Raad van de
Europese Unie

Brussel, 9 december 2022
(OR. en)

15623/22

Interinstitutioneel dossier:
2022/0338(NLE)

PROCIV 149	**ATO 102**
ENV 1248	**CSC 561**
JAI 1617	**ECOFIN 1279**
SAN 650	**CSCI 189**
COSI 315	**DATAPROTECT 346**
CHIMIE 100	**MI 912**
ENFOPOL 619	**CODEC 1916**
RECH 645	**COPS 581**
CT 220	**JAIEX 103**
DENLEG 93	**COPEN 430**
COTER 297	**IND 533**
RELEX 1657	**POLMIL 297**
ENER 654	**IPCR 116**
HYBRID 116	**DIGIT 231**
TRANS 768	**DISINFO 102**
CYBER 397	**CSDP/PSDC 848**
TELECOM 512	**MARE 71**
ESPACE 125	**POLMAR 78**

RESULTAAT BESPREKINGEN

van:	het secretariaat-generaal van de Raad
aan:	de delegaties
nr. vorig doc.:	13713/22, 15454/22
Betreft:	AANBEVELING VAN DE RAAD betreffende een Uniebrede gecoördineerde aanpak om de weerbaarheid van kritieke infrastructuur te versterken

In de bijlage vinden de delegaties de aanbeveling van de Raad betreffende een Uniebrede gecoördineerde aanpak om de weerbaarheid van kritieke infrastructuur te versterken, die de Raad tijdens zijn 3920e zitting van 8 december 2022 heeft aangenomen.

BIJLAGE

AANBEVELING (EU) 2022/… VAN DE RAAD

van...

betreffende een Uniebrede gecoördineerde aanpak om de weerbaarheid van kritieke infrastructuur te versterken

(Voor de EER relevante tekst)

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114 en artikel 292, eerste en tweede zin,

Gezien het voorstel van de Europese Commissie,

Overwegende hetgeen volgt:

(1) Met het oog op de goede werking van de interne markt is het in het belang van alle lidstaten en van de Unie als geheel om kritieke infrastructuur die binnen die markt essentiële diensten levert, duidelijk te identificeren en te beschermen, vooral in sleutelsectoren, zoals energie, digitale infrastructuur, vervoer en ruimtevaart; zulks geldt ook voor kritieke infrastructuur van aanzienlijk grensoverschrijdend belang[1], waarvan de verstoring aanzienlijke gevolgen kan hebben voor andere lidstaten.

[1] De lidstaten zouden dat belang moeten beoordelen in overeenstemming met hun nationale praktijken en kunnen dat doen op basis van onder meer een risicobeoordeling en het effect en de aard van de gebeurtenis.

(2) Deze aanbeveling, die een niet-bindende handeling is, getuigt van de politieke wil van de lidstaten om samen te werken en van hun engagement voor de aanbevolen maatregelen, benadrukt in een vijfpuntenplan van de voorzitter van de Europese Commissie, en eerbiedigt tevens ten volle de bevoegdheden van de lidstaten. Met deze aanbeveling wordt geen afbreuk gedaan aan de bescherming van de wezenlijke belangen van de nationale veiligheid, de openbare veiligheid of defensie van de lidstaten en van geen enkele lidstaat mag worden verwacht dat hij informatie deelt die die belangen schaadt.

(3) Hoewel de lidstaten en hun exploitanten van kritieke infrastructuur er primair verantwoordelijk voor zijn dat de veiligheid van kritieke infrastructuur is gewaarborgd en dat zij essentiële diensten levert, is meer coördinatie op het niveau van de Unie passend, vooral in het licht van veranderende dreigingen die gevolgen kunnen hebben voor meerdere lidstaten tegelijk, zoals de aanvalsoorlog van Rusland tegen Oekraïne en hybride campagnes tegen lidstaten, of die de weerbaarheid en de goede werking van de economie, de interne markt en de samenleving als geheel van de Unie kunnen aantasten. Bijzondere aandacht zou moeten worden besteed aan kritieke infrastructuur buiten het grondgebied van de lidstaten, zoals kritieke onderzeese infrastructuur en offshore-energie-infrastructuur.

(4) De Europese Raad heeft in zijn conclusies van 20 en 21 oktober 2022 de sabotage van kritieke infrastructuur, zoals de sabotage van de Nord Stream-pijplijnen, krachtig veroordeeld, en er daarbij op gewezen dat de Unie op elke opzettelijke verstoring van kritieke infrastructuur en op elke andere hybride actie eensgezind en vastberaden zal reageren.

(5) In het licht van een snel veranderend dreigingslandschap zou in sleutelsectoren, zoals energie, digitale infrastructuur, vervoer en ruimtevaart, en in andere door de lidstaten als relevant aangemerkte sectoren, voorrang moeten worden gegeven aan weerbaarheidsbevorderende maatregelen. Dergelijke maatregelen moeten de weerbaarheid van kritieke infrastructuur vergroten, rekening houdend met relevante risico's, met name cascade-effecten, verstoring van de toeleveringsketen, afhankelijkheid, gevolgen van klimaatverandering, onbetrouwbare verkopers en partners, en hybride dreigingen en campagnes, met inbegrip van buitenlandse informatiemanipulatie en inmenging. Daar waar het gaat om nationale kritieke infrastructuur zou, gezien de mogelijke gevolgen, voorrang moeten worden gegeven aan kritieke infrastructuur van aanzienlijk grensoverschrijdend belang. De lidstaten worden aangemoedigd om in voorkomend geval met spoed dergelijke weerbaarheidsbevorderende maatregelen te treffen, met behoud van de aanpak die is opgenomen in het evoluerende rechtskader.

(6) De bescherming van Europese kritieke infrastructuur in de energie- en de vervoerssector is momenteel geregeld bij Richtlijn 2008/114/EG van de Raad[2], en de beveiliging van netwerk- en informatiesystemen in de hele Unie, met het zwaartepunt op cyberdreigingen, wordt gewaarborgd door Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad[3]. Om een hoger gemeenschappelijk niveau van weerbaarheid en de bescherming van kritieke infrastructuur, cyberbeveiliging en de financiële markt te waarborgen, wordt het bestaande rechtskader gewijzigd en aangevuld met nieuwe regels voor kritieke entiteiten (CER-richtlijn), aangescherpte regels voor een hoog gemeenschappelijk niveau van cyber-beveiliging in de hele Unie (NIS2-richtlijn) en nieuwe regels die van toepassing zijn op digitale operationele weerbaarheid voor de financiële sector (DORA).

