EUROPESE
COMMISSIE

Straatsburg, 18.10.2022
COM(2022) 551 final

2022/0338 (NLE)

Voorstel voor een

AANBEVELING VAN DE RAAD

betreffende een gecoördineerde aanpak van de Unie om de veerkracht van kritieke infrastructuur te versterken

(Voor de EER relevante tekst)

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

• Motivering en doel van het voorstel

Veiligheid is een essentiële doelstelling van de Europese Unie. Terwijl de verantwoordelijkheid voor de bescherming van burgers in de eerste plaats op de lidstaten rust, levert collectief optreden op het niveau van de Unie een belangrijke bijdrage aan de veiligheid van de Unie in haar geheel. Coördinatie zorgt voor grotere veerkracht en alertheid en een krachtigere, gezamenlijke respons. In het kader van de EU-veiligheidsunie zijn belangrijke stappen gezet om vermogens en capaciteiten op te bouwen op het gebied van preventie, opsporing en snelle reactie op tal van veiligheidsdreigingen, en om spelers in de publieke en private sector samen te laten werken.

Om de EU in staat te stellen het hoofd te bieden aan het altijd veranderende dreigingslandschap, is voortdurende waakzaamheid en aanpassing nodig. De Russische aanvalsoorlog tegen Oekraïne heeft nieuwe risico's met zich gebracht, die samen vaak samengaan in de vorm van een hybride dreiging. Een daarvan is het risico van verstoring van de verlening van essentiële diensten door entiteiten die in Europa kritieke infrastructuur exploiteren. De kennelijke sabotage van de Nord Stream-gaspijpleidingen en andere, recente incidenten hebben dit risico nog duidelijker gemaakt. De samenleving is sterk afhankelijk van zowel fysieke als digitale infrastructuur en de onderbreking van essentiële diensten – of dat nu het gevolg is van conventionele fysieke aanvallen, cyberaanvallen, of een combinatie van beide – kan ernstige gevolgen hebben voor het welzijn van de burgers, onze economieën en het vertrouwen in onze democratische systemen.

Het waarborgen van de goede werking van de interne markt is een andere belangrijke doelstelling van de EU, ook waar het gaat om de essentiële diensten die worden verleend door entiteiten die kritieke infrastructuur exploiteren. De EU heeft daarom al een aantal maatregelen genomen om de kwetsbaarheid van kritieke entiteiten te verminderen en hun veerkracht te vergroten, zowel wat cyber- als niet-cyberrisico's betreft.

Er is dringend actie nodig om de EU beter in staat te stellen zich te verweren tegen mogelijke aanvallen op kritieke infrastructuur, voornamelijk binnen de EU zelf, maar, daar waar relevant, ook in haar directe omgeving.

Met de voorgestelde aanbeveling van de Raad wordt beoogd de steun van de EU voor het vergroten van de veerkracht van kritieke infrastructuur op te voeren en te zorgen voor coördinatie op EU-niveau op het gebied van paraatheid en respons. Zij heeft tot doel de werkzaamheden ter bescherming van de activa, faciliteiten en systemen die binnen de interne markt nodig zijn voor het functioneren van de economie en het leveren van essentiële diensten waarop burgers zijn aangewezen, te maximaliseren en te versnellen, alsmede de gevolgen van eventuele aanvallen te beperken door het waarborgen van een zo snel mogelijk herstel. Hoewel al dergelijke infrastructuur zou moeten worden beschermd, geldt de eerste prioriteit momenteel de sectoren energie, digitale infrastructuur, vervoer en ruimtevaart, vanwege hun bij uitstek horizontale karakter voor de samenleving en de economie, en vanwege de actuele risicobeoordelingen.

Er is voor de EU een bijzondere rol weggelegd bij het waarborgen van de veerkracht van infrastructuur die land- of zeegrenzen overschrijdt en gevolgen heeft voor de belangen van meerdere lidstaten, of die wordt gebruikt om essentiële grensoverschrijdende diensten te verlenen. Kritieke infrastructuur die relevant is voor meerdere lidstaten kan echter in één lidstaat liggen of zelfs buiten het grondgebied van een lidstaat, bijvoorbeeld in het geval van

onderzeese kabels of pijpleidingen. Een duidelijke identificatie van de kritieke infrastructuur en de entiteiten die haar exploiteren, alsook van de risico's die deze infrastructuur bedreigen, en een collectieve inzet om haar te beschermen, zijn in het belang van alle lidstaten en de EU als geheel.

Het Europees Parlement en de Raad hebben reeds een politiek akkoord bereikt om het wetgevingskader te verdiepen zodat de EU entiteiten die kritieke infrastructuur exploiteren, veerkrachtiger kan helpen maken. In de zomer van 2022 werd overeenstemming bereikt over de richtlijn betreffende de veerkracht van kritieke infrastructuur ("CER-richtlijn")[1] en over de herziene richtlijn inzake de beveiliging van netwerk- en informatiesystemen ("NIS2-richtlijn")[2]. Deze richtlijnen zullen een aanzienlijke intensivering van de capaciteiten inhouden in vergelijking met het bestaande wetgevingskader, te weten Richtlijn 2008/114/EG 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 ("ECI-richtlijn")[3] en Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie ("NIS-richtlijn")[4]. De nieuwe wetgeving zal naar verwachting eind 2022 of begin 2023 in werking treden, en de lidstaten zouden prioriteit moeten geven aan de omzetting en toepassing daarvan, overeenkomstig het recht van de Unie.

Gelet daarop en gelet op het feit dat wellicht snel moet worden gereageerd op dreigingen ten gevolge van de Russische aanvalsoorlog tegen Oekraïne, zouden de in de nieuwe wetgeving omschreven stappen, waar mogelijk en passend, vanaf nu vervroegd moeten worden genomen. Als de wederzijdse samenwerking nu al wordt geïntensiveerd, zou dit ook het momentum helpen creëren voor een doeltreffende uitvoering wanneer de nieuwe wetgeving eenmaal volledig van kracht is.

Dit zou als resultaat hebben dat reeds verder wordt gegaan dan de huidige kaders, zowel wat de intensiteit van de maatregelen als de omvang van de bestreken sectoren betreft. De nieuwe CER-richtlijn bevat een nieuw kader voor samenwerking alsook verplichtingen voor de lidstaten en kritieke entiteiten, die de fysieke niet-cyberveerkracht moeten versterken tegen natuurlijke en door de mens veroorzaakte dreigingen waaraan die entiteiten, die essentiële diensten verlenen op de interne markt, blootstaan, en richt zich specifiek op elf sectoren[5]. De NIS2-richtlijn zal voorzien in een brede sectorale dekking van cyberbeveiligingsverplichtingen. Deze zullen een nieuwe verplichting voor de lidstaten omvatten om, waar relevant, onderzeese kabels op te nemen in hun cyberbeveiligingsstrategieën.

