Europees Parlement
2019-2024

Commissie buitenlandse zaken

2023/0109(COD)

27.10.2023

ADVIES

van de Commissie buitenlandse zaken

aan de Commissie industrie, onderzoek en energie

inzake het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van maatregelen ter versterking van de solidariteit en de capaciteit in de Unie om cyberdreigingen en -incidenten op te sporen, zich erop voor te bereiden en erop te reageren
(COM(2023/0209) – C9-0136/2023 – 2023/0109(COD))

Rapporteur voor advies: Dragoş Tudorache

PA_Legam

Amendement 1

Voorstel voor een verordening
Overweging 1

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

Amendement 2

Voorstel voor een verordening
Overweging 2

Door de Commissie voorgestelde tekst	*Amendement*
(2) De omvang, frequentie en impact van cyberbeveiligingsincidenten nemen toe, met inbegrip van aanvallen op toeleveringsketens (“supplychainaanvallen”) met het oog op cyberspionage, gijzelsoftware of verstoring. Zij vormen een grote bedreiging voor het functioneren van netwerk- en informatiesystemen. Gelet op het snel veranderende dreigingslandschap vereist de dreiging van mogelijke grootschalige incidenten die aanzienlijke verstoringen of schade aan kritieke infrastructuur veroorzaken, een grotere paraatheid op alle niveaus van het cyberbeveiligingskader van de Unie. Deze ***dreiging gaat*** verder dan de militaire agressie van Rusland tegen Oekraïne en ***zal*** waarschijnlijk aanhouden gezien het grote aantal staatsgebonden criminele en hacktivistische actoren ***die*** betrokken ***zijn*** bij de huidige geopolitieke spanningen. Dergelijke incidenten kunnen de verlening	(2) De omvang, frequentie en impact van cyberbeveiligingsincidenten nemen toe, met inbegrip van aanvallen op toeleveringsketens (“supplychainaanvallen”) met het oog op cyberspionage, gijzelsoftware of verstoring. Zij vormen een grote bedreiging voor het functioneren van netwerk- en informatiesystemen. Gelet op het snel veranderende dreigingslandschap vereist de dreiging van mogelijke grootschalige incidenten die aanzienlijke verstoringen of schade aan kritieke infrastructuur veroorzaken, een grotere paraatheid op alle niveaus van het cyberbeveiligingskader van de Unie. ***De ernst van deze dreigingen is nog groter geworden door de terugkeer van oorlog op ons continent. Deze dreigingen gaan*** verder dan de militaire agressie van Rusland tegen Oekraïne en ***zullen*** waarschijnlijk aanhouden gezien het grote aantal staatsgebonden criminele en

van openbare diensten en de uitoefening van economische activiteiten, ook in kritieke of zeer kritieke sectoren, belemmeren, aanzienlijke financiële verliezen veroorzaken, het vertrouwen van de gebruikers ondermijnen, grote schade toebrengen aan de economie van de Unie, en zelfs gevolgen voor de gezondheid of levensbedreigende gevolgen hebben. Bovendien zijn cyberbeveiligingsincidenten onvoorspelbaar, aangezien zij vaak zeer snel ontstaan en evolueren, niet beperkt zijn tot een specifiek geografisch gebied en zich gelijktijdig of onmiddellijk over vele landen verspreiden.

hacktivistische actoren ***dat*** betrokken ***is*** bij de huidige geopolitieke spanningen. Dergelijke incidenten kunnen de verlening van openbare diensten en de uitoefening van economische activiteiten, ook in kritieke of zeer kritieke sectoren, belemmeren, aanzienlijke financiële verliezen veroorzaken, het vertrouwen van de gebruikers ondermijnen, grote schade toebrengen aan de economie ***en de veiligheid*** van de Unie, en zelfs gevolgen voor de gezondheid of levensbedreigende gevolgen hebben ***doordat zij lokale of nationale veiligheidsgerelateerde installaties kunnen ondermijnen***. Bovendien zijn cyberbeveiligingsincidenten onvoorspelbaar, aangezien zij vaak zeer snel ontstaan en evolueren, niet beperkt zijn tot een specifiek geografisch gebied en zich gelijktijdig of onmiddellijk over vele landen verspreiden. ***Cyberbeveiliging speelt een belangrijke rol bij het beschermen van onze Europese waarden en waarborgt het functioneren van onze democratieën door onze verkiezingsinfrastructuur en democratische procedures tegen buitenlandse inmenging te beschermen.***

Amendement 3

Voorstel voor een verordening
Overweging 2 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(2 bis) Cyberbeveiliging is van cruciaal belang om onze Unie veilig te houden en te voorkomen dat kwaadwillige statelijke en niet-statelijke actoren onze democratie, economie en veiligheid ondermijnen. Een versnipperd landschap moet worden voorkomen aangezien een dergelijke situatie geen deugdelijke aanpak zou vormen, met name gezien de uitdaging van toekomstige grootschalige cyberaanvallen op meerdere lidstaten

	tegelijk of op transnationale kritieke infrastructuur. Het is dan ook noodzaak een orgaan van de Unie aan te wijzen dat kan optreden als coördinatieplatform voor alle bestaande en toekomstige instrumenten, middelen en mechanismen op het gebied van cyberbeveiliging.

Amendement 4

Voorstel voor een verordening
Overweging 3

Door de Commissie voorgestelde tekst	*Amendement*
(3) De concurrentiepositie van de industrie en de dienstensector in de Unie in de gedigitaliseerde economie moet worden versterkt en de digitale transformatie ervan moet worden ondersteund door het niveau van cyberbeveiliging in de digitale eengemaakte markt te verhogen. Zoals aanbevolen in drie verschillende voorstellen van de Conferentie over de toekomst van Europa[16], is het noodzakelijk om burgers, bedrijven en entiteiten die kritieke infrastructuur exploiteren weerbaarder te maken tegen de toenemende cyberbedreigingen, die verwoestende maatschappelijke en economische gevolgen kunnen hebben. Daarom is er behoefte aan investeringen in infrastructuur en diensten ter ondersteuning van een snellere opsporing van en respons op cyberdreigingen en -incidenten, en hebben de lidstaten bijstand nodig om zich beter voor te bereiden en beter te kunnen reageren op significante en grootschalige cyberbeveiligingsincidenten. De Unie zou ook haar capaciteit op deze gebieden moeten vergroten, met name wat betreft het verzamelen en analyseren van gegevens over cyberdreigingen en -incidenten.	(3) De concurrentiepositie van de industrie en de dienstensector in de Unie in de gedigitaliseerde economie moet worden versterkt en de digitale transformatie ervan moet worden ondersteund door het niveau van cyberbeveiliging in de digitale eengemaakte markt te verhogen. Zoals aanbevolen in drie verschillende voorstellen van de Conferentie over de toekomst van Europa[16], is het noodzakelijk om burgers, bedrijven en entiteiten die kritieke infrastructuur exploiteren weerbaarder te maken tegen de toenemende cyberbedreigingen, die verwoestende maatschappelijke en economische gevolgen kunnen hebben. Daarom is er behoefte aan investeringen in infrastructuur en diensten ter ondersteuning van een snellere opsporing van en respons op cyberdreigingen en -incidenten, en hebben de lidstaten bijstand nodig om zich beter voor te bereiden en beter te kunnen reageren op significante en grootschalige cyberbeveiligingsincidenten. De Unie zou ook haar capaciteit op deze gebieden moeten vergroten, met name wat betreft het verzamelen en analyseren van gegevens over cyberdreigingen en -incidenten ***alsook haar vermogen om proactief te handelen en in dergelijke gevallen doortastend te reageren***.
_____	_____

[16] https://futureu.europa.eu/en/

[16] https://futureu.europa.eu/en/

Amendement 5

Voorstel voor een verordening
Overweging 4

Door de Commissie voorgestelde tekst	*Amendement*
(4) De Unie heeft reeds een aantal maatregelen genomen om kritieke infrastructuur en entiteiten minder kwetsbaar te maken voor en weerbaarder te maken tegen cyberbeveiligingsrisico's, met name Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad[17], Aanbeveling (EU) 2017/1584 van de Commissie[18], Richtlijn 2013/40/EU van het Europees Parlement en de Raad[19] en Verordening (EU) 2019/881 van het Europees Parlement en de Raad[20]. Daarnaast wordt de lidstaten in de aanbeveling van de Raad betreffende een Uniebrede gecoördineerde aanpak om de weerbaarheid van kritieke infrastructuur te versterken, verzocht dringende en doeltreffende maatregelen te nemen en loyaal, efficiënt, solidair en gecoördineerd met elkaar, de Commissie en andere relevante overheidsinstanties alsook de betrokken entiteiten samen te werken om kritieke infrastructuur die wordt gebruikt om essentiële diensten op de interne markt te verlenen weerbaarder te maken.	(4) De Unie heeft reeds een aantal maatregelen genomen om kritieke infrastructuur en entiteiten minder kwetsbaar te maken voor en weerbaarder te maken tegen cyberbeveiligingsrisico's, met name Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad[17], Aanbeveling (EU) 2017/1584 van de Commissie[18], Richtlijn 2013/40/EU van het Europees Parlement en de Raad[19] en Verordening (EU) 2019/881 van het Europees Parlement en de Raad[20]. Daarnaast wordt de lidstaten in de aanbeveling van de Raad betreffende een Uniebrede gecoördineerde aanpak om de weerbaarheid van kritieke infrastructuur te versterken, verzocht dringende en doeltreffende maatregelen te nemen en loyaal, efficiënt, ***proactief,*** solidair en gecoördineerd met elkaar, de Commissie en andere relevante overheidsinstanties alsook de betrokken entiteiten samen te werken om kritieke infrastructuur die wordt gebruikt om essentiële diensten op de interne markt te verlenen weerbaarder te maken. ***Voorts heeft de Unie in maart 2022 het strategisch kompas voor veiligheid en defensie goedgekeurd en gelanceerd, dat onder meer gericht is op het versterken van de cyberbeveiliging en het vergroten van de internationale samenwerking met gelijkgestemde bondgenoten en democratische partners, met name op dit gebied. Cyberbeveiliging staat bovendien centraal in de recente derde gezamenlijke verklaring over de samenwerking tussen de EU en de NAVO van januari 2023. Met name werd in het definitieve beoordelingsverslag van de***

EU-NAVO-taskforce aanbevolen ten volle gebruik te maken van synergieën tussen de EU en de NAVO [1], waaronder ook van de uitwisseling van beste praktijken tussen civiele en militaire actoren met betrekking tot de uitvoering van relevante cybergerelateerde beleidsmaatregelen en wetgeving.