(7) De lidstaten zouden, overeenkomst het Unierecht en het nationale recht, alle beschikbare instrumenten moeten aanwenden om vooruitgang te boeken en de fysieke en cyber-weerbaarheid te helpen versterken. In dit verband moet onder kritieke infrastructuur worden verstaan: de betrokken kritieke infrastructuur die door een lidstaat op nationaal niveau is geïdentificeerd of die in het kader van Richtlijn 2008/114/EG als Europese kritieke infrastructuur is aangemerkt, en kritieke entiteiten die in het kader van de CER-richtlijn moeten worden geïdentificeerd of, in voorkomend geval, entiteiten die in het kader van de NIS2-richtlijn als kritieke entiteiten worden aangemerkt. Onder het begrip weerbaarheid moet worden verstaan het vermogen van kritieke infrastructuur om gebeurtenissen die de verlening van essentiële diensten op de interne markt aanzienlijk verstoren of kunnen verstoren, te voorkomen, daartegen bescherming te bieden, daarop te reageren, die te weerstaan, te mitigeren of op te vangen, zich daaraan aan te passen of daarvan te herstellen, met andere woorden, diensten die van cruciaal belang zijn om vitale maatschappelijke en economische functies, de openbare veiligheid en beveiliging, de volksgezondheid of het milieu in stand te houden.

---

2 Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren (PB L 345 van 23.12.2008, blz. 75).

3 Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).

(8) Er moeten nationale deskundigen bijeen worden geroepen om de werkzaamheden te coördineren voor een hoger gemeenschappelijk niveau van weerbaarheid en bescherming van kritieke infrastructuur, dat moet worden bewerkstelligd door de nieuwe regels voor kritieke entiteiten. Die gecoördineerde werkzaamheden zullen samenwerking tussen de lidstaten en informatie-uitwisseling over activiteiten mogelijk maken, zoals het uitwerken van methoden voor het identificeren van essentiële diensten die door kritieke infrastructuur worden verleend. De Commissie is al begonnen met het bijeenroepen van deze deskundigen en het faciliteren van hun werkzaamheden, en zij is voornemens daarmee door te gaan. Zodra de CER-richtlijn in werking treedt en er een Groep voor de weerbaarheid van kritieke entiteiten is opgericht uit hoofde van die richtlijn, moet die groep deze anticiperende werkzaamheden voortzetten zoals haar is opgedragen.

(9) Gezien het veranderde dreigingslandschap moet de mogelijkheid om kritieke infrastructuur op nationaal niveau aan stresstests te onderwerpen, verder worden ontwikkeld, aangezien dergelijke tests nuttig kunnen zijn om de weerbaarheid van kritieke infrastructuur te vergroten. Gelet op het specifieke belang van de energiesector en de gevolgen voor de hele Unie als die sector zou worden verstoord, zou die sector het meest gebaat zijn bij stresstests op basis van gezamenlijk overeengekomen beginselen. Dergelijke tests vallen onder de bevoegdheid van de lidstaten, die exploitanten van kritieke infrastructuur zouden moeten aanmoedigen en ondersteunen om deze tests uit te voeren, voor zover dit nuttig wordt geacht en in overeenstemming is met hun nationale rechtskaders.

(10) Om tot een gecoördineerde en doeltreffende respons op de huidige en verwachte dreigingen te komen, wordt de Commissie aangemoedigd de lidstaten extra steun te verlenen, met name door relevante informatie te verstrekken in de vorm van briefings, niet-bindende handboeken en richtsnoeren. De Europese Dienst voor extern optreden (EDEO) zou dreigingsevaluaties moeten opstellen, met name met de hulp van het Inlichtingen- en situatiecentrum van de EU 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). Daarnaast wordt de Commissie verzocht er in samenwerking met de lidstaten, voor te zorgen dat er meer gebruik wordt gemaakt van door de Unie gefinancierde onderzoeks- en innovatieprojecten.

(11) Door de toenemende onderlinge afhankelijkheid van fysieke en digitale infrastructuur is het mogelijk dat kwaadwillige cyberactiviteiten die zich richten op kritieke gebieden, leiden tot verstoring of beschadiging van fysieke infrastructuur, of dat sabotage van fysieke infrastructuur digitale diensten ontoegankelijk maakt. De lidstaten wordt verzocht vaart te zetten achter de voorbereidende werkzaamheden voor de omzetting en toepassing van het nieuwe rechtskader voor kritieke entiteiten en het versterkte rechtskader voor cyber-beveiliging, en daarbij zo spoedig mogelijk voort te bouwen op de ervaring die is opgedaan in de samenwerkingsgroep die is opgericht bij Richtlijn (EU) 2016/1148 (de "NIS-samenwerkingsgroep"), met inachtneming van de termijnen voor omzetting en het feit dat die werkzaamheden parallel en in samenhang moeten plaatsvinden.

(12) Naast het verbeteren van de paraatheid is het ook belangrijk de capaciteiten te versterken, zodat snel en doeltreffend kan worden gereageerd als de essentiële diensten van kritieke infrastructuur worden verstoord. Daarom bevat deze aanbeveling maatregelen op zowel Unie- als nationaal niveau, onder meer door het accent te leggen op de ondersteunende rol en de meerwaarde die kan worden verkregen door een versterkte samenwerking en informatie-uitwisseling in te stellen in het kader van het Uniemechanisme voor civiele bescherming (UCPM) dat is opgericht bij Besluit nr. 1313/2013/EU van het Europees Parlement en de Raad[4], en door gebruik te maken van de betrokken activa van het ruimtevaartprogramma van de Unie dat is vastgesteld in Verordening (EU) 2021/696 van het Europees Parlement en de Raad[5].

(13) De Commissie, de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid (de "hoge vertegenwoordiger") en de NIS-samenwerkingsgroep zouden, in samenwerking met de betrokken civiele en militaire organen en agentschappen en gevestigde netwerken, waaronder het Europees netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe), een risicobeoordeling moeten uitvoeren en risicoscenario's moeten opstellen. Daarnaast voert de NIS-samenwerkingsgroep, met de steun van de Commissie en het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), en in samenwerking met het Orgaan van Europese regulerende instanties voor elektronische communicatie (Berec), momenteel een risicobeoordeling uit, hiermee gevolg gevend aan de gezamenlijke ministeriële oproep van Nevers. Die twee exercities zullen consistent zijn en gecoördineerd worden met de exercitie inzake scenario-opbouw in het kader van het Uniemechanisme voor civiele bescherming die momenteel door de Commissie en de lidstaten wordt ontwikkeld, en die betrekking heeft op cyberbeveiligingsgebeurtenissen en de reële gevolgen daarvan. Met het oog op efficiëntie, doeltreffendheid en consistentie en ter wille van een degelijke toepassing van deze aanbeveling, zouden de resultaten van die exercities terug te vinden moeten zijn op nationaal niveau.

