voor de succesvolle uitvoering van deze verordening. Vandaar dat het ontwikkelen van maatregelen voor (vergroting van) het bewustzijn van burgers nog een manier is om onze democratieën en fundamentele waarden te beschermen.

(38 septies) Om bepaalde niet-essentiële elementen van deze verordening aan te vullen, moet aan de Commissie de bevoegdheid worden verleend om handelingen vast te stellen in overeenstemming met artikel 290 VWEU om de voorwaarden vast te stellen voor interoperabiliteit tussen landsgrensoverschrijdende SOC's, het vaststellen van

procedurele regelingen voor het delen van informatie tussen de landsgrensoverschrijdende SOC's enerzijds en EU-CyCLONe, het CSIRT-netwerk en de Commissie anderzijds, het specificeren van het soort en het aantal responsdiensten die voor de EU-cyberbeveiligingsreserve nodig zijn, en het nader specificeren van de nadere regelingen voor de toewijzing van de ondersteunende diensten van de EU-cyberbeveiligingsreserve. Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden tot passende raadplegingen overgaat, onder meer op deskundigenniveau, en dat die raadplegingen gebeuren in overeenstemming met de beginselen die zijn vastgelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven*. Met name om te zorgen voor gelijke deelname aan de voorbereiding van gedelegeerde handelingen ontvangen het Europees Parlement en de Raad alle documenten op hetzelfde tijdstip als de deskundigen van de lidstaten, en hebben hun deskundigen systematisch toegang tot de vergaderingen van de deskundigengroepen van de Commissie die zich bezighouden met de voorbereiding van de gedelegeerde handelingen.

****PB L 123 van 12.5.2016, blz. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj***

(39) De ***doelstellingen*** van deze verordening***, namelijk het versterken van de capaciteit van de Unie om cyberdreigingen te voorkomen, op te sporen, daarop te reageren en zich daarvan te herstellen, en het vaststellen van een algemeen kader voor het doorbreken van de verkokering bij de communicatie, kunnen niet voldoende door de lidstaten worden verwezenlijkt, maar kunnen*** beter op het niveau van de Unie 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. ***Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat*** deze verordening 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-Europees netwerk*** 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 industriële capaciteit van de Unie en de lidstaten in de sector cyberbeveiliging kan worden versterkt,*** de concurrentiepositie van de industrie***, met name micro-ondernemingen, kmo's met inbegrip van startende ondernemingen,*** en de dienstensector in de Unie in de digitale economie ***versterken, bijdragen*** tot de technologische soevereiniteit***, de open strategische autonomie, het concurrentievermogen en de weerbaarheid*** van de Unie ***in die sector, en de cyberbeveiligingsomgeving versterken om sterke capaciteiten van de Unie te waarborgen, onder meer in de samenwerking met internationale partners***;

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***;***

c bis) op gecoördineerde wijze vaardigheden, knowhow en competenties van de beroepsbevolking ontwikkelen, teneinde cyberbeveiliging te waarborgen en synergieën met de academie voor cyberbeveiligingsvaardigheden tot stand te brengen.

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 bis) ***"nationaal centrum voor beveiligingsoperaties" of "nationaal SOC": een gecentraliseerde nationale capaciteit die voortdurend inlichtingen over cyberdreigingen verzamelt en analyseert en de benadering van cyberbeveiliging verbetert overeenkomstig artikel 4;***

1) **"landsgrensoverschrijdend centrum voor beveiligingsoperaties"** ***of*** **"landsgrensoverschrijdend SOC"**: een meerlandenplatform dat nationale SOC's samenbrengt in een gecoördineerde netwerkstructuur ***overeenkomstig artikel 5***;

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[1];

3) **"onderbrengend consortium"**: een consortium bestaande uit deelnemende staten, vertegenwoordigd door nationale SOC's, ***overeenkomstig artikel 5***;

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

4 bis) ***"kritieke entiteit": een kritieke entiteit zoals gedefinieerd in artikel 2, punt 1), van Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad[2];***

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

5 bis) ***"incidentenbehandeling": incidentenbehandeling zoals gedefinieerd in artikel 6, punt 8, van Richtlijn (EU) 2022/2555;***

5 ter) ***"risico": een risico zoals gedefinieerd in artikel 6, punt 9, van Richtlijn (EU) 2022/2555;***

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

6 bis) ***"significante cyberdreiging": een cyberdreiging zoals gedefinieerd in artikel 6, punt 11, van Richtlijn (EU) 2022/2555;***

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;

---

1 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).

