Europees Parlement
2019-2024

Commissie vervoer en toerisme

2023/0109(COD)

25.10.2023

ADVIES

van de Commissie vervoer en toerisme

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: Gheorghe Falcă

PA_Legam

BEKNOPTE MOTIVERING

Organisaties, waaronder organisaties in de vervoerssector, die het doelwit zijn van cyberaanvallen, melden deze aanvallen zelden. Dit komt doordat zij vrezen voor reputatieschade. De meeste organisaties kiezen ervoor om dergelijke kwesties intern op te lossen en in de meeste gevallen zijn het degenen die een aanval hebben gepleegd, die de publiciteit zoeken. De inwerkingtreding van Richtlijn (EU) 2022/2555 inzake netwerkbeveiliging (de "NIS2-richtlijn"), die door de lidstaten uiterlijk in oktober 2024 moet worden omgezet, zorgt ervoor dat de verplichtingen inzake meldingen van incidenten worden geharmoniseerd en dat is een goede zaak. Hierdoor zal er de komende jaren namelijk vermoedelijk meer inzicht komen in de aard en omvang van het probleem.

Recentelijk publiceerde het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) een rapport1 met gegevens over cyberdreigingen in de vervoerssector. Hieruit bleek dat cybercriminelen achter meer dan de helft (55 %) van de incidenten in 2022 zaten en dat de cybercriminelen in de meeste gevallen op geld uit waren. Uit het rapport bleek tevens dat de meeste cyberaanvallen in de vervoerssector zich richtten op IT-systemen en leidden tot operationele storingen.

Wat betreft paraatheid en respons in verband met cyberbeveiligingsincidenten is er momenteel sprake van beperkte steun op het niveau van de Unie en een beperkte onderlinge solidariteit tussen de lidstaten. In de conclusies van de Raad van mei 2022 wordt benadrukt dat deze problemen moeten worden aangepakt en wordt de Commissie verzocht om te komen met een voorstel voor een nieuw **cyberbeveiligingsnoodfonds**[2].

Met deze verordening wordt uitvoering gegeven aan de in december 2020 aangenomen **EU-strategie inzake cyberbeveiliging**, waarin de oprichting van een **Europees cyberschild** wordt aangekondigd en waarmee de capaciteit voor het opsporen van cyberdreigingen en het uitwisselen van informatie in de Europese Unie wordt versterkt via een federatie van nationale en landsgrensoverschrijdende Security Operation Centres (SOC's). De acties van deze verordening zullen worden ondersteund door **financiering in het kader van de strategische doelstelling "Cyberbeveiliging" van het programma Digitaal Europa**.

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

Een deel van de aanvullende 100 miljoen euro zal dienen ter versterking van de door het Europees Kenniscentrum voor cyberbeveiliging (ECCC) beheerde begroting voor de uitvoering van acties op het gebied van SOC's en paraatheid in het kader van hun werkprogramma('s). Daarnaast zal de aanvullende financiering dienen ter ondersteuning van de oprichting van de EU-cyberbeveiligingsreserve. Deze vormt een aanvulling op de begroting die reeds is voorzien voor soortgelijke acties in het overkoepelende programma Digitaal Europa en het

[1] "Understanding Cyber Threats in Transport", Enisa, gepubliceerd op 21 maart 2023.
[2] Conclusies van de Raad over de ontwikkeling van een cyberstrategie van de Europese Unie, 23 mei 2022 (doc. 9364/22).

werkprogramma cyberbeveiliging van het programma Digitaal Europa voor de periode 2023-2027, waardoor het totale bedrag voor de periode 2023-2027 op 551 miljoen euro kan uitkomen. In de periode 2021-2022 was reeds een bedrag van 115 miljoen euro toegewezen aan proefprojecten. Inclusief de bijdragen van de lidstaten zou de totale begroting kunnen oplopen tot 1,109 miljard euro.

Standpunt van de rapporteur voor advies

De rapporteur voor advies is ingenomen met het nieuwe voorstel en verwacht dat het de verschillende belanghebbenden aanzienlijke voordelen zal opleveren. De rapporteur voor advies wijst erop dat er uitvoeriger gekeken moet worden naar de cyberbeveiligingsbehoeften en cyberbeveiligingsvereisten in de vervoerssector en vindt dat kritieke entiteiten in deze sector toegang moeten krijgen tot passende financiering voor paraatheid voor, respons op en het verhelpen van cyberbeveiligingsincidenten.

