



VERORDENING (EU) 2025/38 VAN HET EUROPEES PARLEMENT EN DE RAAD

van 19 december 2024

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 (verordening cybersolidariteit)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

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

Gezien het voorstel van de Europese Commissie,

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

Gezien het advies van de Rekenkamer ⁽¹⁾,

Gezien het advies van het Europees Economisch en Sociaal Comité ⁽²⁾,

Gezien het advies van het Comité van de Regio's ⁽³⁾,

Handelend volgens de gewone wetgevingsprocedure ⁽⁴⁾,

Overwegende hetgeen volgt:

- (1) Gelet op de steeds grotere onderlinge verbondenheid en afhankelijkheid van overheidsdiensten van de lidstaten, bedrijven en burgers, over sectoren en grenzen heen zijn het gebruik en de afhankelijkheid van informatie- en communicatietechnologieën fundamentele aspecten geworden van alle sectoren van de economische activiteit en de samenleving, waardoor tegelijkertijd mogelijke kwetsbaarheden ontstaan.
- (2) De omvang, frequentie en impact van cyberbeveiligingsincidenten, met inbegrip van aanvallen op toeleveringsketens ten behoeve van cyberspionage, gijzelsoftware of verstoring, nemen overal in de Unie en wereldwijd toe. Zij vormen een grote bedreiging voor het functioneren van netwerk- en informatiesystemen. Gelet op het snel veranderende dreigingslandschap vereist de dreiging van mogelijke grootschalige cyberbeveiligingsincidenten die aanzienlijke verstoringen of schade aan kritieke infrastructuur veroorzaken, een grotere paraatheid van het cyberbeveiligingskader van de Unie. Deze dreiging gaat verder dan de Russische aanvalsoorlog tegen Oekraïne en zal waarschijnlijk aanhouden gezien het grote aantal actoren die betrokken zijn bij de huidige geopolitieke spanningen. Dergelijke incidenten kunnen de verlening van openbare diensten belemmeren, aangezien cyberaanvallen vaak gericht zijn op lokale, regionale of nationale openbare diensten en infrastructuur, waarbij lokale overheden bijzonder kwetsbaar zijn, ook vanwege hun beperkte middelen. Zij kunnen ook de uitoefening van economische activiteiten, ook in zeer kritieke of andere kritieke sectoren, belemmeren, aanzienlijke financiële verliezen veroorzaken, het vertrouwen van de gebruikers ondermijnen, grote schade toebrengen aan de economie en de democratische systemen van de Unie, en zelfs gevolgen voor de gezondheid of levensbedreigende gevolgen hebben. Bovendien zijn cyberbeveiligingsincidenten onvoorspelbaar, aangezien zij vaak snel ontstaan en evolueren, niet beperkt zijn tot een specifiek geografisch gebied en zich gelijktijdig of onmiddellijk over vele landen verspreiden. Het is belangrijk dat de publieke sector, de private sector, de academische wereld, het maatschappelijk middenveld en de media nauw samenwerken.
- (3) Het is nodig de concurrentiepositie van de industrie- en dienstensector in de Unie in de gedigitaliseerde economie te versterken en de digitale transformatie ervan te ondersteunen 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. Het is noodzakelijk om burgers, bedrijven, met inbegrip van micro-ondernemingen, kleine en middelgrote ondernemingen en start-ups, en entiteiten die kritieke infrastructuur exploiteren, weerbaarder te maken tegen de toenemende cyberbedreigingen, die verwoestende maatschappelijke en economische gevolgen kunnen hebben. Daarom is er behoefte aan investeringen in infrastructuur en diensten en capaciteitsopbouw voor het

⁽¹⁾ Advies van 18 april 2023 (nog niet bekendgemaakt in het Publicatieblad).

⁽²⁾ PB C 349 van 29.9.2023, blz. 167.

⁽³⁾ PB C, C/2024/1049, 9.2.2024, ELI: <http://data.europa.eu/eli/C/2024/1049/oj>.

⁽⁴⁾ Standpunt van het Europees Parlement van 24 april 2024 (nog niet bekendgemaakt in het Publicatieblad) en besluit van de Raad van 2 december 2024.

ontwikkelen van cyberbeveiligingsvaardigheden ter ondersteuning van een snellere opsporing van en respons op cyberdreigingen en -incidenten. Daarnaast hebben de lidstaten bijstand nodig om zich beter voor te bereiden en beter te kunnen reageren op significante en grootschalige cyberbeveiligingsincidenten, alsmede hebben zij bijstand nodig bij het initiële herstel van dergelijke incidenten. Voortbouwend op de bestaande structuren en in nauwe samenwerking daarmee moet de Unie ook haar capaciteit op deze gebieden vergroten, met name wat betreft het verzamelen en analyseren van gegevens over cyberdreigingen en -incidenten.

- (4) De Unie heeft reeds een aantal maatregelen genomen om kritieke infrastructuur en entiteiten minder kwetsbaar te maken voor en weerbaarder te maken tegen risico's, met name Verordening (EU) 2019/881 van het Europees Parlement en de Raad⁽⁵⁾, Richtlijnen 2013/40/EU⁽⁶⁾ en (EU) 2022/2555⁽⁷⁾ van het Europees Parlement en de Raad en Aanbeveling (EU) 2017/1584 van de Commissie⁽⁸⁾. Daarnaast wordt de lidstaten in de aanbeveling van de Raad van 8 december 2022 betreffende een Uniebrede gecoördineerde aanpak om de weerbaarheid van kritieke infrastructuur te versterken, verzocht maatregelen te nemen, en 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 beveiligingsincidenten snel overslaan van de ene lidstaat naar de andere en van een derde land naar de Unie, vereisen versterking van de 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 beter ervan te kunnen herstellen, met name door de capaciteiten van bestaande structuren te versterken. In de conclusies van de Raad van 23 mei 2022 over de ontwikkeling van de cyberstrategie van de Europese Unie werd de Commissie bovendien verzocht om een voorstel voor een nieuw cyberbeveiligingsnoodfonds in te dienen.
- (6) In de gezamenlijke mededeling van de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid van 10 november 2022 aan het Europees Parlement en de Raad over het EU-beleid op het gebied van cyberdefensie werd een EU-initiatief voor cybersolidariteit aangekondigd met de volgende doelstellingen: versterken van de gemeenschappelijke vermogens van de EU op het gebied van opsporing, situationeel bewustzijn en respons door de uitrol van een EU-infrastructuur van operationele beveiligingscentra (Security Operation Centres — SOC's) te bevorderen, de geleidelijke totstandbrenging van een cyberreserve op EU-niveau met diensten van betrouwbare private aanbieders te ondersteunen en kritieke entiteiten op basis van EU-risicobeoordelingen op potentiële 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 capaciteit ter voorkoming van en om te reageren op significante cyberbeveiligingsincidenten en grootschalige cyberbeveiligingsincidenten te versterken. Daarom moet een pan-Europees netwerk van cyberhubs (het "Europees waarschuwingssysteem voor cyberbeveiliging") worden opgericht om gecoördineerde capaciteiten op het gebied van opsporing en situationeel bewustzijn op te bouwen, en de capaciteiten van de Unie op het gebied van opsporing van dreigingen en informatiedeling te versterken; een noodmechanisme voor cyberbeveiliging moet worden ingesteld om de lidstaten op hun verzoek te ondersteunen bij de voorbereiding en respons op, het beperken van de gevolgen van en het initiëren van het herstel van significante cyberbeveiligingsincidenten en grootschalige cyberbeveiligingsincidenten, en om andere gebruikers te ondersteunen bij het reageren op significante cyberbeveiligingsincidenten en aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten, en een Europees evaluatiemechanisme voor cyberbeveiligingsincidenten moet worden ingesteld om specifieke significante cyberbeveiligingsincidenten of grootschalige cyberbeveiligingsincidenten te evalueren en te beoordelen. De uit hoofde van deze verordening ondernomen acties moeten worden uitgevoerd met inachtneming van de bevoegdheden van de lidstaten en moeten een aanvulling vormen op, en geen herhaling zijn van, de activiteiten van het CSIRT-netwerk, het Europees netwerk van verbindingsorganisaties voor cybercrises ("EU-CyCLoNe") of de samenwerkingsgroep (de "NIS-samenwerkingsgroep"), die allen zijn opgericht bij Richtlijn (EU) 2022/2555. Die acties laten de artikelen 107 en 108 van het Verdrag betreffende de werking van de Europese Unie ("VWEU") onverlet.

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

⁽⁶⁾ 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 (PB L 218 van 14.8.2013, blz. 8).

⁽⁷⁾ 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).

⁽⁸⁾ 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).

- (8) Om deze doelstellingen te bereiken is het noodzakelijk Verordening (EU) 2021/694 van het Europees Parlement en de Raad⁽⁹⁾ op bepaalde gebieden te wijzigen. Deze verordening moet met name Verordening (EU) 2021/694 wijzigen wat betreft de toevoeging van nieuwe operationele doelstellingen in verband met het Europees waarschuwingssysteem voor cyberbeveiliging en het noodmechanisme voor cyberbeveiliging 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 en coördinatie op het gebied van cyberbeveiliging te versterken. Het Europees waarschuwingssysteem voor cyberbeveiliging kan een belangrijke rol spelen bij de ondersteuning van de lidstaten bij het anticiperen op en beschermen tegen cyberdreigingen, en de EU-cyberbeveiligingsreserve kan een belangrijke rol spelen bij de ondersteuning van de lidstaten, de instellingen, organen en instanties van de Unie en met het programma Digitaal Europa geassocieerde derde landen bij het reageren op en het beperken van de gevolgen van significante cyberbeveiligingsincidenten, grootschalige cyberbeveiligingsincidenten en aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten. Die gevolgen kunnen aanzienlijke materiële of immateriële schade en ernstige risico's voor de openbare veiligheid en veiligheid omvatten. In het licht van de specifieke rol die het Europees waarschuwingssysteem voor cyberbeveiliging en de EU-cyberbeveiligingsreserve kunnen spelen, moet bij deze verordening Verordening (EU) 2021/694 worden gewijzigd wat betreft de deelname van juridische entiteiten die in de Unie zijn gevestigd maar onder zeggenschap staan van derde landen, wanneer er een reëel risico bestaat dat de nodige en toereikende instrumenten, infrastructuur en diensten, of technologie, expertise en capaciteit, niet beschikbaar zijn in de Unie en de voordelen van de deelname van dergelijke entiteiten zwaarder wegen dan het beveiligingsrisico. De specifieke voorwaarden waaronder financiële steun kan worden verleend voor acties ter uitvoering van het Europees waarschuwingssysteem voor cyberbeveiliging en de EU-cyberbeveiligingsreserve moeten worden vastgesteld en de governance- en coördinatiemechanismen die nodig zijn om de beoogde doelstellingen te verwezenlijken, moeten worden gedefinieerd. 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 die nieuwe operationele doelstellingen te monitoren.
- (9) Om de respons van de Unie op cyberdreigingen en -incidenten te versterken, is samenwerking met internationale organisaties en betrouwbare en gelijkgestemde internationale partners van vitaal belang. In dit verband moeten als betrouwbare en gelijkgestemde internationale partners worden beschouwd de landen die de beginselen delen waarop de totstandbrenging van de Unie is geïnspireerd, namelijk de democratie, de rechtsstaat, de universaliteit en ondeelbaarheid van de mensenrechten en de fundamentele vrijheden, de eerbiediging van de menselijke waardigheid, de beginselen van gelijkheid en solidariteit en de eerbiediging van de beginselen van het Handvest van de Verenigde Naties en het internationaal recht, en die de essentiële veiligheidsbelangen van de Unie of haar lidstaten niet ondermijnen. Een dergelijke samenwerking zou ook nuttig kunnen zijn met betrekking tot de op grond van deze verordening ondernomen acties, met name het Europees waarschuwingssysteem voor cyberbeveiliging en de EU-cyberbeveiligingsreserve. Verordening (EU) 2021/694 moet bepalen dat, met inachtneming van bepaalde beschikbaarheids- en beveiligingsvoorwaarden, inschrijvingen voor aanbestedingen voor het Europees waarschuwingssysteem voor cyberbeveiliging en de EU-cyberbeveiligingsreserve openstaan voor juridische entiteiten die onder zeggenschap van derde landen staan, mits aan de vereisten op het gebied van beveiliging wordt voldaan. Bij de beoordeling van het beveiligingsrisico van het op deze wijze openstellen van de aanbesteding is het van belang rekening te houden met de beginselen en waarden die de Unie deelt met gelijkgestemde internationale partners, wanneer die beginselen en waarden verband houden met wezenlijke veiligheidsbelangen van de Unie. Wanneer dergelijke beveiligingsvereisten worden overwogen in het kader van Verordening (EU) 2021/694, kan bovendien rekening worden gehouden met verschillende elementen, zoals de bedrijfsstructuur en het besluitvormingsproces van een entiteit, de beveiliging van gegevens en gerubriceerde of gevoelige informatie en de garantie dat de resultaten van de actie niet worden gecontroleerd of beperkt door niet in aanmerking komende derde landen.
- (10) De financiering van acties uit hoofde van deze verordening moet worden bepaald in Verordening (EU) 2021/694, die de relevante basishandeling moet blijven voor de 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 Verordening (EU) 2021/694.
- (11) 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. Die regels zijn vastgelegd in Verordening (EU, Euratom) 2024/2506 van het Europees Parlement en de Raad⁽¹⁰⁾ en bepalen met name de procedure voor het opstellen en uitvoeren van de begroting van de Unie, alsook voorzien in controles op de verantwoordelijkheid van financiële

⁽⁹⁾ Verordening (EU) 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).

⁽¹⁰⁾ Verordening (EU, Euratom) 2024/2509 van het Europees Parlement en de Raad van 23 september 2024 tot vaststelling van de financiële regels van toepassing op de algemene begroting van de Unie (PB L, 2024/2509, 26.9.2024, ELI: <http://data.europa.eu/eli/reg/2024/2509/oj>).

actoren. De op grond van artikel 322 VWEU vastgestelde regels omvatten ook een algemeen conditionaliteitsregime zoals vastgesteld in Verordening (EU, Euratom) 2020/2092 van het Europees Parlement en de Raad⁽¹⁾ ter bescherming van de Uniebegroting.

- (12) Hoewel preventie- en paraatheidsmaatregelen van essentieel belang zijn om de weerbaarheid van de Unie bij de aanpak van significante cyberbeveiligingsincidenten, grootschalige cyberbeveiligingsincidenten en aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten te vergroten, zijn het voorkomen, de timing en de omvang van dergelijke incidenten vanwege hun aard onvoorspelbaar. De financiële middelen die nodig zijn om een adequate respons te waarborgen, kunnen van jaar tot jaar aanzienlijk verschillen en moeten onmiddellijk ter beschikking kunnen worden gesteld. Om het begrotingsbeginsel van voorspelbaarheid te verzoenen met de noodzaak om snel te reageren op nieuwe behoeften is het vereist dat de financiële uitvoering van de werkprogramma's dan ook wordt aangepast. Bijgevolg is het passend de overdracht van ongebruikte kredieten toe te staan, maar uitsluitend naar het volgende jaar en de EU-cyberbeveiligingsreserve en de acties ter ondersteuning van wederzijdse bijstand, in aanvulling op de overdracht van kredieten die zijn toegestaan krachtens artikel 12, lid 4, van Verordening (EU, Euratom) 2024/2509.
- (13) Om cyberdreigingen en -incidenten doeltreffender te voorkomen en te beoordelen, er doeltreffender op te reageren en ervan 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 cyberdreigingen aan het licht te brengen, te beperken en te voorkomen, omvat een verhoogd vermogen van geavanceerde opsporingscapaciteiten. Het Europees waarschuwingssysteem voor cyberbeveiliging moet bestaan uit verscheidene interoperabele landsgrensoverschrijdende cyberhubs, die elk drie of meer nationale cyberhubs 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 om relevante, en, in voorkomend geval geanonimiseerde, gegevens en informatie op geavanceerde wijze te verzamelen, en van instrumenten voor gegevensanalyse, door de capaciteit voor de gecoördineerde opsporing en het beheer van cyberdreigingen en -incidenten te verbeteren en door realtime situationeel bewustzijn te bieden. Die infrastructuur moet dienen om de strategie te verbeteren, door opsporing, aggregatie en de analyse van gegevens en informatie te versterken teneinde cyberdreigingen en -incidenten te voorkomen en aldus de entiteiten en netwerken van de Unie die verantwoordelijk zijn voor cybercrisisbeheersing in de Unie, met name EU-CyCLONE aan te vullen en te ondersteunen.
- (14) Deelname aan het Europees waarschuwingssysteem voor cyberbeveiliging is vrijwillig voor de lidstaten. Elke lidstaat moet één centrale entiteit op nationaal niveau aanwijzen die belast is met de coördinatie van de activiteiten voor het opsporen van cyberdreigingen in die lidstaat. Die nationale cyberhubs moeten fungeren als referentiepunt en toegangspoor op nationaal niveau voor deelname aan het Europees waarschuwingssysteem voor cyberbeveiliging 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. Nationale cyberhubs kunnen de samenwerking en informatiedeling tussen publieke en private entiteiten versterken en kunnen ook de uitwisseling van relevante gegevens en informatie met relevante sectorale en sectoroverschrijdende gemeenschappen ondersteunen, met inbegrip van relevante centra voor sectorspecifieke informatie-uitwisseling en -analyse ("ISAC's"). Nauwe en gecoördineerde samenwerking tussen publieke en private entiteiten is essentieel om de cyberweerbaarheid van de Unie te versterken. Dergelijke samenwerking is met name waardevol in de context van het delen van inlichtingen over cyberdreigingen om de actieve cyberbescherming te verbeteren. In het kader van dergelijke samenwerking en informatiedeling kunnen de nationale cyberhubs om specifieke informatie verzoeken en deze ontvangen. Die nationale cyberhubs zijn op grond van deze verordening niet verplicht of bevoegd om dergelijke verzoeken af te dwingen. In voorkomend geval en in overeenstemming met het Unie- en nationale recht kan de gevraagde of ontvangen informatie telemetrie-, sensor- en registratiegegevens omvatten van entiteiten, zoals aanbieders van beheerde beveiligingsdiensten, die actief zijn in zeer kritieke sectoren of andere kritieke sectoren binnen die lidstaat, teneinde de snelle opsporing van potentiële cyberdreigingen en -incidenten in een vroeger stadium te versterken en zo het situationele bewustzijn te verbeteren. Indien de nationale cyberhub niet de bevoegde autoriteit is die door de betrokken lidstaat is aangewezen of ingesteld uit hoofde van artikel 8, lid 1, van Richtlijn (EU) 2022/2555, is het van cruciaal belang dat de nationale cyberhub met die bevoegde autoriteit coördineert met betrekking tot verzoeken om dergelijke gegevens en de ontvangst ervan.
- (15) Als onderdeel van het Europees waarschuwingssysteem voor cyberbeveiliging moet een aantal landsgrensoverschrijdende cyberhubs worden opgericht. Die landsgrensoverschrijdende cyberhubs moeten de nationale cyberhubs van ten minste drie lidstaten samenbrengen, om ervoor te zorgen dat er ten volle voordeel wordt gehaald uit de landsgrensoverschrijdende opsporing van dreigingen en uit informatiedeling en -beheer. De algemene

⁽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 433 I van 22.12.2020, blz. 1, ELI: <http://data.europa.eu/eli/reg/2020/2092/oj>).

doelstelling van landsgrensoverschrijdende cyberhubs moet zijn: het versterken van de capaciteit voor het analyseren, voorkomen en opsporen van cyberdreigingen en het ondersteunen van de productie van hoogwaardige inlichtingen over cyberdreigingen, met name door het delen van relevante, en in voorkomend geval geanonimiseerde, gegevens in een betrouwbare en beveiligde omgeving, uit diverse publieke of private bronnen, alsook door het delen en gezamenlijk gebruiken van geavanceerde instrumenten, en het gezamenlijk ontwikkelen van opsporings-, analyse- en preventiecapaciteiten in een betrouwbare en beveiligde omgeving. Landsgrensoverschrijdende cyberhubs moeten nieuwe aanvullende capaciteit bieden, voortbouwend en als aanvulling op bestaande SOC's, CSIRT's en andere relevante actoren, waaronder het CSIRT-netwerk.