---

4 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).

5 Verordening (EU) 2021/696 van het Europees Parlement en de Raad van 28 april 2021 tot vaststelling van het ruimtevaartprogramma van de Unie, tot oprichting van het Agentschap van de Europese Unie voor het ruimtevaartprogramma en tot intrekking van de Verordeningen (EU) nr. 912/2010, (EU) nr. 1285/2013 en (EU) nr. 377/2014 en Besluit nr. 541/2014/EU (PB L 170 van 12.5.2021, blz. 69).

(14) Om de paraatheid en de capaciteit voor respons op grootschalige cyberbeveiligingsincidenten per direct te versterken, heeft de Commissie ter ondersteuning van de lidstaten een kortetermijnprogramma opgezet, via de toewijzing van aanvullende financiering aan Enisa. De voorgestelde diensten kunnen onder meer paraatheidsacties omvatten, zoals penetratietests van entiteiten om kwetsbaarheden te identificeren. Het programma kan ook meer mogelijkheden bieden om de lidstaten bij te staan in geval van een grootschalig cyberbeveiligingsincident dat kritieke entiteiten treft. Dit is een eerste stap in lijn met de conclusies van de Raad van 23 mei 2022 over de ontwikkeling van de cyberstrategie van de Europese Unie (de "conclusies van de Raad over de EU-cyberstrategie"), waarin de Commissie wordt verzocht met een voorstel voor een cyberbeveiligingsnoodfonds te komen. De lidstaten zouden die mogelijkheden ten volle moeten benutten, overeenkomstig de toepasselijke vereisten, en worden aangemoedigd de werkzaamheden op het gebied van EU-cybercrisisbeheer voort te zetten, met name door regelmatig te bezien en te evalueren hoever de uitvoering van het onlangs in de Raad ontwikkelde stappenplan voor cybercrisisbeheersing is gevorderd. Dit stappenplan is een levend document en moet zo nodig worden herzien en geactualiseerd.

(15) Onderzeese communicatiekabels die de wereld verbinden zijn van essentieel belang voor de mondiale connectiviteit en de connectiviteit binnen de EU. Voor de meeste segmenten van dit netwerk is visuele inspectie uiterst moeilijk vanwege de aanzienlijke lengte van die kabels en de locatie ervan op de zeebodem. De gedeelde jurisdictie en andere bevoegdheidskwesties in verband met dergelijke kabels vormen een specifiek thema voor Europese en internationale samenwerking op het gebied van de bescherming en het herstel van infrastructuur. Daarom moeten lopende en geplande risicobeoordelingen voor digitale en fysieke infrastructuur die dient ter ondersteuning van digitale diensten, worden aangevuld met specifieke risicobeoordelingen en opties voor risicobeperkende maatregelen met betrekking tot onderzeese kabels. De lidstaten verzoeken de Commissie daartoe studies uit te voeren en haar bevindingen met de lidstaten te delen.

(16) Ook de sectoren energie en vervoer kunnen worden getroffen door dreigingen op het gebied van digitale infrastructuur, bijvoorbeeld wanneer het gaat om energietechnologieën met digitale componenten. De beveiliging van de betrokken toeleveringsketens is belangrijk voor de continuïteit van de verlening van essentiële diensten en voor de strategische controle van kritieke infrastructuur in de energiesector. Met die omstandigheden moet rekening worden gehouden wanneer overeenkomstig deze aanbeveling maatregelen worden genomen om de weerbaarheid van kritieke infrastructuur te versterken.

(17) Omdat ruimtevaartinfrastructuur, ruimtegerelateerde activa op de grond, waaronder productie-installaties, en ruimtegebaseerde diensten steeds belangrijker worden voor veiligheidsgerelateerde activiteiten, is het van essentieel belang dat de weerbaarheid en de bescherming van de ruimtevaartsector van de Unie en van zijn activa en diensten op de grond binnen de Unie worden gewaarborgd. Om dezelfde redenen is het ook van essentieel belang dat in het kader van deze aanbeveling op meer gestructureerde wijze gebruik wordt gemaakt van ruimtegebaseerde gegevens en diensten die worden verstrekt door ruimte-systemen en -programma's voor bewaking en tracering en voor bescherming van kritieke infrastructuur in andere sectoren. In de komende EU-ruimtevaartstrategie voor veiligheid en defensie zullen passende maatregelen in dit verband worden voorgesteld, waarmee rekening moet worden gehouden bij de uitvoering van deze aanbeveling.

(18) Samenwerking op internationaal niveau is ook nodig om risico's voor kritieke infrastructuur doeltreffend te kunnen aanpakken, onder meer in internationale wateren. Daarom wordt de lidstaten verzocht met de Commissie en de hoge vertegenwoordiger samen te werken om bepaalde stappen te zetten om een dergelijke samenwerking tot stand te brengen, met dien verstande dat die stappen in overeenstemming moeten zijn met hun respectieve taken en verantwoordelijkheden uit hoofde van het recht van de Unie, met name de bepalingen van de Verdragen inzake externe betrekkingen.

(19) Zoals de Commissie in haar mededeling van 15 februari 2022 met als titel "Bijdrage van de Commissie aan de Europese defensie", ter ondersteuning van het "Strategisch kompas voor veiligheid en defensie – Voor een Europese Unie die haar burgers, waarden en belangen beschermt en bijdraagt aan de internationale vrede en veiligheid", heeft aangekondigd, zal zij in samenwerking met de hoge vertegenwoordiger en de lidstaten tegen 2023 de sectorale uitgangswaarden voor weerbaarheid beoordelen door lacunes en behoeften vast te stellen, alsook maatregelen om deze aan te pakken. Dat initiatief zou als input voor de werkzaamheden in het kader van deze aanbeveling moeten dienen en moeten bijdragen tot een betere uitwisseling van informatie en coördinatie van maatregelen om de weerbaarheid, waaronder die van kritieke infrastructuur, te versterken.

(20) In de EU-strategie voor maritieme veiligheid van 2014 en het bijbehorende herziene actieplan werd opgeroepen tot een betere bescherming van kritieke maritieme infrastructuur, waaronder onderwaterinfrastructuur, en in het bijzonder maritieme infrastructuur voor vervoer, energie en communicatie, onder meer door het maritiem bewustzijn te bevorderen door middel van betere interoperabiliteit en gestroomlijnde informatie-uitwisseling (verplicht en vrijwillig). Die strategie en dat actieplan worden momenteel bijgewerkt en zullen versterkte acties omvatten die de bescherming van kritieke maritieme infrastructuur tot doel hebben. Die acties zouden moeten dienen als aanvulling op deze aanbeveling.