De rapporteur voor advies spreekt zijn waardering uit voor de "Transport cybersecurity toolkit", die bedoeld is om het cyberbewustzijn en de cyberhygiëne te verbeteren en waarin de focus ligt op de vervoerssector. De toolkit richt zich tot vervoersorganisaties, ongeacht hun omvang en werkterrein, en heeft betrekking op kritieke vervoersinfrastructuur en militaire mobiliteit, in het bijzonder in verband met de oorlog in Oekraïne, en dan met name, doch niet uitsluitend:

- luchtvaartmaatschappijen, luchthavenbeheerders, tot het kernnetwerk behorende luchthavens, luchtverkeersbeheers- en luchtverkeersleidingscentra, het Agentschap van de Europese Unie voor de veiligheid van de luchtvaart en Eurocontrol;
- infrastructuurbeheerders, spoorwegondernemingen en het Europees beheersysteem voor het spoorverkeer (ERTMS);
- bedrijven voor vervoer over water (binnenvaart, kust- en zeevervoer) van passagiers en vracht, havenbeheerders, met inbegrip van hun havenfaciliteiten, entiteiten die werken en uitrusting in havens beheren, exploitanten van verkeersbegeleidingssystemen;
- wegenautoriteiten die verantwoordelijk zijn voor verkeersbeheer, exploitanten van intelligente vervoerssystemen;
- post- en koeriersdiensten.

De rapporteur is van mening dat de omvang van de begroting voor de werking van het **noodfonds voor cyberbeveiliging** (Emergency Response Fund for Cybersecurity, ERFC) bepalend zal zijn voor het succes ervan. Daarom moet het fonds groot genoeg zijn om de lidstaten te kunnen ondersteunen bij **de voorbereiding en de respons op en het herstel na** significante en grootschalige cyberbeveiligingsincidenten. Ook instellingen, organen en instanties van de Unie moeten steun kunnen krijgen voor respons op incidenten.

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

AMENDEMENT

De Commissie vervoer en toerisme verzoekt de bevoegde Commissie industrie, onderzoek en energie onderstaande amendementen in aanmerking te nemen:

Amendement 1

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 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	(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 ***en kritieke IT- en fysieke infrastructuur***. Gelet op het snel veranderende dreigingslandschap vereist de dreiging van mogelijke grootschalige incidenten die aanzienlijke verstoringen of schade aan kritieke infrastructuur veroorzaken, een grotere paraatheid op alle niveaus van het cyberbeveiligingskader van de Unie. Deze dreiging gaat verder dan de militaire agressie van Rusland tegen Oekraïne en zal waarschijnlijk aanhouden gezien het grote aantal staatsgebonden criminele en hacktivistische actoren die betrokken zijn bij de huidige geopolitieke spanningen. Dergelijke incidenten kunnen de verlening van openbare diensten***, openbaar en particulier vervoer,*** 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 alsook de mobiliteit binnen*** de Unie, en zelfs gevolgen voor de gezondheid of levensbedreigende gevolgen hebben. Bovendien zijn

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

Amendement 2

Voorstel voor een verordening
Overweging 2 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(2 bis) Door de staat gesteunde actoren, cybercriminelen en hacktivisten, die het gemunt hebben op autoriteiten, exploitanten, fabrikanten, leveranciers en dienstverleners in de luchtvaart, de zeevaart en het spoor- en wegvervoer vormen een steeds ernstiger cyberdreiging voor de vervoerssector. Het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) heeft geconstateerd dat het maandelijkse gemiddelde aantal gemelde incidenten met gevolgen voor de vervoerssector in 2022 met 25 % is gestegen ten opzichte van het niveau van 2021. De meeste aanvallen op de vervoerssector zijn gericht op informatietechnologiesystemen (IT), met mogelijke operationele verstoringen als gevolg[14bis].
	[14bis] Enisa (2023), rapport "Enisa threat landscape: transport sector", blz. 7 en blz. 17.