2 ***Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (PB L 333 van 27.12.2022, blz. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).***

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;

10 bis) "aanbieder van beheerde beveiligingsdiensten": een aanbieder van beheerde diensten zoals gedefinieerd in artikel 6, punt 40, van Richtlijn (EU) 2022/2555;

11) **"betrouwbare aanbieders *van beheerde beveiligingsdiensten*"**: aanbieders van beheerde beveiligingsdiensten geselecteerd overeenkomstig artikel 16 van deze verordening ***om te worden opgenomen in de EU-cyberbeveiligingsreserve***.

Hoofdstuk II

HET EUROPEES CYBERSCHILD

Artikel 3

Oprichting van het Europees cyberschild

1. Er wordt een ***netwerk*** van centra voor beveiligingsoperaties ("Europees cyberschild") opgezet om voor de Unie geavanceerde capaciteiten op het gebied van het opsporen en analyseren van cyberdreigingen en ***het voorkomen van 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 ***en wisselt, in voorkomend geval, informatie uit met het CSIRT-netwerk***;

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***, mede door entiteiten concrete aanbevelingen te doen***;

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 ***kunnen*** nemen aan het Europees Cyberschild wijst elke lidstaat ten minste één nationaal SOC aan. Het nationale SOC is een ***gecentraliseerde capaciteit binnen een*** overheidsinstantie. ***Indien mogelijk worden de nationale SOC's geïntegreerd in de CSIRT's of andere bestaande cyberbeveiligingsinfrastructuur en -governance.***

Het kan fungeren als referentiepunt en toegangspoort tot andere publieke en private organisaties op nationaal niveau***, met name hun nationale SOC's,*** voor het verzamelen en analyseren van informatie over cyberdreigingen en -incidenten ***en, in voorkomend geval, het delen van die informatie met leden van het CSIRT-netwerk van dit lidstaat,*** en voor het bijdragen tot een landsgrensoverschrijdend SOC. Het wordt uitgerust met geavanceerde technologieën waarmee gegevens over cyberdreigingen en -incidenten kunnen worden ***voorkomen,*** opgespoord, samengevoegd en geanalyseerd.

Een nationaal SOC of CSIRT kan aanbieders van beheerde beveiligingsdiensten die een dienst leveren aan een kritieke entiteit verzoeken om telemetrie-, sensor- of registratiegegevens van hun nationale kritieke entiteiten. Die gegevens worden gedeeld in overeenstemming met de Uniewetgeving inzake gegevensbescherming en uitsluitend om het nationale SOC of CSIRT te ondersteunen bij het opsporen en voorkomen van cyberdreigingen en -incidenten.

2. Na een oproep tot het indienen van blijken van belangstelling ***kunnen*** de nationale SOC's door het Europees Kenniscentrum voor cyberbeveiliging ("ECCC") ***worden*** 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. ***Een landsgrensoverschrijdende SOC wordt opgezet voor het opsporen en analyseren van cyberdreigingen, het voorkomen van incidenten en het ondersteunen van de productie van hoogwaardige inlichtingen, met name door het uitwisselen van gegevens uit diverse publieke en private bronnen, alsook door het delen van geavanceerde instrumenten, en het gezamenlijk ontwikkelen van capaciteiten op het gebied van opsporing, analyse, preventie en bescherming in een betrouwbare en veilige omgeving.***

2. Na een 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. 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.

2 bis. In afwijking van artikel 176 van Verordening (EU, Euratom) 2018/1046 nemen in derde landen gevestigde entiteiten die geen partijen bij de Overeenkomst inzake overheidsopdrachten zijn niet deel aan de gezamenlijke aanbesteding van instrumenten en infrastructuur.