- (16) Een lidstaat die na een oproep tot het indienen van blijken van belangstelling door het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging (European Cybersecurity Industrial, Technology and Research Competence Centre — ECCC), dat is opgericht bij Verordening (EU) 2021/887 van het Europees Parlement en de Raad⁽¹²⁾, wordt geselecteerd om een nationale cyberhub op te zetten of de capaciteiten ervan te versterken, moet samen met het ECCC relevante instrumenten, infrastructuur of diensten aankopen. Een dergelijke lidstaat moet in aanmerking komen voor een subsidie voor de exploitatie van de instrumenten, infrastructuur of diensten. Een onderbrengend consortium, bestaande uit tenminste drie lidstaten, dat door het ECCC is geselecteerd na een oproep tot het indienen van blijken van belangstelling om een landsgrensoverschrijdende cyberhub op te zetten of de capaciteiten ervan te versterken, moet samen met het ECCC relevante instrumenten, infrastructuur of diensten aankopen. Het onderbrengend consortium moet in aanmerking komen voor een subsidie voor de exploitatie van de instrumenten, infrastructuur of diensten. De aanbestedingsprocedure voor de aankoop van de relevante instrumenten, infrastructuur of diensten moet gezamenlijk worden uitgevoerd door het ECCC en desbetreffende aanbestedende diensten van de geselecteerde lidstaten, na dergelijke oproepen tot het indienen van blijken van belangstelling. Dergelijke aanbesteding moet artikel 168, lid 2, van Verordening (EU, Euratom) 2024/2509 en de financiële regels van het ECCC naleven. Private entiteiten mogen daarom niet in aanmerking komen voor deelname aan de oproepen tot het indienen van blijken van belangstelling om samen met het ECCC instrumenten, infrastructuur of diensten aan te kopen of om subsidies te ontvangen voor de exploitatie van die instrumenten, infrastructures of diensten. De lidstaten moeten echter in staat zijn om private entiteiten te betrekken bij het opzetten, verbeteren en exploiteren van hun nationale cyberhubs en landsgrensoverschrijdende cyberhubs op andere manieren die zij passend achten, in overeenstemming met het Unie- en nationale recht. Private entiteiten kunnen ook in aanmerking komen voor Uniefinanciering op grond van Verordening (EU) 2021/887 met het oog op steunverlening aan nationale cyberhubs.
- (17) Om de opsporing van cyberdreigingen en het situationeel bewustzijn in de Unie te verbeteren, moet een lidstaat die na een oproep tot het indienen van blijken van belangstelling wordt geselecteerd om een nationale cyberhub op te zetten of de capaciteiten ervan te versterken, zich ertoe verbinden een aanvraag in te dienen om deel te nemen aan een landsgrensoverschrijdende cyberhub. Indien een lidstaat niet deelneemt aan een landsgrensoverschrijdende cyberhub binnen twee jaar na de datum waarop de instrumenten, infrastructuur of diensten zijn verworven of, indien dit eerder is, waarop de lidstaat subsidiefinanciering heeft ontvangen, mag de lidstaat niet in aanmerking komen voor aanvullende ondersteunende acties van de Unie in het kader van Europees waarschuwingssysteem voor cyberbeveiliging ter verbetering van de capaciteiten van zijn nationale cyberhub. In dergelijke gevallen kunnen entiteiten uit de lidstaten nog steeds deelnemen aan oproepen tot het indienen van voorstellen met betrekking tot andere onderwerpen in het kader van het programma Digitaal Europa of andere Europese financieringsprogramma's, met inbegrip van oproepen voor capaciteit voor opsporing van cyberdreigingen en informatiedeling, mits die entiteiten voldoen aan de in die programma's vastgestelde subsidiabiliteitscriteria.
- (18) CSIRT's wisselen informatie in het CSIRT-netwerk overeenkomstig Richtlijn (EU) 2022/2555. Het Europees waarschuwingssysteem voor cyberbeveiliging moet een nieuwe capaciteit vormen die een aanvulling vormt op het CSIRT-netwerk door bij te dragen tot de ontwikkeling van een situationeel bewustzijn in de Unie waardoor de capaciteiten van het CSIRT-netwerk kunnen worden versterkt. Landsgrensoverschrijdende cyberhubs moeten coördineren en nauw samenwerken met het CSIRT-netwerk. Zij moeten optreden door gegevens te bundelen en relevante en, in voorkomend geval, geanonimiseerde informatie over cyberdreigingen van publieke en private entiteiten te delen, de waarde van dergelijke gegevens en informatie te vergroten door middel van deskundige analyses en gezamenlijk verworven infrastructuur en geavanceerde instrumenten, en door bij te dragen tot de technologische soevereiniteit, de open strategische autonomie, het concurrentievermogen en de weerbaarheid van de Unie, en tot de ontwikkeling van de capaciteiten van de Unie.
- (19) De landsgrensoverschrijdende cyberhubs moeten fungeren als centrale punten hetgeen toelaat relevante gegevens en inlichtingen over cyberdreigingen breed te bundelen, en het mogelijk maken dreigingsinformatie te verspreiden onder een grote en diverse groep belanghebbenden, zoals computercrisisresponsteams ("CERT's"), CSIRT's, ISAC's en exploitanten van kritieke infrastructuur. De leden van een onderbrengend consortium moeten in de consortiumovereenkomst specificeren welke relevante informatie onder de deelnemers aan de betrokken landsgrensoverschrijdende cyberhub wordt gedeeld. De informatie die tussen deelnemers aan een landsgrensoverschrijdende cyberhub wordt uitgewisseld, kan onder meer bestaan uit gegevens afkomstig van netwerken en sensoren, informatiebronnen over dreigingen, indicatoren voor aantasting, en gecontextualiseerde informatie over incidenten, cyberdreigingen, bijna-incidenten, kwetsbaarheden, technieken en procedures, vijandige tactieken,

⁽¹²⁾ 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, ELI: <http://data.europa.eu/eli/reg/2021/887/oj>).

dreigingsactorspecifieke informatie, cyberbeveiligingswaarschuwingen en aanbevelingen betreffende de configuratie van cyberbeveiligingsinstrumenten om cyberaanvallen op te sporen. Daarnaast moeten landsgrensoverschrijdende cyberhubs ook samenwerkingsovereenkomsten sluiten met elkaar. In dergelijke samenwerkingsovereenkomsten moeten met name beginselen voor informatiedeling en interoperabiliteit worden gespecificeerd. De clausules ervan inzake interoperabiliteit, met name modellen en protocollen voor het delen van informatie, moeten gebaseerd zijn op interoperabiliteitsrichtsnoeren die worden uitgevaardigd door het Agentschap van de Europese Unie voor cyberbeveiliging dat is opgericht bij Verordening (EU) 2019/881 (Enisa), die derhalve als uitgangspunt dienen. Die richtsnoeren moeten snel worden uitgevaardigd opdat landsgrensoverschrijdende cyberhubs er in een vroeg stadium rekening mee kunnen houden. Zij moeten rekening houden met internationale normen en beste praktijken, en de werking van gevestigde landsgrensoverschrijdende cyberhubs.

- (20) Landsgrensoverschrijdende cyberhubs en het CSIRT-netwerk moeten nauw samenwerken om synergieën en complementariteit van activiteiten te verzekeren. Daartoe moeten zij overeenstemming bereiken over procedurele regelingen voor samenwerking en het delen van relevante informatie. Dit kan onder meer inhouden dat relevante informatie over cyberdreigingen en significante cyberbeveiligingsincidenten wordt gedeeld en dat ervoor wordt gezorgd dat ervaringen met geavanceerde instrumenten, met name technologieën op het gebied van kunstmatige intelligentie en gegevensanalyse, die binnen de landsgrensoverschrijdende cyberhubs worden gebruikt, worden gedeeld met het CSIRT-netwerk.
- (21) Een gedeeld situationeel bewustzijn onder de betrokken autoriteiten is een absolute voorwaarde voor paraatheid en coördinatie in de hele Unie met betrekking tot significante cyberbeveiligingsincidenten en grootschalige cyberbeveiligingsincidenten. Bij Richtlijn (EU) 2022/2555 is 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. Richtlijn (EU) 2022/2555 heeft ook voorzien in de oprichting van een CSIRT-netwerk om een soepele en doeltreffende operationele samenwerking tussen alle lidstaten te bevorderen. Om situationeel bewustzijn te waarborgen en de solidariteit te versterken moeten landsgrensoverschrijdende cyberhubs in situaties waarin zij informatie verkrijgen over een mogelijk of lopend grootschalig cyberbeveiligingsincident, relevante informatie verstrekken aan het CSIRT-netwerk en, bij wijze van vroegtijdige waarschuwing, EU-CyCLONe in kennis stellen. 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. 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⁽¹³⁾ ingestelde Uniemechanisme voor civiele bescherming, alsmede voor het verstrekken van de analytische verslagen voor de geïntegreerde EU-regeling politieke crisisrespons ("IPCR-regeling") in het kader van Uitvoeringsbesluit (EU) 2018/1993 van de Raad⁽¹⁴⁾. Wanneer landsgrensoverschrijdende cyberhubs relevante informatie en vroegtijdige waarschuwingen in verband met een mogelijk of lopend grootschalig cyberbeveiligingsincident delen met EU-CyCLONe en het CSIRT-netwerk, is het van essentieel belang dat deze informatie via die netwerken wordt gedeeld met de autoriteiten van de lidstaten alsook met de Commissie. In dit verband voorziet Richtlijn (EU) 2022/2555 erin dat EU-CyCLONe tot doel heeft het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en -crises op operationeel niveau te ondersteunen en ervoor te zorgen dat relevante informatie regelmatig tussen de lidstaten en de instellingen, organen en instanties van de Unie wordt uitgewisseld. Tot de taken van EU-CyCLONe behoort het ontwikkelen van een gedeeld situationeel bewustzijn voor dergelijke incidenten en crises. Het is van het grootste belang dat EU-CyCLONe, in overeenstemming met dat doel en zijn taken, ervoor zorgt dat dergelijke informatie onmiddellijk wordt verstrekt aan de relevante vertegenwoordigers van de lidstaten en aan de Commissie. Daartoe is het van cruciaal belang dat het reglement van orde van EU-CyCLONe passende bepalingen bevat.
- (22) Entiteiten die deelnemen aan het Europees waarschuwingssysteem voor cyberbeveiliging, moeten zorgen voor een hoog niveau van interoperabiliteit, onder meer, in voorkomend geval, wat betreft gegevensformaten, taxonomie, gegevensverwerking en instrumenten voor gegevensanalyse. Zij moeten ook zorgen voor 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 oorzaken van opgespoorde cyberdreigingen en -risico's te beschrijven, moet rekening worden gehouden met de bestaande werkzaamheden die zijn gedaan in het kader van de uitvoering van Richtlijn (EU) 2022/2555.

⁽¹³⁾ 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, ELI: <http://data.europa.eu/eli/dec/2013/1313/oj>).

⁽¹⁴⁾ 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).

- (23) Om de grootschalige uitwisseling van relevante gegevens en informatie over cyberdreigingen uit verschillende bronnen in een betrouwbare en beveiligde omgeving mogelijk te maken, moeten entiteiten die deelnemen aan het Europees waarschuwingssysteem voor cyberbeveiliging 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 en gegevensanalyse.
- (24) Door relevante gegevens en informatie te verzamelen, te analyseren, te delen en uit te wisselen, moet het Europees waarschuwingssysteem voor cyberbeveiliging de technologische soevereiniteit, en de strategische autonomie op het gebied van cyberbeveiliging, het concurrentievermogen en de weerbaarheid, van de Unie versterken. De bundeling van hoogwaardige samengestelde gegevens kan ook bijdragen tot de ontwikkeling van geavanceerde technologieën op het gebied van artificiële intelligentie en gegevensanalyse. Menselijk toezicht en daarvoor geschoolde arbeidskrachten blijven van essentieel belang voor het effectief bundelen van gegevens van hoge kwaliteit.
- (25) Hoewel het Europees waarschuwingssysteem voor cyberbeveiliging een civiel project is, zou de cyberdefensiegemeenschap baat kunnen hebben bij sterkere capaciteiten op het gebied van civiele opsporing en situationeel bewustzijn die zijn ontwikkeld voor de bescherming van kritieke infrastructuur.
- (26) De informatiedeling tussen deelnemers aan het Europees waarschuwingssysteem voor cyberbeveiliging moet in overeenstemming zijn met de bestaande wettelijke voorschriften en in het bijzonder met het Unie- en nationale recht 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, en de gegevens vernietigen zodra zij niet langer nodig zijn voor het aangegeven doel en de entiteit die de gegevens ter beschikking stelt ervan in kennis stellen dat de gegevens zijn vernietigd.
- (27) Het waarborgen van vertrouwelijkheid en informatiebeveiliging is van het grootste belang voor alle drie de pijlers van deze verordening, of het nu gaat om het aanmoedigen van het delen of uitwisselen van informatie in het kader van het Europees waarschuwingssysteem voor cyberbeveiliging, om het beschermen van de belangen van de entiteiten die steun aanvragen in het kader van het noodmechanisme voor cyberbeveiliging, of om ervoor te zorgen dat verslagen in het kader van het Europees evaluatiemechanisme voor cyberbeveiligingsincidenten nuttige informatie kunnen opleveren waaruit lering kan worden getrokken zonder negatieve gevolgen te hebben voor de door de incidenten getroffen entiteiten. De deelname van lidstaten en entiteiten aan die mechanismen is afhankelijk van de vertrouwensrelatie tussen hun componenten. Wanneer informatie vertrouwelijk is op grond van Unie- of nationale voorschriften, moet de deling of uitwisseling ervan uit hoofde van deze verordening beperkt blijven tot hetgeen relevant is voor en evenredig is aan het doel van de deling of uitwisseling. Bij die deling of uitwisseling van informatie moet de vertrouwelijkheid van die informatie gewaarborgd worden en de veiligheids- en commerciële belangen van de betrokken entiteiten beschermd worden. Informatiedeling of -uitwisseling op grond van deze verordening kan plaatsvinden aan de hand van geheimhoudingsovereenkomsten of richtsnoeren voor de verspreiding van informatie, zoals het verkeerslichtprotocol. Onder het verkeerslichtprotocol moet worden verstaan een middel om informatie te verstrekken over beperkingen ten aanzien van de verdere verspreiding van informatie. Het wordt in bijna alle CSIRT's en in enkele ISAC's gebruikt. Naast die algemene vereisten moeten, wat het Europees waarschuwingssysteem voor cyberbeveiliging betreft, in overeenkomsten met onderbrengende consortia specifieke regels worden vastgesteld met betrekking tot de voorwaarden voor informatiedeling binnen de betreffende landsgrensoverschrijdende cyberhub. Die overeenkomsten zouden met name kunnen vereisen dat informatie alleen wordt uitgewisseld in overeenstemming met het Unie- en nationale recht.
- (28) Met betrekking tot de uitrol van de EU-cyberbeveiligingsreserve zijn specifieke vertrouwelijkheidsregels nodig. Steun zal worden gevraagd, beoordeeld en verleend in een crisiscontext en met betrekking tot entiteiten die actief zijn in gevoelige sectoren. Voor een doeltreffende werking van de EU-cyberbeveiligingsreserve is het van essentieel belang dat gebruikers en entiteiten onverwijld alle informatie kunnen delen en toegankelijk maken die elke entiteit nodig heeft om haar rol te spelen bij de beoordeling van verzoeken om en de aanwending van steun. Dienovereenkomstig moet in deze verordening worden bepaald dat al dergelijke informatie alleen wordt gebruikt of gedeeld wanneer dat nodig is voor de werking van de EU-cyberbeveiligingsreserve, en dat informatie die vertrouwelijk is of gerubriceerd op grond van het Unie- en nationale recht uitsluitend in overeenstemming met dat recht mag worden gebruikt en gedeeld. Daarnaast moeten gebruikers in voorkomend geval gebruik kunnen maken van protocollen voor het delen van informatie, zoals het verkeerslichtprotocol, om beperkingen nader te specificeren. Hoewel de gebruikers in dit verband over discretionaire bevoegdheid beschikken, is het belangrijk dat zij bij de toepassing van dergelijke beperkingen rekening houden met de mogelijke gevolgen, met name wat betreft de vertraagde beoordeling of levering van de gevraagde diensten. Met het oog op een efficiënte EU-cyberbeveiligingsreserve is het belangrijk dat de

aanbestedende dienst deze gevolgen voor de gebruiker verduidelijkt voordat hij een verzoek indient. Die waarborgen zijn beperkt tot het verzoek om, en de verlening van, diensten van de EU-cyberbeveiligingsreserve en hebben geen invloed op de informatie-uitwisseling in andere kaders, zoals bij de aanbesteding van de EU-cyberbeveiligingsreserve.