Amendement 3

Voorstel voor een verordening
Overweging 2 ter (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(2 ter) De niet-uitgelokte inval van

	Rusland in Oekraïne heeft geleid tot een aanzienlijke toename van de hoeveelheid cyberbeveiligingsincidenten, waaronder DDoS-cyberaanvallen (Distributed Denial-of-Service), gericht tegen de vervoersector in de EU en in gebieden in de nabijheid van de EU, met name luchthavens, spoorwegen en vervoersautoriteiten[14ter]. Deze toename van het aantal aanvallen zal hoogstwaarschijnlijk aanhouden.
	[14ter] Enisa (2023), rapport: "Enisa threat landscape: transport sector", blz. 9.

Amendement 4

Voorstel voor een verordening
Overweging 2 quater (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(2 quater) Cyberaanvallen zijn gericht tegen autoriteiten en instanties in alle subsectoren van het vervoer. Zo zijn spoorwegondernemingen, infrastructuurbeheerders en havenexploitanten het doelwit geweest van dergelijke aanvallen. Wat de sector wegvervoer betreft, zijn er fabrikanten van originele onderdelen (OEM's), leveranciers en dienstverleners getroffen, evenals exploitanten van openbaar vervoer. In de luchtvaartsector waren luchtvaartmaatschappijen en luchthavenexploitanten de belangrijkste doelwitten, gevolgd door dienstverleners, exploitanten van grondtransport en de toeleveringsketen[14quater].
	[14quater] Enisa (2023), rapport: "Enisa threat landscape: transport sector", blz. 17.

Amendement 5

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***, vervoerders*** 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 ***en over de toestand en de ontwikkeling van de cyberbeveiligingsarbeidsmarkt aangezien zij een belangrijke rol speelt bij het leveren van de nodige opsporings- en responsdiensten***.
[16] https://futureu.europa.eu/nl/	[16] https://futureu.europa.eu/nl/

Amendement 6

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]***, alsook het voorstel voor een verordening betreffende richtsnoeren van de Unie voor de ontwikkeling van het trans-Europees vervoersnetwerk en het voorstel voor een verordening betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen (verordening cyberweerbaarheid)***. 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.
[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).	[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	[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).

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 (***PB*** 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 7

Voorstel voor een verordening
Overweging 4 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(4 bis) De toolkit voor de cyberbeveiliging van de vervoerssector[2bis] van de Europese Commissie, met daarin basisinformatie over dreigingen die gevolgen kunnen hebben voor vervoersorganisaties (verspreiding van malware, DDoS-aanvallen, ongeoorloofde toegang, gegevensdiefstal en softwaremanipulatie) en diverse opsommingen van goede praktijken op het gebied van cyberbeveiliging, is een welkom instrument, maar daarnaast moet voorzien worden in goede opleidingen op het gebied van cyberbeveiliging ten behoeve van vervoersbedrijven en in passende instrumenten om cyberdreigingen te voorkomen. De begroting van de Unie moet de kosten dekken van de ondersteuning die geboden

wordt door Enisa, bijvoorbeeld in de vorm van scholing, zodat vervoerders in staat zijn om de beste risicobeperkende praktijken, zoals opgenomen in de toolkit, op doeltreffende wijze toe te passen.

[1bis] Rapport "Enisa threat landscape: transport sector", Enisa, maart 2023

[2bis] Europese Commissie, (2021). https://transport.ec.europa.eu/system/files/2021-10/cybersecurity-toolkit_nl.pdf

Amendement 8

Voorstel voor een verordening
Overweging 4 ter (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(4 ter) Een Uniebrede gecoördineerde aanpak die erop gericht is de paraatheid en veerkracht van kritieke infrastructuur, zoals vervoersinfrastructuur, te versterken, berust op capaciteitsopbouw van de lidstaten. Zoals onderkend in de recente mededeling van de Commissie aan het Europees Parlement en de Raad getiteld "Wegwerken van het tekort aan cyberbeveiligingsprofessionals om het concurrentievermogen, de groei en de veerkracht van Europa te versterken"[19bis], kan de veiligheid van de EU niet worden gewaarborgd zonder de meest waardevolle troef van de EU: de mensen.