De wetgeving vereist dat de Commissie een belangrijke coördinerende rol op zich neemt. Op grond van de CER-richtlijn heeft de Commissie een ondersteunende en faciliterende rol, die moet worden uitgevoerd met de steun en betrokkenheid van de bij die richtlijn opgerichte Groep voor de veerkracht van kritieke entiteiten (Critical Entities Resilience Group (CERG), en zou zij de activiteiten van de lidstaten moeten aanvullen door beste praktijken, richtsnoeren en methodes te ontwikkelen. Wat cyberbeveiliging betreft, heeft de Raad reeds in zijn conclusies over de cyberstrategie van de EU in de zomer van 2022 de Commissie, de hoge

---

1 COM(2020) 829 final
2 COM(2020) 823 final
3 PB L 345 van 23.12.2008
4 PB L 194 van 19.7.2016
5 Energie, vervoer, digitale infrastructuur, bankwezen, financiëlemarktinfrastructuur, gezondheid, drinkwater, afvalwater, openbaar bestuur, ruimtevaart en voedsel

vertegenwoordiger en de NIS-samenwerkingsgroep uitgenodigd om te werken aan risicobeoordelingen en scenario's vanuit het oogpunt van cyberbeveiliging. Een dergelijke coördinatie kan als inspiratiebron dienen voor een aanpak voor andere cruciale kritieke infrastructuur.

Op 5 oktober 2022 presenteerde voorzitter Von der Leyen een 5-puntenplan, met een gecoördineerde aanpak van de noodzakelijke werkzaamheden. De belangrijkste elementen daarvan waren: verbetering van de paraatheid; samenwerking met de lidstaten om hun kritieke infrastructuur aan een stresstest te onderwerpen, te beginnen met de energiesector, gevolgd door andere sectoren met een hoog risico; vergroting van de responscapaciteit, met name via het Uniemechanisme voor civiele bescherming; goede gebruikmaking van satellietcapaciteit voor het opsporen van potentiële dreigingen; en versterking van de samenwerking met de NAVO en belangrijke partners op het gebied van de veerkracht van kritieke infrastructuur. In het 5-puntenplan werd benadrukt dat het belangrijk is te anticiperen op de wetgeving waarover reeds een politiek akkoord is bereikt.

In dit voorstel voor een aanbeveling van de Raad wordt deze aanpak om de steun aan de lidstaten te structureren en hun inspanningen ter versterking van het risicobewustzijn, de paraatheid en de respons op de actuele dreigingen, te coördineren, verwelkomd. In dit verband worden vergaderingen van deskundigen belegd om de veerkracht van entiteiten die kritieke infrastructuur exploiteren te bespreken, vooruitlopend op de inwerkingtreding van de CER-richtlijn en de daarbij ingestelde CERG.

Nauwere samenwerking met belangrijke partners en naburige en andere relevante derde landen op het gebied van de veerkracht van entiteiten die kritieke infrastructuur exploiteren, met name via de gestructureerde dialoog tussen de EU en de NAVO over veerkracht, zal van essentieel belang zijn.

De nadruk van deze aanbeveling ligt op het versterken van het vermogen van de Unie om te anticiperen en reageren op de nieuwe dreigingen ten gevolge van de Russische aanvalsoorlog tegen Oekraïne en om dergelijke dreigingen te voorkomen. De voorgestelde aanbevelingen zijn daarom gericht op het aanpakken van veiligheidsgerelateerde risico's en bedreigingen voor kritieke infrastructuur. Niettemin moet worden opgemerkt dat recente gebeurtenissen ook de noodzaak hebben onderstreept dringend meer aandacht te besteden aan de gevolgen van de klimaatverandering voor kritieke infrastructuur en diensten, bijvoorbeeld waar het gaat om seizoensgebonden problemen en onvoorspelbaarheid inzake watervoorraden voor de koeling van kerncentrales, waterkracht en binnenvaart, of het risico van materiële schade aan de vervoersinfrastructuur, waardoor ernstige verstoringen van essentiële diensten kunnen ontstaan. Deze punten van zorg zullen het voorwerp blijven vormen van relevante wetgeving en coördinatie.

- **Verenigbaarheid met bestaande bepalingen op het beleidsterrein**

Dit voorstel voor een aanbeveling van de Raad is volledig in overeenstemming met het huidige en toekomstige rechtskader inzake de veerkracht van entiteiten die kritieke infrastructuur exploiteren, respectievelijk de ECI-richtlijn en de CER-richtlijn, aangezien het onder meer tot doel heeft de samenwerking tussen de lidstaten op dit gebied te vergemakkelijken en concrete maatregelen te ondersteunen om de veerkracht te vergroten ten aanzien van de actuele imminente dreigingen voor entiteiten die kritieke infrastructuur in de EU exploiteren.

Het vormt ook een aanvulling op en anticipeert op de CER-richtlijn, door de lidstaten nu al uit te nodigen prioriteit te geven aan de tijdige omzetting van die richtlijn, door samen te werken via bijeenkomsten van deskundigen die worden belegd in het kader van het door de

Commissie aangekondigde 5-puntenplan en door te streven naar coördinatie bij de totstandkoming van een gemeenschappelijke aanpak voor het uitvoeren van stresstests inzake kritieke infrastructuur in de EU.

Het voorstel is ook in overeenstemming met de NIS-richtlijn en de toekomstige NIS2-richtlijn waarbij de NIS-richtlijn zal worden ingetrokken, omdat erin wordt opgeroepen tot een spoedige start van de uitvoering en omzetting. Het weerspiegelt ook de gezamenlijke oproep van Nevers van maart 2022 en de conclusies van de Raad over de EU-cyberstrategie van mei 2022 voor wat betreft het verzoek van de lidstaten aan de Commissie om risicobeoordelingen en risicoscenario's te ontwikkelen.

Het voorstel is ook in overeenstemming met het EU-beleid inzake civiele bescherming, op grond waarvan de lidstaten en derde landen in geval van een overweldigende verstoring van de werking van kritieke infrastructuur/entiteiten, in het kader van het Uniemechanisme voor civiele bescherming bijstand kunnen vragen via het Coördinatiecentrum voor respons in noodsituaties. In geval van activering van het Uniemechanisme voor civiele bescherming kan het Coördinatiecentrum voor respons in noodsituaties de inzet in het getroffen land van essentiële uitrusting, materialen en expertise die in de lidstaten (deels in het kader van de Europese pool voor civiele bescherming) en in het kader van rescEU beschikbaar zijn, coördineren en meefinancieren. Bij de bijstand die op verzoek kan worden gegeven, gaat het bijvoorbeeld om brandstof, generatoren, elektriciteitsinfrastructuur, opvangcapaciteit, waterzuiveringscapaciteit en medische noodcapaciteit.

Het voorstel is ook in overeenstemming met het EU-acquis op het gebied van energievoorzieningszekerheid.