- (29) Gezien de toenemende risico's en het groeiende aantal incidenten waarmee de lidstaten te maken krijgen, moet een instrument voor crisisondersteuning worden opgezet, namelijk het noodmechanisme voor cyberbeveiliging, om de Unie weerbaarder te maken tegen significante cyberbeveiligingsincidenten, grootschalige cyberbeveiligingsincidenten en aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten en moeten de acties van de lidstaten worden aangevuld met financiële noodsteun voor paraatheid, respons op incidenten en initieel herstel van essentiële diensten. Aangezien het volledig herstel van een incident een uitgebreid proces is waarbij de werking van de door het incident getroffen entiteit wordt hersteld in de toestand van vóór het incident en een langdurig proces kan zijn dat aanzienlijke kosten met zich meebrengt, moet de steun uit de EU-cyberbeveiligingsreserve worden beperkt tot de eerste fase van het herstelproces, hetgeen moet leiden tot het herstel van de basisfuncties van de systemen. Het noodmechanisme voor cyberbeveiliging moet het mogelijk maken om in welbepaalde omstandigheden en onder duidelijke voorwaarden snel en doeltreffend bijstand te verlenen en om het gebruik van de middelen zorgvuldig te monitoren en te evalueren. Hoewel de primaire verantwoordelijkheid voor de preventie van, en voor de voorbereiding en respons op, incidenten en crises bij de lidstaten ligt, bevordert het noodmechanisme voor cyberbeveiliging de solidariteit tussen de lidstaten overeenkomstig artikel 3, lid 3, van het Verdrag betreffende de Europese Unie (VEU).
- (30) Het noodmechanisme voor cyberbeveiliging moet steun verlenen aan de lidstaten ter aanvulling van hun eigen maatregelen en middelen, en andere bestaande steunmogelijkheden in geval van respons op en initieel herstel van significante cyberbeveiligingsincidenten en grootschalige cyberbeveiligingsincidenten, zoals de diensten die 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 waaronder, in het kader van artikel 42, lid 7, VEU, en de op grond van Besluit (GBVB) 2017/2315 van de Raad⁽¹⁵⁾ opgerichte snellereactieteams bij cyberbeveiligingsincidenten van de permanente gestructureerde samenwerking (PESCO). Het moet voorzien in de noodzaak ervoor te zorgen dat er gespecialiseerde middelen beschikbaar zijn om de paraatheid voor, de respons op en het herstel na dergelijke incidenten in de hele Unie en in met het programma Digitaal Europa geassocieerde derde landen te ondersteunen.
- (31) Deze verordening doet geen afbreuk aan procedures en kaders voor de coördinatie van crisisrespons op het niveau van de Unie, met name Richtlijn (EU) 2022/2555, het Uniemechanisme voor civiele bescherming, dat is ingesteld bij Besluit nr. 1313/2013/EU van het Europees Parlement en de Raad⁽¹⁶⁾, de IPCR-regeling en Aanbeveling (EU) 2017/1584 van de Commissie⁽¹⁷⁾. Steun die wordt verleend in het kader van het noodmechanisme voor cyberbeveiliging, kan 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, waarbij rekening gehouden wordt met de civiele aard van het noodmechanisme voor cyberbeveiliging. Steun die wordt verleend uit hoofde van het noodmechanisme voor cyberbeveiliging, kan een aanvulling vormen op acties die worden uitgevoerd in het kader van artikel 42, lid 7, VEU, met inbegrip van bijstand die door een lidstaat aan een andere lidstaat wordt verleend, of deel uitmaken van de gezamenlijke respons van de Unie en de lidstaten of in situaties als bedoeld in artikel 222 VWEU. De uitvoering van deze verordening moet in voorkomend geval ook worden gecoördineerd met de uitvoering van de maatregelen in het kader van het instrumentarium voor cyberdiplomatie.
- (32) De uit hoofde 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, de lidstaten en, in voorkomend geval, het ECCC. Bij een verzoek om steun in het kader van het noodmechanisme voor cyberbeveiliging moeten de lidstaten relevante informatie verstrekken die de noodzaak van de steun rechtvaardigt.
- (33) Richtlijn (EU) 2022/2555 vereist van de lidstaten dat zij 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 vereist die richtlijn van de lidstaten dat zij capaciteiten, middelen en procedures vaststellen die in geval van een crisis kunnen worden ingezet, alsook dat 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 wordt ook voorgeschreven dat zij een of meer CSIRT's oprichten die belast zijn met de behandeling van incidenten volgens een welomschreven proces

⁽¹⁵⁾ 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 (PB L 331 van 14.12.2017, blz. 57, ELI: <http://data.europa.eu/eli/dec/2017/2315/oj>).

⁽¹⁶⁾ 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).

⁽¹⁷⁾ 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).

en die ten minste de sectoren, subsectoren en soorten entiteiten bestrijken die onder het toepassingsgebied van die richtlijn vallen, en 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 noodmechanisme voor cyberbeveiliging moet bijstand verlenen voor acties die gericht zijn op het verbeteren van de paraatheid en voor responsacties bij incidenten om de gevolgen van significante cyberbeveiligingsincidenten en grootschalige cyberbeveiligingsincidenten te beperken, initieel herstel te ondersteunen of de basisfuncties van diensten van in zeer kritieke sectoren actieve entiteiten of in andere kritieke sectoren actieve entiteiten te herstellen.

- (34) 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 op grond van Richtlijn (EU) 2022/2555 aangemerkte in zeer kritieke sectoren actieve entiteiten, onder meer door middel van oefening en opleiding. Daartoe moet de Commissie, na raadpleging van Enisa, de NIS-samenwerkingsgroep en EU-CyCLONe, regelmatig relevante sectoren of subsectoren vaststellen die in aanmerking moeten komen om financiële steun te ontvangen voor gecoördineerde paraatheidstests op het niveau van de Unie. De sectoren of subsectoren moeten worden gekozen uit de zeer kritieke sectoren die zijn opgesomd in bijlage I bij Richtlijn (EU) 2022/2555. De gecoördineerde paraatheidstests 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 die door de Commissie, de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid (de "hoge vertegenwoordiger") en de NIS-samenwerkingsgroep wordt uitgevoerd, in coördinatie met 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 dat is opgericht bij Verordening (EU) 2018/1971 van het Europees Parlement en de Raad ⁽¹⁸⁾, de op Unieniveau gecoördineerde risicobeoordelingen van kritieke toeleveringsketens die moeten worden uitgevoerd krachtens artikel 22 van Richtlijn (EU) 2022/2555 en het testen van de digitale operationele weerbaarheid als bepaald in Verordening (EU) 2022/2554 van het Europees Parlement en de Raad ⁽¹⁹⁾. 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.
- (35) Daarnaast moet het noodmechanisme voor cyberbeveiliging steun bieden voor andere paraatheidsacties en de paraatheid ondersteunen in andere sectoren die niet vallen onder de gecoördineerde paraatheidstests van in zeer kritieke sectoren actieve entiteiten of in andere kritieke sectoren actieve entiteiten. Deze acties kunnen verschillende soorten nationale paraatheidsactiviteiten omvatten.
- (36) Wanneer de lidstaten subsidies ontvangen ter ondersteuning van paraatheidsacties, kunnen entiteiten in zeer kritieke sectoren op vrijwillige basis aan die acties deelnemen. Het geldt als goede praktijk dat de deelnemende entiteiten na dergelijke acties een saneringsplan opstellen om alle daaruit voortvloeiende aanbevelingen van specifieke maatregelen uit te voeren om zo veel mogelijk voordeel uit de paraatheidsactie te halen. Hoewel het belangrijk is dat de lidstaten in het kader van de acties erom verzoeken dat deelnemende entiteiten dergelijke herstelplannen opstellen en uitvoeren, zijn de lidstaten op grond van deze verordening niet verplicht of bevoegd om dergelijke verzoeken af te dwingen. Dergelijke verzoeken doen geen afbreuk aan de vereisten voor entiteiten en toezichtbevoegdheden voor bevoegde autoriteiten in overeenstemming met Richtlijn (EU) 2022/2555.
- (37) Het noodmechanisme voor cyberbeveiliging moet ook steun verlenen voor responsacties bij incidenten om de gevolgen van significante cyberbeveiligingsincidenten, grootschalige cyberbeveiligingsincidenten en aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten te beperken, initieel herstel te ondersteunen of de werking van essentiële diensten te herstellen. In voorkomend geval moet het noodmechanisme voor cyberbeveiliging het Uniemechanisme voor civiele bescherming aanvullen om te zorgen voor een alomvattende aanpak van de gevolgen van incidenten voor de burgers.

⁽¹⁸⁾ Verordening (EU) 2018/1971 van het Europees Parlement en de Raad van 11 december 2018 tot instelling van het Orgaan van Europese regulerende instanties voor elektronische communicatie (Berec) en het Bureau voor ondersteuning van Berec (Berec-Bureau), tot wijziging van Verordening (EU) 2015/2120 en tot intrekking van Verordening (EG) nr. 1211/2009 (PB L 321 van 17.12.2018, blz. 1).

⁽¹⁹⁾ 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 (PB L 333 van 27.12.2022, blz. 1).

- (38) Het noodmechanisme voor cyberbeveiliging moet de door een lidstaat verleende technische bijstand aan een andere lidstaat die is getroffen door een significant cyberbeveiligingsincident of grootschalig cyberbeveiligingsincident steunen, onder meer via de in artikel 11, lid 3, punt f), van Richtlijn (EU) 2022/2555 bedoelde CSIRT's. De lidstaten die dergelijke 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 reis- en verblijfkosten en dagvergoedingen van cyberbeveiligingsdeskundigen omvatten.
- (39) Gezien de essentiële rol die private bedrijven spelen bij de opsporing van, paraatheid voor en respons op grootschalige cyberbeveiligingsincidenten en aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten, is het belangrijk de waarde te erkennen van vrijwillige pro-bonosamenwerking met dergelijke bedrijven, waarbij zij zonder vergoeding diensten aanbieden in geval van grootschalige cyberbeveiligingsincidenten en -crises en aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten en -crises. Enisa kan, in samenwerking met EU-CyCLONE, de ontwikkeling van dergelijke pro-bono-initiatieven kunnen monitoren en kunnen bevorderen dat deze voldoen aan de criteria die op grond van deze verordening van toepassing zijn op betrouwbare aanbieders van beheerde beveiligingsdiensten, onder meer met betrekking tot de betrouwbaarheid van private bedrijven, hun ervaring en het vermogen om gevoelige informatie op een veilige manier te verwerken.
- (40) Als onderdeel van het noodmechanisme voor cyberbeveiliging moet geleidelijk een EU-cyberbeveiligingsreserve worden opgezet, bestaande uit betrouwbare aanbieders van beheerde beveiligingsdiensten van, ter ondersteuning van responsacties en acties gericht op initieel herstel in geval van significante cyberbeveiligingsincidenten, grootschalige cyberbeveiligingsincidenten of aan grootschalig cyberbeveiligingsincidenten gelijkwaardige incidenten die gevolgen hebben voor de lidstaten, de instellingen, organen of instanties van de Unie of met het programma Digitaal Europa geassocieerde derde landen. De EU-cyberbeveiligingsreserve moet de beschikbaarheid en paraatheid van de diensten waarborgen. De reserve moet daarom diensten omvatten die vooraf zijn vastgelegd, met inbegrip van bijvoorbeeld capaciteit die op korte termijn bereikbaar en inzetbaar is. De diensten van de EU-cyberbeveiligingsreserve moeten dienen om de nationale autoriteiten te ondersteunen bij het verlenen van bijstand aan getroffen in zeer kritieke sectoren actieve entiteiten of getroffen in andere kritieke sectoren actieve entiteiten, als aanvulling op hun eigen acties op nationaal niveau. De diensten van de EU-cyberbeveiligingsreserve moeten ook kunnen dienen ter ondersteuning van instellingen, organen en instanties van de Unie, onder vergelijkbare voorwaarden. De EU-cyberbeveiligingsreserve kan ook bijdragen aan het versterken van de concurrentiepositie van de industrie en diensten in de Unie in de hele digitale economie, met inbegrip van micro-ondernemingen en kleine en middelgrote ondernemingen en start-ups, ook door een impuls te geven aan investeringen in onderzoek en innovatie. Het is belangrijk om bij de aankoop van de diensten voor de EU-cyberbeveiligingsreserve rekening te houden met het Europees kader voor vaardigheden op het gebied van cyberbeveiliging van Enisa. Bij een verzoek om steun uit de EU-cyberbeveiligingsreserve moeten gebruikers in hun aanvraag passende informatie opnemen over de getroffen entiteit en de mogelijke gevolgen, informatie over de gevraagde dienst uit de EU-cyberbeveiligingsreserve, en de steun die op nationaal niveau aan de getroffen entiteit is verleend, waarmee rekening moet worden gehouden bij de beoordeling van het verzoek van de aanvrager. Om te zorgen voor complementariteit met andere vormen van steun aan de getroffen entiteit moet het verzoek in voorkomend geval ook informatie bevatten over bestaande contractuele regelingen inzake incidentresponsdiensten en diensten op het gebied van initieel herstel, alsook verzekeringscontracten die een dergelijk soort incident kunnen dekken.
- (41) Om ervoor te zorgen dat de financiering van de Unie doeltreffend wordt gebruikt, moeten vooraf vastgelegde diensten in het kader van de EU-cyberbeveiligingsreserve overeenkomstig het desbetreffende contract converteerbaar zijn in paraatheidsdiensten in verband met de preventie van en respons op incidenten, in gevallen waarin die vooraf vastgelegde diensten niet worden gebruikt voor respons op incidenten gedurende de periode waarvoor zij vooraf zijn vastgelegd. Die diensten moeten complementair zijn en mogen niet overlappen met de paraatheidsacties die door het ECCC worden beheerd.
- (42) Verzoeken om steun uit de EU-cyberbeveiligingsreserve van de cybercrisisbeheerautoriteiten van de lidstaten en CSIRT's, of CERT-EU namens instellingen, organen en instanties van de Unie, moeten worden beoordeeld door de aanbestedende dienst. Wanneer het beheer en de werking van de EU-cyberbeveiligingsreserve aan Enisa zijn toevertrouwd, is die aanbestedende dienst Enisa. Verzoeken om steun van met het programma Digitaal Europa geassocieerde derde landen moeten worden beoordeeld door de Commissie. Om de indiening en beoordeling van verzoeken om steun te vergemakkelijken, zou Enisa een beveiligd platform kunnen opzetten.
- (43) Wanneer meerdere gelijktijdige verzoeken worden ontvangen, moet prioriteit worden gegeven aan die verzoeken overeenkomstig de in deze verordening vastgestelde criteria. In het licht van de algemene doelstellingen van deze verordening moeten deze criteria betrekking hebben op de omvang en ernst van het incident, het soort getroffen entiteit, de mogelijke gevolgen van het incident voor de getroffen lidstaten of gebruikers, de potentiële grensoverschrijdende aard van het incident en het risico van overloopeffecten, en de maatregelen die de gebruiker reeds heeft genomen om de respons en het initieel herstel te ondersteunen. In het licht van die doelstellingen en

gezien het feit dat verzoeken van gebruikers uit de lidstaten uitsluitend bedoeld zijn om in zeer kritieke sectoren actieve entiteiten of in andere kritieke sectoren actieve entiteiten in de hele Unie te ondersteunen, is het passend hogere prioriteit te geven aan verzoeken van gebruikers uit de lidstaten wanneer die criteria ertoe leiden dat twee of meer verzoeken als gelijkwaardig worden beoordeeld. Dit doet geen afbreuk aan eventuele verplichtingen van de lidstaten uit hoofde van relevante onderbrengingsovereenkomsten om maatregelen te nemen om de instellingen, organen en instanties van de Unie te beschermen en bij te staan.