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) ***bijdraagt aan een betere uitwisseling van inlichtingen over cyberdreigingen tussen nationale en landsgrensoverschrijdende SOC's en ISAC's van het bedrijfsleven gericht op het voorkomen, detecteren of beperken van dreigingen;***

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 ***relevante*** ▌ 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 ***en met ISAC's van het bedrijfsleven*** te bevorderen, zorgen de landsgrensoverschrijdende SOC's voor een hoog niveau van onderlinge interoperabiliteit ***en, waar mogelijk, met ISAC's van het bedrijfsleven***. Om de interoperabiliteit tussen de landsgrensoverschrijdende SOC's ***en met ISAC's van het bedrijfsleven*** te faciliteren, ***kunnen de normen en protocollen inzake informatie-uitwisseling worden afgestemd op de internationale normen en beste praktijken in het bedrijfsleven. De gezamenlijke aanbesteding van cyberinfrastructuur, -diensten en -instrumenten wordt ook aangemoedigd. Bovendien is de Commissie bevoegd om,*** na raadpleging van het ECCC ***en Enisa, uiterlijk ... [zes maanden na de datum van inwerkingtreding van deze verordening] overeenkomstig artikel 20 bis gedelegeerde handelingen vast te stellen om deze verordening aan te vullen***, ***door*** de voorwaarden voor deze interoperabiliteit ***te*** specificeren ***in nauwe samenwerking met de landsgrensoverschrijdende SOC's en op basis van internationale normen en de beste praktijken in de sector***.

4. Landsgrensoverschrijdende SOC's sluiten samenwerkingsovereenkomsten met elkaar ***en, in voorkomend geval, met ISAC's van het bedrijfsleven***, waarin de beginselen voor informatie-uitwisseling ***en interoperabiliteit*** tussen de landsgrensoverschrijdende platforms worden gespecificeerd***, daarbij rekening houdend met de in Richtlijn (EU) 2022/2555 bedoelde reeds bestaande relevante mechanismen voor informatie-uitwisseling***. ***In voorkomend geval sluiten landsgrensoverschrijdende SOC's samenwerkingsovereenkomsten met ISAC's van het bedrijfsleven. In het kader van een mogelijk of lopend grootschalig***

cyberbeveiligingsincident voldoen de mechanismen voor de uitwisseling van informatie aan de relevante voorschriften van Richtlijn (EU) 2022/2555.

Artikel 7

Samenwerking en informatie-uitwisseling met *het CSIRT-netwerk*

1. Wanneer de landsgrensoverschrijdende SOC's informatie verkrijgen over een mogelijk of lopend grootschalig cyberbeveiligingsincident, ***verstrekt de coördinerende SOC ten behoeve van het gedeeld situationeel bewustzijn onverwijld de relevante informatie aan het CSIRT of de bevoegde autoriteit, die dit meldt*** aan EU-CyCLONe, het CSIRT-netwerk en de Commissie ***en Enisa***, ***in overeenstemming met*** hun respectieve taken ***en procedures*** op het gebied van crisisbeheersing overeenkomstig Richtlijn (EU) 2022/2555. ***Dit lid behelst geen verdere verplichtingen voor publieke of particuliere entiteiten om een mogelijk of lopend grootschalig cyberbeveiligingsincident te melden voor het nakomen van de verplichtingen van Richtlijn (EU) 2022/2555.***

2. De Commissie ***is bevoegd om overeenkomstig artikel 20 bis, na raadpleging van het CSIRT-netwerk, gedelegeerde handelingen vast te stellen teneinde deze verordening aan te vullen*** door de procedurele regelingen voor de in lid 1 ***van dit artikel en overeenkomstig Richtlijn (EU) 2022/2555*** bedoelde informatie-uitwisseling ***vast te stellen***.

Artikel 8

Beveiliging

1. De lidstaten die deelnemen aan het Europees cyberschild zorgen voor een hoog niveau van ***vertrouwelijkheid en*** 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. ***Zij voldoen aan de Richtlijnen (EU) 2022/2555 en (EU) 2022/2557***. De Commissie ***houdt in haar uitvoeringshandelingen***, 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 ▌***mechanisme*** 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 ***van beheerde beveiligingsdiensten*** 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.

1 bis. Nadat het mechanisme in werking wordt gesteld, beoordeelt de Commissie op jaarbasis zowel de positieve als de negatieve aspecten van de werking van het mechanisme en brengt ze daarover een verslag uit, waarbij zij tevens aangeeft of er verdere samenwerking of opleidingsvereisten nodig zijn.

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 ***in overeenstemming met de***

regelingen die zijn vastgesteld voor de entiteiten in zeer kritieke sectoren zoals bedoeld in bijlage I bij Richtlijn (EU) 2022/2555.