[19 bis] Mededeling van de Commissie aan het Europees Parlement en de Raad - Wegwerken van het tekort aan cyberbeveiligingsprofessionals om het concurrentievermogen, de groei en de veerkracht van Europa te versterken ("De academie voor cyberbeveiligingsvaardigheden") COM(2023) 207 final.

Amendement 9

Voorstel voor een verordening
Overweging 12

Door de Commissie voorgestelde tekst	*Amendement*
(12) Om cyberdreigingen en -incidenten doeltreffender te voorkomen en te beoordelen en er doeltreffender op te reageren, is het noodzakelijk meer kennis te ontwikkelen over de bedreigingen voor kritieke activa en infrastructuur op het grondgebied van de Unie, met inbegrip van de geografische spreiding, interconnectie en mogelijke gevolgen ervan in geval van cyberaanvallen die deze infrastructuur treffen. Er moet een grootschalige EU-infrastructuur van SOC's worden uitgerold ("het Europees cyberschild"), bestaande uit verscheidene interoperabele landsgrensoverschrijdende platforms, die elk verscheidene nationale SOC's groeperen. Die infrastructuur moet de belangen en behoeften van de lidstaten en de Unie op het gebied van cyberbeveiliging dienen, door gebruik te maken van de modernste technologie voor geavanceerde instrumenten voor gegevensverzameling en -analyse, de capaciteit voor de opsporing en het beheer van cyberdreigingen en -incidenten te verbeteren en realtime situationeel bewustzijn te bieden. Die infrastructuur moet dienen om de opsporing van cyberdreigingen en -incidenten te verbeteren en aldus de entiteiten en netwerken van de Unie die verantwoordelijk zijn voor crisisbeheersing in de Unie, met name het Europees Netwerk van verbindingsorganisaties voor cybercrises ("EU-CyCLONe"), zoals gedefinieerd in Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad[24], aan te vullen en te ondersteunen.	(12) Om cyberdreigingen en -incidenten doeltreffender te voorkomen en te beoordelen en er doeltreffender op te reageren, is het noodzakelijk meer kennis te ontwikkelen over de bedreigingen voor kritieke activa en infrastructuur op het grondgebied van de Unie, met inbegrip van de geografische spreiding, interconnectie en mogelijke gevolgen ervan in geval van cyberaanvallen die deze infrastructuur treffen. ***Tot deze kritieke activa en infrastructuur behoren intelligente vervoerssystemen, die essentieel zijn voor geautomatiseerde en multimodale mobiliteit, maar functioneren op basis van cruciale uitwisseling van gevoelige gegevens.*** Er moet een grootschalige EU-infrastructuur van SOC's worden uitgerold ("het Europees cyberschild"), bestaande uit verscheidene interoperabele landsgrensoverschrijdende platforms, die elk verscheidene nationale SOC's groeperen. Die infrastructuur moet de belangen en behoeften van de lidstaten en de Unie op het gebied van cyberbeveiliging dienen, door gebruik te maken van de modernste technologie voor geavanceerde instrumenten voor gegevensverzameling en -analyse, de capaciteit voor de opsporing en het beheer van cyberdreigingen en -incidenten te verbeteren en realtime situationeel bewustzijn te bieden. Die infrastructuur moet dienen om de opsporing van cyberdreigingen en -incidenten te verbeteren en aldus de entiteiten en netwerken van de Unie die verantwoordelijk zijn voor crisisbeheersing in de Unie, met name het Europees Netwerk van verbindingsorganisaties voor cybercrises ("EU-CyCLONe"), zoals gedefinieerd in Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad[24],

aan te vullen en te ondersteunen.