[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en

---

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

[18] 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).

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

[20] 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).

---

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

[18] 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).

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

[20] 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).

Amendement 6

Voorstel voor een verordening
Overweging 6

Door de Commissie voorgestelde tekst	*Amendement*
(6) In de op 10 november 2022 aangenomen gezamenlijke mededeling over het EU-beleid op het gebied van cyberdefensie[22] werd een EU-initiatief voor cybersolidariteit aangekondigd met de volgende doelstellingen: versterken van de gemeenschappelijke capaciteiten van de EU op het gebied van opsporing, situationeel bewustzijn en respons door de uitrol van een EU-infrastructuur van centra voor beveiligingsoperaties ("SOC's") te bevorderen, de geleidelijke opbouw van een cyberbeveiligingsreserve op EU-niveau met diensten van betrouwbare particuliere aanbieders te ondersteunen en kritieke entiteiten op basis van EU-risicobeoordelingen op mogelijke kwetsbaarheden te testen.	(6) In de op 10 november 2022 aangenomen gezamenlijke mededeling over het EU-beleid op het gebied van cyberdefensie[22] werd een EU-initiatief voor cybersolidariteit aangekondigd met de volgende doelstellingen: versterken van de gemeenschappelijke capaciteiten van de EU op het gebied van opsporing, situationeel bewustzijn en respons door de uitrol van een EU-infrastructuur van centra voor beveiligingsoperaties ("SOC's") te bevorderen, de geleidelijke opbouw van een cyberbeveiligingsreserve op EU-niveau met diensten van betrouwbare particuliere aanbieders te ondersteunen en kritieke entiteiten op basis van EU-risicobeoordelingen op mogelijke kwetsbaarheden te testen. ***Bovendien blijkt uit het snel evoluerende cyberdreigingslandschap en het snelle tempo van de technologische ontwikkeling ook dat er behoefte is aan meer civiel-militaire coördinatie en samenwerking, zoals de Raad heeft benadrukt in zijn conclusies over het EU-beleid op het gebied van cyberdefensie[1].***
	[1] Conclusies van de Raad over het EU-beleid op het gebied van cyberdefensie, goedgekeurd door de Raad tijdens zijn zitting van 22 mei 2023 (9618/23).
[22] Gezamenlijke mededeling aan het Europees Parlement en de Raad, Het EU-beleid op het gebied van cyberdefensie, JOIN(2022) 49 final.	[22] Gezamenlijke mededeling aan het Europees Parlement en de Raad, Het EU-beleid op het gebied van cyberdefensie, JOIN(2022) 49 final.

Amendement 7

Voorstel voor een verordening
Overweging 6 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(6 bis) Aangezien de grens tussen civiele en militaire aangelegenheden vervaagt en cyberinstrumenten en -technologieën vaak voor tweeërlei gebruik bestemd zijn, is er behoefte aan een alomvattende en holistische benadering ten aanzien van het digitale domein. Wanneer zich een grootschalig cyberbeveiligingsincident of een cyberbeveiligingscrisis voordoet waarbij meer dan één lidstaat betrokken is, moet er in passende crisisbeheersing worden voorzien. Zulke structuren moeten instaan voor de organisatie van de informatie-uitwisseling, coördinatie en samenwerking met de structuren van de Unie voor externe veiligheid en militaire crisisbeheersing en met de organen van de lidstaten die belast zijn met veiligheid en defensie (de cyberdefensiegemeenschap). Dit dient ook te gelden voor operaties en missies in het kader van het gemeenschappelijk veiligheids- en defensiebeleid die door de Unie worden uitgevoerd om vrede en stabiliteit in haar buurlanden en daarbuiten te waarborgen.

Amendement 8

Voorstel voor een verordening
Overweging 7

Door de Commissie voorgestelde tekst	*Amendement*
(7) Het is noodzakelijk de opsporing en het situationeel bewustzijn van cyberdreigingen en -incidenten in de hele Unie te versterken en de solidariteit te versterken door de paraatheid van de lidstaten en de Unie voor, alsook hun vermogen om te reageren op, significante	(7) Het is noodzakelijk de opsporing en het situationeel bewustzijn van cyberdreigingen en -incidenten in de hele Unie te versterken en de solidariteit te versterken door de paraatheid van de lidstaten en de Unie voor, alsook hun vermogen om te reageren op, significante

en grootschalige cyberbeveiligingsincidenten te verbeteren. Daarom zou een pan-Europese infrastructuur van SOC's (Europees cyberschild) moeten worden uitgerold om gemeenschappelijke capaciteiten op het gebied van opsporing en situationeel bewustzijn op te bouwen en te versterken; er zou een cybernoodmechanisme moeten worden ingesteld om de lidstaten te ondersteunen bij de voorbereiding en respons op, en bij het onmiddellijke herstel van, significante en grootschalige cyberbeveiligingsincidenten; er zou een evaluatiemechanisme voor cyberbeveiligingsincidenten moeten worden ingesteld om specifieke significante of grootschalige incidenten te evalueren en te beoordelen. Deze acties laten de artikelen 107 en 108 van het Verdrag betreffende de werking van de Europese Unie ("VWEU") onverlet.

en grootschalige cyberbeveiligingsincidenten te verbeteren. Daarom zou een pan-Europese infrastructuur van SOC's (Europees cyberschild) moeten worden uitgerold om gemeenschappelijke capaciteiten op het gebied van opsporing en situationeel bewustzijn op te bouwen en te versterken; er zou een cybernoodmechanisme moeten worden ingesteld om de lidstaten te ondersteunen bij de voorbereiding en respons op, en bij het onmiddellijke herstel van, significante en grootschalige cyberbeveiligingsincidenten***, waaronder de incidenten die meerdere lidstaten betreffen. Waar haalbaar en noodzakelijk, moet een cybernoodmechanisme de informatie-uitwisseling en samenwerking met de defensieautoriteiten van de lidstaten organiseren, met steun van de EU-instellingen, -organen en -instanties (de EU-cyberdefensiegemeenschap)***; er zou een evaluatiemechanisme voor cyberbeveiligingsincidenten moeten worden ingesteld om specifieke significante of grootschalige incidenten te evalueren en te beoordelen***. Deze nieuwe structuren moeten ook GVDB-missies en -operaties van de EU ondersteunen***. Deze acties laten de artikelen 107 en 108 van het Verdrag betreffende de werking van de Europese Unie ("VWEU") onverlet.

Amendement 9

Voorstel voor een verordening
Overweging 11

Door de Commissie voorgestelde tekst	*Amendement*
(11) Met het oog op een goed financieel beheer moeten specifieke regels worden vastgesteld voor de overdracht van ongebruikte vastleggings- en betalingskredieten. Met inachtneming van het beginsel dat de begroting van de Unie jaarlijks wordt vastgesteld, zou deze verordening, vanwege de onvoorspelbare,	(11) Met het oog op een goed financieel beheer moeten specifieke regels worden vastgesteld voor de overdracht van ongebruikte vastleggings- en betalingskredieten. Met inachtneming van het beginsel dat de begroting van de Unie jaarlijks wordt vastgesteld, zou deze verordening, vanwege de onvoorspelbare,

uitzonderlijke en specifieke aard van het cyberbeveiligingslandschap, moeten voorzien in mogelijkheden om ongebruikte middelen over te dragen naast de in het Financieel Reglement vastgestelde middelen, zodat de capaciteit van het cybernoodmechanisme om de lidstaten te ondersteunen bij de doeltreffende bestrijding van cyberdreigingen, wordt gemaximaliseerd.

uitzonderlijke en specifieke aard van het cyberbeveiligingslandschap, moeten voorzien in mogelijkheden om ongebruikte middelen over te dragen naast de in het Financieel Reglement vastgestelde middelen, zodat de capaciteit van het cybernoodmechanisme om de lidstaten te ondersteunen bij de doeltreffende bestrijding van cyberdreigingen, wordt gemaximaliseerd. ***Deze specifieke regels zouden het ook op langere termijn mogelijk maken dat er financiële steun wordt verleend voor gezamenlijke aanbestedingen van ultrabeveiligde instrumenten en infrastructuur van de volgende generatie, om de collectieve detectiecapaciteit te verbeteren met behulp van de meest geavanceerde artificiële intelligentie (AI) en gegevensanalyse.***

Amendement 10

Voorstel voor een verordening
Overweging 13

Door de Commissie voorgestelde tekst	*Amendement*
(13) Elke lidstaat moet een overheidsinstantie op nationaal niveau aanwijzen die belast is met de coördinatie van de activiteiten voor het opsporen van cyberdreigingen in die lidstaat. Deze nationale SOC's moeten fungeren als referentiepunt en toegangspoort op nationaal niveau voor deelname aan het Europees cyberschild en moeten ervoor zorgen dat informatie over cyberdreigingen van publieke en private entiteiten op doeltreffende en gestroomlijnde wijze op nationaal niveau wordt gedeeld en verzameld.	(13) Elke lidstaat moet een overheidsinstantie op nationaal niveau aanwijzen die belast is met de coördinatie van de activiteiten voor het opsporen van cyberdreigingen in die lidstaat. Deze nationale SOC's moeten fungeren als referentiepunt en toegangspoort op nationaal niveau voor deelname aan het Europees cyberschild en moeten ervoor zorgen dat informatie over cyberdreigingen van publieke en private entiteiten op doeltreffende en gestroomlijnde wijze op nationaal niveau wordt gedeeld en verzameld. ***Waar haalbaar en noodzakelijk moeten SOC's ook de deelname van defensie-entiteiten mogelijk maken door daarvoor een "defensiepijler" op te zetten om aspecten te regelen als de bestuursvorm en het soort gedeelde informatie, zoals uiteengezet in de gezamenlijke mededeling over het***

EU-beleid op het gebied van cyberdefensie[1] en ondersteund door de hoge vertegenwoordiger.