2. De NIS-samenwerkingsgroep ontwikkelt in samenwerking met de Commissie, Enisa***,*** de hoge vertegenwoordiger ***en de entiteiten die overeenkomstig lid 1 aan de gecoördineerde paraatheidstest worden onderworpen*** gemeenschappelijke risicoscenario's en -methoden voor de gecoördineerde ***paraatheidstests, hetgeen resulteert in een gezamenlijk werkplan***. ***Entiteiten die aan gecoördineerde paraatheidstests worden onderworpen, ontwikkelen en voeren een herstelplan uit waarmee uitvoering wordt gegeven aan de aanbevelingen die uit de paraatheidstests voortvloeien.***

De NIS-samenwerkingsgroep kan een bijdrage leveren aan de prioritering van sectoren, of subsectoren voor de gecoördineerde paraatheidstests.

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.

Wanneer duidelijk is dat de aanbestede diensten niet volledig kunnen worden gebruikt voor het bieden van ondersteuning aan de respons op significante of grootschalige incidenten, kunnen die diensten bij wijze van uitzondering worden aangewend voor oefeningen of opleidingen voor het omgaan met incidenten, en op verzoek door de aanbestedende dienst aan de gebruikers worden verleend.

2. De EU-cyberbeveiligingsreserve bestaat uit incidentresponsdiensten van betrouwbare aanbieders ***van beheerde beveiligingsdiensten*** die zijn geselecteerd overeenkomstig de criteria van artikel 16. De ***EU-cyberbeveiligingsreserve*** omvat vooraf vastgelegde diensten. De diensten kunnen in alle lidstaten worden geleverd ***en versterken de technologische soevereiniteit, de open strategische autonomie, het concurrentievermogen en de weerbaarheid van de Unie in de sector cyberbeveiliging, onder meer door innovatie in de digitale eengemaakte markt in de hele Unie te stimuleren***.

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 ***als bedoeld in artikel 3, punt 1, van Verordening (EU) .../2023 van het Europees Parlement en de Raad[1] en CERT-EU***.

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

[1] ***Verordening (EU) .../2023 tot vaststelling van maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie (PB C , , blz., , ELI: ...).***

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 ***in samenspraak met de samenwerkingsgroep van NIS2*** 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 ***vertrouwt*** de werking en het beheer van de EU-cyberbeveiligingsreserve geheel of gedeeltelijk ***toe*** 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 ***en, in voorkomend geval, aanbieders van beheerde beveiligingsdiensten en andere vertegenwoordigers van de sector cyberbeveiliging***, de benodigde diensten in kaart***, waaronder de daarvoor benodigde vaardigheden en capaciteit van het cyberbeveiligingspersoneel***. Na raadpleging van de Commissie***, aanbieders van beheerde beveiligingsdiensten en, in voorkomend geval, andere vertegenwoordigers van de sector cyberbeveiliging*** 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 ***en informeert zij de Raad over de behoeften van derde landen***.

8. De Commissie ***is bevoegd overeenkomstig artikel 20 bis gedelegeerde handelingen vast te stellen teneinde deze verordening aan te vullen door*** de soorten en het aantal responsdiensten ***te*** specificeren die voor de EU-cyberbeveiligingsreserve vereist zijn. ▌..

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. De Commissie ***is bevoegd overeenkomstig artikel 20 bis gedelegeerde handelingen vast te stellen teneinde deze verordening aan te vullen door*** de nadere regelingen voor de toewijzing van de ondersteunende diensten van de EU-cyberbeveiligingsreserve nader ***te*** specificeren. ▌

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 ***en uiterlijk binnen 24 uur*** 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 ***omvang en 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 ***en alle verdere bepalingen die de partijen bij de overeenkomst noodzakelijk achten voor de levering van de desbetreffende dienst***.

4. De in lid 3 bedoelde overeenkomsten ***worden*** gebaseerd op modellen die Enisa na overleg met de lidstaten ***en, in voorkomend geval, andere gebruikers van de EU-cyberbeveiligingsreserve*** 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***, behalve in geval van grove nalatigheid bij de beoordeling van de aanvraag van de dienstverlener of in het geval dat de Commissie en Enisa gebruikers van de EU-cyberbeveiligingsreserve zijn overeenkomstig artikel 14, lid 3***.

6. Binnen een maand na het einde van de ondersteuningsactie dienen de gebruikers bij de Commissie***,*** Enisa***, het CSIRT-netwerk en, in voorkomend geval, EU-CyCLONe*** 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.
Bij het opstellen van het verslag worden het Unierecht en het nationale recht inzake de bescherming van gevoelige of gerubriceerde informatie in acht genomen.