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

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

Amendement 10

Voorstel voor een verordening
Overweging 14 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(14 bis) De vervoerssector is een van de meest lucratieve sectoren voor cybercriminelen geworden. Cybercriminelen beschouwen klantgegevens als zeer waardevolle handelswaar en richten zich steeds meer op de toeleveringsketen van het vervoer. Om die reden moeten nationale en met name grensoverschrijdende SOC's zich intensief richten op de analyse en monitoring van grensoverschrijdende infrastructuur en infrastructuur in het kader waarvan gebruik wordt gemaakt van gegevensuitwisseling via draadloze technologieën. In het recente voorstel tot herziening van de TEN-T-verordening wordt bijvoorbeeld meer solidariteit en samenwerking verlangd bij het delen van informatie over mogelijke grensoverschrijdende cyberdreigingen in verband met dit transnationale netwerk. Intelligente vervoerssystemen zijn uiterst belangrijk om het vervoer veiliger, efficiënter en duurzamer te maken, maar ze maken vervoerssystemen kwetsbaarder voor cyberaanvallen, die tot ongevallen of verkeersopstoppingen kunnen leiden en

	economische verliezen voor zowel particuliere als publieke exploitanten kunnen veroorzaken. Om de veiligheid van passagiers en de bescherming van gegevens van gebruikers en aanbieders te waarborgen en financiële schade te voorkomen, is het zeer belangrijk dat het uitvoeringsprogramma van de herziene richtlijn betreffende intelligente vervoerssystemen bepalingen en instrumenten bevat ter versterking van de samenwerking tussen de lidstaten op het gebied van het opsporen van cyberdreigingen en -incidenten en paraatheid en respons op dit gebied.

Amendement 11

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 de technologische soevereiniteit van de Unie. ***Om de autonomie van de Unie op cybergebied te versterken en in het licht van artikel 47, lid 4, van het voorstel voor een verordening betreffende richtsnoeren voor***

	de ontwikkeling van het trans-Europees vervoersnetwerk (COM(2021)0812) is het in dit verband ook noodzakelijk om toegang tot gegevens die tot cyberdreigingen leidt te voorkomen met behulp van een robuust regelgevingskader met bepalingen inzake buitenlands eigendom en buitenlandse investeringen in kritieke infrastructuur, waaronder in het vervoer.

Amendement 12

Voorstel voor een verordening
Overweging 21

Door de Commissie voorgestelde tekst	*Amendement*
(21) Hoewel het Europees cyberschild een civiel project is, zou de cyberdefensiegemeenschap kunnen profiteren van sterkere capaciteiten op het gebied van civiele opsporing en situationeel bewustzijn die zijn ontwikkeld voor de bescherming van kritieke infrastructuur. Landsgrensoverschrijdende SOC's moeten, met steun van de Commissie en het Europees Kenniscentrum voor cyberbeveiliging ("ECCC"), en in samenwerking met de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid (de "hoge vertegenwoordiger"), geleidelijk specifieke protocollen en normen ontwikkelen om samenwerking met de cyberdefensiegemeenschap mogelijk te maken, met inbegrip van doorlichting en beveiligingsvoorwaarden. De ontwikkeling van het Europees cyberschild moet gepaard gaan met een reflectie die het mogelijk maakt om in de toekomst samen te werken met netwerken en platforms die verantwoordelijk zijn voor informatie-uitwisseling in de cyberdefensiegemeenschap, in nauwe samenwerking met de hoge vertegenwoordiger.	(21) Hoewel het Europees cyberschild een civiel project is, zou de cyberdefensiegemeenschap kunnen profiteren van sterkere capaciteiten op het gebied van civiele opsporing en situationeel bewustzijn die zijn ontwikkeld voor de bescherming van kritieke infrastructuur. Landsgrensoverschrijdende SOC's moeten, met steun van de Commissie en het Europees Kenniscentrum voor cyberbeveiliging ("ECCC"), en in samenwerking met de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid (de "hoge vertegenwoordiger"), geleidelijk specifieke protocollen en normen ontwikkelen om samenwerking met de cyberdefensiegemeenschap mogelijk te maken, met inbegrip van doorlichting en beveiligingsvoorwaarden. De ontwikkeling van het Europees cyberschild moet gepaard gaan met een reflectie die het mogelijk maakt om in de toekomst samen te werken met netwerken en platforms die verantwoordelijk zijn voor informatie-uitwisseling in de cyberdefensiegemeenschap, in nauwe samenwerking met de hoge vertegenwoordiger. ***In dit kader moet gestreefd worden naar synergieën met het***

actieplan voor militaire mobiliteit 2.0. Een militaire-mobiliteitsnetwerk moet, om goed te kunnen functioneren, veerkrachtig zijn, onder meer in de context van cyber- en andere hybride dreigingen in verband met kritieke knooppunten voor tweeërlei gebruik binnen het vervoerssysteem. Zo kan een cyberaanval gericht tegen systemen die gebruikt worden op luchthavens, in havens of in verband met spoorwegen, of een cyberaanval gericht tegen militaire middelen grote gevolgen hebben. Om die reden moet in het kader van de digitalisering van processen en procedures, onder meer in verband met de noodzakelijke civiele en militaire samenwerking, de weerbaarheid van computerinformatiesystemen (CIS) tegen cyberdreigingen worden versterkt.