(21) Het versterken van de weerbaarheid van kritieke infrastructuur draagt bij tot bredere inspanningen om hybride dreigingen en campagnes tegen de Unie en haar lidstaten tegen te gaan. Deze aanbeveling bouwt voort op de gezamenlijke mededeling aan het Europees Parlement en de Raad met als titel "Gezamenlijk kader voor de bestrijding van hybride bedreigingen – een reactie van de Europese Unie". Actie 1 van het gezamenlijk kader, namelijk de analyse van hybride risico's, speelt een belangrijke rol bij het identificeren van kwetsbaarheden die gevolgen kunnen hebben voor nationale en pan-Europese structuren en netwerken. Daarnaast zal de uitvoering van de conclusies van de Raad van 21 juni 2022 over een kader voor een gecoördineerde EU-respons op hybride campagnes zorgen voor een sterker gecoördineerd optreden door de toepassing van de EU-toolbox tegen hybride dreigingen op alle betrokken gebieden,

HEEFT DE VOLGENDE AANBEVELING VASTGESTELD:

HOOFDSTUK I: DOEL, TOEPASSINGSGEBIED EN PRIORITERING

(1) Deze aanbeveling bevat een reeks gerichte acties op Unie- en nationaal niveau om de weerbaarheid van kritieke infrastructuur op vrijwillige basis te ondersteunen en te vergroten, met de nadruk op kritieke infrastructuur van aanzienlijk grensoverschrijdend belang en in aangewezen sleutelsectoren, zoals energie, digitale infrastructuur, vervoer en ruimtevaart. Deze gerichte acties bestaan uit betere paraatheid, betere respons en internationale samenwerking.

(2) Informatie die met het oog op de verwezenlijking van de doelstellingen van deze aanbeveling wordt gedeeld en die op grond van Unie- en nationale regelgeving, alsook voorschriften inzake de vertrouwelijkheid van bedrijfsinformatie, vertrouwelijk is, mag uitsluitend met de Commissie en andere betrokken autoriteiten worden uitgewisseld indien dat noodzakelijk is voor de toepassing van deze aanbeveling. Met deze aanbeveling wordt geen afbreuk gedaan aan de bescherming van de wezenlijke belangen van de nationale veiligheid, de openbare veiligheid of defensie van de lidstaten, en van geen enkele lidstaat mag worden verwacht dat hij informatie deelt die deze belangen schaadt.

HOOFDSTUK II: BETERE PARAATHEID

Acties op het niveau van de lidstaten

(3) De lidstaten zouden een alle risico's omvattende aanpak moeten overwegen wanneer zij hun risicobeoordelingen of hun bestaande gelijkwaardige analyses actualiseren, in lijn met de veranderende aard van de huidige dreigingen voor hun kritieke infrastructuur, met name in aangewezen sleutelsectoren en, waar mogelijk, in alle sectoren die onder het komende nieuwe rechtskader voor kritieke entiteiten vallen.

(4) De lidstaten wordt verzocht vaart te zetten achter de voorbereidende werkzaamheden en, waar mogelijk, weerbaarheidsbevorderende maatregelen vast te stellen, overeenkomstig het komende rechtskader voor kritieke entiteiten, met bijzondere aandacht voor samenwerking en relevante informatie-uitwisseling tussen de lidstaten en met de Commissie met betrekking tot het identificeren van kritieke entiteiten van aanzienlijk grensoverschrijdend belang en het versterken van de steun aan geïdentificeerde kritieke entiteiten om hun weerbaarheid te vergroten.

(5) De lidstaten zouden de opleiding en exercities van deskundigen en de uitwisseling van beste praktijken en geleerde lessen onder deskundigen moeten ondersteunen. De lidstaten zouden deskundigen moeten aanmoedigen om deel te nemen aan bestaande nationale en internationale opleidingsplatforms, bijvoorbeeld in het kader van het Uniemechanisme voor civiele bescherming.

(6) De lidstaten zouden exploitanten van kritieke infrastructuur, in elk geval in de energiesector, waar nodig moeten aanmoedigen en ondersteunen bij het uitvoeren van stresstests, met inachtneming van de beginselen die op Unieniveau gezamenlijk zijn overeengekomen. Stresstests zouden de weerbaarheid van kritieke infrastructuur tegen antagonistische door de mens veroorzaakte dreigingen moeten beoordelen. Daarom zouden de lidstaten ernaar moeten streven relevante kritieke infrastructuur te identificeren die moet worden getest en zo spoedig mogelijk, doch uiterlijk voor het einde van het eerste kwartaal van 2023, overleg moeten plegen met relevante exploitanten van kritieke infrastructuur. Daarnaast zouden de lidstaten de exploitanten van kritieke infrastructuur moeten ondersteunen zodat zij deze tests zo spoedig mogelijk kunnen uitvoeren en ernaar moeten streven deze voor eind 2023 te voltooien, overeenkomstig het nationale recht. De Raad is voornemens de stand van zaken met betrekking tot de stresstests uiterlijk eind april 2023 te evalueren.

(7) Gezien de snel veranderende dreigingen voor kritieke infrastructuur is het van vitaal belang dat het hoge beschermingsniveau van die infrastructuur wordt gehandhaafd. De lidstaten worden aangemoedigd voldoende financiële middelen toe te wijzen om de capaciteit van hun bevoegde nationale autoriteiten te versterken en om hen te ondersteunen bij het weerbaarder maken van hun kritieke infrastructuur. De lidstaten worden ook aangemoedigd voldoende financiële middelen toe te wijzen aan autoriteiten die verantwoordelijk zijn voor het beheer van grootschalige cyberincidenten om hen te ondersteunen en ervoor te zorgen dat hun Computer Security Incident Response Teams (CSIRT's) en bevoegde autoriteiten volledig worden gemobiliseerd in respectievelijk het CSIRT-netwerk en EU-CyCLONe.