- (44) De Commissie moet de algemene verantwoordelijkheid dragen voor de uitvoering van de EU-cyberbeveiligingsreserve. Gezien de uitgebreide ervaring die Enisa heeft opgedaan met de ondersteunende actie op het gebied van cyberbeveiliging, is Enisa het meest geschikte agentschap om de EU-cyberbeveiligingsreserve uit te voeren. De Commissie dient Enisa dan ook gedeeltelijk of, wanneer zij dat passend acht, volledig te belasten met de werking en het beheer van de EU-cyberbeveiligingsreserve. De opdracht moet worden uitgevoerd overeenkomstig de toepasselijke regels van Verordening (EU, Euratom) 2024/2509 en moet met name afhankelijk worden gesteld van de vervulling van de relevante voorwaarden voor de ondertekening van een bijdrageovereenkomst. Alle aspecten van de werking en het beheer van de EU-cyberbeveiligingsreserve die niet aan Enisa worden toevertrouwd, moeten in direct beheer worden uitgevoerd door de Commissie, ook vóór de ondertekening van de bijdrageovereenkomst.
- (45) De lidstaten moeten een sleutelrol spelen bij de oprichting, bij de uitrol en na de uitrol van de EU-cyberbeveiligingsreserve. Aangezien Verordening (EU) 2021/694 de relevante basishandeling is voor acties tot uitvoering van de EU-cyberbeveiligingsreserve, moeten de acties in het kader van de EU-cyberbeveiligingsreserve worden opgenomen in de in artikel 24 van Verordening (EU) 2021/694 bedoelde werkprogramma's als. Op grond van lid 6 van dat artikel moet de Commissie die werkprogramma's door middel van uitvoeringshandelingen vaststellen overeenkomstig de onderzoeksprocedure. Voorts moet de Commissie, in coördinatie met de NIS-samenwerkingsgroep, de prioriteiten en de ontwikkeling van de EU-cyberbeveiligingsreserve bepalen.
- (46) De in het kader van de EU-cyberbeveiligingsreserve vastgestelde contracten mogen geen gevolgen hebben voor de onderlinge relatie tussen bedrijven en bestaande verplichtingen tussen de betrokken entiteit of gebruikers en de dienstverlener.
- (47) Met het oog op de selectie van private aanbieders die diensten verlenen in het kader van de EU-cyberbeveiligingsreserve is het nodig een reeks minimumcriteria en -vereisten vast te stellen die moeten worden opgenomen in de oproepen tot het indienen van inschrijvingen voor aanbestedingen met het oog op de selectie van die dienstverleners teneinde ervoor te zorgen dat wordt voldaan aan de behoeften van de autoriteiten van de lidstaten, in zeer kritieke sectoren actieve entiteiten en in andere kritieke sectoren actieve entiteiten. Om tegemoet te komen aan de specifieke behoeften van de lidstaten moet de aanbestedende dienst, bij de aankoop van diensten voor de EU-cyberbeveiligingsreserve, in voorkomend geval aanvullende selectiecriteria en -vereisten ontwikkelen naast de in deze verordening vastgestelde selectiecriteria en -vereisten. Het is belangrijk om de deelname van kleinere aanbieders, die actief zijn op regionaal en lokaal niveau, aan te moedigen.
- (48) Bij de selectie van aanbieders voor opname in de EU-cyberbeveiligingsreserve moet de aanbestedende dienst ernaar streven ervoor te zorgen dat de EU-cyberbeveiligingsreserve, in haar geheel beschouwd, aanbieders bevat die kunnen voldoen aan de taaleisen van gebruikers. Daartoe moet de aanbestedende dienst, alvorens een bestek op te stellen, nagaan of de potentiële gebruikers van de EU-cyberbeveiligingsreserve specifieke taaleisen stellen, zodat ondersteunende diensten van de EU-cyberbeveiligingsreserve kunnen worden verleend in een van de officiële talen van de instellingen van de Unie of van de lidstaat die de gebruiker of de betrokken entiteit waarschijnlijk begrijpt. Indien een gebruiker in het kader van de verlening van ondersteunende diensten van de EU-cyberbeveiligingsreserve meer dan één taal verlangt en die diensten voor deze gebruiker in die talen zijn aangekocht, moet de gebruiker in zijn verzoek om ondersteuning van de EU-cyberbeveiligingsreserve kunnen aangeven in welke van deze talen de diensten moeten worden verleend met betrekking tot het specifieke incident dat aanleiding heeft gegeven tot het verzoek.
- (49) Om de instelling van de EU-cyberbeveiligingsreserve te ondersteunen, is het van belang dat de Commissie Enisa verzoekt een potentiële regeling voor cyberbeveiligingscertificering voor beheerde beveiligingsdiensten op grond van Verordening (EU) 2019/881 op te stellen, op de gebieden die onder het noodmechanisme voor cyberbeveiliging vallen.
- (50) 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 cyberbeveiligingsincidenten en grootschalige cyberbeveiligingsincidenten, moet de Commissie of EU-CyCLONe Enisa kunnen verzoeken om, met de ondersteuning van het CSIRT-netwerk en met instemming van de betrokken lidstaten, cyberdreigingen, bekende kwetsbaarheden die kunnen worden uitgebuit en mitigatiemaatregelen met betrekking tot een specifiek significant cyberbeveiligingsincident of grootschalig cyberbeveiligingsincident te evalueren en te beoordelen. Na de voltooiing van een evaluatie en beoordeling van een incident moet Enisa in samenwerking met de betrokken lidstaat, relevante belanghebbenden, waaronder vertegenwoordigers van de private

sector, de Commissie en andere relevante instellingen, organen en instanties van de Unie een evaluatieverslag over het incident opstellen. Voortbouwend op de samenwerking met belanghebbenden, ook van de private 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 van hoogste professionele integriteit, onpartijdigheid en vereiste technische deskundigheid, zoals in deze verordening vereist. Het verslag moet worden ingediend bij EU-CyCLONe, het CSIRT-netwerk en de Commissie en moet als informatie dienen voor zowel hun werkzaamheden en die van Enisa. Als het incident betrekking heeft op een met het programma Digitaal Europa geassocieerd derde land, moet de Commissie het verslag ook verstrekken aan de hoge vertegenwoordiger.

- (51) 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 cyberbeveiligingsincidenten en aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten bij tot de bescherming van de Unie, en met name haar interne markt en industrie, als geheel. Dergelijke activiteiten kunnen een extra bijdrage leveren aan de cyberdiplomatie van de Unie. Daarom moeten met het programma Digitaal Europa geassocieerde derde landen om steun kunnen verzoeken uit de EU-cyberbeveiligingsreserve, op hun gehele grondgebied of delen daarvan, indien dit is bepaald in de overeenkomst op grond waarvan het derde land met het programma Digitaal Europa geassocieerd is. De financiering voor met het programma Digitaal Europa 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 initieel herstel van significante cyberbeveiligingsincidenten of aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten.
- (52) De in deze verordening vastgestelde voorwaarden voor de EU-cyberbeveiligingsreserve en betrouwbare aanbieders van beheerde beveiligingsdiensten moeten gelden wanneer steun wordt verleend aan de met het programma Digitaal Europa geassocieerde derde landen. Met het programma Digitaal Europa geassocieerde derde landen moeten om steun van de EU-cyberbeveiligingsreserve kunnen verzoeken wanneer de entiteiten die het doelwit zijn en waarvoor zij om steun van de EU-cyberbeveiligingsreserve verzoeken, in zeer kritieke sectoren actieve entiteiten of in andere kritieke sectoren actieve entiteiten zijn en wanneer de gedetecteerde incidenten leiden tot aanzienlijke operationele verstoringen of overloopeffecten in de Unie zouden kunnen hebben. Met het programma Digitaal Europa geassocieerde derde landen mogen alleen in aanmerking komen voor steun indien de overeenkomst op grond waarvan zij met het programma Digitaal Europa geassocieerd zijn specifiek in dergelijke steun voorziet. Bovendien mogen dergelijke derde landen alleen in aanmerking blijven komen als aan drie criteria is voldaan. Ten eerste moet het derde land volledig voldoen aan de relevante bepalingen van die overeenkomst. Ten tweede moet het derde land, gezien de complementaire aard van de EU-cyberbeveiligingsreserve, passende maatregelen hebben genomen om zich voor te bereiden op significante cyberbeveiligingsincidenten of aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten. Ten derde moet de steunverlening uit de EU-cyberbeveiligingsreserve stroken met het beleid van de Unie ten aanzien van en met de algemene betrekkingen met dat land en verenigbaar zijn met ander beleid van de Unie op het gebied van veiligheid. In het kader van haar beoordeling van de naleving van dit derde criterium moet de Commissie de hoge vertegenwoordiger raadplegen om de toekenning van dergelijke steun af te stemmen op het gemeenschappelijk buitenlands en veiligheidsbeleid.
- (53) Steunverlening aan met het programma Digitaal Europa geassocieerde derde landen kan gevolgen hebben voor de betrekkingen met derde landen en het veiligheidsbeleid van de Unie, onder meer in het kader van het gemeenschappelijk buitenlands en veiligheidsbeleid en het gemeenschappelijk veiligheids- en defensiebeleid. Het is derhalve passend dat aan de Raad uitvoeringsbevoegdheden worden toegekend om toestemming te verlenen voor de toekenning van dergelijke steun en om de periode vast te stellen waarin deze steun mag worden verleend. De Raad moet een besluit nemen op basis van een voorstel van de Commissie en daarbij terdege rekening houden met de beoordeling van de drie criteria door de Commissie. Hetzelfde moet gelden voor verlengingen en voorstellen om die uitvoeringshandelingen te wijzigen of in te trekken. Wanneer de Raad, in uitzonderlijke omstandigheden, van oordeel is dat de omstandigheden ten aanzien van het derde criterium aanzienlijk zijn gewijzigd, moet de Raad op eigen initiatief kunnen optreden om uitvoeringshandelingen te wijzigen of in te trekken zonder een voorstel van de Commissie af te wachten. Dergelijke ingrijpende wijzigingen vereisen waarschijnlijk dringende maatregelen, hebben wellicht bijzonder belangrijke gevolgen voor de betrekkingen met derde landen en vereisen waarschijnlijk geen voorafgaande gedetailleerde beoordeling door de Commissie. Bovendien moet de Commissie samenwerken met de hoge vertegenwoordiger in verband met dergelijke verzoeken voor steun van met het programma Digitaal Europa geassocieerde derde landen en de uitvoering van steun die is verleend aan dergelijke derde landen. De Commissie moet ook rekening houden met de standpunten van Enisa met betrekking tot dergelijke verzoeken en steun. De Commissie moet de Raad in kennis stellen van het resultaat van de beoordeling van de verzoeken, met inbegrip van de daarbij gemaakte relevante overwegingen, en de diensten die worden ingezet.

- (54) In de mededeling van de Commissie van 18 april 2023 over de academie voor cybervaardigheden wordt het tekort aan geschoolde professionals erkend. Dergelijke vaardigheden zijn nodig om de doelstellingen van deze verordening na te streven. De Unie heeft dringend behoefte aan professionals met de vaardigheden en competenties die nodig zijn om cyberaanvallen te voorkomen, op te sporen, af te schrikken en de Unie, met inbegrip van haar meest kritieke infrastructuur, te verdedigen tegen dergelijke aanvallen en haar weerbaarheid te waarborgen. Daarom is het belangrijk de samenwerking tussen belanghebbenden, ook van de private sector, de academische wereld en de publieke sector, aan te moedigen. Het is even belangrijk om in alle regio's van de Unie synergieën tot stand te brengen voor investeringen in onderwijs en opleiding, om de invoering van voorzorgsmaatregelen ter voorkoming van braindrain aan te moedigen en ervoor te zorgen dat het tekort aan vaardigheden in sommige regio's niet verder toeneemt dan in andere. Het is dringend noodzakelijk om de lacunes op het gebied van cyberbeveiligingsvaardigheden op te vullen, met bijzondere aandacht voor het verkleinen van de genderkloof bij de arbeidskrachten op het gebied van cyberbeveiliging om de betrokkenheid en deelname van vrouwen aan het ontwerp van digitale governance te bevorderen.
- (55) Om de innovatie in de digitale eengemaakte markt te stimuleren, is het belangrijk onderzoek en innovatie op het gebied van cyberbeveiliging te versterken, teneinde bij te dragen tot het vergroten van de weerbaarheid van de lidstaten en de open strategische autonomie van de Unie, die beide doelstellingen van deze verordening zijn. Synergieën zijn essentieel om de samenwerking en coördinatie tussen de verschillende belanghebbenden, ook van de private sector, het maatschappelijk middenveld en de academische wereld, te versterken.
- (56) Deze verordening moet rekening houden met de toezegging uiteengezet in de gezamenlijke verklaring van 26 januari 2022 van het Europees Parlement, de Raad en de Commissie getiteld "Europese verklaring over digitale rechten en beginselen voor het digitale decennium" om de belangen van de democratieën, bevolkingen, bedrijven en openbare instellingen van de Unie te beschermen tegen cyberbeveiligingsrisico's en cybercriminaliteit, waaronder gegevenslekken en identiteitsdiefstal of -manipulatie.
- (57) Om bepaalde niet-essentiële onderdelen van deze verordening aan te vullen, moet aan de Commissie de bevoegdheid worden overgedragen om overeenkomstig artikel 290 VWEU handelingen vast te stellen om de soorten en het aantal responsdiensten te specificeren die voor de EU-cyberbeveiligingsreserve vereist zijn. 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⁽²⁰⁾. 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.
- (58) Om eenvormige voorwaarden voor de uitvoering van deze verordening te waarborgen, moeten aan de Commissie uitvoeringsbevoegdheden worden toegekend om de nadere procedurele regelingen voor de toewijzing van de 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⁽²¹⁾.
- (59) Onverminderd de regels inzake de jaarlijkse begroting van de Unie zoals vastgelegd in de Verdragen, moet de Commissie bij de beoordeling van de budgettaire en personeelsbehoeften van Enisa rekening houden met de verplichtingen die uit deze verordening voortvloeien.
- (60) De Commissie moet de in deze verordening vastgestelde maatregelen regelmatig evalueren. De eerste dergelijke evaluatie moet plaatsvinden in de eerste twee jaar na de datum van inwerkingtreding van deze verordening en vervolgens ten minste om de vier jaar, rekening houdend met het tijdschema voor de herziening van het meerjarig financieel kader dat is ingesteld op grond van artikel 312 VWEU. De Commissie moet bij het Europees Parlement en de Raad een verslag indienen over de geboekte vooruitgang. Om de verschillende vereiste elementen te beoordelen, waaronder de omvang van de informatie die binnen het Europees waarschuwingssysteem voor cyberbeveiliging wordt gedeeld, dient de Commissie zich uitsluitend te baseren op informatie die reeds beschikbaar is of vrijwillig wordt verstrekt. Gelet op de geopolitieke ontwikkelingen en om de continuïteit en de verdere ontwikkeling van de maatregelen waarin deze verordening voorziet na 2027 te waarborgen, is het belangrijk dat de Commissie beoordeelt of het nodig is een passend budget toe te wijzen in het kader van het meerjarig financieel kader 2028-2034.

⁽²⁰⁾ PB L 123 van 12.5.2016, blz. 1, ELI: http://data.europa.eu/eli/agree_interinsttit/2016/512/oj.

⁽²¹⁾ 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>).

- (61) Daar de doelstellingen van deze verordening, namelijk het versterken van de concurrentiepositie van de industrie en diensten in de Unie in de digitale economie en het bijdragen aan de technologische soevereiniteit en open strategische autonomie van de Unie op het gebied van cyberbeveiliging, niet voldoende door de lidstaten kunnen worden verwezenlijkt, maar vanwege de omvang of de gevolgen van het optreden beter door de Unie kunnen worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie neergelegde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze verordening niet verder dan nodig is om die doelstellingen te verwezenlijken,

HEBBERN DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I
ALGEMENE BEPALINGEN

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:
 - a) de oprichting van een pan-Europees netwerk van cyberhubs (Europees waarschuwingssysteem voor cyberbeveiliging) om gecoördineerde capaciteiten op het gebied van opsporing en gemeenschappelijk situationeel bewustzijn op te bouwen en te versterken;
 - b) de instelling van een noodmechanisme voor cyberbeveiliging om de lidstaten te ondersteunen bij de voorbereiding op, de respons op, de beperking van de gevolgen van, en het initiëren van, het herstel na significante cyberbeveiligingsincidenten en grootschalige cyberbeveiligingsincidenten, en om andere gebruikers te ondersteunen bij de respons op significante cyberbeveiligingsincidenten en aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten;
 - c) de instelling van een Europees evaluatiemechanisme voor cyberbeveiligingsincidenten om significante cyberbeveiligingsincidenten of grootschalige cyberbeveiligingsincidenten te evalueren en te beoordelen.
2. Met deze verordening worden de algemene doelstellingen nagestreefd om de concurrentiepositie van de industrie en diensten van de digitale economie in de Unie, met inbegrip van micro-ondernemingen en kleine en middelgrote ondernemingen alsook start-ups, te versterken en bij te dragen tot de technologische soevereiniteit en open strategische autonomie van de Unie op het gebied van cyberbeveiliging, onder meer door innovatie op de digitale eengemaakte markt te bevorderen. Deze doelstellingen worden door deze verordening nagestreefd door de solidariteit op het niveau van de Unie te versterken, het ecosysteem voor cyberbeveiliging te versterken, de cyberweerbaarheid van de lidstaten te vergroten en de vaardigheden, expertise, bekwaamheden en competenties van de arbeidskrachten op het gebied van cyberbeveiliging te ontwikkelen.
3. De in lid 2 bedoelde algemene doelstellingen worden nagestreefd aan de hand van de volgende specifieke doelstellingen:
 - a) het versterken van de gemeenschappelijke gecoördineerde opsporingscapaciteiten van de Unie en het gemeenschappelijk situationeel bewustzijn van cyberdreigingen en -incidenten;
 - b) het vergroten van de paraatheid van in zeer kritieke sectoren actieve entiteiten of in andere kritieke sectoren actieve entiteiten in de hele Unie en het versterken van de solidariteit door gecoördineerde paraatheidstests en versterkte respons- en herstelcapaciteiten te ontwikkelen, voor de behandeling van significante cyberbeveiligingsincidenten, grootschalige cyberbeveiligingsincidenten of aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten, met inbegrip van de mogelijkheid om steun van de Unie voor respons op cyberbeveiligingsincidenten beschikbaar te stellen aan derde landen die geassocieerd zijn met het programma Digitaal Europa;
 - c) het vergroten van de weerbaarheid van de Unie en bijdragen tot een doeltreffende respons door significante cyberbeveiligingsincidenten of grootschalige cyberbeveiligingsincidenten te evalueren en te beoordelen, en daaruit lering te trekken en, in voorkomend geval, aanbevelingen te doen.
4. De acties uit hoofde van deze verordening worden uitgevoerd met inachtneming van de bevoegdheden van de lidstaten en vormen een aanvulling op de activiteiten van het CSIRT-netwerk, EU-CyCLONe en de NIS-samenwerkingsgroep.