Amendement 13

Voorstel voor een verordening
Overweging 21 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(21 bis) In geval van een cyberbeveiligingscrisis is een doeltreffende uitwisseling van informatie van cruciaal belang om het situationeel bewustzijn in de sectoren militair en civiel vervoer te waarborgen. Deze uitwisseling van informatie moet ook de samenwerking tussen relevante sectorale autoriteiten die verantwoordelijk zijn voor vervoer, bevoegde cyberbeveiligingsautoriteiten, SOC's en CSIRT's bevorderen.

Amendement 14

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, 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	(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”). ***Er moet bijzondere aandacht worden besteed aan de vervoerssector en de subsectoren daarvan (lucht, spoor, water, weg), aangezien de kritieke infrastructuur van deze sectoren en subsectoren kwetsbaar is voor cyberincidenten en -aanvallen die veiligheid van passagiers en exploitanten ernstig kunnen aantasten.*** De gecoördineerde tests moeten gebaseerd zijn op gemeenschappelijke risicoscenario’s en -methoden. Bij de selectie van sectoren en de ontwikkeling van risicoscenario’s moet rekening worden gehouden met relevante Uniebrede risicobeoordelingen en risicoscenario’s, met inbegrip van de noodzaak om dubbel werk te voorkomen, zoals de risicobeoordeling en risicoscenario’s waarom wordt verzocht in de conclusies van de Raad over de ontwikkeling van de cyberstrategie van de Europese Unie en die door de Commissie, de hoge vertegenwoordiger en de NIS-samenwerkingsgroep moeten worden uitgevoerd, in coördinatie met de betrokken civiele en militaire organen en instanties en gevestigde netwerken,

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.

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.

[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 15

Voorstel voor een verordening
Overweging 30 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(30 bis) Gezien het kritieke karakter van de sector en de gevolgen van cyberdreigingen voor de mobiliteit en dus ook voor het leven van passagiers en voetgangers, moet bij het gecoördineerd testen van de paraatheid van entiteiten prioriteit worden gegeven aan de

vervoerssector.

Amendement 16

Voorstel voor een verordening
Overweging 35 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(35 bis) Aangezien Enisa in dit voorstel en in het voorstel voor de verordening cyberweerbaarheid met meer taken wordt belast en meer verantwoordelijkheden krijgt, is vaststelling van de gewijzigde begroting 1/2022 van Enisa voor de proeffase van een ondersteunende actie op het gebied van cyberbeveiliging noodzakelijk. Voorts moeten er, omdat er belangen van de Unie op het spel staan, aan Enisa aanvullende financiële en personele middelen worden toegewezen.

Amendement 17

Voorstel voor een verordening
Overweging 38 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(38 bis) De ontwikkeling van vaardigheden en competenties moet daarom centraal staan in alle sectoren en vooral in sectoren die kwetsbaar zijn voor cyberbeveiligingsdreigingen, en is onder meer belangrijk voor personeelsleden die werkzaamheden verrichten in verband met openbaarvervoers- of kritieke infrastructuur, zoals treinbesturingssystemen en digitale vervoersplanningsinstrumenten voor alle vervoerswijzen. Voor een succesvolle tenuitvoerlegging van deze verordening is het van het grootste belang dat er een cyberbeveiligingscultuur wordt gerealiseerd en dat deze verder wordt ontwikkeld zodat het bewustzijn onder de

	burgers en de kennis van deskundigen in alle sectoren van kritieke infrastructuur worden versterkt.