7. De Commissie brengt regelmatig ***en ten minste tweemaal per jaar*** verslag uit aan de NIS-samenwerkingsgroep over het gebruik en de resultaten van de steun. ***Zij beschermt vertrouwelijke informatie overeenkomstig het Unierecht en het nationale recht inzake de bescherming van gevoelige of gerubriceerde informatie.***

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[1], 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, ***VEU***.

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 ***VWEU***.

[1] 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).

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:

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***, het tot stand brengen van genderevenwicht in de sector en het versterken van de technologische soevereiniteit, de open strategische autonomie, het concurrentievermogen en de weerbaarheid van de Unie***.

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 ***actuele*** technische hardware en software die nodig zijn om de gevraagde dienst te ondersteunen ***en voldoet, in voorkomend geval, aan Verordening (EU) .../... van het Europees Parlement en de Raad[1] (2022/0272(COD))***;

[1] Verordening (EU) .../... van het Europees Parlement en de Raad van ... inzake ... (PB L, …, ELI: …).

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***, of in een van de werktalen van de instellingen van de Unie***;

j) zodra een ***Europese regeling voor cyberbeveiligingscertificering*** voor beheerde beveiligingsdiensten overeenkomstig Verordening (EU) 2019/881 van kracht is, wordt de aanbieder ***binnen twee jaar na de vaststelling ervan*** overeenkomstig die regeling gecertificeerd***;***

j bis) de aanbieder is in staat de dienst onafhankelijk te verlenen en niet als onderdeel van een pakket, waarmee de mogelijkheid voor de gebruiker om naar een andere dienstverlener over te stappen, wordt gewaarborgd;

j ter) voor de toepassing van artikel 12, lid 1, neemt de aanbieder in de aanbieding de mogelijkheid op om ongebruikte incidentresponsdiensten voor oefeningen of opleidingen te gebruiken;

j quater) de aanbieder is gevestigd en heeft zijn uitvoerende bestuursstructuren in de Unie, in een geassocieerd land of in een derde land dat partij is bij de Overeenkomst inzake overheidsopdrachten in de context van de Wereldhandelsorganisatie.

j quinquies) de aanbieder staat niet onder zeggenschap van een niet-geassocieerd derde land of een entiteit uit een niet-geassocieerd derde land die geen partij is bij de Overeenkomst inzake overheidsopdrachten, ofwel is een dergelijke entiteit onderworpen geweest aan een screening in de zin van Verordening (EU) 2019/452 en, indien nodig, mitigerende maatregelen, rekening houdend met de doelstellingen van deze verordening.

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 ***stelt de Raad onverwijld op de hoogte en*** 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 ***en verzamelt het feedback van*** alle relevante belanghebbenden, waaronder vertegenwoordigers van de lidstaten, de Commissie, andere relevante EU-instellingen, -organen en -instanties, aanbieders van beheerde beveiligingsdiensten ***in de nationale en landsgrensoverschrijdende SOC's*** en gebruikers van cyberbeveiligingsdiensten***, aangevuld met passende waarborgen en monitoring die ervoor zorgt dat de geleerde lessen en in kaart gebrachte beste praktijken door de actoren in de cyberbeveiligingsdienstensector worden opgevolgd***. 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. ***Het bevat geen details over actief uitgebuite kwetsbaarheden die nog niet verholpen zijn.***

3 bis. Het in lid 1 van dit artikel bedoelde verslag bevat de lessen die geleerd zijn naar

aanleiding van de overeenkomstig artikel 19 van Richtlijn (EU) 2022/2555 uitgevoerde collegiale toetsingen.

4. In voorkomend geval worden in het verslag aanbevelingen gedaan***, mede voor alle relevante belanghebbenden,*** 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:

i) 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";

ii) 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";

b) 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*, met uitzondering van acties ter uitvoering van de EU-cyberbeveiligingsreserve, die door de Commissie en Enisa worden uitgevoerd.