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

Amendement 11

Voorstel voor een verordening
Overweging 14

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

Incident Response Teams (CSIRT's) en andere relevante actoren.

Amendement 12

Voorstel voor een verordening
Overweging 15

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

Amendement 13

Voorstel voor een verordening
Overweging 16

Door de Commissie voorgestelde tekst	*Amendement*
(16) De landsgrensoverschrijdende SOC's moeten fungeren als centraal punt dat het mogelijk maakt relevante gegevens en informatie over cyberdreigingen breed te bundelen en dreigingsinformatie te verspreiden onder een grote en diverse groep actoren (bv. computercrisisresponsteams ("CERT's"),	(16) De landsgrensoverschrijdende SOC's moeten fungeren als centraal punt dat het mogelijk maakt relevante gegevens en informatie over cyberdreigingen breed te bundelen en dreigingsinformatie te verspreiden onder een grote en diverse groep actoren (bv. computercrisisresponsteams ("CERT's"),

CSIRT's, centra voor informatie-uitwisseling en -analyse ("ISAC's"), exploitanten van kritieke infrastructuur***)***. De informatie die tussen deelnemers aan een landsgrensoverschrijdend SOC wordt uitgewisseld, kan onder meer bestaan uit gegevens afkomstig van netwerken en sensoren, informatiebronnen over dreigingen, indicatoren voor aantasting en gecontextualiseerde informatie over incidenten, dreigingen en kwetsbaarheden. Daarnaast moeten landsgrensoverschrijdende SOC's ook samenwerkingsovereenkomsten sluiten met andere landsgrensoverschrijdende SOC's.	CSIRT's, centra voor informatie-uitwisseling en -analyse ("ISAC's"), exploitanten van kritieke infrastructuur ***en de cyberdefensiegemeenschap***. De informatie die tussen deelnemers aan een landsgrensoverschrijdend SOC wordt uitgewisseld, kan onder meer bestaan uit gegevens afkomstig van netwerken en sensoren, informatiebronnen over dreigingen, indicatoren voor aantasting en gecontextualiseerde informatie over incidenten, dreigingen en kwetsbaarheden. Daarnaast moeten landsgrensoverschrijdende SOC's ook samenwerkingsovereenkomsten sluiten met andere landsgrensoverschrijdende SOC's ***en het operationeel netwerk voor milCERT's (MICNET) wanneer dat is opgezet***.

Amendement 14

Voorstel voor een verordening
Overweging 17

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

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

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

Amendement 15

Voorstel voor een verordening
Overweging 19

Door de Commissie voorgestelde tekst	*Amendement*
(19) Om de grootschalige uitwisseling van gegevens over cyberdreigingen uit verschillende bronnen in een betrouwbare omgeving mogelijk te maken, moeten entiteiten die deelnemen aan het Europees cyberschild worden uitgerust met geavanceerde en zeer veilige instrumenten, apparatuur en infrastructuur. Dit moet het mogelijk maken de collectieve opsporingscapaciteit en de tijdige waarschuwingen aan autoriteiten en relevante entiteiten te verbeteren, met	(19) Om de grootschalige uitwisseling van gegevens over cyberdreigingen uit verschillende bronnen in een betrouwbare omgeving mogelijk te maken, moeten entiteiten die deelnemen aan het Europees cyberschild worden uitgerust met geavanceerde en zeer veilige instrumenten, apparatuur en infrastructuur***, mits die niet afkomstig zijn van aanbieders met een hoog risico van kritieke producten die digitale elementen bevatten***. Dit moet het mogelijk maken de collectieve

name door gebruik te maken van de nieuwste technologieën op het gebied van artificiële intelligentie (AI) en gegevensanalyse.	opsporingscapaciteit en de tijdige waarschuwingen aan autoriteiten en relevante entiteiten te verbeteren, met name door gebruik te maken van de nieuwste technologieën op het gebied van artificiële intelligentie (AI) en gegevensanalyse. ***Bij het gebruik van AI moet worden gezorgd voor menselijk toezicht, alsook voor een toereikend niveau van AI-geletterdheid en de nodige ondersteuning en autoriteit om die functie te kunnen uitoefenen.***

Amendement 16

Voorstel voor een verordening
Overweging 19 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(19 bis) Overeenkomstig Verordening [XX/XXXX (verordening cyberweerbaarheid)] moeten entiteiten die deelnemen aan het Europees cyberschild ook voldoen de in deze verordening vastgestelde vereisten voor alle producten met digitale elementen. Gezien de toenemende risico's als gevolg van economische afhankelijkheden moet de blootstelling aan aanbieders met een hoog risico van kritieke producten tot een minimum worden beperkt door middel van een gemeenschappelijk strategisch kader voor de economische veiligheid van de EU. Afhankelijkheid van aanbieders met een hoog risico van kritieke producten met digitale elementen vormt een strategisch risico dat op het niveau van de Unie moet worden aangepakt, met name als een land zich bezighoudt met economische spionage of economische dwang en zijn wetgeving willekeurige toegang tot alle soorten bedrijfsactiviteiten of -gegevens verplicht stelt en vooral als de kritieke producten bestemd zijn voor gebruik door essentiële entiteiten als bedoeld in Richtlijn (EU)

	2022/2555.

Amendement 17

Voorstel voor een verordening
Overweging 20

Door de Commissie voorgestelde tekst	*Amendement*
(20) Door gegevens te verzamelen, te delen en uit te wisselen, moet het Europees cyberschild de technologische soevereiniteit van de Unie versterken. De bundeling van hoogwaardige samengestelde gegevens moet ook bijdragen tot de ontwikkeling van geavanceerde technologieën op het gebied van artificiële intelligentie (AI) en gegevensanalyse. Dit moet worden vergemakkelijkt door het Europees cyberschild te verbinden met de pan-Europese high-performance computing-infrastructuur die is opgericht bij Verordening (EU) 2021/1173 van de Raad[25].	(20) Door gegevens te verzamelen, te delen en uit te wisselen, moet het Europees cyberschild de technologische soevereiniteit***, de strategische autonomie, het concurrentievermogen en de weerbaarheid*** van de Unie versterken. De bundeling van hoogwaardige samengestelde gegevens moet ook bijdragen tot de ontwikkeling van geavanceerde technologieën op het gebied van artificiële intelligentie (AI) en gegevensanalyse. Dit moet worden vergemakkelijkt door het Europees cyberschild te verbinden met de pan-Europese high-performance computing-infrastructuur die is opgericht bij Verordening (EU) 2021/1173 van de Raad[25].
[25] Verordening (EU) 2021/1173 van de Raad van 13 juli 2021 tot oprichting van de Gemeenschappelijke Onderneming Europese high-performance computing en tot intrekking van Verordening (EU) 2018/1488 (PB L 256 van 19.7.2021, blz. 3).	[25] Verordening (EU) 2021/1173 van de Raad van 13 juli 2021 tot oprichting van de Gemeenschappelijke Onderneming Europese high-performance computing en tot intrekking van Verordening (EU) 2018/1488 (PB L 256 van 19.7.2021, blz. 3).

Amendement 18

Voorstel voor een verordening
Overweging 25

Door de Commissie voorgestelde tekst	*Amendement*
(25) Het cybernoodmechanisme moet steun verlenen aan de lidstaten ter aanvulling van hun eigen maatregelen en	(25) Het cybernoodmechanisme moet steun verlenen aan de lidstaten ter aanvulling van hun eigen maatregelen en

middelen, en andere bestaande steunmogelijkheden in geval van respons op en onmiddellijk herstel van significante en grootschalige cyberbeveiligingsincidenten, zoals de diensten die het Agentschap van de Europese Unie voor cyberbeveiliging (“Enisa”) overeenkomstig zijn mandaat verleent, de gecoördineerde respons en de bijstand van het CSIRT-netwerk, de mitigatiesteun van EU-CyCLONe, alsook wederzijdse bijstand tussen de lidstaten, onder meer in het kader van artikel 42, lid 7, VEU, de snellereactieteams bij cyberbeveiligingsincidenten van de PESCO[26] en de snellereactieteams bij hybride dreigingen. Het moet voorzien in de noodzaak ervoor te zorgen dat er gespecialiseerde middelen beschikbaar zijn om de paraatheid voor en de respons op cyberbeveiligingsincidenten in de hele Unie en in derde landen te ondersteunen.

[26] Besluit (GBVB) 2017/2315 van de Raad van 11 december 2017 tot instelling van de permanente gestructureerde samenwerking

middelen, en andere bestaande steunmogelijkheden in geval van respons op en onmiddellijk herstel van significante en grootschalige cyberbeveiligingsincidenten, zoals de diensten die het Agentschap van de Europese Unie voor cyberbeveiliging (“Enisa”) overeenkomstig zijn mandaat verleent, de gecoördineerde respons en de bijstand van het CSIRT-netwerk, de mitigatiesteun van EU-CyCLONe, alsook wederzijdse bijstand tussen de lidstaten, onder meer in het kader van artikel 42, lid 7, VEU, de snellereactieteams bij cyberbeveiligingsincidenten van de PESCO[26]***, het nieuwe PESCO-project Coördinatiecentrum voor het cyberinformatiedomein (CIDCC) en de voorgestelde opvolger daarvan, het EU-coördinatiecentrum voor cyberdefensie (EUCDCC),*** en de snellereactieteams bij hybride dreigingen. Het moet voorzien in de noodzaak ervoor te zorgen dat er gespecialiseerde middelen beschikbaar zijn om de paraatheid voor en de respons op cyberbeveiligingsincidenten in de hele Unie en in derde landen te ondersteunen***, met name in de kandidaat-lidstaten die zich hebben aangesloten bij het gemeenschappelijk buitenlands en veiligheidsbeleid en het gemeenschappelijk veiligheids- en defensiebeleid van de EU, om hen te ondersteunen bij de opbouw van hun cybercapaciteiten en de landsgrensoverschrijdende en regionale samenwerking tussen die kandidaat-lidstaten op cybergebied te vergroten***.

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

[26] 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.

(PESCO) en tot opstelling van de lijst van deelnemende lidstaten.