5. Deze verordening doet geen afbreuk aan de essentiële staatsfuncties van de lidstaten, waaronder het waarborgen van de territoriale integriteit van de staat, de handhaving van de openbare orde en de bescherming van de nationale veiligheid. Met name de nationale veiligheid blijft uitsluitend de verantwoordelijkheid van elke lidstaat.

6. Het delen of de uitwisseling van informatie uit hoofde van deze verordening die op grond van Unie- of nationale regelgeving vertrouwelijk is, blijft beperkt tot informatie die relevant is voor en in verhouding staat tot het doel van die uitwisseling. Bij het dergelijke delen of uitwisselen van informatie wordt de vertrouwelijkheid van de informatie gewaarborgd en worden de veiligheids- en commerciële belangen van de betrokken entiteiten beschermd. Dat brengt niet met zich mee dat informatie wordt verstrekt waarvan de bekendmaking strijdig zou zijn met de wezenlijke belangen van de lidstaten inzake nationale veiligheid, openbare veiligheid of defensie.

Artikel 2

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

- 1) “landsgrensoverschrijdende cyberhub”: een meerlandenplatform, opgericht bij een schriftelijke consortiumovereenkomst, dat nationale cyberhubs uit ten minste drie lidstaten samenbrengt in een gecoördineerde netwerkstructuur, en dat bedoeld is om de monitoring, opsporing en analyse van cyberdreigingen te versterken, incidenten te voorkomen en de productie van inlichtingen over cyberdreigingen te ondersteunen, met name door het uitwisselen van relevante en in voorkomend geval, geanonimiseerde gegevens en informatie, het delen van geavanceerde instrumenten en het gezamenlijk ontwikkelen van capaciteit op het gebied van de opsporing, analyse en preventie van, alsook de bescherming tegen cyberdreigingen en -incidenten in een betrouwbare omgeving;
- 2) “onderbrengend consortium”: een consortium bestaande uit deelnemende lidstaten, die zijn overeengekomen om een landsgrensoverschrijdende cyberhub op te richten en bij te dragen aan de verwerving van instrumenten, infrastructuur of diensten voor, en de exploitatie van, die hub;
- 3) “CSIRT”: een CSIRT dat is aangewezen of ingesteld op grond van artikel 10 van Richtlijn (EU) 2022/2555;
- 4) “entiteit”: een entiteit zoals gedefinieerd in artikel 6, punt 38), van Richtlijn (EU) 2022/2555;
- 5) “in zeer kritieke sectoren actieve entiteiten”: de soorten entiteiten die zijn opgenomen in bijlage I bij Richtlijn (EU) 2022/2555;
- 6) “in andere kritieke sectoren actieve entiteiten”: de soorten entiteiten die zijn opgenomen in bijlage II bij Richtlijn (EU) 2022/2555;
- 7) “risico”: een risico zoals gedefinieerd in artikel 6, punt 9), van Richtlijn (EU) 2022/2555;
- 8) “cyberdreiging”: een cyberdreiging zoals gedefinieerd in artikel 2, punt 8, van Verordening (EU) 2019/881;
- 9) “incident”: een incident zoals gedefinieerd in artikel 6, punt 6), van Richtlijn (EU) 2022/2555;
- 10) “significant cyberbeveiligingsincident”: een cyberbeveiligingsincident dat voldoet aan de criteria van artikel 23, lid 3, van Richtlijn (EU) 2022/2555;
- 11) “ernstig incident”: een ernstig incident zoals gedefinieerd in artikel 3, punt 8), van Verordening (EU, Euratom) 2023/2841 van het Europees Parlement en de Raad ⁽²²⁾,
- 12) “grootschalig cyberbeveiligingsincident”: een grootschalig cyberbeveiligingsincident zoals gedefinieerd in artikel 6, punt 7), van Richtlijn (EU) 2022/2555;

⁽²²⁾ Verordening (EU, Euratom) 2023/2841 van het Europees Parlement en de Raad van 13 december 2023 tot vaststelling van maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie (PB L, 2023/2841, 18.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2841/oj>).

- 13) “een aan grootschalige cyberbeveiligingsincidenten gelijkwaardig incident”: in het geval van instellingen, organen en instanties van de Unie, een ernstig incident en, in het geval van met het programma Digitaal Europa geassocieerde derde landen, een incident dat een mate van verstoring veroorzaakt die het responsvermogen van het betrokken met het programma Digitaal Europa geassocieerd derde land overstijgt;
- 14) “met het programma Digitaal Europa geassocieerd derde land”: een derde land dat partij is bij een overeenkomst met de Unie waardoor het kan deelnemen aan het programma Digitaal Europa op grond van artikel 10 van Verordening (EU) 2021/694;
- 15) “aanbestedende dienst”: de Commissie of, voor zover de exploitatie en het beheer van de EU-cyberbeveiligingsreserve op grond van artikel 14, lid 5, aan Enisa zijn toevertrouwd, Enisa;
- 16) “aanbieder van beheerde beveiligingsdiensten”: een aanbieder van beheerde beveiligingsdiensten zoals gedefinieerd in artikel 6, punt 40), van Richtlijn (EU) 2022/2555;
- 17) “betrouwbare aanbieders van beheerde beveiligingsdiensten”: aanbieders van beheerde beveiligingsdiensten geselecteerd overeenkomstig artikel 17 om te worden opgenomen in de EU-cyberbeveiligingsreserve.

HOOFDSTUK II

HET EUROPEES WAARSCHUWINGSSYSTEEM VOOR CYBERBEVEILIGING

Artikel 3

Oprichting van het Europees waarschuwingssysteem voor cyberbeveiliging

1. Er wordt een Europees waarschuwingssysteem voor cyberbeveiliging opgericht, een pan-Europees infrastructuurnetwerk bestaande uit nationale en landsgrensoverschrijdende cyberhubs die op zich op vrijwillige basis aansluiten, om de ontwikkeling van geavanceerde capaciteiten te ondersteunen waarmee de Unie haar opsporings-, analyse- en gegevensverwerkingscapaciteiten met betrekking tot cyberdreigingen en de preventie van incidenten in de Unie kan verbeteren.
2. Het Europees waarschuwingssysteem voor cyberbeveiliging:
 - a) draagt bij tot een betere bescherming tegen en respons op cyberdreigingen door ondersteuning van relevante entiteiten, met name CSIRT's, het CSIRT-netwerk, EU-CyCLONe en de op grond van artikel 8, lid 1, van Richtlijn (EU) 2022/2555 aangewezen of ingestelde bevoegde autoriteiten, door met hen samen te werken en hun capaciteiten te versterken;
 - b) bundelt relevante gegevens en informatie over cyberdreigingen en -incidenten uit verschillende bronnen binnen de landsgrensoverschrijdende cyberhubs en deelt geanalyseerde of geaggregeerde informatie via landsgrensoverschrijdende cyberhubs, in voorkomend geval met het CSIRT-netwerk;
 - c) verzamelt en ondersteunt de productie van hoogwaardige, bruikbare informatie en inlichtingen over cyberdreigingen door gebruik te maken van geavanceerde instrumenten en technologieën, en deelt die informatie en inlichtingen over cyberdreigingen;
 - d) draagt bij tot de versterking van gecoördineerde opsporing van cyberdreigingen en gemeenschappelijk situationeel bewustzijn in de hele Unie, en tot het versturen van waarschuwingen, onder meer, in voorkomend geval, door het verstrekken van concrete aanbevelingen aan entiteiten;
 - e) levert diensten en activiteiten voor de cyberbeveiligingsgemeenschap in de Unie, waaronder het bijdragen aan de ontwikkeling van geavanceerde instrumenten en technologieën zoals artificiële intelligentie en instrumenten voor gegevensanalyse.
3. De acties ter uitvoering van het Europees waarschuwingssysteem voor cyberbeveiliging worden ondersteund door financiering uit het programma Digitaal Europa en uitgevoerd overeenkomstig Verordening (EU) 2021/694, met name specifieke doelstelling 3 daarvan.

*Artikel 4***Nationale cyberhubs**

1. Wanneer een lidstaat besluit deel te nemen aan het Europees waarschuwingssysteem voor cyberbeveiliging, wijst hij een nationale cyberhub aan, of richt hij in voorkomend geval een nationale cyberhub op, voor de toepassing van deze verordening.
2. Een nationale cyberhub is één centrale entiteit die optreedt onder het gezag van een lidstaat. De nationale cyberhub kan een CSIRT zijn, of, in voorkomend geval, een nationale cybercrisisbeheerautoriteit of een andere bevoegde autoriteit die is aangewezen of ingesteld op grond van artikel 8, lid 1, van Richtlijn (EU) 2022/2555, of een andere entiteit. De nationale cyberhub:
 - a) heeft de capaciteit te fungeren als referentiepunt voor en toegangspoort tot andere publieke en private organisaties op nationaal niveau voor het verzamelen en analyseren van informatie over cyberdreigingen en -incidenten en voor het bijdragen tot een in artikel 5 van deze verordening bedoelde landsgrensoverschrijdende cyberhub, en
 - b) is in staat gegevens en informatie met betrekking op cyberdreigingen en -incidenten, zoals inlichtingen over cyberdreigingen, op te sporen, samen te voegen en te analyseren, met name door gebruik te maken van geavanceerde technologieën, met als doel incidenten te voorkomen.
3. Als onderdeel van de in lid 2 van dit artikel bedoelde functies kunnen nationale cyberhubs samenwerken met entiteiten uit de private sector om relevante gegevens en informatie uit te wisselen met het oog op het opsporen en voorkomen van cyberdreigingen en -incidenten, onder meer met sectorale en sectoroverschrijdende gemeenschappen van essentiële en belangrijke entiteiten zoals bedoeld in artikel 3 van Richtlijn (EU) 2022/2555. In voorkomend geval en in overeenstemming met het Unierecht en het nationale recht kan de door nationale cyberhubs gevraagde of ontvangen informatie telemetrie-, sensor- en registratiegegevens omvatten.
4. Een op grond van artikel 9, lid 1, geselecteerde lidstaat verbindt zich ertoe voor zijn nationale cyberhub een aanvraag tot deelname aan een landsgrensoverschrijdende cyberhub in te dienen.

*Artikel 5***Landsgrensoverschrijdende cyberhubs**

1. Wanneer ten minste drie lidstaten zich ertoe verbinden ervoor te zorgen dat hun nationale cyberhubs samenwerken om hun activiteiten op het gebied van het opsporen en monitoren van cyberdreigingen en -incidenten te coördineren, kunnen die lidstaten voor de toepassing van deze verordening een onderbrengend consortium oprichten.
2. Een onderbrengend consortium bestaat uit ten minste drie deelnemende lidstaten die zijn overeengekomen een landsgrensoverschrijdende cyberhub op te richten en bij te dragen aan de verwerving van instrumenten, infrastructuur of diensten voor die hub, en aan de exploitatie daarvan, overeenkomstig lid 4.
3. Wanneer een onderbrengend consortium is geselecteerd overeenkomstig artikel 9, lid 3, sluiten de leden daarvan een schriftelijke consortiumovereenkomst:
 - a) waarin de interne regelingen voor de uitvoering van de in artikel 9, lid 3, bedoelde onderbrengings- en gebruiksovereenkomst worden vastgelegd;
 - b) waarbij de landsgrensoverschrijdende cyberhub van het onderbrengend consortium wordt opgericht, en
 - c) die de specifieke bepalingen bevat die op grond van artikel 6, leden 1 en 2, vereist zijn.
4. Een landsgrensoverschrijdende cyberhub is een meerlandenplatform dat is opgericht bij een in lid 3 bedoelde schriftelijke consortiumovereenkomst. Het brengt de nationale cyberhubs van de lidstaten van het onderbrengend consortium samen in een gecoördineerde netwerkstructuur. Het is bedoeld om de monitoring, opsporing en analyse van cyberdreigingen te versterken, incidenten te voorkomen en de productie van inlichtingen over cyberdreigingen te ondersteunen, met name door het uitwisselen van relevante en in voorkomend geval, geanonimiseerde gegevens en informatie, door het delen van geavanceerde instrumenten en het gezamenlijk ontwikkelen van capaciteit op het gebied van de opsporing, analyse en preventie van, alsook de bescherming tegen cyberdreigingen en -incidenten in een betrouwbare omgeving.
5. Een landsgrensoverschrijdende cyberhub wordt voor juridische doeleinden vertegenwoordigd door een lid van het overeenkomstige onderbrengend consortium dat optreedt als een coördinator, of door het onderbrengend consortium indien dit rechtspersoonlijkheid bezit. De verantwoordelijkheid voor de naleving door de landsgrensoverschrijdende cyberhub van deze verordening en de onderbrengings- en gebruiksovereenkomst wordt bepaald in de in lid 3 bedoelde schriftelijke consortiumovereenkomst.

6. Een lidstaat kan zich aansluiten bij een bestaand onderbrengend consortium met instemming van de leden van het onderbrengend consortium. De in lid 3 bedoelde schriftelijke consortiumovereenkomst en de onderbrengings- en gebruiksovereenkomst worden dienovereenkomstig gewijzigd. Dit doet geen afbreuk aan de eigendomsrechten van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging ("ECCC") met betrekking tot de instrumenten, infrastructuur of diensten die reeds gezamenlijk met dat onderbrengend consortium zijn verworven.

Artikel 6

Samenwerking en informatiedeling binnen en tussen landsgrensoverschrijdende cyberhubs

1. De leden van een onderbrengend consortium zorgen ervoor dat hun nationale cyberhubs, overeenkomstig de in artikel 5, lid 3, bedoelde schriftelijke consortiumovereenkomst, relevante informatie, waar passend geanonimiseerd, zoals 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 op te sporen, onder de landsgrensoverschrijdende cyberhubs delen wanneer dat delen van informatie:

- a) de opsporing van cyberdreigingen bevordert en verbetert en de capaciteiten van het CSIRT-netwerk versterkt om incidenten te voorkomen en erop te reageren of de gevolgen ervan te beperken;
- b) het niveau van de cyberbeveiliging verhoogt, bijvoorbeeld 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 private entiteiten te bevorderen.

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

- a) een verbintenis om tussen de leden van het onderbrengend consortium informatie als bedoeld in lid 1 uit te wisselen en de voorwaarden waaronder die informatie moet worden gedeeld;
- b) een governancekader dat het delen door alle deelnemers van in lid 1 bedoelde relevante informatie, waar nodig geanonimiseerd, verduidelijkt en stimuleert;
- c) doelstellingen voor de bijdrage aan de ontwikkeling van geavanceerde instrumenten en technologieën, zoals artificiële intelligentie en instrumenten voor gegevensanalyse.

In de schriftelijke consortiumovereenkomst kan worden gespecificeerd dat de in lid 1 bedoelde informatie moet worden gedeeld overeenkomstig het Unie- en het nationale recht.

3. Landsgrensoverschrijdende cyberhubs sluiten samenwerkingsovereenkomsten met elkaar, waarin de beginselen voor interoperabiliteit en informatiedeling tussen de landsgrensoverschrijdende cyberhubs worden gespecificeerd. Landsgrensoverschrijdende cyberhubs stellen de Commissie in kennis van de gesloten samenwerkingsovereenkomsten.

4. Het in lid 1 bedoelde delen van informatie tussen landsgrensoverschrijdende cyberhubs wordt gewaarborgd door een hoog niveau van interoperabiliteit. Om die interoperabiliteit te ondersteunen, vaardigt Enisa, in nauw overleg met de Commissie, onverwijld en uiterlijk op 5 februari 2026 interoperabiliteitsrichtsnoeren uit waarin met name modellen en protocollen voor informatiedeling worden gespecificeerd, rekening houdend met internationale normen en beste praktijken, alsook de werking van bestaande landsgrensoverschrijdende cyberhubs. Interoperabiliteitsvoorschriften die zijn bepaald in de samenwerkingsovereenkomsten voor landsgrensoverschrijdende cyberhubs worden gebaseerd op de richtsnoeren van Enisa.

Artikel 7

Samenwerking en informatiedeling met netwerken op Unieniveau

1. Landsgrensoverschrijdende cyberhubs en het CSIRT-netwerk werken nauw samen, met name met het oog op het delen van informatie. Daartoe komen zij procedurele regelingen overeen inzake samenwerking en delen van relevante informatie en, onverminderd lid 2, inzake de soorten informatie die moeten worden gedeeld.

2. Wanneer de landsgrensoverschrijdende cyberhubs informatie verkrijgen over een mogelijk of lopend grootschalig cyberbeveiligingsincident, zorgen zij er ten behoeve van een gemeenschappelijk situationeel bewustzijn voor dat relevante informatie en vroegtijdige waarschuwingen onverwijld aan de autoriteiten van de lidstaten en de Commissie worden verstrekt via EU-CyCLONe en het CSIRT-netwerk.

Artikel 8

Beveiliging

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

2. De lidstaten die deelnemen aan het Europees waarschuwingssysteem voor cyberbeveiliging zorgen ervoor dat het delen van de in artikel 6, lid 1, bedoelde informatie binnen het Europees waarschuwingssysteem voor cyberbeveiliging met een andere entiteit dan een overheidsautoriteit of -orgaan van een lidstaat geen negatieve gevolgen heeft voor de veiligheidsbelangen van de Unie of van de lidstaten.