De kernenergiesector is niet specifiek opgenomen in de voorgestelde aanbeveling van de Raad, met uitzondering van bijvoorbeeld daarmee verband houdende infrastructuur (zoals transmissielijnen naar kerncentrales) die van invloed kan zijn op de voorzieningszekerheid. Specifiek nucleaire elementen vallen onder de vigerende nucleaire wetgeving, met inbegrip van het Euratom-Verdrag en/of nationale wetgeving[6]. Op basis van de lessen die uit het ongeval in Fukushima zijn getrokken, is de Europese wetgeving inzake nucleaire veiligheid aangescherpt en als gevolg daarvan moeten de nationale autoriteiten voor elke installatie regelmatig periodieke veiligheidsevaluaties uitvoeren, teneinde ervoor te zorgen dat steeds aan de hoogste veiligheidseisen wordt voldaan, te bepalen welke verbeteringen op het gebied van veiligheid mogelijk zijn en zes jaarlijkse thematische collegiale toetsingen op EU-niveau vast te stellen.

In de EU-strategie voor maritieme veiligheid[7] en het bijbehorende actieplan[8] wordt gewezen op de veranderende aard van dreigingen op maritiem gebied en opgeroepen tot hernieuwde inzet voor de bescherming van kritieke maritieme infrastructuur, met inbegrip van onderwaterinfrastructuur, en met name maritieme vervoers-, energie- en communicatie-infrastructuur, onder meer door het maritieme bewustzijn te vergroten door middel van verbeterde interoperabiliteit en gestroomlijnde informatie-uitwisseling.

Het voorstel is ook in overeenstemming met andere relevante sectorale wetgeving. Daarom zou de uitvoering van deze aanbeveling moeten stroken met specifieke maatregelen die bepaalde aspecten van de veerkracht van entiteiten die actief zijn in de betrokken sectoren, zoals vervoer, reguleren of in de toekomst kunnen reguleren. Daarbij gaat het onder meer om

6 Overweging 9 van Richtlijn 2008/114/EG van de Raad (ECI-richtlijn)
7 11205/14
8 10494/18

andere relevante initiatieven, zoals het noodplan voor vervoer[9] of het noodplan voor voedselvoorziening en voedselzekerheid in tijden van crisis[10] en het daarmee verband houdende Europees mechanisme voor paraatheid en respons op het gebied van voedselzekerheid. Meer in het algemeen zou de aanbeveling uiteraard ten uitvoer moeten worden gelegd met volledige inachtneming van alle toepasselijke regels van het EU-recht, waaronder de regels die zijn neergelegd in de ECI-richtlijn en de NIS-richtlijn.

Het voorstel is ook in overeenstemming met het strategisch kompas inzake veiligheid en defensie, waarin wordt benadrukt dat de veerkracht en het vermogen om hybride dreigingen en cyberaanvallen tegen te gaan, aanzienlijk moeten worden vergroot, dat de veerkracht van partnerlanden moet worden versterkt en dat moet worden samengewerkt met de NAVO. Het is ook in overeenstemming met het kader voor een gecoördineerde EU-respons op hybride dreigingen en campagnes die gevolgen hebben voor de EU, de lidstaten en haar partners[11].

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

• Rechtsgrondslag

Het voorstel is gebaseerd op artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU), dat de onderlinge aanpassing van wetgevingen ter verbetering van de interne markt betreft, en daarnaast op artikel 292 VWEU. Dit wordt gerechtvaardigd door het feit dat met de voorgestelde aanbeveling van de Raad voornamelijk wordt beoogd te anticiperen op maatregelen in de nieuwe CER- en NIS2-richtlijnen, die beide óók op artikel 114 VWEU zijn gebaseerd. In overeenstemming met de logica die het gebruik van dat artikel als rechtsgrondslag voor die richtlijnen rechtvaardigt, is EU-optreden nodig om de goede werking van de interne markt te waarborgen, met name gezien de grensoverschrijdende aard en reikwijdte van de betrokken diensten en de mogelijke gevolgen in geval van verstoringen, alsook de bestaande en in de maak zijnde nationale maatregelen ter versterking van de veerkracht van entiteiten die kritieke infrastructuur exploiteren die wordt gebruikt om op de interne markt essentiële diensten te verlenen.

• Subsidiariteit (bij niet-exclusieve bevoegdheid)

Verdere stappen op Europees niveau op het gebied van de veerkracht van entiteiten die kritieke infrastructuur exploiteren, zijn gerechtvaardigd gezien de onderling afhankelijke, grensoverschrijdende verbanden tussen activiteiten op het gebied van kritieke infrastructuur en de essentiële diensten die worden verleend, en gezien de noodzaak van een meer gemeenschappelijke en gecoördineerde Europese aanpak, teneinde ervoor te zorgen dat de betrokken entiteiten in de huidige geopolitieke context voldoende veerkrachtig zijn. Aangezien veel van de gemeenschappelijke problemen, zoals de kennelijke sabotage van de North Stream-gaspijpleidingen, eerst en vooral worden aangepakt met nationale maatregelen of door entiteiten die kritieke infrastructuur exploiteren, is de steun van de EU, in voorkomend geval met inbegrip van relevante agentschappen, noodzakelijk om de veerkracht te versterken, de alertheid te verbeteren en de collectieve respons van de EU kracht bij te zetten.

---

9 COM(2022) 211

10 COM(2021) 689

11 Raad van de Europese Unie, doc. 10016/22 van 21 juni 2022.

- **Evenredigheid**

Dit voorstel is in overeenstemming met het evenredigheidsbeginsel van artikel 5, lid 4, van het Verdrag betreffende de Europese Unie.

Noch de inhoud noch de vorm van deze voorgestelde aanbeveling van de Raad gaat verder dan wat nodig is om de doelstellingen ervan te verwezenlijken. De voorgestelde maatregelen staan in verhouding tot de nagestreefde doelen, aangezien zij de prerogatieven en verplichtingen van de lidstaten uit hoofde van het nationale recht eerbiedigen.

Tot slot laat het voorstel ruimte voor een eventuele gedifferentieerde aanpak die rekening houdt met de verschillende interne situaties van de lidstaten wat betreft paraatheid ten opzichte van en respons op fysieke dreigingen voor kritieke infrastructuur.

- **Keuze van het instrument**

Om de bovengenoemde doelstellingen te verwezenlijken, voorziet het VWEU, met name in artikel 292, in de vaststelling door de Raad van aanbevelingen op basis van een voorstel van de Commissie. Een aanbeveling van de Raad is in dit geval een geschikt instrument, mede gelet op het huidige wetgevingskader, zoals dat hierboven uiteen is toegelicht. Als rechtshandeling geeft een aanbeveling van de Raad, ook al is deze niet bindend van aard, uitdrukking aan het feit dat de lidstaten de daarin opgenomen maatregelen onderschrijven en biedt zij een krachtige politieke basis voor samenwerking op de desbetreffende gebieden, met volledige inachtneming van de bevoegdheden van de lidstaten.