Amendement 19

Voorstel voor een verordening
Overweging 26

Door de Commissie voorgestelde tekst	*Amendement*
(26) Dit instrument doet geen afbreuk aan procedures en kaders voor de coördinatie van crisisrespons op het niveau van de Unie, met name het Uniemechanisme voor civiele bescherming[27], de geïntegreerde EU-regeling politieke crisisrespons (IPCR[28]) en Richtlijn (EU) 2022/2555. Het kan bijdragen tot of een aanvulling vormen op acties die worden uitgevoerd in het kader van artikel 42, lid 7, VEU of in situaties als omschreven in artikel 222 VWEU. Het gebruik van dit instrument moet ***in voorkomend geval*** ook worden gecoördineerd met de uitvoering van de maatregelen van het instrumentarium voor cyberdiplomatie.	(26) Dit instrument doet geen afbreuk aan procedures en kaders voor de coördinatie van crisisrespons op het niveau van de Unie, met name het Uniemechanisme voor civiele bescherming[27], de geïntegreerde EU-regeling politieke crisisrespons (IPCR[28]) en Richtlijn (EU) 2022/2555. Het kan bijdragen tot of een aanvulling vormen op acties die worden uitgevoerd in het kader van artikel 42, lid 7, VEU of in situaties als omschreven in artikel 222 VWEU. Het gebruik van dit instrument moet ook worden gecoördineerd met de uitvoering van de maatregelen van het instrumentarium voor cyberdiplomatie***, waarbij de samenwerking op strategisch, operationeel en technisch niveau tussen de cyberdefensiegemeenschap en andere cybergemeenschappen vergroot moet worden, met name om de capaciteit met betrekking tot cyberbeveiligingsdreigingen van buiten de Unie te versterken, met inbegrip van beperkende maatregelen, die kan worden ingezet om kwaadwillige cyberactiviteiten te voorkomen en daarop te reageren***.

[27] 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).

[28] Geïntegreerde regelingen politieke crisisrespons (IPCR) en in overeenstemming met Aanbeveling (EU)

[27] 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).

[28] Geïntegreerde regelingen politieke crisisrespons (IPCR) en in overeenstemming met Aanbeveling (EU)

2017/1584 van de Commissie van 13 september 2017 inzake een gecoördineerde respons op grootschalige cyberbeveiligingsincidenten en -crises.

2017/1584 van de Commissie van 13 september 2017 inzake een gecoördineerde respons op grootschalige cyberbeveiligingsincidenten en -crises.

Amendement 20

Voorstel voor een verordening
Overweging 28

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

onmiddellijk herstel te ondersteunen en/of de werking van essentiële diensten te herstellen.

onmiddellijk herstel te ondersteunen en/of de werking van essentiële diensten te herstellen***, waarbij op passende wijze gebruik wordt gemaakt van het hele scala aan defensieve opties waarover de civiele en militaire gemeenschappen beschikken***.

Amendement 21

Voorstel voor een verordening
Overweging 29

Door de Commissie voorgestelde tekst	*Amendement*
(29) Om een consistente aanpak te bevorderen en de veiligheid in de hele Unie en haar interne markt te verbeteren, moet als onderdeel van de paraatheidsacties steun worden verleend voor het op gecoördineerde wijze testen en beoordelen van de cyberbeveiliging van entiteiten die actief zijn in sectoren die in Richtlijn (EU) 2022/2555 als zeer kritieke sectoren zijn aangemerkt. Daartoe moet de Commissie, met de steun van Enisa en in samenwerking met de bij Richtlijn (EU) 2022/2555 opgerichte NIS-samenwerkingsgroep, regelmatig relevante sectoren of subsectoren vaststellen die in aanmerking moeten komen om financiële steun te ontvangen voor gecoördineerde tests op het niveau van de Unie. De sectoren of subsectoren moeten worden gekozen uit bijlage I bij Richtlijn (EU) 2022/2555 (“zeer kritieke sectoren”). De gecoördineerde tests moeten gebaseerd zijn op gemeenschappelijke risicoscenario’s en -methoden. Bij de selectie van sectoren en de ontwikkeling van risicoscenario’s moet rekening worden gehouden met relevante Uniebrede risicobeoordelingen en risicoscenario’s, met inbegrip van de noodzaak om dubbel werk te voorkomen, zoals de risicobeoordeling en risicoscenario’s waarom wordt verzocht in de conclusies van de Raad over de ontwikkeling van de cyberstrategie van de Europese Unie en die door de Commissie,	(29) Om een consistente aanpak te bevorderen en de veiligheid in de hele Unie en haar interne markt te verbeteren, moet als onderdeel van de paraatheidsacties steun worden verleend voor het op gecoördineerde wijze testen en beoordelen van de cyberbeveiliging van entiteiten die actief zijn in sectoren die in Richtlijn (EU) 2022/2555 als zeer kritieke sectoren zijn aangemerkt. Daartoe moet de Commissie, met de steun van Enisa en in samenwerking met de bij Richtlijn (EU) 2022/2555 opgerichte NIS-samenwerkingsgroep, regelmatig relevante sectoren of subsectoren vaststellen die in aanmerking moeten komen om financiële steun te ontvangen voor gecoördineerde tests op het niveau van de Unie. ***In voorkomend geval moet de Europese Dienst voor extern optreden (EDEO), met name via het inlichtingencentrum van de EU (Intcen) en de EU-Fusiecel voor analyse van hybride dreigingen, met steun van het directoraat Inlichtingen van de Militaire Staf van de Europese Unie (EUMS) in het kader van de gezamenlijke capaciteit op het gebied van inlichtingenanalyse (SIAC), ook worden betrokken bij het geven van actuele beoordelingen en daarmee bijdragen tot de vaststelling van*** de sectoren of subsectoren ***die*** moeten worden gekozen uit bijlage I bij Richtlijn (EU) 2022/2555 (“zeer kritieke sectoren”). De

de hoge vertegenwoordiger en de NIS-samenwerkingsgroep moeten worden uitgevoerd, in coördinatie met de betrokken civiele en militaire organen en instanties en gevestigde netwerken, waaronder EU-CyCLONe, alsmede de risicobeoordeling van communicatienetwerken en -infrastructuur waarom is verzocht in het kader van de gezamenlijke ministeriële oproep van Nevers en die wordt uitgevoerd door de NIS-samenwerkingsgroep, met de steun van de Commissie en Enisa, en in samenwerking met het Orgaan van Europese regulerende instanties voor elektronische communicatie (Berec), de gecoördineerde risicobeoordelingen die moeten worden uitgevoerd krachtens artikel 22 van Richtlijn (EU) 2022/2555 en het testen van de digitale operationele weerbaarheid als bedoeld in Verordening (EU) 2022/2554 van het Europees Parlement en de Raad[29]. 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.

gecoördineerde tests moeten gebaseerd zijn op gemeenschappelijke risicoscenario's en -methoden. ***Deze tests moeten ook een belangrijke rol spelen bij de verbetering van de samenwerking tussen civiele en militaire entiteiten. Bij het organiseren van tests moeten de Commissie, de EDEO en Enisa daarom systematisch overwegen om deelnemers uit andere cybergemeenschappen, zoals het Europees Defensieagentschap (EDA) en andere relevante entiteiten, te laten deelnemen.*** Bij de selectie van sectoren en de ontwikkeling van risicoscenario's moet rekening worden gehouden met relevante Uniebrede risicobeoordelingen en risicoscenario's, met inbegrip van de noodzaak om dubbel werk te voorkomen, zoals de risicobeoordeling en risicoscenario's waarom wordt verzocht in de conclusies van de Raad over de ontwikkeling van de cyberstrategie van de Europese Unie en die door de Commissie, de hoge vertegenwoordiger en de NIS-samenwerkingsgroep moeten worden uitgevoerd, in coördinatie met de betrokken civiele en militaire organen en instanties en gevestigde netwerken, waaronder EU-CyCLONe, alsmede de risicobeoordeling van communicatienetwerken en -infrastructuur waarom is verzocht in het kader van de gezamenlijke ministeriële oproep van Nevers en die wordt uitgevoerd door de NIS-samenwerkingsgroep, met de steun van de Commissie en Enisa, en in samenwerking met het Orgaan van Europese regulerende instanties voor elektronische communicatie (Berec), de gecoördineerde risicobeoordelingen die moeten worden uitgevoerd krachtens artikel 22 van Richtlijn (EU) 2022/2555 en het testen van de digitale operationele weerbaarheid als bedoeld in Verordening (EU) 2022/2554 van het Europees Parlement en de Raad[29]. 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.
	[1] Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011
[29] 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.	[29] 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.

Amendement 22

Voorstel voor een verordening
Overweging 32

Door de Commissie voorgestelde tekst	*Amendement*
(32) Het cybernoodmechanisme moet de door de lidstaten verleende bijstand aan een lidstaat die is getroffen door een significant of grootschalig cyberbeveiligingsincident steunen, onder meer via het in artikel 15 van Richtlijn (EU) 2022/2555 bedoelde CSIRT-netwerk. De lidstaten die bijstand verlenen, moeten kunnen verzoeken om dekking van de kosten in verband met het uitzenden van deskundigenteams in het kader van wederzijdse bijstand. De subsidiabele kosten kunnen de reis- en verblijfkosten en de dagvergoedingen van cyberbeveiligingsdeskundigen omvatten.	(32) Het cybernoodmechanisme moet de door de lidstaten verleende bijstand aan een lidstaat die is getroffen door een significant of grootschalig cyberbeveiligingsincident steunen, onder meer via het in artikel 15 van Richtlijn (EU) 2022/2555 bedoelde CSIRT-netwerk. De lidstaten die bijstand verlenen, moeten kunnen verzoeken om dekking van de kosten in verband met het uitzenden van deskundigenteams in het kader van wederzijdse bijstand***, waarbij wordt gezorgd voor een efficiënte coördinatie tussen de betrokken programma's en instrumenten van de EU, waaronder de Europese Vredesfaciliteit (EPF), het GBVB en het NDICI, wanneer bijstand aan derde landen, in het bijzonder Oekraïne en Moldavië, wordt verleend***.