(8) De lidstaten worden uitgenodigd om overeenkomstig de toepasselijke vereisten, gebruik te maken van potentiële financieringsmogelijkheden op Unie- en nationaal niveau om kritieke infrastructuur in de Unie voor henzelf weerbaarder te maken tegen alle significante dreigingen, en tevens om de exploitanten van kritieke infrastructuur aan te moedigen gebruik te maken van dergelijke financieringsmogelijkheden, waaronder bijvoorbeeld trans-Europese netwerken, met name in het kader van de programma's die worden gefinancierd door het Fonds voor interne veiligheid dat is opgericht bij Verordening (EU) 2021/1149 van het Europees Parlement en de Raad[6], het Europees Fonds voor regionale ontwikkeling dat is opgericht bij Verordening (EU) nr. 1301/2013 van het Europees Parlement en de Raad[7], het Uniemechanisme voor civiele bescherming en REPowerEU. De lidstaten worden ook aangemoedigd optimaal gebruik te maken van de resultaten van relevante projecten in het kader van onderzoeksprogramma's, zoals het bij Verordening (EU) 2021/695 van het Europees Parlement en de Raad opgezette programma Horizon Europa[8].

---

6 Verordening (EU) 2021/1149 van het Europees Parlement en de Raad van 7 juli 2021 tot oprichting van het Fonds voor interne veiligheid (PB L 251 van 15.7.2021, blz. 94).

7 Verordening (EU) nr. 1301/2013 van het Europees Parlement en de Raad van 17 december 2013 betreffende het Europees Fonds voor Regionale Ontwikkeling en specifieke bepalingen met betrekking tot de doelstelling "Investeren in groei en werkgelegenheid", en tot intrekking van Verordening (EG) nr. 1080/2006 (PB L 347 van 20.12.2013, blz. 289).

8 Verordening (EU) 2021/695 van het Europees Parlement en de Raad van 28 april 2021 tot vaststelling van Horizon Europa – het kaderprogramma voor onderzoek en innovatie, tot vaststelling van de regels voor deelname en verspreiding en tot intrekking van Verordeningen (EU) nr. 1290/2013 en (EU) nr. 1291/2013 (PB L 170 van 12.5.2021, blz. 1).

(9) Wat de communicatie- en netwerkinfrastructuur in de Unie betreft, wordt de NIS-samenwerkingsgroep uitgenodigd om, in overeenstemming met artikel 11 van Richtlijn (EU) 2016/1148, haar op de gezamenlijke ministeriële oproep van Nevers gebaseerde lopende werkzaamheden met betrekking tot een gerichte risicobeoordeling te versnellen en zo snel mogelijk haar eerste aanbevelingen te doen. Die risicobeoordeling moet als input dienen voor de lopende sectoroverschrijdende risicobeoordeling en risicoscenario's op het vlak van cyberbeveiliging, waar de Raad in zijn conclusies over de EU-cyberstrategie om heeft gevraagd. Die werkzaamheden zouden coherent moeten zijn met en een aanvulling moeten vormen op de werkzaamheden van de NIS-samenwerkingsgroep op het gebied van de beveiliging van de toeleveringsketen van informatie- en communicatietechnologie, en de werkzaamheden van andere relevante groepen.

(10) De NIS-samenwerkingsgroep wordt tevens uitgenodigd om, met de steun van de Commissie en Enisa, haar werkzaamheden op het gebied van de beveiliging van de digitale infrastructuur voort te zetten, ook met betrekking tot onderzeese infrastructuur zoals onderzeese communicatiekabels. De groep wordt ook uitgenodigd om haar werkzaamheden op het gebied van de ruimtevaartsector te beginnen, onder meer door, waar nodig, beleids-richtsnoeren en methodologieën voor het beheer van cyberbeveiligingsrisico's op te stellen op basis van een alle risico's omvattende aanpak en een risicogebaseerde aanpak voor exploitanten in de ruimtevaartsector, teneinde de weerbaarheid van grondinfrastructuur ter ondersteuning van vanuit de ruimte opererende diensten, te vergroten.

(11) De lidstaten zouden ten volle gebruik moeten maken van de diensten voor paraatheid op het gebied van cyberbeveiliging die worden aangeboden in het met Enisa geïmplementeerde kortetermijnsteunprogramma van de Commissie, bijvoorbeeld penetratietests om kwetsbaarheden te identificeren. De lidstaten worden in dit verband aangemoedigd om prioriteit te geven aan entiteiten die kritieke infrastructuur exploiteren in de sectoren energie, digitale infrastructuur en vervoer.

(12) De lidstaten zouden ten volle gebruik moeten maken van het Europees Kenniscentrum voor cyberbeveiliging (ECCC). De lidstaten zouden hun nationale coördinatiecentra moeten aanmoedigen proactief samen te werken met de leden van de cyberbeveiligingsgemeenschap om capaciteit op te bouwen op Unie- en nationaal niveau om aanbieders van essentiële diensten beter te ondersteunen.

(13) Het is belangrijk dat de lidstaten werk maken van de in de EU-toolbox inzake 5G-cyberbeveiliging aanbevolen maatregelen en het is daarbij met name van belang dat de lidstaten beperkingen opleggen aan leveranciers met een hoog risico, aangezien tijdverlies de kwetsbaarheid van netwerken in de Unie kan vergroten, en daarnaast de fysieke en niet-fysieke bescherming van kritieke en gevoelige delen van de 5G-netwerken versterken, onder meer door middel van strikte toegangscontroles. Daarnaast zouden de lidstaten in samenwerking met de Commissie moeten beoordelen of aanvullende maatregelen nodig zijn om een consistent niveau van beveiliging en weerbaarheid van de 5G-netwerken te waarborgen.

(14) De lidstaten zouden zich samen met de Commissie en Enisa moeten concentreren op de uitvoering van de conclusies van de Raad van 17 oktober 2022 over de beveiliging van de ICT-toeleveringsketens.

(15) De lidstaten zouden rekening moeten houden met de komende netcode inzake cyberbeveiligingsaspecten van grensoverschrijdende elektriciteitsstromen [...], voortbouwend op de ervaring die is opgedaan met de uitvoering van Richtlijn (EU) 2016/1148 en de relevante richtsnoeren van de NIS-samenwerkingsgroep, met name het door die groep opgestelde referentiedocument over beveiligingsmaatregelen voor aanbieders van essentiële diensten.

(16) De lidstaten zouden het gebruik van Copernicus, Galileo en de European Geostationary Navigation Overlay Service (Egnos) voor bewakingsdoeleinden verder moeten ontwikkelen en relevante informatie delen met de overeenkomstig punt 15 bijeengeroepen deskundigen. Voor de monitoring van kritieke infrastructuur en de ondersteuning van crisisvoorspelling en -respons, moet goed gebruik worden gemaakt van de capaciteiten voor satelliet-communicatie voor overheidsgebruik (GOVSATCOM) in het kader van het ruimtevaartprogramma van de Unie.