Artikel 9

Financiering van het Europees waarschuwingssysteem voor cyberbeveiliging

1. Na een oproep tot het indienen van blijken van belangstelling voor lidstaten die voornemens zijn deel te nemen aan het Europees waarschuwingssysteem voor cyberbeveiliging selecteert het ECCC lidstaten om samen met het ECCC deel te nemen aan een gezamenlijke aanbesteding van instrumenten, infrastructuur of diensten, teneinde op grond van artikel 4, lid 1, aangewezen of opgerichte nationale cyberhubs op te zetten of de capaciteiten van die cyberhubs te vergroten. Het ECCC kan aan de geselecteerde lidstaten subsidies toekennen om de werking van dergelijke instrumenten, infrastructuur en diensten te financieren. De financiële bijdrage van de Unie dekt tot 50 % van de verwervingskosten van de instrumenten, infrastructuur of diensten en tot 50 % van de exploitatiekosten. De resterende kosten komen voor rekening van de geselecteerde lidstaten. Alvorens de procedure voor de verwerving van instrumenten, infrastructuur of diensten in gang te zetten, sluiten het ECCC en de geselecteerde lidstaten een onderbrengings- en gebruiksovereenkomst waarin het gebruik van de instrumenten, infrastructuur of diensten wordt geregeld.

2. Indien de nationale cyberhub van een lidstaat niet deelneemt aan een landsgrensoverschrijdende cyberhub binnen twee jaar na de datum waarop de instrumenten, infrastructuur of diensten zijn verworven of, indien dit eerder is, waarop de lidstaat subsidiefinanciering heeft ontvangen, komt de lidstaat niet in aanmerking voor aanvullende steun van de Unie uit hoofde van dit hoofdstuk totdat deze lidstaat zich bij een landsgrensoverschrijdende cyberhub heeft aangesloten.

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

4. Het ECCC brengt ten minste om de twee jaar de instrumenten, infrastructuur of diensten in kaart die nodig en van toereikende kwaliteit zijn om nationale cyberhubs en landsgrensoverschrijdende cyberhubs op te richten, of de capaciteit ervan te versterken, alsmede de beschikbaarheid ervan, onder meer bij juridische entiteiten die in de lidstaten gevestigd zijn of geacht worden te zijn gevestigd en waarover lidstaten of onderdanen van lidstaten zeggenschap hebben. Bij het in kaart brengen, raadpleegt het ECCC het CSIRT-netwerk, bestaande landsgrensoverschrijdende cyberhubs, Enisa en de Commissie.

HOOFDSTUK III
NOODMECHANISME VOOR CYBERBEVEILIGING

Artikel 10

Instelling van het noodmechanisme voor cyberbeveiliging

1. Er wordt een noodmechanisme voor cyberbeveiliging ingesteld om de verbetering van de weerbaarheid van de Unie tegen cyberdreigingen te ondersteunen en om in een geest van solidariteit de kortetermijngevolgen van significante cyberbeveiligingsincidenten, grootschalige cyberbeveiligingsincidenten en aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten te beperken en zich daarop voor te bereiden.
2. In het geval van de lidstaten worden acties in het kader van het noodmechanisme voor cyberbeveiliging op verzoek uitgevoerd en vormen zij een aanvulling op de inspanningen en acties van de lidstaten om zich voor te bereiden op, te reageren op en te herstellen van incidenten.
3. De acties ter uitvoering van het noodmechanisme voor cyberbeveiliging worden ondersteund door financiering uit het programma Digitaal Europa en uitgevoerd overeenkomstig Verordening (EU) 2021/694, met name specifieke doelstelling 3 daarvan.
4. De acties in het kader van het noodmechanisme voor cyberbeveiliging worden voornamelijk uitgevoerd via het ECCC overeenkomstig Verordening (EU) 2021/887. Acties ter uitvoering van de EU-cyberbeveiligingsreserve als bedoeld in artikel 11, lid 1, punt b), van deze verordening worden evenwel door de Commissie en Enisa uitgevoerd.

Artikel 11

Soorten acties

Het noodmechanisme voor cyberbeveiliging ondersteunt de volgende soorten acties:

- a) paraatheidsacties, namelijk:
 - i) de gecoördineerde paraatheidstests van in zeer kritieke sectoren actieve entiteiten in de hele Unie zoals gespecificeerd in artikel 12;
 - ii) andere paraatheidsacties voor in zeer kritieke sectoren actieve entiteiten of in andere kritieke sectoren actieve entiteiten, zoals gespecificeerd in artikel 13;
- b) acties ter ondersteuning van de respons op en het initiëren van herstel van significante cyberbeveiligingsincidenten, grootschalige cyberbeveiligingsincidenten en aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten, die moeten worden uitgevoerd door betrouwbare aanbieders van beheerde beveiligingsdiensten die deelnemen aan de bij artikel 14 ingestelde EU-cyberbeveiligingsreserve;
- c) in artikel 18 bedoelde acties ter ondersteuning van wederzijdse bijstand.

Artikel 12

Gecoördineerde paraatheidstests van entiteiten

1. Het noodmechanisme voor cyberbeveiliging steunt het vrijwillig gecoördineerd testen van de paraatheid van in zeer kritieke sectoren actieve entiteiten.
2. De gecoördineerde paraatheidstest kan bestaan uit paraatheidsactiviteiten, zoals penetratietests, en dreigingsevaluatie.
3. Steun voor paraatheidsacties uit hoofde van dit artikel wordt verleend aan de lidstaten voornamelijk in de vorm van subsidies en onder de voorwaarden die zijn vastgesteld in de desbetreffende werkprogramma's als bedoeld in artikel 24 van Verordening (EU) 2021/694.
4. Teneinde de in artikel 11, lid 1, punt a), i), van deze verordening bedoelde gecoördineerde paraatheidstests van entiteiten in de hele Unie te ondersteunen, stelt de Commissie, na raadpleging van de NIS-samenwerkingsgroep, EU-CyCLONE en Enisa, uit de in bijlage I bij Richtlijn (EU) 2022/2555 vermelde zeer kritieke sectoren, de sectoren of

subsectoren vast waarvoor een oproep tot het indienen van voorstellen voor toekenning van subsidies kan worden gedaan. Deelname van de lidstaten aan deze oproepen van voorstellen geschiedt op vrijwillige basis.

5. Bij de vaststelling van de in lid 4 bedoelde sectoren of subsectoren houdt de Commissie rekening met gecoördineerde risicobeoordelingen en weerbaarheidstests op het niveau van de Unie en de resultaten daarvan.

6. De NIS-samenwerkingsgroep ontwikkelt in samenwerking met de Commissie, de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid (de "hoge vertegenwoordiger") en Enisa, en, binnen de grenzen van zijn mandaat, EU-CyCLONe, gemeenschappelijke risicoscenario's en -methoden voor de in artikel 11, punt a), i), bedoelde gecoördineerde paraatheidstests en, in voorkomend geval, voor andere in punt a), ii), van dat artikel bedoelde paraatheidsacties.

7. Wanneer een entiteit die actief is in een zeer kritieke sector vrijwillig deelneemt aan gecoördineerde paraatheidstests en deze tests resulteren in aanbevelingen voor specifieke maatregelen, die door de deelnemende entiteit in een herstelplan kunnen worden geïntegreerd, evalueert de voor de gecoördineerde paraatheidstests verantwoordelijke autoriteit van de lidstaat in voorkomend geval de follow-up van die maatregelen door de deelnemende entiteiten, teneinde de paraatheid te versterken.

Artikel 13

Andere paraatheidsacties

1. Het noodmechanisme voor cyberbeveiliging ondersteunt paraatheidsacties die niet onder artikel 12 vallen. Dergelijke acties omvatten paraatheidsacties voor entiteiten in sectoren die niet in aanmerking komen voor gecoördineerde tests op grond van artikel 12. Dergelijke acties kunnen kwetsbaarheidsmonitoring, risicomonitoring, tests en opleidingen ondersteunen.

2. Steun voor paraatheidsacties uit hoofde van dit artikel wordt aan de lidstaten verleend op verzoek en voornamelijk in de vorm van subsidies en onder de voorwaarden die zijn vastgesteld in de desbetreffende werkprogramma's als bedoeld in artikel 24 van Verordening (EU) 2021/694.

Artikel 14

Instelling van de EU-cyberbeveiligingsreserve

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

2. De EU-cyberbeveiligingsreserve bestaat uit responsdiensten van betrouwbare aanbieders van beheerde beveiligingsdiensten die zijn geselecteerd overeenkomstig de criteria van artikel 17, lid 2. De EU-cyberbeveiligingsreserve kan vooraf vastgelegde diensten omvatten. De vooraf vastgelegde diensten van een betrouwbare aanbieder van beheerde beveiligingsdiensten zijn, in gevallen waarin die diensten niet worden gebruikt voor respons op incidenten tijdens de periode waarvoor die diensten vooraf zijn vastgelegd, converteerbaar in paraatheidsdiensten in verband met de preventie van en respons op incidenten. De EU-cyberbeveiligingsreserve kan op verzoek worden ingezet in alle lidstaten, instellingen, organen en instanties van de Unie en in artikel 19, lid 1, bedoelde met het programma Digitaal Europa geassocieerde derde landen.

3. De gebruikers van de diensten van de EU-cyberbeveiligingsreserve bestaan uit de volgende:

- 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) CERT-EU overeenkomstig artikel 13 van Verordening (EU, Euratom) 2023/2841;
- c) bevoegde autoriteiten zoals computer security incident response teams en cybercrisisbeheerautoriteiten van met het programma Digitaal Europa geassocieerde derde landen overeenkomstig artikel 19, lid 8.

4. De Commissie draagt de algemene verantwoordelijkheid voor de uitvoering van de EU-cyberbeveiligingsreserve. De Commissie bepaalt in coördinatie met de NIS-samenwerkingsgroep 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 alsook met andere acties en programma's van de Unie. Deze prioriteiten worden elke twee jaar geëvalueerd en, zo nodig, herzien. De Commissie stelt het Europees Parlement en de Raad van die prioriteiten en herzieningen daarvan in kennis.

5. Onverminderd de algemene verantwoordelijkheid van de Commissie voor de uitvoering van de in lid 4 van dit artikel bedoelde EU-cyberbeveiligingsreserve en onder voorbehoud van een bijdrageovereenkomst als gedefinieerd in artikel 2, punt 19), van Verordening (EU, Euratom) 2024/2509, vertrouwt de Commissie de exploitatie en het beheer van de EU-cyberbeveiligingsreserve geheel of gedeeltelijk toe aan Enisa. Aspecten die niet aan Enisa zijn toevertrouwd, blijven onder direct beheer door de Commissie.

6. Enisa brengt ten minste om de twee jaar de diensten in kaart die de in lid 3, punten a) en b), van dit artikel bedoelde gebruikers nodig hebben. Het in kaart brengen omvat ook de beschikbaarheid van dergelijke diensten, onder meer van juridische entiteiten die in de lidstaten gevestigd zijn of geacht worden te zijn gevestigd en waarover lidstaten of onderdanen van lidstaten zeggenschap hebben. Bij het in kaart brengen van die beschikbaarheid beoordeelt Enisa de vaardigheden en capaciteit van de arbeidskrachten op het gebied van de cyberbeveiliging in de Unie, die relevant zijn voor de doelstellingen van de EU-cyberbeveiligingsreserve. Bij het in kaart brengen, raadpleegt Enisa de NIS-samenwerkingsgroep, EU-CyCLONe, de Commissie en, in voorkomend geval, de op grond van artikel 10 van Verordening (EU, Euratom) 2023/2841 opgerichte interinstitutionele raad voor cyberbeveiliging (IICB). Bij het in kaart brengen van de beschikbaarheid van diensten raadpleegt Enisa ook relevante belanghebbenden uit de cyberbeveiligingssector, met inbegrip van aanbieders van beheerde beveiligingsdiensten. Enisa stelt, na de Raad daarvan in kennis te hebben gesteld en na raadpleging van EU-CyCLONe, de Commissie en, indien relevant, de hoge vertegenwoordiger, een soortgelijk overzicht op om de behoeften van de in lid 3, punt c), van dit artikel bedoelde gebruikers vast te stellen.

7. De Commissie is bevoegd overeenkomstig artikel 23 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. Bij de voorbereiding van die gedelegeerde handelingen houdt de Commissie rekening met het in lid 6 van dit artikel bedoelde overzicht en kan zij advies uitwisselen en samenwerken met de NIS-samenwerkingsgroep en Enisa.

Artikel 15

Verzoeken om steun uit de EU-cyberbeveiligingsreserve

1. De in artikel 14, lid 3, bedoelde gebruikers kunnen om diensten van de EU-cyberbeveiligingsreserve verzoeken ter ondersteuning van de respons op en het initiëren van herstel van significante cyberbeveiligingsincidenten, grootschalige cyberbeveiligingsincidenten of aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten.

2. Om steun uit de EU-cyberbeveiligingsreserve te ontvangen, nemen de in artikel 14, lid 3, bedoelde gebruikers alle nodige maatregelen om de gevolgen van het incident waarvoor om steun wordt verzocht te beperken, met inbegrip van, in voorkomend geval, het verlenen van directe technische bijstand en andere middelen om de respons op het incident en de inspanningen voor herstel te ondersteunen.

3. Ondersteuningsverzoeken worden als volgt aan de aanbestedende dienst toegezonden:

a) in het geval van in artikel 14, lid 3, punt a), van deze verordening bedoelde gebruikers via het op grond van artikel 8, lid 3, van Richtlijn (EU) 2022/2555 aangewezen of ingestelde centrale contactpunt;

b) in het geval van de in artikel 1142, lid 3, punt b), bedoelde gebruiker door die gebruiker;

c) in het geval van de in artikel 14, lid 3, punt c), bedoelde gebruikers via het in artikel 19, lid 9, bedoelde centrale contactpunt.

4. In het geval van verzoeken van in artikel 14, lid 3, punt a), bedoelde gebruikers, stellen de lidstaten het CSIRT-netwerk en, in voorkomend geval, EU-CyCLONe in kennis van de verzoeken van hun gebruikers om ondersteuning bij de respons op incidenten en bij het initieel herstel op grond van dit artikel.

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

a) de nodige informatie over de getroffen entiteit en de potentiële gevolgen van het incident voor:

i) in het geval van artikel 14, lid 3, punt a), bedoelde gebruikers, de getroffen lidstaten en gebruikers, met inbegrip van het risico op overloopeffecten naar een andere lidstaat;

- ii) in het geval van de in artikel 14, lid 3, punt b), bedoelde gebruikers, de getroffen instellingen, organen of instanties van de Unie;
 - iii) in het geval van artikel 14, lid 3, punt c), bedoelde gebruikers, de getroffen met het programma Digitaal Europa geassocieerde landen;
- b) informatie over de gevraagde dienst, samen met het geplande gebruik van de gevraagde steun, waaronder een indicatie van de geraamde behoeften;
 - c) de nodige informatie over de maatregelen die zijn genomen om het incident waarvoor om steun wordt verzocht, te beperken, als bedoeld in lid 2;
 - d) in voorkomend geval, beschikbare informatie over andere vormen van steun die beschikbaar zijn voor de getroffen entiteit.
6. In samenwerking met de Commissie en EU-CyCLONe ontwikkelt Enisa een model om de indiening van verzoeken om steun uit de EU-cyberbeveiligingsreserve te vergemakkelijken.
7. De Commissie kan door middel van uitvoeringshandelingen de nadere procedurele regelingen vaststellen voor de wijze waarop om de ondersteunende diensten van de EU-cyberbeveiligingsreserve wordt verzocht en op die verzoeken wordt geantwoord uit hoofde van dit artikel, artikel 16, lid 1, en artikel 19, lid 10, waaronder regelingen voor het indienen van dergelijke verzoeken en het verstrekken van antwoorden en modellen voor de in artikel 16, lid 9, bedoelde verslagen. Die uitvoeringshandelingen worden vastgesteld volgens de in artikel 24, lid 2, bedoelde onderzoeksprocedure.

Artikel 16

Uitvoering van de steun uit de EU-cyberbeveiligingsreserve

1. In het geval van verzoeken van in artikel 14, lid 3, punten a) en b), bedoelde gebruikers worden verzoeken om steun uit de EU-cyberbeveiligingsreserve beoordeeld door de aanbestedende dienst. Om de doeltreffendheid van de steun te waarborgen, wordt onverwijld en in elk geval uiterlijk 48 uur na de indiening van het verzoek een antwoord aan de in artikel 14, lid 3, punten a) en b), bedoelde gebruikers toegezonden. De aanbestedende dienst stelt de Raad en de Commissie in kennis van de resultaten van het proces.
2. Wat betreft informatie die wordt gedeeld bij het verzoeken om en verlenen van de diensten van de EU-cyberbeveiligingsreserve, geldt dat alle bij de toepassing van deze verordening betrokken partijen:
- a) het gebruik en het delen van die informatie beperken tot wat nodig is om hun verplichtingen of functies uit hoofde van deze verordening na te komen of te vervullen;
 - b) alle informatie die vertrouwelijk of gerubriceerd is volgens het Unie- en nationale recht uitsluitend gebruiken en delen in overeenstemming met dat recht, en
 - c) zorgen voor doeltreffende, efficiënte en veilige informatie-uitwisseling, in voorkomend geval door gebruik te maken en het naleven van relevante protocollen voor informatie-uitwisseling, met inbegrip van het verkeerslichtprotocol.
3. Bij de beoordeling van individuele verzoeken uit hoofde van artikel 16, lid 1, en artikel 19, lid 10, beoordeelt de aanbestedende dienst of de Commissie, naargelang het geval, eerst of aan de in artikel 15, leden 1 en 2, bedoelde criteria is voldaan. Als dat het geval is, beoordeelt zij de duur en de aard van de passende steun, rekening houdend met de in artikel 1, lid 3, punt b), genoemde doelstelling en in voorkomend geval de volgende criteria:
- a) de omvang en ernst van het incident;
 - b) het soort getroffen entiteit, met een hogere prioriteit voor incidenten die in artikel 3, lid 1, van Richtlijn (EU) 2022/2555 bedoelde essentiële entiteiten treffen;
 - c) de mogelijke gevolgen van het incident voor de getroffen lidstaten, instellingen, organen of instanties van de Unie, dan wel met het programma Digitaal Europa geassocieerde derde landen;
 - d) de mogelijke landgrensoverschrijdende aard van het incident en het risico op overloopeffecten naar andere lidstaten, instellingen, organen of instanties van de Unie, dan wel met het programma Digitaal Europa geassocieerde derde landen;
 - e) de door de gebruiker genomen maatregelen ter ondersteuning van de respons en inspanningen voor initieel herstel, als bedoeld in artikel 15, lid 2.