_____

* 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***, ELI: http://data.europa.eu/eli/reg/2021/887/oj).";***

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) ***1 620 566 000*** EUR voor specifieke doelstelling 3 – Cyberbeveiliging en vertrouwen;

d) ***500 347 000*** EUR voor specifieke doelstelling 4 – Geavanceerde digitale vaardigheden";

a bis) het volgende nieuwe lid 2 bis wordt ingevoegd:

"2 bis. Het in lid 2, punt c), genoemde bedrag wordt hoofdzakelijk gebruikt voor het verwezenlijken van de in artikel 6, lid 1, punten a) tot en met f), van het programma bedoelde operationele doelstellingen.";

a ter) het volgende nieuwe lid 2 ter wordt ingevoegd:

"2 ter. Het bedrag voor de vaststelling en uitvoering van de EU-cyberbeveiligingsreserve bedraagt niet meer dan 27 miljoen EUR voor de beoogde looptijd van de verordening 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.";

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 ***in het kader van de uitvoering van de EU-cyberbeveiligingsreserve*** 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.

De Commissie stelt het Parlement en de Raad overeenkomstig artikel 12, lid 6, van Verordening (EU, Euratom) 2018/1046 in kennis van overgedragen kredieten.";

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 ***Verordening (EU, Euratom) 2018/1046*** 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.

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/**…** 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) **…/…** 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) **…/…** 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:

“Artikel 16 bis

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/**…**. In geval van strijdigheid tussen de bepalingen van deze verordening en de artikelen 4 en 5 van Verordening (EU) 2023/**…** 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 ***Verordening (EU, Euratom) 2018/1046*** en mogen tot 100 % van de subsidiabele kosten dekken, onverminderd het medefinancieringsbeginsel dat is vastgelegd in artikel 190 van ***Verordening (EU, Euratom) 2018/1046***. 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 ***(EU) .../...*** en het onderbrengend consortium als bedoeld in artikel 5 van Verordening ***(EU) .../...***, overeenkomstig artikel 195, lid 1, punt d), van ***Verordening (EU, Euratom) 2018/1046***.

Steun in de vorm van subsidies voor het cybernoodmechanisme als bedoeld in artikel 10 van Verordening ***(EU) .../...*** 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 ***Verordening (EU, Euratom) 2018/1046***.

Voor de in artikel 10, lid 1, punt c), van Verordening ***(EU) .../...*** 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 ***(EU) .../...***en overeenkomstig artikel 193, lid 2, tweede alinea, punt a), van ***Verordening (EU, Euratom) 2018/1046*** 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 ***bij Verordening (EU) 2021/694*** worden gewijzigd overeenkomstig de bijlage bij deze verordening.

Artikel 19 bis
Aanvullende middelen voor Enisa

Enisa ontvangt aanvullende middelen om de bij deze verordening aan hem toegekende extra taken uit te voeren. De aanvullende steun, met inbegrip van financiering, brengt de verwezenlijking van de doelstellingen van andere programma's van de Unie, met name het programma Digitaal Europa, niet in het gedrang.

Artikel 20

Evaluatie *en herziening*

1. Uiterlijk [***twee*** jaar na de datum van toepassing van deze verordening] ***en vervolgens om de twee jaar voert*** de Commissie ***een evaluatie uit van de werking van de in deze verordening vastgestelde maatregelen en dient zij hiervan een verslag in*** bij het Europees Parlement en de Raad.

2. Tijdens deze evaluatie wordt met name het volgende beoordeeld:

a) het gebruik en de toegevoegde waarde van de landsgrensoverschrijdende SOC's en de mate waarin zij bijdragen tot het bevorderen van de opsporing van en de respons op cyberdreigingen en het situationeel bewustzijn; de actieve deelname van nationale SOC's aan het Europees cyberschild, waaronder het aantal opgerichte nationale SOC's en landsgrensoverschrijdende SOC's en de mate waarin het heeft bijgedragen tot de productie en uitwisseling van hoogwaardige, bruikbare informatie en inlichtingen over cyberdreigingen; het aantal en de kosten van gezamenlijk verworven infrastructuurvoorzieningen en/of instrumenten inzake cyberbeveiliging; het aantal tussen landsgrensoverschrijdende SOC's en met ISAC's van het bedrijfsleven gesloten samenwerkingsovereenkomsten; het aantal incidenten dat is gemeld bij het CSIRT-netwerk en de gevolgen ervan voor de werkzaamheden van het CSIRT-netwerk;

b) zowel de positieve als de negatieve werking van het cybernoodmechanisme, onder andere of verdere samenwerkings- of opleidingsvereisten nodig zijn;