Acties op het niveau van de Unie

(17) De dialoog en de samenwerking tussen de aangewezen deskundigen van de lidstaten en met de Commissie moeten worden versterkt om de fysieke weerbaarheid van kritieke infrastructuur te vergroten, met name door:

a) bij te dragen aan de voorbereiding, ontwikkeling en bevordering van gemeenschappelijke vrijwillige instrumenten om de lidstaten te helpen die weerbaarheid te vergroten, onder meer aan de hand van methodologieën en risicoscenario's;

b) de lidstaten te ondersteunen bij de uitvoering van het nieuwe rechtskader voor kritieke entiteiten, onder meer door de Commissie aan te moedigen de gedelegeerde handeling tijdig vast te stellen;

c) ondersteuning te verlenen voor de uitvoering van de in punt 6 bedoelde, op gemeenschappelijke beginselen gebaseerde stresstests, te beginnen met tests gericht op antagonistische door de mens veroorzaakte dreigingen in de energiesector en vervolgens in andere sleutelsectoren, alsook ondersteuning te verlenen voor en te adviseren over deze stresstests, op verzoek van een lidstaat;

d) gebruik te maken van een nog door de Commissie op te richten beveiligd platform om op vrijwillige basis beste praktijken, lessen uit nationale ervaringen en andere informatie met betrekking tot die weerbaarheid te verzamelen, te inventariseren en uit te wisselen.

Bij de werkzaamheden van die aangewezen deskundigen zou bijzondere aandacht moeten worden besteed aan sectoroverschrijdende afhankelijkheden en kritieke infrastructuur van aanzienlijk grensoverschrijdend belang, en deze werkzaamheden zouden waar passend moet worden opgevolgd door de Raad en de Commissie.

(18) De lidstaten worden aangemoedigd gebruik te maken van de steun die door de Commissie wordt aangeboden, bijvoorbeeld door het verstrekken van handleidingen en richtsnoeren, zoals een handboek over de bescherming van kritieke infrastructuur en openbare ruimten tegen onbemande luchtvaartuigsystemen, en instrumenten voor risicobeoordelingen. De EDEO wordt uitgenodigd om, met name via het Inlichtingen- en situatiecentrum van de EU en de EU-Fusiecel voor analyse van hybride dreigingen, met steun van het directoraat Inlichtingen van de EUMS in het kader van de gezamenlijke capaciteit op het gebied van inlichtingenanalyse (SIAC), briefings te houden over de dreigingen voor kritieke infrastructuur in de Unie, teneinde het situationeel bewustzijn te vergroten.

(19) De lidstaten zouden door de Commissie ondernomen acties moeten ondersteunen om ervoor te zorgen dat de resultaten van projecten die betrekking hebben op de weerbaarheid van kritieke infrastructuur en die worden gefinancierd in het kader van de onderzoeks- en innovatieprogramma's van de Unie, worden benut. De Raad neemt nota van het voornemen van de Commissie om de financiering voor die weerbaarheid te verhogen, met inachtneming van de grenzen van de begroting die in het meerjarig financieel kader 2021-2027 aan Horizon Europa is toegewezen, zonder afbreuk te doen aan de financiering van de andere projecten voor onderzoek en innovatie op het gebied van civiele veiligheid in het kader van Horizon Europa.

(20) Wegens de taakstelling die in de conclusies van de Raad over de EU-cyberstrategie is vastgelegd, worden de Commissie, de hoge vertegenwoordiger en de NIS-samenwerkingsgroep verzocht om overeenkomstig hun respectieve taken en verantwoordelijkheden uit hoofde van het Unierecht, intensiever samen te werken met relevante netwerken en civiele en militaire organen en agentschappen bij het uitvoeren van risico-evaluaties en het opzetten van risicoscenario's inzake cyberbeveiliging, waarbij met name rekening wordt gehouden met het belang van energie-, digitale, vervoers- en ruimtevaartinfrastructuur en de onderlinge afhankelijkheden tussen sectoren en lidstaten. Bij die exercitie zou rekening moeten worden gehouden met de betrokken risico's voor de infrastructuur waarvan die sectoren gebruikmaken. Indien dit voordeel oplevert, kunnen er regelmatig risico-evaluaties en scenario's worden uitgevoerd die de bestaande of geplande risicobeoordelingen in die sectoren zouden moeten aanvullen en hierop voort zouden moeten bouwen zonder deze evenwel te overlappen. Ze zouden als input moeten dienen voor discussies over de wijze waarop de algehele weerbaarheid van entiteiten die kritieke infrastructuur exploiteren, kan worden versterkt en kwetsbaarheden kunnen worden aangepakt.

(21) De Commissie wordt verzocht om, overeenkomstig haar respectieve taken in het kader van cybercrisisbeheer, haar activiteiten ter ondersteuning van de paraatheid en respons van de lidstaten op grootschalige cyberincidenten te versnellen, en dan met name om:

a) in aanvulling op relevante risicobeoordelingen in het kader van netwerk- en informatiebeveiliging, een uitgebreide studie[9] uit te voeren waarin de onderzeese infrastructuur, met name onderzeese communicatiekabels die de lidstaten met elkaar en Europa met de wereld verbinden, wordt geïnventariseerd. De bevindingen van deze studie zouden met de lidstaten moeten worden gedeeld;

b) de paraatheid van de lidstaten en de instellingen, organen en instanties van de Unie voor, en hun respons op, grootschalige cyberincidenten of ernstige incidenten te ondersteunen, overeenkomstig het versterkte rechtskader voor cyberbeveiliging en andere toepasselijke regels[10];

c) vaart te zetten achter het hoofdconcept van het cyberbeveiligingsnoodfonds en dit naar behoren te bespreken met de lidstaten.

(22) De Commissie wordt aangemoedigd om, onder meer in samenwerking met de lidstaten uit hoofde van de artikelen 6 en 10 van Besluit 1313/2013/EU en door middel van noodplanning, intensiever te werken aan toekomstgerichte anticiperende maatregelen om de operationele paraatheid voor en respons op storingen van kritieke infrastructuur van het Coördinatiecentrum voor respons in noodsituaties (ERCC) te ondersteunen; de investeringen op het gebied van preventiegerichte benaderingen en de paraatheid van de bevolking, te verhogen; en meer steun te verlenen voor capaciteitsopbouw in het kader van het kennisnetwerk op het gebied van Europese civiele bescherming.

---

9 Deze studie moet de capaciteiten en reserves, kwetsbaarheden, dreigingen en risico's voor de beschikbaarheid van diensten, de impact van de downtime van (trans-Atlantische) onderzeese kabels voor de lidstaten en de Unie als geheel en risicobeperking in kaart brengen, rekening houdend met de gevoeligheid van dergelijke informatie en de noodzaak om deze te beschermen.