Amendement 18

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 ***sectoren*** industrie***, vervoersinfrastructuur*** en ***diensten*** 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;

Amendement 19

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 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;	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, ***met bijzondere aandacht voor kritieke IT- en fysieke infrastructuur,*** 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;

Amendement 20

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

Door de Commissie voorgestelde tekst	*Amendement*
	c bis) de paraatheid en doeltreffendheid van de Unie en de samenwerking binnen de Unie in het kader van de bescherming van vervoersinfrastructuur en -diensten in de lidstaten tegen cyberbeveiligingsincidenten versterken, om de continue werking van de vervoerssector, de integriteit van toeleveringsketens en de mobiliteit in de hele Unie te waarborgen.

Amendement 21

Voorstel voor een verordening
Artikel 3 – lid 2 – alinea 1 – punt c

Door de Commissie voorgestelde tekst	*Amendement*
c) draagt bij tot een betere bescherming tegen en respons op cyberdreigingen***;***	c) draagt bij tot een betere bescherming tegen en respons op cyberdreigingen***, onder meer voor vervoersinfrastructuur met een grensoverschrijdend karakter, zoals het TEN-T, of vervoersinfrastructuur in het kader waarvan gegevens worden uitgewisseld via draadloze technologieën, zoals intelligente vervoerssystemen.***

Amendement 22

Voorstel voor een verordening
Artikel 3 – lid 2 – alinea 2

Door de Commissie voorgestelde tekst	*Amendement*
Het cyberschild wordt ontwikkeld in samenwerking met de bij Verordening (EU) 2021/1173 opgerichte pan-Europese high-performance computing-infrastructuur.	Het cyberschild wordt ontwikkeld in samenwerking met de bij Verordening (EU) 2021/1173 opgerichte pan-Europese high-performance computing-infrastructuur. ***Het maakt samenwerking mogelijk, via specifieke protocollen en normen, met de***

	cyberdefensiegemeenschap, om de ontwikkeling van sterkere capaciteiten op het gebied van civiele opsporing en situationeel bewustzijn in verband met de bescherming van kritieke infrastructuur te waarborgen. In dit verband worden ook synergieën met het actieplan voor militaire mobiliteit 2.0 ontwikkeld en wordt gezorgd voor een doeltreffende uitwisseling van informatie om situationeel bewustzijn te creëren in de sectoren militair en civiel vervoer.

Amendement 23

Voorstel voor een verordening
Artikel 8 – lid 2 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	2 bis. De Commissie betrekt het Europees cyberschild, met name de grensoverschrijdende SOC's, bij de opstelling van haar adviezen aan de lidstaten in het kader van het voorstel voor een verordening betreffende het trans-Europees vervoersnetwerk (COM(2021)0812) wanneer de deelname of bijdrage van enigerlei aard door een natuurlijke persoon of een onderneming uit een derde land van invloed kan zijn op de cyberbeveiliging van grensoverschrijdende kritieke infrastructuur, zoals het TEN-T.

Amendement 24

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 in de hele Unie***, met bijzondere aandacht voor de in bijlage I bij Richtlijn (EU)***

	2022/2255 opgenomen vervoersinfrastructuur en de subsectoren daarvan;

Amendement 25

Voorstel voor een verordening
Artikel 18 – lid 2

Door de Commissie voorgestelde tekst	*Amendement*
2. Om het in lid 1 bedoelde evaluatieverslag over het incident op te stellen, werkt Enisa samen met alle relevante belanghebbenden, waaronder vertegenwoordigers van de lidstaten, de Commissie, andere relevante EU-instellingen, -organen en -instanties, aanbieders van beheerde beveiligingsdiensten en gebruikers van cyberbeveiligingsdiensten. In voorkomend geval werkt Enisa ook samen met entiteiten die getroffen zijn door significante of grootschalige cyberbeveiligingsincidenten. Ter ondersteuning van de evaluatie kan Enisa ook andere soorten belanghebbenden raadplegen. De geraadpleegde vertegenwoordigers maken elk mogelijk belangenconflict bekend.	2. Om het in lid 1 bedoelde evaluatieverslag over het incident op te stellen, werkt Enisa samen met alle relevante belanghebbenden, waaronder vertegenwoordigers van de lidstaten, de Commissie, andere relevante EU-instellingen, -organen en -instanties, aanbieders van beheerde beveiligingsdiensten en gebruikers van cyberbeveiligingsdiensten. In voorkomend geval werkt Enisa ook samen met entiteiten die getroffen zijn door significante of grootschalige cyberbeveiligingsincidenten***, met inbegrip van vervoersondernemingen***. Ter ondersteuning van de evaluatie kan Enisa ook andere soorten belanghebbenden raadplegen. De geraadpleegde vertegenwoordigers maken elk mogelijk belangenconflict bekend.