4. Onverminderd het beginsel van loyale samenwerking tussen de lidstaten en de instellingen, organen en instanties van de Unie wordt, wanneer door in artikel 14, lid 3, bedoelde gebruikers gelijktijdig verscheidene verzoeken worden ingediend, voor het vaststellen van de prioriteit van de verzoeken in voorkomend geval rekening gehouden met de in lid 3 van dit artikel bedoelde criteria. Wanneer twee of meer verzoeken op grond van die criteria als gelijkwaardig worden beoordeeld, wordt hogere prioriteit gegeven aan verzoeken van gebruikers van de lidstaten. Wanneer de exploitatie en het beheer van de EU-cyberbeveiligingsreserve geheel of gedeeltelijk aan Enisa zijn toevertrouwd uit hoofde van artikel 14, lid 5, werken Enisa en de Commissie nauw samen om prioriteit te geven aan verzoeken overeenkomstig dit lid.

5. De diensten van de EU-cyberbeveiligingsreserve worden verleend in overeenstemming met specifieke overeenkomsten tussen de betrouwbare aanbieder van beheerde beveiligingsdiensten en de gebruiker aan wie de steun in het kader van de EU-cyberbeveiligingsreserve wordt verleend. Die diensten kunnen worden verleend in overeenstemming met specifieke overeenkomsten tussen de betrouwbare aanbieder van beheerde beveiligingsdiensten, de gebruiker en de getroffen entiteit. Alle in dit lid bedoelde overeenkomsten bevatten onder meer aansprakelijkheidsvoorwaarden.

6. De in lid 5 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.

7. De Commissie, Enisa en de gebruikers van de EU-cyberbeveiligingsreserve 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.

8. Gebruikers mogen de diensten uit de EU-cyberbeveiligingsreserve die als respons op een verzoek uit hoofde van artikel 15, lid 1, worden verleend, uitsluitend voor de ondersteuning van de respons op en het initiële herstel van significante cyberbeveiligingsincidenten, grootschalige cyberbeveiligingsincidenten of aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten gebruiken. Zij mogen deze diensten uitsluitend gebruiken voor:

a) in zeer kritieke sectoren actieve entiteiten of in andere kritieke sectoren actieve entiteiten, in het geval van gebruikers als bedoeld in artikel 14, lid 3, punt a), en gelijkwaardige entiteiten in het geval van gebruikers als bedoeld in artikel 14, lid 3, punt c), en

b) instellingen, organen en instanties van de Unie, in het geval van de in artikel 14, lid 3, punt b), bedoelde gebruiker.

9. Binnen twee maanden na het einde van steun verstrekken gebruikers die steun hebben ontvangen een samenvattend verslag over de verleende dienst, de bereikte resultaten en de geleerde lessen, aan:

a) de Commissie, Enisa, het CSIRT-netwerk en EU-CyCLONE in het geval van in artikel 14, lid 3, punt a), bedoelde gebruikers;

b) de Commissie, Enisa en de IIBC in het geval van in artikel 14, lid 3, punt b), bedoelde gebruiker;

c) de Commissie in het geval van in artikel 14, lid 3, punt c), bedoelde gebruikers.

De Commissie zendt elk samenvattend verslag dat zij overeenkomstig dit lid, eerste alinea, punt c), van in artikel 14, lid 3, bedoelde gebruikers heeft ontvangen, toe aan de Raad en de hoge vertegenwoordiger.

10. Wanneer de exploitatie en het beheer van de EU-cyberbeveiligingsreserve geheel of gedeeltelijk aan Enisa zijn toevertrouwd uit hoofde van artikel 14, lid 5, van deze verordening, brengt Enisa dienaangaande regelmatig verslag uit aan en raadpleegt het de Commissie. In dat verband zendt Enisa de Commissie onmiddellijk alle verzoeken toe die het ontvangt van in artikel 14, lid 3, punt c), van deze verordening bedoelde gebruikers en, indien nodig met het oog op prioritering uit hoofde van dit artikel, alle verzoeken die het van in artikel 14, lid 3, punt a) of punt b), van deze verordening bedoelde gebruikers heeft ontvangen. De verplichtingen in dit lid laten artikel 14 van Verordening (EU) 2019/881 onverlet.

11. In het geval van in artikel 14, lid 3, punten a) en b), bedoelde gebruikers brengt de aanbestedende dienst regelmatig en ten minste tweemaal per jaar verslag uit aan de NIS-samenwerkingsgroep over het gebruik en de resultaten van de steun.

12. In het geval van in artikel 14, lid 3, punt c), bedoelde gebruikers brengt de Commissie verslag uit aan de Raad en stelt zij de hoge vertegenwoordiger regelmatig, en ten minste tweemaal per jaar, in kennis van het gebruik en de resultaten van de steun.

Artikel 17

Betrouwbare aanbieders van beheerde beveiligingsdiensten

1. Bij aanbestedingsprocedures voor de instelling van de EU-cyberbeveiligingsreserve handelt de aanbestedende dienst in overeenstemming met de beginselen van Verordening (EU, Euratom) 2024/2509 en met de volgende beginselen:

- a) ervoor zorgen dat de diensten die in de EU-cyberbeveiligingsreserve zijn opgenomen, over het geheel genomen zodanig zijn dat de EU-cyberbeveiligingsreserve diensten omvat die in alle lidstaten kunnen worden verleend, waarbij met name rekening gehouden wordt met nationale vereisten voor het verlenen van dergelijke diensten, met inbegrip van talen, certificering of accreditatie;
- b) de bescherming van de wezenlijke veiligheidsbelangen van de Unie en haar lidstaten waarborgen;
- c) ervoor zorgen dat de EU-cyberbeveiligingsreserve meerwaarde voor de Unie 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 Unie.

2. Bij de aanbesteding van diensten voor de EU-cyberbeveiligingsreserve neemt de aanbestedende dienst in de aanbestedingsdocumenten de volgende criteria en vereisten 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 en continuïteit van de deskundigheid en de vereiste technische middelen;
- b) de aanbieder en alle relevante dochterondernemingen en onderaannemers voldoen aan de toepasselijke regels inzake de bescherming van gerubriceerde informatie en beschikken over passende maatregelen, waaronder, in voorkomend geval, onderlinge overeenkomsten, om vertrouwelijke informatie met betrekking tot de dienst, en met name bewijsmateriaal, bevindingen en verslagen, te beschermen;
- c) de aanbieder levert voldoende bewijs dat zijn bestuursstructuur transparant is, zijn onpartijdigheid en de kwaliteit van zijn diensten niet in het gedrang brengt en geen belangenconflicten veroorzaakt;
- d) de aanbieder beschikt over een passende veiligheidsmachtiging, ten minste voor het personeel dat de dienst gaat verlenen, indien een lidstaat dat vereist;
- e) de aanbieder beschikt over het relevante beveiligingsniveau voor zijn IT-systemen;
- f) de aanbieder beschikt over de hardware en software die nodig zijn om de gevraagde dienst te ondersteunen, die geen bekende kwetsbaarheden bevatten die kunnen worden uitgebuit, de meest recente beveiligingsupdates bevatten en in elk geval voldoen aan alle toepasselijke bepalingen van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad ⁽²³⁾;
- g) de aanbieder kan aantonen dat hij ervaring heeft met het verlenen van soortgelijke diensten aan relevante nationale autoriteiten, in zeer kritieke sectoren actieve entiteiten of in andere 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 een of meer officiële talen van de instellingen van de Unie of van een lidstaat, zoals eventueel vereist door de lidstaat of lidstaten of in artikel 14, lid 3, punten b) en c), bedoelde gebruikers, waar de aanbieder de dienst kan verlenen;
- j) zodra een Europese regeling voor cyberbeveiligingscertificering voor beheerde beveiligingsdiensten op grond van Verordening (EU) 2019/881 van kracht is, wordt de aanbieder binnen twee jaar na de toepassingsdatum van de regeling overeenkomstig die regeling gecertificeerd;

⁽²³⁾ Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Verordening cyberweerbaarheid) (PB L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>).

- k) de aanbieder neemt in de inschrijving de conversievoorwaarden op voor elke ongebruikte incidentresponsdienst die kan worden omgezet in paraatheidsdiensten die nauw verband houden met de respons op incidenten, zoals tests of opleidingen.
3. Met het oog op de aanbesteding van diensten voor de EU-cyberbeveiligingsreserve kan de aanbestedende dienst, in voorkomend geval, in nauwe samenwerking met de lidstaten criteria en vereisten ontwikkelen als aanvulling op de in lid 2 bedoelde criteria.

Artikel 18

Acties ter ondersteuning van wederzijdse bijstand

1. Het noodmechanisme voor cyberbeveiliging verleent steun voor technische bijstand van een lidstaat aan een andere lidstaat die getroffen is door een significant cyberbeveiligingsincident of grootschalig cyberbeveiligingsincident, met inbegrip van in de in artikel 11, lid 3, punt f), van Richtlijn (EU) 2022/2555 bedoelde gevallen.
2. De steun voor technische wederzijdse bijstand als bedoeld in lid 1 van dit artikel wordt verleend in de vorm van subsidies en onder de voorwaarden die zijn vastgesteld in de desbetreffende werkprogramma's als bedoeld in artikel 24 van Verordening (EU) 2021/69.

Artikel 19

Steun aan met het programma Digitaal Europa geassocieerde derde landen

1. Een met het programma Digitaal Europa geassocieerd derde land kan om steun uit de EU-cyberbeveiligingsreserve verzoeken indien de overeenkomst, op grond waarvan het geassocieerd is met het programma Digitaal Europa, voorziet in deelname aan de EU-cyberbeveiligingsreserve. Die overeenkomst bevat bepalingen die het met het programma Digitaal Europa geassocieerde derde land verplichten de in de leden 2 en 9 van dit artikel genoemde verplichtingen na te komen. Ten behoeve van de deelname van een derde land aan de EU-cyberbeveiligingsreserve kan de gedeeltelijke associatie van een derde land met het programma Digitaal Europa een associatie omvatten die beperkt is tot de in artikel 6, lid 1, punt g), van Verordening (EU) 2021/694 bedoelde operationele doelstelling.
2. Binnen drie maanden na de sluiting van de in lid 1 bedoelde overeenkomst en in ieder geval voordat zij steun uit de EU-cyberbeveiligingsreserve ontvangen, verstrekken de met het programma Digitaal Europa geassocieerde derde landen de Commissie informatie over hun cyberweerbaarheid en risicobeheercapaciteiten, met inbegrip van ten minste informatie over nationale maatregelen ter voorbereiding op significante cyberbeveiligingsincidenten of aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten, alsook informatie over verantwoordelijke nationale entiteiten, met inbegrip van computer security incident response teams of gelijkwaardige entiteiten, hun capaciteiten en de daaraan toegewezen middelen. Het met het programma Digitaal Europa geassocieerde derde land actualiseert die informatie regelmatig en ten minste eenmaal per jaar. De Commissie verstrekt de hoge vertegenwoordiger en Enisa die informatie om de toepassing van lid 11 te vergemakkelijken.
3. De Commissie beoordeelt regelmatig, en ten minste eenmaal per jaar, de volgende criteria met betrekking tot elk in lid 1 bedoeld met het programma Digitaal Europa geassocieerde derde land:
- a) of dat land de voorwaarden van de in lid 1 bedoelde overeenkomst naleeft, voor zover die voorwaarden betrekking hebben op deelname aan de EU-cyberbeveiligingsreserve;
 - b) of dat land passende maatregelen heeft genomen om zich voor te bereiden op significante cyberbeveiligingsincidenten of aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten, op basis van de in lid 2 bedoelde informatie, en
 - c) of de steunverlening in overeenstemming is met het beleid van de Unie ten aanzien van en met de algemene betrekkingen met dat land en of deze steun verenigbaar is met ander beleid van de Unie op het gebied van veiligheid.

De Commissie raadpleegt de hoge vertegenwoordiger bij de uitvoering van de in de eerste alinea bedoelde beoordeling met betrekking tot het in punt c) van die alinea bedoelde criterium.

Indien de Commissie concludeert dat een met het programma Digitaal Europa geassocieerd derde land aan alle in de eerste alinea bedoelde voorwaarden voldoet, dient de Commissie bij de Raad een voorstel in om overeenkomstig lid 4 een uitvoeringshandeling vast te stellen waarbij toestemming wordt verleend voor het verlenen van steun uit de EU-cyberbeveiligingsreserve aan dat land.

4. De Raad kan de in lid 3 bedoelde uitvoeringshandelingen vaststellen. Die uitvoeringshandelingen zijn van toepassing gedurende ten hoogste één jaar. De geldigheidsduur daarvan kan worden verlengd. Zij kunnen een limiet bevatten, die niet minder dan 75 dagen mag zijn, voor het aantal dagen waarvoor in antwoord op één verzoek ondersteuning kan worden geboden.

Voor de toepassing van dit artikel handelt de Raad snel en stelt de in dit lid bedoelde uitvoeringshandelingen in de regel binnen acht weken na goedkeuring van het desbetreffende voorstel van de Commissie op grond van lid 3, derde alinea, vast.

5. De Raad kan een op grond van lid 3 vastgestelde uitvoeringshandeling te allen tijde op voorstel van de Commissie wijzigen of intrekken.

Wanneer de Raad van oordeel is dat zich een significante verandering heeft voorgedaan met betrekking tot het in lid 3, eerste alinea, punt c), bedoelde criterium, kan de Raad een op grond van lid 4 vastgestelde uitvoeringshandeling wijzigen of intrekken op grond van een met redenen omkleed initiatief van een of meer lidstaten.

6. Bij de uitoefening van zijn uitvoeringsbevoegdheden uit hoofde van dit artikel past de Raad de in lid 3, eerste alinea, bedoelde criteria toe en licht hij zijn beoordeling van die criteria toe. Met name wanneer de Raad uit hoofde van lid 5, tweede alinea, op eigen initiatief besluit, licht hij de significante verandering als bedoeld in die alinea toe.

7. Steun uit de EU-cyberbeveiligingsreserve aan een met het programma Digitaal Europa geassocieerd derde land voldoet aan alle specifieke voorwaarden die in de in lid 1 bedoelde overeenkomst zijn vastgesteld.

8. Tot de gebruikers uit met het programma Digitaal Europa geassocieerde derde landen die in aanmerking komen om diensten uit de EU-cyberbeveiligingsreserve te ontvangen, behoren bevoegde autoriteiten zoals computer security incident and response Teams of gelijkwaardige entiteiten en cybercrisisbeheerautoriteiten.

9. Elk met het programma Digitaal Europa geassocieerd 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.

10. Verzoeken om steun uit de EU-cyberbeveiligingsreserve uit hoofde van dit artikel worden beoordeeld door de Commissie. De aanbestedende dienst mag alleen steun verlenen aan een derde land indien en zolang een op grond van lid 4 van dit artikel vastgestelde uitvoeringshandeling van de Raad waarbij dergelijke steun ten aanzien van dat land wordt toegestaan, van kracht is. Een antwoord wordt onverwijld toegezonden aan de in artikel 14, lid 3, punt c), bedoelde gebruikers.

11. Na ontvangst van een verzoek om steun uit hoofde van dit artikel stelt de Commissie de Raad daarvan onverwijld in kennis. De Commissie houdt de Raad op de hoogte van de beoordeling van het verzoek. De Commissie werkt ook samen met de hoge vertegenwoordiger met betrekking tot de ontvangen verzoeken en de uitvoering van de steun aan met het programma Digitaal Europa geassocieerde derde landen uit de EU-cyberbeveiligingsreserve. Daarnaast houdt de Commissie ook rekening met eventuele standpunten van Enisa met betrekking tot die verzoeken.

Artikel 20

Coördinatie met crisisbeheersingsmechanismen van de Unie

1. In gevallen waarin een significant cyberbeveiligingsincident, een grootschalig cyberbeveiligingsincident of een aan grootschalige cyberbeveiligingsincidenten gelijkwaardig incident voortkomt uit of resulteert in een ramp zoals gedefinieerd in artikel 4, punt 1, van Besluit 1313/2013/EU, vormt de steun uit hoofde van deze verordening voor de respons op dergelijke incidenten een aanvulling op acties uit hoofde van, en geldt onverminderd, dat besluit.

2. In het geval van een grootschalig cyberbeveiligingsincident of een aan grootschalige cyberbeveiligingsincidenten gelijkwaardig incident waarbij de geïntegreerde EU-regeling politieke crisisrespons uit hoofde van Uitvoeringsbesluit (EU) 2018/1993 ("ICPR-regeling") geactiveerd wordt, wordt de steun uit hoofde van deze verordening voor de respons op een dergelijk incident behandeld overeenkomstig de relevante procedures in het kader van de ICPR-regeling.