10 Er zou ook bijzondere aandacht moeten worden besteed aan alle voorbereidende activiteiten voor een doeltreffende gecoördineerde respons op Unieniveau in het geval van een grensoverschrijdend ernstig cyberincident of een daarmee samenhangende dreiging die een systemische impact kan hebben op de financiële sector van de Unie, zoals voorgeschreven door het nieuwe rechtskader voor digitale operationele weerbaarheid.

(23) De Commissie moet het gebruik van bewakingsmiddelen van de Unie (Copernicus, Galileo en Egnos) bevorderen teneinde de lidstaten te ondersteunen bij de monitoring van kritieke infrastructuur en, in voorkomend geval, de onmiddellijke omgeving van die infrastructuur, en teneinde steun te geven aan andere bewakingsopties waarin het ruimtevaartprogramma van de Unie voorziet, zoals het kader voor omgevingsbewustzijn in de ruimte en het kader voor ruimtebewaking en -monitoring.

(24) In voorkomend geval en in overeenstemming met hun respectieve mandaat worden de agentschappen en andere relevante organen van de Unie uitgenodigd steun te verlenen in aangelegenheden die verband houden met de weerbaarheid van kritieke infrastructuur, met name op de volgende manieren:

a) het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol), op het gebied van informatieverzameling, criminaliteitsanalyse en ondersteuning van onderzoek bij grensoverschrijdende rechtshandhavingsacties en, indien relevant en passend, het delen van de resultaten met de lidstaten;

b) het Europees Agentschap voor maritieme veiligheid (EMSA), op het gebied van beveiliging en veiligheid van de maritieme sector in de Unie, met inbegrip van maritieme bewakingsdiensten voor aangelegenheden die verband houden met maritieme beveiliging en veiligheid;

c) het Agentschap van de Europese Unie voor het ruimtevaartprogramma (Euspa) en het Satellietcentrum van de EU (Satcen), die bijstand kunnen verlenen via operaties in het kader van het ruimtevaartprogramma van de Unie;

d) het ECCC, op het gebied van cyberbeveiliging, ook in samenwerking met Enisa, die innovatie en industriebeleid op het gebied van cyberbeveiliging kunnen ondersteunen.

HOOFDSTUK III: BETERE RESPONS

Acties op het niveau van de lidstaten

(25) De lidstaten wordt verzocht:

a) hun respons, indien relevant, te blijven coördineren en het overzicht over de sectoroverschrijdende respons op acute verstoringen van essentiële diensten die worden verleend door kritieke infrastructuur, te behouden. Dit zou gerealiseerd kunnen worden in het kader van een toekomstige blauwdruk voor een gecoördineerde respons op verstoringen van kritieke infrastructuur van aanzienlijk grensoverschrijdend belang; de bestaande geïntegreerde EU-regeling politieke crisisrespons (IPCR) voor de coördinatie van de politieke respons, indien het gaat om kritieke infrastructuur van grensoverschrijdend belang; de blauwdruk voor een gecoördineerde respons op grootschalige cyberincidenten en -crises uit hoofde van Aanbeveling (EU) 2017/1584 van de Commissie[11]; EU-CyCLONe; het kader voor een gecoördineerde EU-respons op hybride campagnes en de EU-toolbox in het geval van hybride dreigingen en campagnes; en het systeem voor snelle waarschuwing in het geval van desinformatie;

b) de informatie-uitwisseling op operationeel niveau met het ERCC in het kader van het Uniemechanisme voor civiele bescherming te intensiveren om tot betere vroegtijdige waarschuwing te komen en hun respons op verstoringen van kritieke infrastructuur van aanzienlijk grensoverschrijdend belang in het kader van het Uniemechanisme te coördineren, en zo te zorgen voor een snellere, door de Unie gefaciliteerde reactie wanneer dat nodig is;

c) hun paraatheid om te reageren op dergelijke in punt a), bedoelde aanzienlijke verstoringen, indien relevant, via bestaande of te ontwikkelen instrumenten te verhogen;

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

d) te werken aan de verdere ontwikkeling van relevante responscapaciteiten in het kader van de Europese pool voor civiele bescherming (ECPP) en in het kader van rescEU;

e) exploitanten van kritieke infrastructuur en relevante nationale autoriteiten aan te moedigen om hun capaciteiten te versterken zodat zij in staat zijn hun essentiële dienstverlening snel tot een basisniveau te herstellen;

f) exploitanten van kritieke infrastructuur aan te moedigen om, wanneer kritieke infrastructuur moet worden heropgebouwd, deze infrastructuur zodanig te bouwen, rekening houdend met de evenredigheid van maatregelen met betrekking tot risicobeoordelingen en kosten, dat deze zoveel mogelijk bestand is tegen alle significante risico's waaraan ze kan worden blootgesteld, ook in ongunstige klimaatscenario's.

(26) De lidstaten worden uitgenodigd om waar mogelijk vaart te zetten achter de voorbereidingen zoals bepaald door het versterkte rechtskader voor cyberbeveiliging, door er, in verband met de nieuwe taken van de CSIRT's en met het grotere aantal entiteiten uit nieuwe sectoren, naar te streven de capaciteiten van de nationale CSIRT's te vergroten door hun cyberbeveiligingsstrategieën tijdig te evalueren en bij te werken en door zo spoedig mogelijk nationale plannen voor incidenten en crisisrespons op het gebied van cyberbeveiliging vast te stellen, mochten deze nog niet bestaan.

(27) De lidstaten worden verzocht op nationaal niveau na te denken over de meest relevante middelen om ervoor te zorgen dat de belanghebbenden zich bewust zijn van de noodzaak om de weerbaarheid van kritieke infrastructuur te vergroten door middel van samenwerking met betrouwbare verkopers en partners. Het is belangrijk te investeren in extra capaciteit, met name in de sectoren waar de huidige infrastructuur zich aan het einde van de levensduur bevindt, bijvoorbeeld onderzeese communicatie-kabelinfrastructuur, om de continuïteit van de verlening van essentiële diensten in geval van verstoringen te waarborgen en ongewenste afhankelijkheden te verminderen.

(28) De lidstaten worden aangemoedigd om aandacht te besteden aan proactieve strategische communicatie op nationaal niveau in de context van de bestrijding van hybride dreigingen en campagnes en gezien de mogelijkheid dat tegenstanders zich kunnen proberen in te laten met buitenlandse informatiemanipulatie en inmenging door een eigen draai te geven aan verhalen over tegen kritieke infrastructuur gerichte incidenten.