Amendement 26

Voorstel voor een verordening
Artikel 19 – alinea 1 – punt 1 – b
Verordening (EU) 2021/694
Artikel 6 – lid 2 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	2 bis. Gezien de belangen van de Unie die op het spel staan, gezien de verantwoordelijkheden van Enisa in verband met het opstellen van potentiële certificeringsregelingen uit hoofde van Verordening (EU) 2019/881, het uitvoeren van evaluaties en beoordelingen met

	betrekking tot cyberdreigingen, kwetsbaarheden en mitigatie, het opstellen van een evaluatie in het kader van het evaluatiemechanisme voor cyberbeveiligingsincidenten en het bieden van opleidingen op het gebied van de bescherming tegen cyberaanvallen en -incidenten aan exploitanten van kritieke infrastructuur, en in het licht van de nieuwe taken van Enisa in het kader van het voorstel voor de verordening cyberweerbaarheid, worden aan Enisa de nodige middelen toegekend uit de begroting van de Unie, overeenkomstig de toepasselijke wetgeving.

Amendement 27

Voorstel voor een verordening
Artikel 19 – alinea 1 – punt 1 bis (nieuw)
Verordening (EU) 2021/694
Artikel 7 – lid 1 – punt c bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	1 bis) Artikel 7 wordt als volgt gewijzigd:
	a) lid 1 wordt als volgt gewijzigd:
	1. het volgende punt c bis) wordt ingevoegd:
	c bis) ondersteunen van hoogwaardige opleidingen voor vervoerders en beheerders van kritieke infrastructuur in de vervoerssector en personen die werkzaam zijn op dit gebied, onder meer gericht op het doeltreffend delen van praktijken en uitvoeren van mitigatiemaatregelen in verband met cyberaanvallen en cyberbeveiligingsincidenten met betrekking tot kritieke infrastructuur, zoals de praktijken en maatregelen als vermeld in de toolkit voor de cyberbeveiliging van de vervoerssector.

PROCEDURE VAN DE ADVISERENDE COMMISSIE

Titel	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
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	TRAN 1.6.2023
Rapporteur voor advies Datum benoeming	Gheorghe Falcă 7.7.2023
Datum goedkeuring	25.10.2023
Uitslag eindstemming	+: 38 –: 0 0: 0
Bij de eindstemming aanwezige leden	Magdalena Adamowicz, Andris Ameriks, José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Karolin Braunsberger-Reinhold, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Carlo Fidanza, Jens Gieseke, Elsi Katainen, Elena Kountoura, Bogusław Liberadzki, Peter Lundgren, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Rovana Plumb, Thomas Rudner, Massimiliano Salini, Vera Tax, Barbara Thaler, István Ujhelyi, Achille Variati, Petar Vitanov, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Bij de eindstemming aanwezige vaste plaatsvervangers	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker

HOOFDELIJKE EINDSTEMMING IN DE ADVISERENDE COMMISSIE

38	+
ECR	Carlo Fidanza, Peter Lundgren, Dorien Rookmaker
ID	Roman Haider
PPE	Magdalena Adamowicz, Karolin Braunsberger-Reinhold, Gheorghe Falcă, Jens Gieseke, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Colm Markey, Cláudia Monteiro de Aguiar, Ljudmila Novak, Massimiliano Salini, Barbara Thaler, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Renew	José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Pierre Karleskind, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen
S&D	Andris Ameriks, Sara Cerdas, Josianne Cutajar, Bogusław Liberadzki, Rovana Plumb, Thomas Rudner, Vera Tax, István Ujhelyi, Achille Variati, Petar Vitanov
The Left	Elena Kountoura
Verts/ALE	Karima Delli, Anna Deparnay-Grunenberg, Pär Holmgren, Tilly Metz

0	-

0	0

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