c) de bijdrage van deze verordening aan de weerbaarheid en de open strategische autonomie van de Unie, de verbetering van het concurrentievermogen van de relevante bedrijfstakken, micro-ondernemingen, kmo's met inbegrip van startende ondernemingen, en de ontwikkeling van cyberbeveiligingsvaardigheden in de Unie;

d) het gebruik en de toegevoegde waarde van de EU-cyberbeveiligingsreserve, waaronder het aantal betrouwbare aanbieders van beveiligingsdiensten in het kader van de EU-cyberbeveiligingsreserve; het aantal, soort, de kosten en de gevolgen van de acties die zijn uitgevoerd ter ondersteuning van de respons op cyberbeveiligingsincidenten, alsook de gebruikers en aanbieders ervan; de gemiddelde tijd die de Commissie nodig heeft om incidenten te erkennen, die voor de EU-cyberbeveiligingsreserve nodig is om te worden uitgerold en te reageren, en die de gebruiker nodig heeft om daarvan te herstellen; de vraag of het bereik van de EU-cyberbeveiligingsreserve moet worden uitgebreid tot diensten ter voorbereiding op incidenten of gemeenschappelijke oefeningen met de betrouwbare aanbieders van beheerde beveiligingsdiensten en potentiële gebruikers van de EU-cyberbeveiligingsreserve om waar nodig een efficiënte werking van de EU-cyberbeveiligingsreserve te waarborgen;

e) de bijdrage van deze verordening aan de ontwikkeling en verbetering van de vaardigheden en competenties van het personeel in de cyberbeveiligingssector, die

nodig zijn om het vermogen van de Unie om cyberdreigingen en -incidenten op te sporen, te voorkomen, hierop te reageren en zich hiervan te herstellen, te versterken;

f) de bijdrage van deze verordening aan de ontwikkeling en toepassing van geavanceerde technologieën in de Unie.

3. Op basis van de in lid 1 bedoelde verslagen dient de Commissie zo nodig bij het Europees Parlement en bij de Raad een wetgevingsvoorstel in om deze verordening te wijzigen.

Artikel 20 bis

Uitoefening van de bevoegdheidsdelegatie

1. De bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend onder de in dit artikel neergelegde voorwaarden.

2. De in artikel 6, lid 3, artikel 7, lid 2, artikel 12, lid 8, en artikel 13, lid 7, bedoelde bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend voor een periode van ... jaar met ingang van ... [datum van inwerkingtreding van de basiswetgevingshandeling of een andere door de medewetgevers vastgestelde datum]. De Commissie stelt uiterlijk negen maanden voor het einde van de termijn van ... jaar een verslag op over de bevoegdheidsdelegatie. De bevoegdheidsdelegatie wordt stilzwijgend met termijnen van dezelfde duur verlengd, tenzij het Europees Parlement of de Raad zich uiterlijk drie maanden voor het einde van elke termijn tegen deze verlenging verzet.

3. Het Europees Parlement of de Raad kan de in artikel 6, lid 3, artikel 7, lid 2, artikel 12, lid 8, en artikel 13, lid 7, bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Het besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheid. Het wordt van kracht op de dag na die van de bekendmaking ervan in het Publicatieblad van de Europese Unie of op een daarin genoemde latere datum. Het laat de geldigheid van de reeds van kracht zijnde gedelegeerde handelingen onverlet.

4. Vóór de vaststelling van een gedelegeerde handeling raadpleegt de Commissie de door elke lidstaat aangewezen deskundigen overeenkomstig de beginselen die zijn neergelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven.

5. Zodra de Commissie een gedelegeerde handeling heeft vastgesteld, doet zij daarvan gelijktijdig kennisgeving aan het Europees Parlement en de Raad.

6. Een overeenkomstig artikel 6, lid 3, artikel 7, lid 2, artikel 12, lid 8, en artikel 13, lid 7, vastgestelde gedelegeerde handeling treedt alleen in werking indien het Europees Parlement

noch de Raad daartegen binnen een termijn van twee maanden na de kennisgeving van die handeling aan het Europees Parlement en de Raad bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad voor het verstrijken van deze termijn de Commissie heeft medegedeeld daartegen geen bezwaar te zullen maken. Die termijn wordt op initiatief van het Europees Parlement of de Raad met [twee maanden] verlengd.