Acties op het niveau van de Unie

(29) De Commissie wordt verzocht nauw samen te werken met de lidstaten om de relevante organen, instrumenten en responscapaciteiten verder te ontwikkelen, met het oog op een betere operationele paraatheid voor het aanpakken van de onmiddellijke en indirecte gevolgen van aanzienlijke verstoringen in de verlening van relevante essentiële diensten door kritieke infrastructuur, met name deskundigen en middelen die beschikbaar zijn via de ECPP en rescEU in het kader van het Uniemechanisme voor civiele bescherming of toekomstige EU-teams voor snelle reactie op hybride dreigingen.

(30) Rekening houdend met het veranderende dreigingslandschap en in samenwerking met de lidstaten wordt de Commissie in het kader van het Uniemechanisme voor civiele bescherming verzocht om:

a) de adequaatheid en operationele paraatheid van de bestaande responscapaciteiten voortdurend te analyseren en te testen;

b) potentieel belangrijke responscapaciteitstekorten in het kader van de ECPP en in het kader van rescEU regelmatig te monitoren en in kaart te brengen;

c) de sectoroverschrijdende samenwerking verder te intensiveren om te zorgen voor een adequate respons op Unieniveau, en, in samenwerking met een of meer lidstaten, regelmatig opleidingen of oefeningen te organiseren om die samenwerking te testen;

d) het ERCC verder te ontwikkelen tot een sectoroverschrijdend noodcentrum op Unieniveau voor de coördinatie van steun aan getroffen lidstaten.

(31) De Raad is vastbesloten een begin te maken met de werkzaamheden voor de goedkeuring van een blauwdruk voor een gecoördineerde respons op verstoringen van kritieke infrastructuur van aanzienlijk grensoverschrijdend belang, waarin de doelstellingen en vormen van samenwerking tussen de lidstaten en de instellingen, organen en instanties van de Unie wanneer zij reageren op incidenten inzake die kritieke infrastructuur, worden beschreven. De Raad kijkt uit naar het ontwerp van de Commissie voor een dergelijke blauwdruk, die voortbouwt op de steun en bijdragen van de relevante agentschappen van de Unie. De blauwdruk is volledig coherent en interoperabel met het herziene operationele Unieprotocol voor de bestrijding van hybride bedreigingen ("EU-draaiboek"), houdt rekening met de bestaande blauwdruk voor een gecoördineerde respons op grootschalige grensoverschrijdende cyberincidenten[12] en -crises en het EU-CyCLONe-mandaat zoals bepaald in de NIS2-richtlijn, en voorkomt overlapping van structuren en activiteiten. Wat de coördinatie van de respons betreft, moet de bestaande IPCR in die blauwdruk volledig worden geëerbiedigd.

[12] Aanbeveling (EU) 2017/1584 van de Commissie van 13 september 2017 inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises.

(32) De Commissie wordt verzocht relevante belanghebbenden en deskundigen te raadplegen over passende maatregelen in verband met mogelijke incidenten inzake onderzeese infrastructuur (die in samenhang met de in punt 20 a bedoelde inventarisatiestudie moeten worden gepresenteerd), alsook noodplannen, risicoscenario's en de in Besluit nr. 1313/2013/EU vervatte Uniedoelstellingen inzake rampbestendigheid verder uit te werken.

HOOFDSTUK IV: INTERNATIONALE SAMENWERKING

Acties op het niveau van de lidstaten

(33) De lidstaten zouden, waar passend en in overeenstemming met het Unierecht, moeten samenwerken met relevante derde landen met betrekking tot de weerbaarheid van kritieke infrastructuur van aanzienlijk grensoverschrijdend belang.

(34) De lidstaten worden aangemoedigd samen te werken met de Commissie en de hoge vertegenwoordiger om risico's voor kritieke infrastructuur in internationale wateren doeltreffend te kunnen aanpakken.

(35) De lidstaten worden uitgenodigd om, in samenwerking met de Commissie en de hoge vertegenwoordiger, bij te dragen tot de versnelde ontwikkeling en toepassing van de EU-toolbox tegen hybride dreigingen en de uitvoeringsrichtsnoeren als bedoeld in de conclusies van de Raad van 21 juni 2022 over een kader voor een gecoördineerde EU-respons op hybride campagnes, en deze vervolgens te gebruiken, teneinde het kader voor een gecoördineerde EU-respons op hybride campagnes ten volle ten uitvoer te leggen, met name bij het overwegen en voorbereiden van een alomvattende en gecoördineerde Unierespons op hybride campagnes en hybride dreigingen, onder meer tegen exploitanten van kritieke infrastructuur.

Acties op het niveau van de Unie

(36) De Commissie en de hoge vertegenwoordiger worden verzocht om, in voorkomend geval en in overeenstemming met hun respectieve taken en verantwoordelijkheden uit hoofde van het Unierecht, ondersteuning te verlenen aan relevante derde landen om kritieke infrastructuur op hun grondgebied en met name kritieke infrastructuur die fysiek verbonden is met hun grondgebied en dat van een lidstaat, weerbaarder te maken.

(37) De Commissie en de hoge vertegenwoordiger zullen, in overeenstemming met hun respectieve taken en verantwoordelijkheden uit hoofde van het Unierecht, de coördinatie met de NAVO op het gebied van de weerbaarheid van kritieke infrastructuur van gemeenschappelijk belang versterken via de gestructureerde dialoog tussen de EU en de NAVO over weerbaarheid, met volledige inachtneming van de bevoegdheden van de Unie en de lidstaten uit hoofde van de Verdragen, en de belangrijkste leidende beginselen voor de samenwerking tussen de EU en de NAVO zoals goedgekeurd door de Europese Raad, met name wederkerigheid, inclusiviteit en beslissingsautonomie. In dit verband zal die samenwerking worden voortgezet in het kader van de gestructureerde dialoog tussen de EU en de NAVO over weerbaarheid, die is ingebed in het bestaande mechanisme op stafniveau voor de uitvoering van de gezamenlijke verklaringen, waarbij volledige transparantie en betrokkenheid van alle lidstaten worden gewaarborgd.

(38) De Commissie wordt verzocht, indien nodig en passend, de deelname van vertegenwoordigers van betrokken derde landen in overweging te nemen in het kader van de samenwerking en informatie-uitwisseling tussen de lidstaten op het gebied van de weerbaarheid van kritieke infrastructuur die fysiek verbonden is met het grondgebied van een lidstaat en dat van een derde land.

Gedaan te …, …

Voor de Raad

De voorzitter