3. EVALUATIE, RAADPLEGING VAN BELANGHEBBENDEN EN EFFECTBEOORDELING

- **Raadpleging van belanghebbenden**

Bij de uitwerking van dit voorstel is rekening gehouden met de standpunten die de deskundigen van de lidstaten tijdens de bijeenkomst van 12 oktober 2022 over het voetlicht hebben gebracht. Er bestond brede consensus over het nut van meer coördinatie op het niveau van de Unie met betrekking tot paraatheid en respons in de actuele dreigingscontext en over het anticiperen op bepaalde elementen van de CER-richtlijn vóór de formele vaststelling daarvan. De lidstaten toonden zich bereid ervaringen en beste praktijken uit te wisselen met betrekking tot de maatregelen en methoden ter vergroting van de veerkracht van entiteiten die kritieke infrastructuur exploiteren. De lidstaten verklaarden ook open te staan voor een gecoördineerde aanpak van stresstests voor entiteiten die kritieke infrastructuur exploiteren, op basis van vrijwilligheid en van gemeenschappelijke beginselen. De lidstaten gaven te kennen dat in het kader van deze aanbeveling prioriteit zou moeten worden gegeven aan entiteiten die kritieke infrastructuur exploiteren in de sectoren energie, digitale infrastructuur en vervoer, met name die welke voor meerdere lidstaten relevant zijn. De lidstaten waren ook ingenomen met het voornemen van de Commissie om in de komende weken verdere bijeenkomsten van deskundigen van de lidstaten te beleggen.

- **Artikelsgewijze toelichting**

Het voorstel voor een aanbeveling is als volgt opgezet:

– In hoofdstuk I worden het doel van het voorstel, de inhoud ervan en de prioritering van de aanbevolen maatregelen uiteengezet.

– Hoofdstuk II is gericht op maatregelen die zouden moeten worden genomen om de paraatheid te verbeteren, zowel op het niveau van de Unie als dat van de lidstaten.

– Hoofdstuk III heeft betrekking op een betere respons, zowel op het niveau van de EU als dat van de lidstaten.

– Hoofdstuk IV heeft betrekking op internationale samenwerking en de maatregelen die zouden moeten worden genomen om entiteiten die kritieke infrastructuur exploiteren, veerkrachtiger te maken.

2022/0338 (NLE)

Voorstel voor een

AANBEVELING VAN DE RAAD

betreffende een gecoördineerde aanpak van de Unie om de veerkracht 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 de artikelen 114 en 292,

Gezien het voorstel van de Europese Commissie,

Overwegende hetgeen volgt:

(1) Er is voor de Unie een bijzondere rol weggelegd ten aanzien van grensoverschrijdende infrastructuur die aan de belangen van meerdere lidstaten raakt, of die door entiteiten wordt gebruikt voor de verlening van essentiële grensoverschrijdende diensten. Een dergelijke, voor meerdere lidstaten relevante dienstverlening en kritieke infrastructuur kan echter in één lidstaat of zelfs buiten het grondgebied van de lidstaten gesitueerd zijn, bijvoorbeeld in het geval van onderzeese kabels of pijpleidingen. Een duidelijke identificatie van dergelijke infrastructuren en entiteiten en van de dreigingen waaraan deze blootstaan, alsook een collectieve inzet om deze te beschermen, zijn in het belang van alle lidstaten en de EU als geheel.

(2) De bescherming van kritieke infrastructuur is in twee sectoren momenteel geregeld bij Richtlijn 2008/114/EG van de Raad[12]. Bij die richtlijn is een procedure ingesteld voor de identificatie van Europese kritieke infrastructuren en voor de aanmerking van infrastructuur als Europese kritieke infrastructuur, alsmede een gemeenschappelijke aanpak vastgesteld om te beoordelen of het nodig is de bescherming van dergelijke infrastructuur te verbeteren teneinde mensen te helpen beschermen. Zij heeft betrekking op de sectoren energie en vervoer. Om de veerkracht van kritieke entiteiten en van de essentiële diensten die zij verlenen en de kritieke infrastructuur die zij nodig hebben, te verbeteren, doorloopt een nieuwe richtlijn betreffende de veerkracht van kritieke entiteiten[13] (de CER-richtlijn) momenteel de procedure van vaststelling door de Uniewetgever; zij zal Richtlijn 2008/114/EG vervangen en meer sectoren bestrijken, waaronder digitale infrastructuur.

(3) Daarnaast legt Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van

[12] 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).

[13] COM(2020) 829

netwerk- en informatiesystemen in de Unie[14] de nadruk op cybergerelateerde dreigingen. Die richtlijn zal worden vervangen door een nieuwe richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie[15] ("NIS2-richtlijn"), die thans ook de procedure van vaststelling door de Uniewetgever doorloopt.

(4) In het licht van een snel evoluerend dreigingslandschap, met name in de context van de kennelijke sabotage van de gaspijpleidingen Nord Stream 1 en 2, worden entiteiten die kritieke infrastructuur exploiteren geconfronteerd met bijzondere problemen wat betreft hun veerkracht ten aanzien van vijandige handelingen en andere door de mens veroorzaakte bedreigingen, terwijl problemen als gevolg van natuurlijke factoren en klimaatverandering toenemen en met vijandige handelingen in wisselwerking kunnen treden. Daarom moeten zij, met steun van de lidstaten, passende veerkrachtbevorderende maatregelen nemen. Die maatregelen en steun zouden verder moeten gaan dan de maatregelen uit hoofde van Richtlijn 2008/114/EG en Richtlijn (EU) 2016/1148 en zelfs vóór de vaststelling, inwerkingtreding en omzetting van de nieuwe CER- en NIS2-richtlijnen moeten worden gerealiseerd.

(5) In afwachting van de vaststelling, inwerkingtreding en omzetting van die nieuwe richtlijnen worden de Unie en de lidstaten aangespoord om, overeenkomstig het Unierecht, gebruik te maken van alle instrumenten die beschikbaar zijn om vooruitgang te boeken en de fysieke en cyberveerkracht te helpen versterken van de betrokken entiteiten en de kritieke infrastructuur die deze exploiteren om essentiële diensten op de interne markt te verlenen, dat wil zeggen diensten, die van cruciaal belang zijn voor de instandhouding van vitale maatschappelijke functies, economische activiteiten, volksgezondheid en veiligheid of het milieu. In dit verband zou het begrip veerkracht moeten worden opgevat als het vermogen van een entiteit om gebeurtenissen die de verlening van de essentiële diensten in kwestie aanzienlijk kunnen verstoren of verstoren, te voorkomen, tegen die gebeurtenissen te beschermen, daarop te reageren, deze te weerstaan, mitigeren of op te vangen, zich daaraan aan te passen en daarvan te herstellen.

(6) Om te zorgen voor een aanpak die zowel doeltreffend als zoveel mogelijk in overeenstemming met de nieuwe CER-richtlijn is, zouden de in deze aanbeveling vervatte maatregelen betrekking moeten hebben op infrastructuur die door een lidstaat als kritieke infrastructuur is aangemerkt, waarbij het zowel om nationale kritieke infrastructuur als Europese kritieke infrastructuur kan gaan, ongeacht of de entiteit die de kritieke infrastructuur exploiteert in het kader van die nieuwe richtlijn reeds als kritieke entiteit is aangemerkt. Voor de toepassing van deze aanbeveling zou de term "kritieke infrastructuur" dienovereenkomstig moeten worden opgevat.