De subsidiabele kosten kunnen de reis- en verblijfkosten en de dagvergoedingen van cyberbeveiligingsdeskundigen omvatten.

Amendement 23

Voorstel voor een verordening
Overweging 33

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

Amendement 24

Voorstel voor een verordening
Overweging 34

Door de Commissie voorgestelde tekst	*Amendement*
(34) Met het oog op de selectie van particuliere aanbieders die diensten verlenen in het kader van de EU-cyberbeveiligingsreserve moet een reeks minimumcriteria worden vastgesteld die moeten worden opgenomen in de aanbesteding voor de selectie van deze dienstverleners teneinde ervoor te zorgen dat wordt voldaan aan de behoeften van de autoriteiten van de lidstaten en de in kritieke of zeer kritieke sectoren actieve entiteiten.	(34) Met het oog op de selectie van particuliere aanbieders die diensten verlenen in het kader van de EU-cyberbeveiligingsreserve moet een reeks minimumcriteria worden vastgesteld die moeten worden opgenomen in de aanbesteding voor de selectie van deze dienstverleners teneinde ervoor te zorgen dat wordt voldaan aan de behoeften van de autoriteiten van de lidstaten en de in kritieke of zeer kritieke sectoren actieve entiteiten***, waarbij ook rekening wordt gehouden met de risico's in verband met de deelname van aanbieders uit strategisch concurrerende landen, hetgeen gevaren met zich mee kan brengen voor de economische veiligheid, en met de gevolgen voor de strategische veiligheid van de Unie***.

Amendement 25

Voorstel voor een verordening
Overweging 36

Door de Commissie voorgestelde tekst	*Amendement*
(36) Om de doelstellingen van deze verordening te ondersteunen, namelijk het bevorderen van gedeeld situationeel bewustzijn, het vergroten van de weerbaarheid van de Unie en het mogelijk maken van een doeltreffende respons op significante en grootschalige cyberbeveiligingsincidenten, moeten EU-CyCLONe, het CSIRT-netwerk of de Commissie Enisa kunnen verzoeken om dreigingen, kwetsbaarheden en mitigatiemaatregelen met betrekking tot een specifiek significant of grootschalig cyberbeveiligingsincident te evalueren en te beoordelen. Na de voltooiing van een evaluatie en beoordeling van een incident moet Enisa in samenwerking met relevante belanghebbenden, waaronder	(36) Om de doelstellingen van deze verordening te ondersteunen, namelijk het bevorderen van gedeeld situationeel bewustzijn, het vergroten van de weerbaarheid van de Unie en het mogelijk maken van een doeltreffende respons op significante en grootschalige cyberbeveiligingsincidenten, moeten EU-CyCLONe, het CSIRT-netwerk of de Commissie Enisa kunnen verzoeken om dreigingen, kwetsbaarheden en mitigatiemaatregelen met betrekking tot een specifiek significant of grootschalig cyberbeveiligingsincident te evalueren en te beoordelen. ***Met het oog op de ontwikkeling van een veilig connectiviteitssysteem, dat voortbouwt op de Europese kwantumcommunicatie-***

vertegenwoordigers van de particuliere sector, de lidstaten, de Commissie en andere relevante instellingen, organen en instanties van de EU een evaluatieverslag over het incident opstellen. Wat de particuliere sector betreft, ontwikkelt Enisa kanalen voor de uitwisseling van informatie met gespecialiseerde aanbieders, waaronder aanbieders van beheerde beveiligingsoplossingen en verkopers, om bij te dragen tot de opdracht van Enisa om in de hele Unie een hoog gemeenschappelijk niveau van cyberbeveiliging te bereiken. Voortbouwend op de samenwerking met belanghebbenden, met inbegrip van de particuliere sector, moet het evaluatieverslag over specifieke incidenten gericht zijn op het beoordelen van de oorzaken en gevolgen van een incident alsook de maatregelen om het incident te beperken nadat het zich heeft voorgedaan. Bijzondere aandacht dient uit te gaan naar de inbreng van, en de lessen die worden gedeeld door, de aanbieders van beheerde beveiligingsdiensten die voldoen aan de voorwaarden hoogste professionele integriteit, onpartijdigheid en vereiste technische deskundigheid, zoals in deze verordening vereist. Het verslag moet worden ingediend bij en als input dienen voor de werkzaamheden van EU-CyCLONe, het CSIRT-netwerk en de Commissie. Als het incident betrekking heeft op een derde land, zal de Commissie het verslag ook delen met de hoge vertegenwoordiger.

infrastructuur (EuroQCI) en de satellietcommunicatie voor de overheid van de Europese Unie (GOVSATCOM), in het bijzonder de implementatie van GALILEO GNSS voor defensiegebruikers, moet bij elke mogelijke toekomstige ontwikkeling rekening worden gehouden met de komst van "hyperwars", waarin de snelheid en de verfijning van kwantumcomputing worden gecombineerd met zeer autonome militaire systemen. Na de voltooiing van een evaluatie en beoordeling van een incident moet Enisa in samenwerking met relevante belanghebbenden, waaronder vertegenwoordigers van de particuliere sector, de lidstaten, de Commissie en andere relevante instellingen, organen en instanties van de EU een evaluatieverslag over het incident opstellen. Wat de particuliere sector betreft, ontwikkelt Enisa kanalen voor de uitwisseling van informatie met gespecialiseerde aanbieders, waaronder aanbieders van beheerde beveiligingsoplossingen en verkopers, om bij te dragen tot de opdracht van Enisa om in de hele Unie een hoog gemeenschappelijk niveau van cyberbeveiliging te bereiken. Voortbouwend op de samenwerking met belanghebbenden, met inbegrip van de particuliere sector, moet het evaluatieverslag over specifieke incidenten gericht zijn op het beoordelen van de oorzaken en gevolgen van een incident alsook de maatregelen om het incident te beperken nadat het zich heeft voorgedaan. Bijzondere aandacht dient uit te gaan naar de inbreng van, en de lessen die worden gedeeld door, de aanbieders van beheerde beveiligingsdiensten die voldoen aan de voorwaarden hoogste professionele integriteit, onpartijdigheid en vereiste technische deskundigheid, zoals in deze verordening vereist. Het verslag moet worden ingediend bij en als input dienen voor de werkzaamheden van EU-CyCLONe, het CSIRT-netwerk en de Commissie. Als het incident betrekking

heeft op een derde land, zal de Commissie het verslag ook delen met de hoge vertegenwoordiger***, de EDEO en alle GVDB-missies in het door het incident getroffen land via hun hoofdkwartier***.

Amendement 26

Voorstel voor een verordening
Overweging 37

Door de Commissie voorgestelde tekst	*Amendement*
(37) Gezien de onvoorspelbare aard van cyberaanvallen en het feit dat deze vaak niet beperkt zijn tot een specifiek geografisch gebied en een groot risico op overloopeffecten inhouden, draagt de versterking van de weerbaarheid van buurlanden en hun capaciteit om doeltreffend te reageren op significante en grootschalige cyberbeveiligingsincidenten bij tot de bescherming van de Unie als geheel. Daarom ***kunnen*** met het programma Digitaal Europa geassocieerde derde landen steun ontvangen uit de EU-cyberbeveiligingsreserve ***indien daarin is voorzien in de desbetreffende associatieovereenkomst met het programma Digitaal Europa.*** De financiering voor geassocieerde derde landen moet door de Unie worden ondersteund in het kader van relevante partnerschappen en financieringsinstrumenten voor die landen. De steun moet betrekking hebben op diensten op het gebied van respons op en onmiddellijk herstel van significante of grootschalige cyberbeveiligingsincidenten. De in deze verordening vastgestelde voorwaarden voor de EU-cyberbeveiligingsreserve en betrouwbare aanbieders moeten gelden wanneer steun wordt verleend aan de met het programma Digitaal Europa geassocieerde derde landen.	(37) 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***, met name Oekraïne en Moldavië,*** en hun capaciteit om doeltreffend te reageren op significante en grootschalige cyberbeveiligingsincidenten bij tot de bescherming van de Unie als geheel. Daarom ***moeten*** met het programma Digitaal Europa geassocieerde derde landen steun ontvangen uit de EU-cyberbeveiligingsreserve***. De steun moet ook gelden voor derde landen waar een GVDB-missie wordt ingezet met een specifiek mandaat om de weerbaarheid tegen hybride dreigingen, waaronder cyberdreigingen, te versterken of waar een EVF-steunmaatregel is vastgesteld om de cyberweerbaarheid van het land te versterken.*** De financiering voor geassocieerde derde landen moet door de Unie worden ondersteund in het kader van relevante partnerschappen en financieringsinstrumenten voor die landen. De steun moet betrekking hebben op diensten op het gebied van respons op en onmiddellijk herstel van significante of grootschalige cyberbeveiligingsincidenten. De in deze verordening vastgestelde voorwaarden voor de EU-cyberbeveiligingsreserve en betrouwbare aanbieders moeten gelden wanneer steun

	wordt verleend aan de met het programma Digitaal Europa geassocieerde derde landen.

Amendement 27

Voorstel voor een verordening
Artikel 1 – lid 1 – punt c

Door de Commissie voorgestelde tekst	*Amendement*
c) de instelling van een Europees evaluatiemechanisme voor cyberbeveiligingsincidenten om significante of grootschalige incidenten te evalueren en te beoordelen.	c) de instelling van een Europees evaluatiemechanisme voor cyberbeveiligingsincidenten om significante of grootschalige incidenten ***of dreigingen*** te evalueren en te beoordelen.