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*

BIJLAGE

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

(1) In bijlage I wordt de afdeling/het hoofdstuk "Specifieke doelstelling 3 – Cyberbeveiliging en vertrouwen" vervangen door:

"Specifieke doelstelling 3 – Cyberbeveiliging en vertrouwen

Met het programma wordt de versterking, opbouw en verwerving van essentiële capaciteiten ter beveiliging van de digitale economie, de samenleving en de democratie van de Unie gestimuleerd door versterking van het potentieel en de concurrentiekracht van de cyberbeveiligingssector van de Unie, en door verbetering van de capaciteiten van de private en de publieke sector met betrekking tot de bescherming van burgers en bedrijven tegen cyberdreigingen, onder meer door ondersteuning van de uitvoering van Richtlijn (EU) 2016/1148.

Tot de initiële en, in voorkomend geval, de vervolgacties uit hoofde van deze doelstelling behoren:

1. Gezamenlijke investeringen met de lidstaten in geavanceerde cyberbeveiligingsapparatuur, -infrastructuur en -expertise die van essentieel belang zijn voor de bescherming van kritieke infrastructuur en de digitale eengemaakte markt in het algemeen. Mogelijke gezamenlijke investeringen zijn investeringen in kwantumvoorzieningen en gegevensbronnen voor cyberbeveiliging, situationeel bewustzijn in de cyberruimte, ***met inbegrip van nationale en grensoverschrijdende centra voor beveiligingsoperaties (SOC's) die het Europees cyberschild vormen***, alsmede andere instrumenten waarover de publieke en de private sector in heel Europa moeten kunnen beschikken.

2. Vergroten van de technologische capaciteiten en koppelen van de kenniscentra in de lidstaten, en ervoor zorgen dat deze capaciteiten tegemoetkomen aan de behoeften van de publieke sector en het bedrijfsleven, onder meer door middel van producten en diensten die de cyberbeveiliging en het vertrouwen binnen de digitale eengemaakte markt versterken.

3. Zorgen voor een brede uitrol van doeltreffende uiterst geavanceerde oplossingen inzake cyberbeveiliging en vertrouwen in alle lidstaten. Deze uitrol omvat het versterken van de beveiliging en veiligheid van producten, van het ontwerp tot de commercialisering ervan.

4. Ondersteuning voor het dichten van de kloof op het gebied van cyberbeveiligingsvaardigheden***, met bijzondere aandacht voor het tot stand brengen van genderevenwicht in de sector***, bijvoorbeeld door programma's betreffende cyberbeveiligingsvaardigheden op elkaar af te stemmen, deze aan te passen aan de specifieke behoeften van sectoren***, inclusief een interdisciplinaire en algemene focus, en de toegang tot gerichte, gespecialiseerde opleiding te vergemakkelijken om iedereen overal in de gelegenheid te stellen gebruik te maken van de kansen die deze verordening biedt***.

5. Het bevorderen van solidariteit tussen de lidstaten bij de voorbereiding en respons op significante cyberbeveiligingsincidenten door de grensoverschrijdende uitrol van cyberbeveiligingsdiensten, met inbegrip van steun voor wederzijdse bijstand tussen overheidsinstanties en de vorming van een reserve van betrouwbare aanbieders van ***beheerde beveiligingsdiensten*** op het niveau van de Unie.

(2) In bijlage II wordt de afdeling/het hoofdstuk "Specifieke doelstelling 3 – Cyberbeveiliging en vertrouwen" vervangen door:

"Specifieke doelstelling 3 – Cyberbeveiliging en vertrouwen

3.1. Het aantal gezamenlijk verworven infrastructuurvoorzieningen en/of instrumenten inzake cyberbeveiliging ***in het kader van het cyberbeveiligingsschild***.

3.2. Het aantal gebruikers en gemeenschappen van gebruikers die toegang hebben tot Europese voorzieningen inzake cyberbeveiliging

3.3. Het aantal***, het soort, de kosten en de gevolgen van de*** acties ***die zijn uitgevoerd*** ter ondersteuning van de paraatheid voor en de respons op cyberbeveiligingsincidenten in het kader van het cybernoodmechanisme. ***De mate waarin aanbevelingen van paraatheidstests zijn toegepast en uitgevoerd door de gebruiker alsook de gemiddelde***

tijd die de Commissie nodig heeft om incidenten te erkennen, die voor de EU-cyberbeveiligingsreserve nodig is om te reageren, en die de gebruiker nodig heeft om daarvan te herstellen.