(7) In het licht van de actuele dreigingen zou in de sleutelsectoren energie, digitale infrastructuur, vervoer en ruimtevaart prioriteit moeten worden gegeven aan het nemen van veerkracht bevorderende maatregelen en dergelijke maatregelen zouden erop gericht moeten zijn entiteiten die kritieke infrastructuur exploiteren veerkrachtiger te maken ten aanzien van door de mens veroorzaakte risico's. Waar het gaat om nationale kritieke infrastructuur zou, gezien de mogelijke gevolgen wanneer de risico's

[14] 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).

[15] COM(2020) 823

intreden, voorrang moeten worden gegeven aan infrastructuur die van grensoverschrijdend belang is.

(8) De in deze aanbeveling vastgestelde maatregelen zijn dan ook hoofdzakelijk bedoeld om de nieuwe CER- en NIS2-richtlijnen, die gebaseerd zijn op artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU), aan te vullen, door te anticiperen op de maatregelen waarin die nieuwe richtlijnen zullen voorzien en deze te complementeren. Daarom, en gezien de grensoverschrijdende aard en relevantie van de essentiële diensten en kritieke infrastructuur in kwestie en de bestaande en zich ontwikkelende verschillen in nationale wetten die de interne markt verstoren, is het passend deze aanbeveling niet alleen te baseren op artikel 292 VWEU, maar ook op artikel 114 VWEU.

(9) De uitvoering van deze aanbeveling zou niet mogen worden opgevat als zou deze van invloed zijn op de huidige en toekomstige vereisten van het Unierecht met betrekking tot bepaalde aspecten van de veerkracht van de betrokken entiteiten en moet met die vereisten in overstemming zijn. Dergelijke vereisten zijn vastgelegd in algemene instrumenten zoals Richtlijn 2008/114/EG en Richtlijn (EU) 2016/1148 en de nieuwe CER- en NIS2-richtlijnen, die deze vervangen, maar ook in bepaalde sectorspecifieke instrumenten, zoals op het gebied van vervoer, waar de Commissie onder meer een initiatief heeft genomen met betrekking tot een noodplan voor vervoer[16]. Overeenkomstig het beginsel van loyale samenwerking moeten de bij de uitvoering van deze aanbeveling betrokken actoren elkaar ten volle respecteren en bijstand verlenen.

(10) De Commissie heeft op 5 oktober 2022 een vijfpuntenplan aangekondigd, met een gecoördineerde aanpak om het hoofd te bieden aan de uitdagingen die in het verschiet liggen, welke aanpak er onder meer in bestaat dat wordt gewerkt aan paraatheid door voort te bouwen en vooruit te lopen op de goedkeuring en inwerkingtreding van de nieuwe CER-richtlijn, en dat met de lidstaten wordt samengewerkt bij de uitvoering op basis van gemeenschappelijke beginselen van stresstests voor entiteiten die kritieke infrastructuur exploiteren, te beginnen in de energiesector. In deze aanbeveling, die aan dat plan zal bijdragen, wordt de voorgestelde aanpak toegejuicht en wordt uiteengezet hoe dit plan concreet kan worden uitgevoerd.

(11) Tegen de achtergrond van een snel evoluerend dreigingslandschap en de huidige risico-omgeving die wordt gekenmerkt door door de mens veroorzaakte risico's, met name met betrekking tot kritieke infrastructuur met grensoverschrijdende relevantie, is het van essentieel belang een nauwkeurig, actueel en volledig beeld te hebben van de belangrijkste risico's waarmee entiteiten die kritieke infrastructuur exploiteren, worden geconfronteerd. Daarom zouden de lidstaten de nodige maatregelen moeten nemen om hun beoordelingen van die risico's uit te voeren of te actualiseren. Hoewel in deze aanbeveling de nadruk op veiligheidsgerelateerde risico's ligt, zouden daarnaast de inspanningen moeten worden voortgezet om de klimaatverandering en milieurisico's aan te pakken, met name daar waar natuurrampen de door de mens veroorzaakte risico's verder kunnen verergeren.

(12) Gezien dat dreigingslandschap zouden de lidstaten moeten worden uitgenodigd om zo spoedig mogelijk passende maatregelen ter vergroting van de veerkracht van kritieke infrastructuur te nemen die straks uit hoofde van de nieuwe CER-richtlijn vereist zullen zijn, ook wanneer die verder gaan dan de genoemde risicobeoordelingen.

[16] COM(2022) 211

(13) In het kader van de uitvoering van het door de Commissie aangekondigde vijfpuntenplan moeten de werkzaamheden worden gecoördineerd door nationale deskundigen bijeen te roepen in afwachting van de oprichting van de Groep voor de veerkracht van kritieke entiteiten krachtens de nieuwe CER-richtlijn, teneinde samenwerking tussen de lidstaten en de uitwisseling van informatie met betrekking tot de veerkracht van entiteiten die kritieke infrastructuur exploiteren, mogelijk te maken. Daarbij zou het onder meer moeten gaan om samenwerking en uitwisseling van informatie met betrekking tot activiteiten als het identificeren van kritieke entiteiten en infrastructuur, het voorbereiden van de ontwikkeling en de verbreiding van een gemeenschappelijke reeks beginselen voor het uitvoeren van stresstests, het trekken van gemeenschappelijke lessen uit stresstests en het in kaart brengen van kwetsbaarheden en mogelijke capaciteiten. Deze processen zouden ook de veerkracht ten opzichte van klimaat- en milieurisico's moeten verbeteren van entiteiten die kritieke infrastructuur exploiteren. Deze werkzaamheden zouden ook een gemeenschappelijke prioritering van de werkzaamheden op het gebied van stresstests mogelijk maken, met nadruk op de sectoren energie, digitale infrastructuur en vervoer. 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 nieuwe CER-richtlijn in werking is getreden en de Groep voor de veerkracht van kritieke entiteiten is opgericht, zou die groep dergelijke anticiperende werkzaamheden moeten voortzetten overeenkomstig haar taken uit hoofde van de CER-richtlijn.

(14) De stresstest-exercitie zou moeten worden aangevuld met de opstelling van een blauwdruk voor incidenten en crises op het gebied van kritieke infrastructuur, waarin de doelstellingen en vormen van samenwerking tussen de lidstaten en de instellingen, organen en instanties van de EU bij de respons op incidenten inzake kritieke infrastructuur worden beschreven, met name voor het geval waarin deze incidenten aanzienlijke verstoringen van de verlening van essentiële diensten voor de interne markt met zich meebrengen. Deze blauwdruk zou gebruik moeten maken van de bestaande geïntegreerde regeling politieke crisisrespons (IPCR) voor de coördinatie van de respons en afgestemd moeten zijn alsook een aanvulling moeten vormen op de blauwdruk inzake grootschalige cyberincidenten en tevens moeten zorgen voor overeenstemming over belangrijke publieke boodschappen, aangezien crisiscommunicatie een belangrijke rol speelt bij het beperken van de negatieve gevolgen van incidenten en crises inzake kritieke infrastructuur.