Amendement 28

Voorstel voor een verordening
Artikel 1 – lid 2 – punt a

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

Amendement 29

Voorstel voor een verordening
Artikel 1 – lid 2 – punt b

Door de Commissie voorgestelde tekst	*Amendement*
b) de paraatheid van in kritieke en zeer kritieke sectoren actieve entiteiten in de hele Unie vergroten en de solidariteit versterken door gemeenschappelijke	b) de paraatheid van in kritieke en zeer kritieke sectoren actieve entiteiten in de hele Unie vergroten en de solidariteit versterken door gemeenschappelijke

capaciteit op het gebied van de respons op significante of grootschalige cyberbeveiligingsincidenten te ontwikkelen, onder meer door steun van de Unie voor respons op cyberbeveiligingsincidenten beschikbaar te stellen aan derde landen die geassocieerd zijn met het programma Digitaal Europa;	capaciteit op het gebied van de respons op significante of grootschalige cyberbeveiligingsincidenten te ontwikkelen, onder meer door steun van de Unie voor respons op cyberbeveiligingsincidenten beschikbaar te stellen aan derde landen die geassocieerd zijn met het programma Digitaal Europa ***of aan derde landen die kandidaat zijn voor toetreding tot de Unie en geen inbreuk maken op de veiligheids- en defensiebelangen van de Unie en haar lidstaten als vastgesteld in het kader van het GBVB uit hoofde van titel V van het VEU; De lidstaten moeten overwegen een actief cyberdefensieprogramma op te nemen in hun nationale cyberbeveiligingsstrategie die regelmatige gezamenlijke opleidingsoefeningen tussen lidstaten en internationale organisaties omvat. Een dergelijk programma moet de mogelijkheid bieden om dreigingen synchroon en in real time te ontdekken, op te sporen, te analyseren en te beperken***;

Amendement 30

Voorstel voor een verordening
Artikel 1 – lid 2 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	2 bis. systemische cyberbeveiligingsrisico's verminderen die voortkomen uit een afhankelijkheid van kritieke apparatuur van landen waar dit indruist tegen de veiligheids- en defensiebelangen van de Unie en haar lidstaten als vastgesteld in het kader van het GBVB uit hoofde van titel V van het VEU;

Amendement 31

Voorstel voor een verordening
Artikel 2 – alinea 1 – punt 2 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	"cyberdefensiegemeenschap": de defensieautoriteiten van de lidstaten, ondersteund door EU-instellingen, -organen en -agentschappen, zoals uiteengezet in de gezamenlijke mededeling over het EU-beleid op het gebied van cyberdefensie[1];
	[1] Gezamenlijke mededeling aan het Europees Parlement en de Raad, Het EU-beleid op het gebied van cyberdefensie, JOIN(2022) 49 final.

Amendement 32

Voorstel voor een verordening
Artikel 3 – lid 2 – alinea 1 – punt b bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	b bis) draagt bij aan de modernisatie van het hele cyberdefensiesysteem, door de kwaliteit van de capaciteiten op het gebied van cyberdefensie te verhogen middels de uitrol van AI-systemen, mede om de uitwisseling van informatie tussen de nationale en landsgrensoverschrijdende SOC's te versnellen;

Amendement 33

Voorstel voor een verordening
Artikel 3 – lid 2 – alinea 1 – punt d bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	d bis) herziet en beoordeelt kritieke cyberbeveiligingstechnologieën en -apparatuur die door SOC's worden gebruikt bij het reageren op

	cyberbeveiligingsincidenten, voor wat betreft systemische risico's die voortkomen uit zeggenschap over aanbieders die een hoog risico vormen door landen waar dit zou indruisen tegen de veiligheids- en defensiebelangen van de Unie en haar lidstaten als vastgesteld in het kader van het GBVB uit hoofde van titel V van het VEU;

Amendement 34

Voorstel voor een verordening
Artikel 4 – lid 1 – alinea 2

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

Amendement 35

Voorstel voor een verordening
Artikel 4 – lid 2

Door de Commissie voorgestelde tekst	*Amendement*
2. Na een oproep tot het indienen van blijken van belangstelling worden de nationale SOC's door het Europees Kenniscentrum voor cyberbeveiliging ("ECCC") geselecteerd om samen met het ECCC deel te nemen aan een gezamenlijke aanbesteding van instrumenten en infrastructuur. Het ECCC kan aan de geselecteerde nationale SOC's subsidies toekennen om de werking van die	2. Na een oproep tot het indienen van blijken van belangstelling worden de nationale SOC's door het Europees Kenniscentrum voor cyberbeveiliging ("ECCC") geselecteerd om samen met het ECCC deel te nemen aan een gezamenlijke aanbesteding van instrumenten en infrastructuur. Het ECCC kan aan de geselecteerde nationale SOC's subsidies toekennen om de werking van die

instrumenten en infrastructuur te financieren. De financiële bijdrage van de Unie dekt tot 50 % van de verwervingskosten van de instrumenten en infrastructuur en tot 50 % van de exploitatiekosten; de resterende kosten komen voor rekening van de lidstaat. Alvorens de procedure voor de verwerving van de instrumenten en infrastructuur in gang te zetten, sluiten het ECCC en het nationale SOC een onderbrengings- en gebruiksovereenkomst waarin het gebruik van de instrumenten en infrastructuur wordt geregeld.	instrumenten en infrastructuur te financieren***, onder strikte voorwaarde dat zulke instrumenten en infrastructuur worden geleverd door betrouwbare aanbieders als bedoeld in artikel 16***. De financiële bijdrage van de Unie dekt tot 50 % van de verwervingskosten van de instrumenten en infrastructuur en tot 50 % van de exploitatiekosten; de resterende kosten komen voor rekening van de lidstaat. Alvorens de procedure voor de verwerving van de instrumenten en infrastructuur in gang te zetten, sluiten het ECCC en het nationale SOC een onderbrengings- en gebruiksovereenkomst waarin het gebruik van de instrumenten en infrastructuur wordt geregeld.

Amendement 36

Voorstel voor een verordening
Artikel 5 – lid 2

Door de Commissie voorgestelde tekst	*Amendement*
2. Na een oproep tot het indienen van blijken van belangstelling selecteert het ECCC een onderbrengend consortium om samen met het ECCC deel te nemen aan een gezamenlijke aanbesteding van instrumenten en infrastructuur. Het ECCC kan het onderbrengend consortium een subsidie toekennen om de werking van de instrumenten en infrastructuur te financieren. De financiële bijdrage van de Unie dekt tot 75 % van de verwervingskosten van de instrumenten en infrastructuur en tot 50 % van de exploitatiekosten; de resterende kosten komen voor rekening van het onderbrengend consortium. Alvorens de procedure voor de verwerving van de instrumenten en infrastructuur in gang te zetten, sluiten het ECCC en het onderbrengend consortium een onderbrengings- en gebruiksovereenkomst waarin het gebruik van de instrumenten en	2. Na een oproep tot het indienen van blijken van belangstelling selecteert het ECCC een onderbrengend consortium om samen met het ECCC deel te nemen aan een gezamenlijke aanbesteding van instrumenten en infrastructuur. Het ECCC kan het onderbrengend consortium een subsidie toekennen om de werking van de instrumenten en infrastructuur te financieren***, onder strikte voorwaarde dat zulke instrumenten en infrastructuur worden geleverd door betrouwbare aanbieders als bedoeld in artikel 16***. De financiële bijdrage van de Unie dekt tot 75 % van de verwervingskosten van de instrumenten en infrastructuur en tot 50 % van de exploitatiekosten; de resterende kosten komen voor rekening van het onderbrengend consortium. Alvorens de procedure voor de verwerving van de instrumenten en infrastructuur in gang te zetten, sluiten het ECCC en het onderbrengend consortium een

infrastructuur wordt geregeld.	onderbrengings- en gebruiksovereenkomst waarin het gebruik van de instrumenten en infrastructuur wordt geregeld.

Amendement 37

Voorstel voor een verordening
Artikel 5 – lid 2 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	2 bis. Alle infrastructuur en aanbieders afkomstig uit een derde land met een hoog risico worden automatisch uitgesloten.

Amendement 38

Voorstel voor een verordening
Artikel 6 – lid 1 — punt b bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	b bis) rechtstreeks bijdraagt aan het versterken van de militaire en defensievermogens van de deelnemende leden of een rechtstreekse en onmiddellijke bedreiging van hun veiligheid voorkomt. Aangezien de exploitatie van kwetsbaarheden in de defensiesector aanzienlijke verstoringen en schade kan veroorzaken, zijn met het oog op de cyberveiligheid van de defensie-industrie speciale maatregelen vereist om de veiligheid van de toeleveringsketens te waarborgen, met name ten aanzien van entiteiten die zich onderaan de toeleveringsketens bevinden en die geen toegang tot gerubriceerde informatie nodig hebben, maar die wel de hele sector ernstig in gevaar kunnen brengen. Er moet bijzondere aandacht worden besteed aan de gevolgen die een inbreuk kan hebben en aan de dreiging van mogelijke manipulatie van netwerkgegevens waardoor kritieke defensiemiddelen volledig geneutraliseerd kunnen worden of zelfs de besturingssystemen ervan

	uitgeschakeld kunnen worden, waardoor ze kwetsbaar worden voor kaping.

Amendement 39

Voorstel voor een verordening
Artikel 6 – lid 1 — punt b ter (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	b ter) bijdraagt aan het versterken van de defensievermogens van de deelnemende leden of een rechtstreekse en onmiddellijke bedreiging van hun veiligheid voorkomt, door de veiligheid van de toeleveringsketens te waarborgen, met name ten aanzien van entiteiten die zich onderaan de toeleveringsketens bevinden en die geen toegang tot gerubriceerde informatie nodig hebben, maar die wel de hele sector ernstig in gevaar kunnen brengen.

Amendement 40

Voorstel voor een verordening
Artikel 7 – lid 1

Door de Commissie voorgestelde tekst	*Amendement*
1. Wanneer de landsgrensoverschrijdende SOC's informatie verkrijgen over een mogelijk of lopend grootschalig cyberbeveiligingsincident, verstrekken zij onverwijld relevante informatie aan EU-CyCLONe, het CSIRT-netwerk en de Commissie, gezien hun respectieve taken op het gebied van crisisbeheersing overeenkomstig Richtlijn (EU) 2022/2555.	1. Wanneer de landsgrensoverschrijdende SOC's informatie verkrijgen over een mogelijk of lopend grootschalig cyberbeveiligingsincident, verstrekken zij onverwijld relevante informatie aan EU-CyCLONe, het CSIRT-netwerk en de Commissie, ***met inbegrip van de hoge vertegenwoordiger en de EDEO wanneer het een derde land betreft,*** gezien hun respectieve taken op het gebied van crisisbeheersing overeenkomstig Richtlijn (EU) 2022/2555.