HOOFDSTUK IV

EUROPEES EVALUATIEMECHANISME VOOR CYBERBEVEILIGINGSINCIDENTEN

*Artikel 21***Europees evaluatiemechanisme voor cyberbeveiligingsincidenten**

1. Op verzoek van de Commissie of EU-CyCLONe, met steun van het CSIRT-netwerk en met goedkeuring van de betrokken lidstaten evalueert en beoordeelt Enisa cyberdreigingen, bekende kwetsbaarheden die kunnen worden uitgebuit, en mitigerende maatregelen met betrekking tot een specifiek significant cyberbeveiligingsincident of grootschalig cyberbeveiligingsincident. Na de voltooiing van een evaluatie en beoordeling van een incident verstrekt Enisa, teneinde daaruit lering te trekken om toekomstige incidenten te voorkomen of te beperken, een evaluatieverslag over het incident aan EU-CyCLONe, het CSIRT-netwerk, de betrokken lidstaten 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. Wanneer een incident gevolgen heeft voor een met het programma Digitaal Europa geassocieerd derde land, verstrekt Enisa het verslag aan de Raad. In die gevallen verstrekt de Commissie het verslag aan de hoge vertegenwoordiger.
2. Om het in lid 1 van dit artikel bedoelde evaluatieverslag over het incident op te stellen, werkt Enisa samen, en verzamelt feedback van, alle relevante belanghebbenden, waaronder vertegenwoordigers van de lidstaten, de Commissie, andere relevante EU-instellingen, -organen en -instanties, de sector, waaronder aanbieders van beheerde beveiligingsdiensten, en gebruikers van cyberbeveiligingsdiensten. In voorkomend geval werkt Enisa, in overleg met CSIRT's en, indien relevant, met uit hoofde van artikel 8, lid 1, van Richtlijn (EU) 2022/2555 aangewezen of ingestelde autoriteiten, ook samen met entiteiten die getroffen zijn door significante cyberbeveiligingsincidenten of grootschalige cyberbeveiligingsincidenten. De geraadpleegde vertegenwoordigers maken elk mogelijk belangenconflict bekend.
3. Het in lid 1 van dit artikel bedoelde evaluatieverslag over het incident omvat een evaluatie en analyse van het specifieke significante cyberbeveiligingsincident of grootschalige cyberbeveiligingsincident, met inbegrip van de belangrijkste oorzaken, bekende kwetsbaarheden die kunnen worden uitgebuit en geleerde lessen. Enisa zorgt ervoor dat het verslag voldoet aan het Unie- of nationale recht inzake de bescherming van gevoelige of gerubriceerde informatie. Indien de betrokken lidstaten of andere in artikel 14, lid 3, bedoelde gebruikers die zijn getroffen door het incident daarom verzoeken, zijn de gegevens en informatie van het verslag alleen geanonimiseerde gegevens. Het verslag bevat geen details over actief uitgebuite kwetsbaarheden die nog niet verholpen zijn.
4. In voorkomend geval worden in het evaluatieverslag over het incident aanbevelingen gedaan om de cyberstrategie van de Unie te verbeteren en kan het verslag beste praktijken en geleerde lessen van relevante belanghebbenden bevatten.
5. Enisa kan een openbaar beschikbare versie van het evaluatieverslag over het incident uitbrengen. Die versie van het verslag bevat uitsluitend betrouwbare openbare informatie, of andere informatie met toestemming van de betrokken lidstaat of lidstaten, en, wat betreft informatie over een in artikel 14, lid 3, punt b) of punt c), bedoelde gebruiker, met toestemming van die gebruiker.

HOOFDSTUK V

SLOTBEPALINGEN

*Artikel 22***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 wordt ingevoegd:

“a bis) ondersteunen van de ontwikkeling van het Europees waarschuwingssysteem voor cyberbeveiliging dat is opgericht bij artikel 3 van Verordening (EU) 2025/38 van het Europees Parlement en de Raad (*) (het “Europees waarschuwingssysteem voor cyberbeveiliging”), met inbegrip van de ontwikkeling, uitrol en exploitatie van nationale cyberhubs en landsgrensoverschrijdende cyberhubs die bijdragen tot het situationeel bewustzijn in de Unie en tot de versterking van de inlichtingencapaciteit van de Unie op het gebied van cyberdreigingen;

(*) Verordening (EU) 2025/38 van het Europees Parlement en de Raad van 19 december 2024 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 (verordening cybersolidariteit) (PB L, 2025/38, 15.1.2025, ELI: <http://data.europa.eu/eli/reg/2025/38/oj>).”;

ii) het volgende punt wordt toegevoegd:

“g) instellen en beheren van het noodmechanisme voor cyberbeveiliging dat is ingesteld bij artikel 10 van Verordening (EU) 2025/38, met inbegrip van de bij artikel 14 van die verordening ingestelde EU-cyberbeveiligingsreserve (de “EU-cyberbeveiligingsreserve”), om de lidstaten te ondersteunen bij de voorbereiding en respons op significante cyberbeveiligingsincidenten en grootschalige cyberbeveiligingsincidenten, in aanvulling op de nationale middelen en capaciteiten en andere vormen van steun die op het niveau van de Unie beschikbaar zijn, en om andere gebruikers te ondersteunen bij de respons op significante cyberbeveiligingsincidenten en aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten.”;

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 (*). De EU-cyberbeveiligingsreserve wordt echter door de Commissie en, overeenkomstig artikel 14, lid 6, van Verordening (EU) 2025/38, door Enisa 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).”.

2) Artikel 9 wordt als volgt gewijzigd:

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

“b) 1 760 806 000 EUR voor specifieke doelstelling 2 — Artificiële intelligentie;

c) 1 372 020 000 EUR voor specifieke doelstelling 3 — Cyberbeveiliging en vertrouwen;

d) 482 640 000 EUR voor specifieke doelstelling 4 — Geavanceerde digitale vaardigheden.”;

b) het volgende lid wordt toegevoegd:

“8. In afwijking van artikel 12, lid 1, van de het Financieel Reglement worden ongebruikte vastleggings- en betalingskredieten voor acties in het kader van de uitvoering van de EU-cyberbeveiligingsreserve en de acties ter ondersteuning van wederzijdse bijstand op grond van Verordening (EU) 2025/38 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. Het Europees Parlement en de Raad worden van op grond van artikel 12, lid 6, van het Financieel Reglement overgedragen kredieten in kennis gesteld.”.

3) Artikel 12 wordt als volgt gewijzigd:

a) de volgende leden worden ingevoegd:

“5 bis. Lid 5 is, wat betreft juridische entiteiten die in de Unie zijn gevestigd maar onder zeggenschap staan van derde landen, niet van toepassing op acties ter uitvoering van het Europees waarschuwingssysteem voor cyberbeveiliging indien met betrekking tot de betreffende actie aan beide volgende voorwaarden is voldaan:

- a) er bestaat een reëel risico, rekening houdend met de resultaten van de op grond van artikel 9, lid 4, van Verordening (EU) 2025/38 uitgevoerde inventarisatie, dat de instrumenten, infrastructuur of diensten die nodig en toereikend zijn voor die actie om adequaat bij te dragen aan de doelstelling van het Europees waarschuwingssysteem voor cyberbeveiliging, niet beschikbaar zullen zijn bij juridische entiteiten die in de lidstaten gevestigd zijn of geacht worden te zijn gevestigd en waarover lidstaten of onderdanen van lidstaten zeggenschap hebben, en
- b) het veiligheidsrisico van aankopen bij dergelijke juridische entiteiten binnen het Europees waarschuwingssysteem voor cyberbeveiliging is evenredig aan de voordelen en vormt geen ondermijning van de wezenlijke veiligheidsbelangen van de Unie en haar lidstaten.

5 ter. Lid 5 is, wat betreft juridische entiteiten die in de Unie zijn gevestigd maar onder zeggenschap staan van derde landen, niet van toepassing op acties ter uitvoering van de EU-cyberbeveiligingsreserve indien met betrekking tot de betreffende actie aan beide volgende voorwaarden is voldaan:

- a) er bestaat een reëel risico, rekening houdend met de resultaten van de op grond van artikel 14, lid 6, van Verordening (EU) 2025/38 uitgevoerde inventarisatie, dat de technologie, expertise of capaciteit die nodig en toereikend zijn voor de EU-cyberbeveiligingsreserve om adequaat zullen zijn taken uit te voeren, niet beschikbaar zijn bij juridische entiteiten die in de lidstaten gevestigd zijn of geacht worden te zijn gevestigd en waarover lidstaten of onderdanen van lidstaten zeggenschap hebben;
- b) het veiligheidsrisico van de opnemings van dergelijke juridische entiteiten binnen de EU-cyberbeveiligingsreserve is evenredig aan de voordelen en vormt geen ondermijning van de wezenlijke veiligheidsbelangen van de Unie en haar lidstaten.”;

b) lid 6 wordt vervangen door:

“6. Om naar behoren gemotiveerde veiligheidsredenen kan in het werkprogramma ook worden bepaald dat juridische entiteiten die in geassocieerde landen zijn gevestigd en juridische entiteiten die in de Unie zijn gevestigd, maar waarover vanuit derde landen zeggenschap wordt uitgeoefend, alleen in aanmerking komen voor deelname aan alle of bepaalde acties in het kader van specifieke doelstellingen 1 en 2 indien zij voldoen aan de vereisten waaraan die juridische entiteiten moeten voldoen om de bescherming van de wezenlijke veiligheidsbelangen van de Unie en de lidstaten te waarborgen en de bescherming van de gegevens in gerubriceerde documenten te verzekeren. Die vereisten worden in het werkprogramma vastgelegd.

De eerste alinea is, wat betreft juridische entiteiten die in de Unie zijn gevestigd maar onder zeggenschap staan van derde landen, ook van toepassing op acties in het kader van specifieke doelstelling 3:

- a) ter uitvoering van het Europees waarschuwingssysteem voor cyberbeveiliging wanneer lid 5 bis van toepassing is, en
- b) ter uitvoering van de EU-cyberbeveiligingsreserve wanneer lid 5 ter van toepassing is.”.

4) In artikel 14 wordt lid 2 vervangen door:

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

Als voor het verwezenlijken van de doelstelling van een actie de aanbesteding van innovatieve goederen en diensten vereist is, kunnen subsidies uitsluitend worden toegekend aan begunstigden die aanbestedende diensten of aanbestedende instanties zijn als gedefinieerd in de Richtlijnen 2014/24/EU (*) en 2014/25/EU (**) 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 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 van deze verordening. 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 168, lid 3, van Verordening (EU, Euratom) 2024/2509 van het Europees Parlement en de Raad (***) 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 EU-cyberbeveiligingsreserve kunnen de Commissie en Enisa optreden als aankoopcentrale voor aanbestedingen namens of in naam van instellingen, organen of 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 of instanties van de Unie door te verkopen of te schenken. In afwijking van artikel 168, lid 3, van Verordening (EU, Euratom) 2024/2509 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.

- (*) 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).
- (**) Richtlijn 2014/25/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende het plaatsen van opdrachten in de sectoren water- en energievoorziening, vervoer en postdiensten en houdende intrekking van Richtlijn 2004/17/EG (PB L 94 van 28.3.2014, blz. 243).
- (***) Verordening (EU, Euratom) 2024/2509 van het Europees Parlement en de Raad van 23 september 2024 tot vaststelling van de financiële regels van toepassing op de algemene begroting van de Unie (PB L, 2024/2509, 26.9.2024, ELI: <http://data.europa.eu/eli/reg/2024/2509/oj>).

5) Het volgende artikel wordt toegevoegd:

“Artikel 16 bis

Strijdigheid van bepalingen

In het geval van acties ter uitvoering van het Europees waarschuwingssysteem voor cyberbeveiliging zijn de toepasselijke regels die van de artikelen 4, 5 en 9 van Verordening (EU) 2025/38. In geval van strijdigheid tussen de bepalingen van deze verordening en de artikelen 4, 5 en 9 van Verordening (EU) 2025/38 hebben laatstgenoemde bepalingen voorrang en zijn zij op die specifieke acties van toepassing.

In het geval van acties ter uitvoering van de EU-cyberbeveiligingsreserve zijn specifieke regels voor de deelname van met het programma geassocieerde derde landen vastgesteld in artikel 19 van Verordening (EU) 2025/38. In geval van strijdigheid tussen de bepalingen van deze verordening en artikel 19 van Verordening (EU) 2025/38 hebben laatstgenoemde bepalingen voorrang en zijn zij op die specifieke acties van toepassing.”.

6) Artikel 19 wordt vervangen door:

“Artikel 19

Subsidies

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

Zonder oproep tot het indienen van voorstellen kan het ECCC steun in de vorm van subsidies rechtstreeks toekennen aan de op grond van artikel 9 van Verordening (EU) 2025/38 geselecteerde lidstaten en het in artikel 5 van Verordening (EU) 2025/38 bedoelde onderbrengend consortium, overeenkomstig artikel 195, lid 1, punt d), van het Financieel Reglement.

Steun in de vorm van subsidies voor het noodmechanisme voor cyberbeveiliging kan door het ECCC rechtstreeks aan de lidstaten worden toegekend zonder een oproep tot het indienen van voorstellen, overeenkomstig artikel 195, lid 1, punt d), van het Financieel Reglement.

Ten aanzien van in artikel 18 van Verordening (EU) 2025/38 gespecificeerde acties stelt het ECCC de Commissie en Enisa in kennis van verzoeken van lidstaten om rechtstreekse subsidies zonder een oproep tot het indienen van voorstellen.

Ten aanzien van acties ter ondersteuning van wederzijdse bijstand zoals bepaald in artikel 18 van Verordening (EU) 2025/38, en overeenkomstig artikel 193, lid 2, tweede alinea, punt a), van het Financieel Reglement, kunnen in naar behoren gemotiveerde gevallen de kosten als subsidiabel worden beschouwd, zelfs als zij vóór de indiening van de subsidieaanvraag zijn gemaakt.”.

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

Artikel 23

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 14, lid 7, bedoelde bevoegdheid om gedelegeerde handelingen vast te stellen wordt aan de Commissie toegekend voor een voor verlenging in aanmerking komende termijn van vijf jaar met ingang vanaf 5 februari 2025. De Commissie stelt uiterlijk negen maanden voor het einde van de termijn van vijf 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 17, 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 op grond van artikel 14, 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 de handeling aan het Europees Parlement en de Raad bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad voor het verstrijken van die termijn de Commissie hebben meegedeeld dat zij daartegen geen bezwaar zullen maken. Die termijn wordt op initiatief van het Europees Parlement of de Raad met twee maanden verlengd.

Artikel 24

Comitéprocedure

1. De Commissie wordt bijgestaan door het in artikel 31, lid 1, van 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 25

Evaluatie en herziening

1. Uiterlijk op 5 februari 2027 en vervolgens ten minste om de vier 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. De in lid 1 bedoelde evaluatie beoordeelt met name:
 - a) het aantal opgerichte nationale cyberhubs en landsgrensoverschrijdende cyberhubs, de omvang van de gedeelde informatie, met inbegrip van, indien mogelijk, de impact op de werkzaamheden van het CSIRT-netwerk, en de mate waarin deze hebben bijgedragen tot de versterking van de gemeenschappelijke opsporing en het gemeenschappelijke situationeel bewustzijn van cyberdreigingen en -incidenten in de Unie en tot de ontwikkeling van geavanceerde technologieën; het gebruik van financiering uit het programma Digitaal Europa voor gezamenlijk verworven instrumenten, infrastructuur, of diensten op het gebied van cyberbeveiliging, en indien de informatie beschikbaar is, de

mate van samenwerking tussen nationale cyberhubs en sectorale en sectoroverschrijdende gemeenschappen van in artikel 3 van Richtlijn (EU) 2022/2555 bedoelde essentiële en belangrijke entiteiten;

- b) het gebruik en de doeltreffendheid van acties in het kader van het noodmechanisme voor cyberbeveiliging ter ondersteuning van de paraatheid, met inbegrip van opleidingen, respons op en initieel herstel van significante cyberbeveiligingsincidenten, grootschalige cyberbeveiligingsincidenten en aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten, met inbegrip van het gebruik van financiering uit het programma Digitaal Europa en de geleerde lessen van en aanbevelingen naar aanleiding van de uitvoering van het noodmechanisme voor cyberbeveiliging;
 - c) het gebruik en de doeltreffendheid van de EU-cyberbeveiligingsreserve met betrekking tot de soorten gebruiker, met inbegrip van het gebruik van financiering uit het programma Digitaal Europa, het gebruik van diensten, met inbegrip van het soort diensten, de gemiddelde tijd om op de verzoeken te reageren en de EU-cyberbeveiligingsreserve in te zetten, het percentage diensten dat is omgezet in paraatheidsdiensten in verband met de preventie en respons op incidenten en de geleerde lessen van en aanbevelingen naar aanleiding van de uitvoering van de EU-cyberbeveiligingsreserve;
 - d) de bijdrage van deze verordening aan het versterken van de concurrentiepositie van de industrie en diensten van de digitale economie in de Unie, met inbegrip van micro-ondernemingen en kleine en middelgrote ondernemingen en start-ups, en de bijdrage aan de verwezenlijking van de algemene doelstelling om de vaardigheden en capaciteiten van de arbeidskrachten te versterken.
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 26

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 Brussel, 19 december 2024.

Voor het Europees Parlement

De voorzitter

R. METSOLA

Voor de Raad

De voorzitter

BÓKA J.

BIJLAGE

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

1) In bijlage I wordt de afdeling “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 cyberhubs en landsgrensoverschrijdende cyberhubs, die het Europees waarschuwingssysteem voor cyberbeveiliging 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, rekening houdend met het genderevenwicht, bijvoorbeeld door programma's betreffende cyberbeveiligingsvaardigheden op elkaar af te stemmen, deze aan te passen aan de specifieke behoeften van sectoren en de toegang tot gerichte, gespecialiseerde opleiding te vergemakkelijken.
5. Het bevorderen van solidariteit tussen de lidstaten bij de voorbereiding en respons op significante cyberbeveiligingsincidenten en grootschalige 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 “Specifieke doelstelling 3 — Cyberbeveiliging en vertrouwen” vervangen door:

“Specifieke doelstelling 3 — Cyberbeveiliging en vertrouwen

- 3.1. Het aantal gezamenlijk verworven infrastructuurvoorzieningen en/of instrumenten, ook in het kader van het Europees waarschuwingssysteem voor cyberbeveiliging
- 3.2. Het aantal gebruikers en gemeenschappen van gebruikers die toegang hebben tot Europese voorzieningen inzake cyberbeveiliging
- 3.3 Het aantal acties ter ondersteuning van de paraatheid voor en de respons op cyberbeveiligingsincidenten in het kader van het noodmechanisme voor cyberbeveiliging”.

Er is een verklaring met betrekking tot deze verordening opgesteld, die te vinden is in PB C, C/2025/308, 15.1.2025, ELI: <http://data.europa.eu/eli/C/2025/308/oj>.