(15) Om te zorgen voor een gecoördineerde en doeltreffende respons op de actuele en verwachte dreigingen, zal de Commissie de lidstaten aanvullende steun verlenen teneinde de veerkracht in het licht van die dreigingen te vergroten, met name door relevante informatie te verstrekken in de vorm van briefings, handboeken en richtsnoeren, de uitvoering van door de Unie gefinancierde onderzoeks- en innovatieprojecten te bevorderen, de nodige anticiperende maatregelen te nemen en het gebruik van de bewakingsmiddelen van de Unie te optimaliseren. De EDEO zou, met name via het inlichtingen- en situatiecentrum van de EU, dreigingsevaluaties moeten opstellen.

(16) Sectorrelevante agentschappen van de Unie en andere relevante organen zouden ook steun moeten verlenen op het gebied van veerkracht, voor zover hun respectieve, in de desbetreffende instrumenten van het Unierecht omschreven mandaten dit toelaten. Met name zou het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) bijstand kunnen verlenen op het gebied van cyberveiligheid, het Europees Agentschap voor maritieme veiligheid (EMSA) zijn deskundigheid kunnen inzetten voor het

ondersteunen van de lidstaten via zijn maritieme bewakingsdienst bij aangelegenheden die verband houden met maritieme beveiliging en veiligheid en het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol) steun kunnen verlenen bij het verzamelen van informatie en onderzoeken in het kader van grensoverschrijdende rechtshandhavingsacties, terwijl het Agentschap van de Europese Unie voor het ruimtevaartprogramma (Euspa) en het Satellietcentrum van de EU (Satcen) bijstand zouden kunnen verlenen via operaties in het kader van het ruimtevaartprogramma van de Unie.

(17) Hoewel de primaire verantwoordelijkheid voor het waarborgen van de veiligheid van kritieke infrastructuur en de betrokken entiteiten bij de lidstaten ligt, is meer coördinatie op het niveau van de Unie passend, met name in het licht van dreigingen die gevolgen kunnen hebben voor meerdere lidstaten tegelijk, zoals de aanvalsoorlog van Rusland tegen Oekraïne, of die gevolgen kunnen hebben voor de veerkracht en de goede werking van de economie, de eengemaakte markt en de samenlevingen van de Unie.

(18) Er wordt op grond van deze aanbeveling geen informatie verstrekt waarvan de openbaarmaking strijdig is met de wezenlijke belangen van de lidstaten op het gebied van nationale veiligheid, openbare veiligheid of defensie.

(19) Door de toenemende onderlinge afhankelijkheid van fysieke en digitale infrastructuur kunnen kwaadwillige cyberactiviteiten die zich richten op kritieke gebieden, leiden tot verstoring of beschadiging van fysieke infrastructuur, terwijl sabotage van fysieke infrastructuur digitale diensten ontoegankelijk kan maken. Gezien de toegenomen dreiging die van geavanceerde hybride aanvallen uitgaat, zouden de lidstaten overwegingen dienaangaande ook in aanmerking moeten nemen bij hun werkzaamheden ter uitvoering van deze aanbeveling. Gelet op de onderlinge verbanden tussen cyberbeveiliging en de fysieke beveiliging van exploitanten is het belangrijk dat de werkzaamheden ter voorbereiding van de omzetting en toepassing van de nieuwe NIS2-richtlijn zo spoedig mogelijk van start gaan en dat tegelijkertijd de werkzaamheden in het kader van de nieuwe CER-richtlijn worden voortgezet.

(20) Naast het verbeteren van de paraatheid is het ook belangrijk de capaciteiten te versterken zodat snel en doeltreffend kan worden gereageerd wanneer zich risico's voordoen die gevolgen hebben voor de verlening van essentiële diensten door entiteiten die kritieke infrastructuur exploiteren. Daarom zou deze aanbeveling moeten aangeven welke maatregelen zowel op het niveau van de lidstaten als op het niveau van de Unie zouden moeten worden genomen, met inbegrip van versterkte samenwerking en informatie-uitwisseling in het kader van het Uniemechanisme voor civiele bescherming en het gebruik van relevante activa van het ruimtevaartprogramma van de Unie.

(21) Naar aanleiding van het verzoek van de Raad in zijn conclusies over de cyberstrategie van de EU[17] zijn de Commissie, de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid ("hoge vertegenwoordiger") en de bij Richtlijn (EU) 2016/1148 ingestelde samenwerkingsgroep voor netwerk- en informatiebeveiliging ("NIS-samenwerkingsgroep") in coördinatie met de betrokken civiele en militaire organen en agentschappen en de bestaande netwerken, waaronder EU-CyCLONe, bezig met het uitvoeren van een risicobeoordeling en het opstellen van risicoscenario's voor cyberbeveiliging in geval van een dreiging of een mogelijke

[17] Cyberstrategie: Raad keurt conclusies goed - Consilium (europa.eu) (niet in het NL)

aanval tegen lidstaten of partnerlanden. Deze exercitie is gericht op kritieke sectoren, waaronder energie, digitale infrastructuur, vervoer en ruimtevaart.

(22) In de gezamenlijke ministeriële oproep van Nevers[18] en in de conclusies van de Raad over de cyberstrategie van de EU werd ook een oproep gedaan om de weerbaarheid van de communicatie-infrastructuur en -netwerken in de Unie te versterken door op basis van een risicobeoordeling aanbevelingen te doen aan de lidstaten en de Commissie. Deze risicobeoordeling wordt momenteel 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). In de risicobeoordeling en de kloofanalyse wordt gekeken naar de risico's van cyberaanvallen voor de verschillende deelsectoren van communicatie-infrastructuren, met inbegrip van vaste en mobiele infrastructuren, satellieten, onderzeese kabels, internetrouting enz., waardoor een basis wordt gelegd voor werkzaamheden in het kader van deze aanbeveling. Deze risicobeoordeling zal als input dienen voor de lopende sectoroverschrijdende risicobeoordeling en risicoscenario's op het vlak van cyberbeveiliging, waarom de Raad in zijn conclusies van 23 mei 2022 heeft verzocht.

(23) Er zal worden gezorgd voor consistentie en coördinatie tussen deze twee exercities en de exercitie inzake de scenario's die gericht zijn op civiele bescherming in de context van allerhande door de natuur of de mens veroorzaakte rampen, waaronder cyberbeveiligingsgebeurtenissen, en de reële gevolgen daarvan, en die momenteel door de Commissie en de lidstaten worden ontwikkeld in het kader van Besluit 1313/2013/EU van het Europees Parlement en de Raad[19]. Met het oog op efficiëntie, doeltreffendheid en consistentie zou bij de uitvoering van deze aanbeveling rekening moeten worden gehouden met de resultaten van die exercities.

(24) De EU-toolbox inzake 5G-cyberbeveiliging[20] bevat maatregelen en mitigatieplannen om de beveiliging van 5G-netwerken te versterken. Omdat veel essentiële diensten gebruikmaken van 5G-netwerken, en de digitale ecosystemen onderling geconnecteerd zijn, is het van essentieel belang dat alle lidstaten dringend uitvoering geven aan de in de toolbox aanbevolen maatregelen en met name voor essentiële voorzieningen die in de gecoördineerde EU-risicobeoordeling als kritiek en gevoelig worden aangemerkt, de desbetreffende beperkingen toepassen op aanbieders met een hoog risico.