Amendement 41

Voorstel voor een verordening
Artikel 8 – lid 1

Door de Commissie voorgestelde tekst	*Amendement*
1. De lidstaten die deelnemen aan het Europees cyberschild zorgen voor een hoog niveau van gegevensbeveiliging en fysieke beveiliging van de infrastructuur van het Europees cyberschild en zien erop toe dat de infrastructuur adequaat wordt beheerd en gecontroleerd zodat deze tegen dreigingen wordt beschermd en zodat de beveiliging van de infrastructuur en van de systemen, met inbegrip van de via de infrastructuur uitgewisselde gegevens**,** wordt gewaarborgd.	1. De lidstaten die deelnemen aan het Europees cyberschild zorgen voor een hoog niveau van gegevensbeveiliging en fysieke beveiliging van de infrastructuur van het Europees cyberschild en zien erop toe dat de infrastructuur adequaat wordt beheerd en gecontroleerd**,** zodat deze tegen dreigingen wordt beschermd en zodat de beveiliging van de infrastructuur en van de systemen ***wordt gewaarborgd en daarmee risico's worden beperkt en dat ook de technologische voorsprong van de EU in kritieke sectoren wordt bevorderd***, ***met inbegrip van maatregelen om bij aanbieders met een hoog risico beperkingen toe te passen of hen uit te sluiten, en om de beveiliging*** van de via de infrastructuur uitgewisselde gegevens ***te beschermen***.

Amendement 42

Voorstel voor een verordening
Artikel 8 – lid 2

Door de Commissie voorgestelde tekst	*Amendement*
2. De lidstaten die deelnemen aan het Europees cyberschild zorgen ervoor dat de uitwisseling van informatie binnen het Europees cyberschild met entiteiten die geen overheidsinstanties van een lidstaat zijn, geen negatieve gevolgen heeft voor de veiligheidsbelangen van de Unie.	2. De lidstaten die deelnemen aan het Europees cyberschild zorgen ervoor dat de uitwisseling van informatie binnen het Europees cyberschild met entiteiten die geen overheidsinstanties van een lidstaat zijn, geen negatieve gevolgen heeft voor de veiligheidsbelangen van de Unie ***en dat eventuele informatie-uitwisseling met aanbieders met een hoog risico tot een minimum wordt beperkt en de veiligheid en de strategische belangen van de Unie niet in gevaar brengt***.

Amendement 43

Voorstel voor een verordening
Artikel 8 – lid 3

Door de Commissie voorgestelde tekst	*Amendement*
3. De Commissie kan uitvoeringshandelingen vaststellen waarin technische voorschriften worden vastgelegd waaraan de lidstaten moeten voldoen om hun verplichting uit hoofde van de leden 1 en 2 na te komen. Deze uitvoeringshandelingen worden vastgesteld volgens de in artikel 21, lid 2, van deze verordening bedoelde onderzoeksprocedure. Daarbij houdt de Commissie, gesteund door de hoge vertegenwoordiger, rekening met de relevante beveiligingsnormen op defensieniveau, teneinde de samenwerking met militaire actoren te vergemakkelijken.	3. De Commissie kan uitvoeringshandelingen vaststellen waarin technische voorschriften worden vastgelegd waaraan de lidstaten moeten voldoen om hun verplichting uit hoofde van de leden 1 en 2 na te komen. Deze uitvoeringshandelingen worden vastgesteld volgens de in artikel 21, lid 2, van deze verordening bedoelde onderzoeksprocedure. Daarbij houdt de Commissie, gesteund door de hoge vertegenwoordiger, rekening met de relevante beveiligingsnormen op defensieniveau, teneinde de samenwerking met militaire actoren te vergemakkelijken***, en maakt zij op passende wijze gebruik van het hele scala aan defensieve opties waarover de civiele en militaire gemeenschappen ten behoeve van de bredere veiligheid en defensie van de EU beschikken, en informeert zij het Europees Parlement***.

Amendement 44

Voorstel voor een verordening
Artikel 9 – lid 2

Door de Commissie voorgestelde tekst	*Amendement*
2. De acties ter uitvoering van het cybernoodmechanisme worden ondersteund door financiering uit het programma Digitaal Europa en worden uitgevoerd overeenkomstig Verordening (EU) 2021/694 en met name specifieke doelstelling 3 daarvan.	2. De acties ter uitvoering van het cybernoodmechanisme worden ondersteund door financiering uit het programma Digitaal Europa en worden uitgevoerd overeenkomstig Verordening (EU) 2021/694 en met name specifieke doelstelling 3 daarvan***, en door de Europese Vredesfaciliteit (EPF) in het geval van bijstandsmaatregelen voor derde landen, in het bijzonder Oekraïne***

en Moldavië;

Amendement 45

Voorstel voor een verordening
Artikel 10 – lid 1 – punt a

Door de Commissie voorgestelde tekst	*Amendement*
a) paraatheidsacties, met inbegrip van de gecoördineerde paraatheidstests van in zeer kritieke sectoren actieve entiteiten in de hele Unie;	a) paraatheidsacties, met inbegrip van de gecoördineerde paraatheidstests van in zeer kritieke sectoren actieve entiteiten***, zoals openbare infrastructuur, verkiezingsinfrastructuur, vervoer, gezondheidszorg, financiën, telecommunicatie, voedselvoorziening en veiligheid,*** in de hele Unie;

Amendement 46

Voorstel voor een verordening
Artikel 10 – lid 1 – punt c

Door de Commissie voorgestelde tekst	*Amendement*
c) wederzijdse-bijstandsacties die bestaan uit het verlenen van bijstand door de nationale autoriteiten van een lidstaat aan een andere lidstaat, met name als bedoeld in artikel 11, lid 3, punt f), van Richtlijn (EU) 2022/2555**.**	c) wederzijdse-bijstandsacties die bestaan uit het verlenen van bijstand door de nationale autoriteiten van een lidstaat aan een andere lidstaat, met name als bedoeld in artikel 11, lid 3, punt f), van Richtlijn (EU) 2022/2555 ***en in het kader van artikel 42, lid 7, VEU en artikel 222 VWEU;***

Amendement 47

Voorstel voor een verordening
Artikel 10 – lid 1 – punt c bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	c bis) vervanging en uitfasering van kritieke apparatuur van aanbieders met een hoog risico waar dit indruist tegen de veiligheids- en defensiebelangen van de Unie en haar lidstaten als vastgesteld in

	het kader van het GBVB uit hoofde van titel V van het VEU;

Amendement 48

Voorstel voor een verordening
Artikel 11 – lid 2

Door de Commissie voorgestelde tekst	*Amendement*
2. De NIS-samenwerkingsgroep ontwikkelt in samenwerking met de Commissie, Enisa ***en*** de hoge vertegenwoordiger gemeenschappelijke risicoscenario's en -methoden voor de gecoördineerde tests.	2. De NIS-samenwerkingsgroep ontwikkelt in samenwerking met de Commissie, Enisa***,*** de hoge vertegenwoordiger***, de EDEO en, in voorkomend geval, het EDA,*** gemeenschappelijke risicoscenario's en -methoden voor de gecoördineerde tests.

Amendement 49

Voorstel voor een verordening
Artikel 12 – lid 2

Door de Commissie voorgestelde tekst	*Amendement*
2. De EU-cyberbeveiligingsreserve bestaat uit incidentresponsdiensten van betrouwbare aanbieders die zijn geselecteerd overeenkomstig de criteria van artikel 16. De reserve omvat vooraf vastgelegde diensten. De diensten kunnen in alle lidstaten worden geleverd.	2. De EU-cyberbeveiligingsreserve bestaat uit incidentresponsdiensten van betrouwbare aanbieders die zijn geselecteerd overeenkomstig de criteria van artikel 16. De reserve omvat vooraf vastgelegde diensten. De diensten kunnen in alle lidstaten ***en derde landen die voldoen aan de toepasselijke eisen van deze verordening,*** worden geleverd.

Amendement 50

Voorstel voor een verordening
Artikel 12 – lid 3 – punt b

Door de Commissie voorgestelde tekst	*Amendement*
b) instellingen, organen en instanties van de Unie.	b) instellingen, organen en instanties van de Unie***, met inbegrip van GVDB-missies***.

Amendement 51

Voorstel voor een verordening
Artikel 12 – lid 4

Door de Commissie voorgestelde tekst	*Amendement*
4. De in lid 3, punt a), bedoelde gebruikers gebruiken de diensten van de EU-cyberbeveiligingsreserve voor de respons, of de ondersteuning van de respons, op en het onmiddellijke herstel van significante of grootschalige incidenten die in kritieke of zeer kritieke sectoren actieve entiteiten treffen.	4. De in lid 3, punt a), bedoelde gebruikers gebruiken de diensten van de EU-cyberbeveiligingsreserve voor de respons, of de ondersteuning van de respons, op en het onmiddellijke herstel van significante of grootschalige incidenten die in kritieke of zeer kritieke sectoren actieve entiteiten treffen***, zoals openbare infrastructuur, verkiezingsinfrastructuur, vervoer, gezondheidszorg, financiën, telecommunicatie, voedselvoorziening en veiligheid***.