(25) Om de paraatheid en de capaciteiten voor respons op grote cyberincidenten onmiddellijk te versterken, heeft de Commissie een kortetermijnprogramma ter ondersteuning van de lidstaten opgezet, middels toewijzing van aanvullende financiering aan Enisa. Bij de diensten in kwestie gaat het onder meer om paraatheidsacties, zoals penetratietests van kritieke entiteiten voor het identificeren van kwetsbaarheden. Het programma zal ook meer mogelijkheden bieden om de lidstaten bij te staan in geval van een ernstig incident dat kritieke entiteiten treft. Dit is een eerste stap in overeenstemming met de conclusies over de cyberstrategie, waarin de Raad de Commissie verzoekt een voorstel over een cyberbeveiligingsnoodfonds in te dienen. De lidstaten zouden deze mogelijkheden ten volle moeten benutten, overeenkomstig de toepasselijke voorschriften.

---

18 https://www.regeringen.se/494477/contentassets/e5f13bec9b1140038eed9a3d0646f8cf/joint-call-to-reinforce-the-eus-cybersecurity-capabilities.pdf

19 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).

20 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

(26) Het wereldwijde onderzeese kabelnetwerk voor data en elektronische communicatie is van essentieel belang voor de wereldwijde connectiviteit en de connectiviteit binnen de EU. Voor de meeste segmenten van dit netwerk is visuele inspectie uiterst moeilijk vanwege de aanzienlijke lengte van de kabels en de locatie ervan op de zeebodem. De gedeelde jurisdictie en andere bevoegdheidskwesties in verband met deze kabels vormen een bijzonder 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 infrastructuren die dienen ter ondersteuning van digitale diensten, worden aangevuld met specifieke risicobeoordelingen en opties voor risicobeperkende maatregelen met betrekking tot onderzeese kabels. De Commissie zal studies hiervoor uitvoeren en haar bevindingen met de lidstaten delen.

(27) De in deze aanbeveling genoemde prioritaire sectoren, energie en vervoer, kunnen ook gevolgen ondervinden van risico's voor digitale infrastructuur, bijvoorbeeld wanneer het gaat om energietechnologieën die digitale componenten bevatten. De beveiliging van de betrokken toeleveringsketens is belangrijk voor de continuïteit van de essentiëledienstverlening en voor de strategische controle van kritieke infrastructuur die door entiteiten in de energiesector wordt geëxploiteerd. Met die omstandigheden moet rekening worden gehouden wanneer overeenkomstig deze aanbeveling maatregelen worden genomen om de veerkracht van entiteiten die kritieke infrastructuur exploiteren, te versterken.

(28) Omdat ruimtevaartinfrastructuur en vanuit de ruimte opererende diensten steeds belangrijker worden voor veiligheidsgerelateerde activiteiten, is het van essentieel belang dat de veerkracht en de bescherming van de ruimtevaartactiva en -diensten van de Unie binnen de EU worden gewaarborgd, maar ook dat in het kader van deze aanbeveling op meer gestructureerde wijze gebruik wordt gemaakt van ruimtegebaseerde gegevens en diensten die worden verstrekt door ruimtesystemen en -programma's voor bewaking en 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.

(29) Samenwerking op internationaal niveau is ook nodig voor een doeltreffende aanpak van risico's voor de veerkracht van entiteiten die kritieke infrastructuur exploiteren, hetzij in de Unie, hetzij in relevante derde landen of in internationale wateren. Daarom zouden de lidstaten moeten worden uitgenodigd samen te werken met de Commissie en de hoge vertegenwoordiger om bepaalde stappen daartoe te ondernemen, met dien verstande dat dergelijke stappen alleen mogen worden genomen in overeenstemming met hun respectieve taken en verantwoordelijkheden uit hoofde van het recht van de Unie, met name de bepalingen van de EU-Verdragen inzake externe betrekkingen.

(30) Zoals de Commissie in de mededeling "Bijdrage van de Commissie aan de Europese defensie"[21], 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"[22], 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

[21] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52022DC0060&qid

[22] Raad van de Europese Unie, doc. 7371/22 van 21 maart 2022.

stellen, alsook maatregelen om deze aan te pakken. Dit 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 voor het verder versterken van de veerkracht, waaronder die van kritieke infrastructuur.

(31) In de EU-strategie voor maritieme veiligheid van 2014 en het bijbehorende actieplan werd opgeroepen tot een betere bescherming van kritieke maritieme infrastructuur, waaronder onderwaterinfrastructuur, en in het bijzondere 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). De strategie en het actieplan worden momenteel bijgewerkt en zullen versterkte acties omvatten die gericht zijn op de bescherming van kritieke maritieme infrastructuur. Die acties zouden moeten dienen als input voor en aanvulling op deze aanbeveling.

(32) De lidstaten zouden gebruik moeten maken van alle mogelijkheden van het programma van de Unie voor veiligheidsonderzoek, en meer bepaald de specifieke prioriteit inzake kritieke infrastructuur, met name in het kader van de door het Fonds voor interne veiligheid gefinancierde programma's, alsook van andere potentiële financieringsmogelijkheden op het niveau van de Unie, met name het Europees Fonds voor regionale ontwikkeling, voor zover de specifieke maatregelen voldoen aan de subsidiabiliteitsvereisten van dat fonds. REPowerEU kan ook mogelijkheden bieden voor financiering met het oog op veerkracht. Elk gebruik dat op deze wijze van de financieringsmogelijkheden van de Unie wordt gemaakt, moet in overeenstemming zijn met de toepasselijke wettelijke vereisten,

HEEFT DE VOLGENDE AANBEVELING VASTGESTELD:

HOOFDSTUK I: DOEL, TOEPASSINGSGEBIED EN PRIORITERING

(1) In deze aanbeveling worden de lidstaten uitgenodigd dringende en doeltreffende maatregelen te nemen en loyaal, efficiënt, solidair en gecoördineerd met elkaar, de Commissie en andere relevante overheidsinstanties en de betrokken entiteiten samen te werken om kritieke infrastructuur die voor de verlening van essentiële diensten op de interne markt wordt gebruikt, veerkrachtiger te maken.

(2) De in deze aanbeveling vervatte maatregelen hebben betrekking op infrastructuur die door een lidstaat is aangemerkt als kritieke infrastructuur, met inbegrip van Europese kritieke infrastructuur.

(3) Bij de uitvoering van deze aanbeveling zou prioriteit moeten worden gegeven aan het veerkrachtiger maken van entiteiten die actief zijn in de sectoren energie, digitale infrastructuur, vervoer en ruimtevaart, en van de door die entiteiten geëxploiteerde kritieke infrastructuur met grensoverschrijdende relevantie ten aanzien van door de mens veroorzaakte risico's.

HOOFDSTUK II: BETERE PARAATHEID

Acties op het niveau van de lidstaten

(4) De lidstaten worden uitgenodigd om risicobeoordelingen uit te voeren of bij te werken met betrekking tot de veerkracht van entiteiten die Europese kritieke infrastructuur exploiteren die in het kader van Richtlijn 2008/114/EG in de vervoers- en de energiesector is aangewezen, en om te streven naar onderlinge samenwerking met betrekking tot deze risicobeoordelingen en de daaruit voortvloeiende veerkracht

bevorderende maatregelen, in voorkomend geval en in overeenstemming met die richtlijn.