Amendement 52

Voorstel voor een verordening
Artikel 12 – lid 5

Door de Commissie voorgestelde tekst	*Amendement*
5. De Commissie draagt de algemene verantwoordelijkheid voor de uitvoering van de EU-cyberbeveiligingsreserve. De Commissie bepaalt de prioriteiten en ontwikkeling van de EU-cyberbeveiligingsreserve in overeenstemming met de vereisten van de in lid 3 bedoelde gebruikers, houdt toezicht op de uitvoering ervan en zorgt voor complementariteit, consistentie, synergieën en koppelingen met andere ondersteunende acties in het kader van deze verordening en met andere acties en programma's van de Unie.	5. De Commissie draagt de algemene verantwoordelijkheid voor de uitvoering van de EU-cyberbeveiligingsreserve. De Commissie bepaalt de prioriteiten en ontwikkeling van de EU-cyberbeveiligingsreserve in overeenstemming met de vereisten van de in lid 3 bedoelde gebruikers, houdt toezicht op de uitvoering ervan en zorgt voor complementariteit, consistentie, synergieën en koppelingen met andere ondersteunende acties in het kader van deze verordening en met andere acties en programma's ***en doelstellingen*** van de Unie***, met name de strategische doelstelling inzake de vermindering van de afhankelijkheid van aanbieders met een hoog risico waarbij inbreuk wordt gemaakt op de veiligheids-***

	en defensiebelangen van de Unie en haar lidstaten als vastgesteld in het kader van het GBVB uit hoofde van titel V van het VEU*.*

Amendement 53

Voorstel voor een verordening
Artikel 12 – lid 7

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

Amendement 54

Voorstel voor een verordening
Artikel 14 – lid 2 – punt a bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	a bis) de gevolgen van het incident voor de veiligheid en defensie van de Unie;

Amendement 55

Voorstel voor een verordening
Artikel 15 – lid 3

Door de Commissie voorgestelde tekst	*Amendement*
3. In overleg met de hoge vertegenwoordiger kan de steun in het kader van het cybernoodmechanisme een	3. In overleg met de hoge vertegenwoordiger kan de steun in het kader van het cybernoodmechanisme een

aanvulling vormen op de bijstand die wordt verleend in het kader van het gemeenschappelijk buitenlands en veiligheidsbeleid en het gemeenschappelijk veiligheids- en defensiebeleid, onder meer via de snellereactieteams bij cyberbeveiligingsincidenten. Deze steun kan ook een aanvulling vormen op of bijdragen aan bijstand die een lidstaat aan een andere lidstaat verleent in het kader van artikel 42, lid 7, van het Verdrag betreffende de Europese Unie.	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 ***(CRRT's)*** bij cyberbeveiligingsincidenten***, teneinde een betere ondersteuning te bieden aan EU-lidstaten, GVDB-missies en -operaties en derde landen die zich bij de opbouw van hun capaciteit op het gebied van cyberdefensie hebben aangesloten bij het gemeenschappelijk buitenlands en veiligheidsbeleid en het gemeenschappelijk veiligheids- en defensiebeleid van de EU, in het bijzonder Oekraïne en Moldavië***. Deze steun kan ook een aanvulling vormen op of bijdragen aan bijstand die een lidstaat aan een andere lidstaat verleent in het kader van artikel 42, lid 7, van het Verdrag betreffende de Europese Unie.

Amendement 56

Voorstel voor een verordening
Artikel 16 – lid 2 – punt b bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	b bis) de aanbieder toont aan dat zijn besluitvormings- en beheersstructuren gevrijwaard zijn tegen ongewenste beïnvloeding door regeringen van staten welke zou indruisen tegen de veiligheids- en defensiebelangen van de Unie en haar lidstaten als vastgesteld in het kader van het GBVB uit hoofde van titel V van het VEU;

Amendement 57

Voorstel voor een verordening
Artikel 16 – lid 2 – punt f

Door de Commissie voorgestelde tekst	*Amendement*
f) de aanbieder beschikt over de technische hardware en software die nodig zijn om de gevraagde dienst te ondersteunen;	f) de aanbieder beschikt over de technische hardware en software die nodig zijn om de gevraagde dienst te ondersteunen***, en voldoet aan de vereisten van artikel X van Verordening XX/XXXX (verordening cyberweerbaarheid)***;

Amendement 58

Voorstel voor een verordening
Artikel 16 – lid 2 – punt j bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	j bis) Geen enkele aanbieder die afkomstig is uit een derde land met een hoog risico wordt toegelaten.

Amendement 59

Voorstel voor een verordening
Artikel 16 – lid 2 – punt j ter (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	j ter) de aanbieder werkt, voor zover mogelijk, nauw samen met relevante kmo's;

Amendement 60

Voorstel voor een verordening
Artikel 17 – lid 1

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

	a) de associatieovereenkomsten die zijn gesloten met betrekking tot hun deelname aan het programma Digitaal Europa daarin voorzien***;***
	b) in die derde landen een GVDB-missie wordt ingezet met een specifiek mandaat om de weerbaarheid tegen hybride dreigingen, waaronder cyberdreigingen, te versterken of waar een EVF-steunmaatregel is vastgesteld om de cyberweerbaarheid van het land te vergroten.

Amendement 61

Voorstel voor een verordening
Artikel 17 – lid 2

Door de Commissie voorgestelde tekst	*Amendement*
2. Steun uit de EU-cyberbeveiligingsreserve is in overeenstemming met deze verordening en voldoet aan alle specifieke voorwaarden die in de in lid 1 bedoelde associatieovereenkomsten zijn vastgesteld.	2. Steun uit de EU-cyberbeveiligingsreserve is in overeenstemming met deze verordening en voldoet aan alle specifieke voorwaarden die in de in lid 1 bedoelde associatieovereenkomsten zijn vastgesteld***, behalve voor de derde landen die onder de bepalingen van lid 1, punt b), vallen***.

Amendement 62

Voorstel voor een verordening
Artikel 18 – lid 1

Door de Commissie voorgestelde tekst	*Amendement*
1. Op verzoek van de Commissie, EU-CyCLONe of het CSIRT-netwerk evalueert en beoordeelt Enisa dreigingen, kwetsbaarheden en mitigerende maatregelen met betrekking tot een specifiek significant of grootschalig cyberbeveiligingsincident. Na de voltooiing van een evaluatie en beoordeling van een incident verstrekt Enisa een evaluatieverslag over het	1. Op verzoek van de Commissie, EU-CyCLONe of het CSIRT-netwerk evalueert en beoordeelt Enisa dreigingen, kwetsbaarheden en mitigerende maatregelen met betrekking tot een specifiek significant of grootschalig cyberbeveiligingsincident. Na de voltooiing van een evaluatie en beoordeling van een incident verstrekt Enisa een evaluatieverslag over het

incident aan het CSIRT-netwerk, EU-CyCLONe en de Commissie om hen te ondersteunen bij de uitvoering van hun taken, met name met het oog op de in de artikelen 15 en 16 van Richtlijn (EU) 2022/2555 vastgestelde taken. Indien relevant deelt de Commissie het verslag met de hoge vertegenwoordiger.	incident aan het CSIRT-netwerk, EU-CyCLONe en de Commissie om hen te ondersteunen bij de uitvoering van hun taken, met name met het oog op de in de artikelen 15 en 16 van Richtlijn (EU) 2022/2555 vastgestelde taken. Indien relevant***, met name wanneer het incident een derde land betreft,*** deelt de Commissie het verslag met de hoge vertegenwoordiger ***en de EDEO***.

Amendement 63

Voorstel voor een verordening
Artikel 18 – lid 3 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	3 bis. Het verslag wordt gedeeld met het Europees Parlement overeenkomstig het Unierecht of het nationale recht inzake de bescherming van gevoelige en gerubriceerde informatie.

Amendement 64

Voorstel voor een verordening
Artikel 19 – alinea 1 – punt 1 – a – 1
Verordening (EU) 2021/694
Artikel 6 – lid 1

Door de Commissie voorgestelde tekst	*Amendement*
a bis) ondersteunen van de ontwikkeling van een EU-cyberschild, met inbegrip van de ontwikkeling, uitrol en exploitatie van nationale en landsgrensoverschrijdende SOC-platforms die bijdragen tot het situationeel bewustzijn in de Unie en tot de versterking van de inlichtingencapaciteit van de Unie op het gebied van cyberdreigingen;	a bis) ondersteunen van de ontwikkeling van een EU-cyberschild, met inbegrip van de ontwikkeling, uitrol en exploitatie van nationale en landsgrensoverschrijdende SOC-platforms die bijdragen tot het situationeel bewustzijn in de Unie en tot de versterking van de inlichtingencapaciteit van de Unie op het gebied van cyberdreigingen ***en tot vermindering van de afhankelijkheid van de Unie van aanbieders met een hoog risico van kritieke cyberbeveiligingsapparatuur of -onderdelen wat zou indruisen tegen de veiligheids- en defensiebelangen van de***

	Unie en haar lidstaten als vastgesteld in het kader van het GBVB uit hoofde van titel V van het VEU;

Amendement 65

Voorstel voor een verordening
Artikel 20 – alinea 1

Door de Commissie voorgestelde tekst	*Amendement*
Uiterlijk ***[vier*** jaar na de datum van toepassing van deze verordening] dient de Commissie bij het Europees Parlement en de Raad een verslag in over de evaluatie en toetsing van deze verordening.	Uiterlijk ***[drie*** jaar na de datum van toepassing van deze verordening ***en vervolgens om de twee jaar]*** dient de Commissie bij het Europees Parlement en de Raad een verslag in over de evaluatie en toetsing van deze verordening.

PROCEDURE VAN DE ADVISERENDE COMMISSIE

Titel	De vaststelling van maatregelen ter versterking van de solidariteit en capaciteiten in de Unie om cyberdreigingen en -incidenten op te sporen, zich erop voor te bereiden en erop te reageren
Document- en procedurenummers	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Bevoegde commissie Datum bekendmaking	ITRE 1.6.2023
Advies uitgebracht door Datum bekendmaking	AFET 1.6.2023
Rapporteur voor advies Datum benoeming	Dragoş Tudorache 16.6.2023
Behandeling in de commissie	18.9.2023
Datum goedkeuring	24.10.2023
Uitslag eindstemming	+: 39 –: 4 0: 0
Bij de eindstemming aanwezige leden	Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Matjaž Nemec, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
Bij de eindstemming aanwezige vaste plaatsvervangers	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

HOOFDELIJKE EINDSTEMMING IN DE ADVISERENDE COMMISSIE

39	+
ECR	Lars Patrick Berg, Dominik Tarczyński
ID	Anna Bonfrisco, Jaak Madison
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Leopoldo López Gil, David McAllister, Vangelis Meimarakis, Francisco José Millán Mon, Željana Zovko
Renew	Petras Auštrevičius, Katalin Cseh, Bernard Guetta, Georgios Kyrtsos, Dragoş Tudorache
S&D	Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergei Stanishev
Verts/ALE	Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz

4	-
ID	Bernhard Zimniok
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Mick Wallace

0	0

Verklaring van de gebruikte tekens:
+ : voor
- : tegen
0 : onthouding