(5) Om ervoor te zorgen dat entiteiten die kritieke infrastructuur exploiteren, een hoog niveau van veerkracht bereiken, zouden de lidstaten bovendien vaart moeten zetten achter de voorbereidende werkzaamheden voor een zo spoedig mogelijke omzetting en toepassing van de nieuwe CER-richtlijn, door:

(a) sneller werk te maken van de vaststelling of de bijwerking van nationale strategieën voor het veerkrachtiger maken van entiteiten die kritieke infrastructuur exploiteren, teneinde het hoofd te bieden aan de bestaande dreiging. Relevante onderdelen van deze strategie zouden ter kennis van de Commissie moeten worden gebracht;

(b) overeenkomstig de evolutie van de bestaande dreigingen, ook in andere relevante sectoren dan energie, digitale infrastructuur, vervoer en ruimtevaart risicobeoordelingen met betrekking tot de veerkracht van entiteiten die kritieke infrastructuur exploiteren, uit te voeren of bij te werken, waar mogelijk ook in de sectoren die onder de nieuwe CER-richtlijn vallen, met name banken, infrastructuur voor de financiële markten, digitale infrastructuur, gezondheid, drinkwater, afvalwater, openbaar bestuur, ruimtevaart en voedselproductie, -verwerking en -distributie, rekening houdend met de mogelijke hybride aard van de betrokken dreigingen, met inbegrip van cascade-effecten en de gevolgen van de klimaatverandering;

(c) de Commissie, eventueel aan de hand van een door haar in samenwerking met de lidstaten opgesteld rapportagemodel, in kennis te stellen van de soorten risico's die per sector en deelsector zijn vastgesteld en van de resultaten van de risicobeoordelingen;

(d) het proces voor de identificatie en aanwijzing van kritieke entiteiten te versnellen, met prioriteit voor kritieke entiteiten die:

(a) gebruikmaken van kritieke infrastructuur met fysieke verbindingen tussen twee of meer lidstaten;

(b) behoren tot bedrijfsstructuren die verbonden zijn met of gekoppeld zijn aan kritieke entiteiten in andere lidstaten;

(c) in één lidstaat als zodanig zijn geïdentificeerd en essentiële diensten verlenen in of aan zes of meer lidstaten en derhalve van bijzonder Europees belang zijn, in welk geval de Commissie daarvan in kennis moet worden gesteld;

(d) met elkaar samen te werken, in het bijzonder waar het gaat om kritieke entiteiten en essentiële diensten en kritieke infrastructuur met grensoverschrijdende relevantie, met name door onderling overleg te plegen voor de toepassing van punt 5 d) en door elkaar te informeren in geval van een incident met een aanzienlijk of potentieel aanzienlijk grensoverschrijdend verstorend effect, en de Commissie op passende wijze op de hoogte te houden;

(e) de steun voor aangewezen kritieke entiteiten te versterken om hen veerkrachtiger te maken, onder meer door richtsnoeren en methodologieën te verstrekken, oefeningen voor het testen van hun veerkracht te organiseren, advies te verstrekken en hun personeel op te leiden, alsook door antecedentenonderzoeken van personen met een gevoelige functie mogelijk te maken, in overeenstemming met de Unie- en nationale wetgeving, als onderdeel van maatregelen van de kritieke entiteiten voor adequaat beheer van personeelsbeveiliging;

(f) de aanwijzing of instelling van een centraal contactpunt bij de bevoegde autoriteit te versnellen zodat dit ten aanzien van de centrale contactpunten van andere lidstaten een verbindingsfunctie kan uitoefenen met het oog op het waarborgen van grensoverschrijdende samenwerking inzake de veerkracht van entiteiten die kritieke infrastructuur exploiteren.

(6) De lidstaten worden aangemoedigd om stresstests uit te voeren op entiteiten die kritieke infrastructuur exploiteren. De lidstaten worden met name uitgenodigd om hun paraatheid en die van de betrokken entiteiten in de energiesector te vergroten en stresstests in deze sector uit te voeren, waar mogelijk volgens gezamenlijk op het niveau van de Unie overeengekomen beginselen, en om tegelijkertijd te zorgen voor doeltreffende communicatie met de betrokken entiteiten. Stresstests in andere prioritaire sectoren, met name digitale infrastructuur, vervoer en ruimtevaart, zouden, waar nodig, vervolgens in overweging kunnen worden genomen, rekening houdend met de inspecties in de deelsectoren luchtvaart en zeevervoer overeenkomstig het Unierecht, en met inachtneming van de desbetreffende bepalingen in de sectorale wetgeving.

(7) De lidstaten worden uitgenodigd om, in voorkomend geval en in overeenstemming met het Unierecht, met relevante derde landen samen te werken op het gebied van de veerkracht van entiteiten die kritieke infrastructuur met grensoverschrijdende relevantie exploiteren.

(8) De lidstaten worden uitgenodigd om overeenkomstig de toepasselijke vereisten gebruik te maken van potentiële financieringsmogelijkheden op Unie- en nationaal niveau om entiteiten die kritieke infrastructuur in de Unie exploiteren, bijvoorbeeld langs trans-Europese netwerken, veerkrachtiger te maken tegen alle significante dreigingen, met name in het kader van de door het Fonds voor interne veiligheid en het Europees Fonds voor regionale ontwikkeling gefinancierde programma's, mits aan de respectieve subsidiabiliteitscriteria wordt voldaan, en in het kader van de Connecting Europe Facility, met inbegrip van bepalingen inzake klimaatbestendigheid. De financiering in het kader van het Uniemechanisme voor civiele bescherming kan ook voor dat doel worden gebruikt, overeenkomstig de toepasselijke vereisten, met name voor projecten die verband houden met risicobeoordelingen, investeringsplannen of -studies, capaciteitsopbouw of verbetering van de kennisbasis. REPowerEU kan ook mogelijkheden bieden voor financiering met het oog op veerkracht.

(9) Wat de communicatie- en netwerkinfrastructuur in de Unie betreft, zou de NIS-samenwerkingsgroep, in overeenstemming met artikel 11 van Richtlijn (EU) 2016/1148 en vervolgens artikel 14 van de NIS2-richtlijn, haar lopende werkzaamheden met betrekking tot een gerichte risicobeoordeling moeten versnellen en begin 2023 eerste aanbevelingen moeten indienen. Die werkzaamheden zou coherent en complementair moeten zijn met de werkzaamheden van de NIS-samenwerkingsgroep op het gebied van de beveiliging van de toeleveringsketen van informatie- en communicatietechnologie, alsook met de werkzaamheden van andere relevante groepen, zoals de Groep voor de veerkracht van kritieke entiteiten die moet worden opgericht in het kader van de nieuwe CER-richtlijn en het toezichtforum dat moet worden opgericht in het kader van de nieuwe verordening betreffende digitale operationele veerkracht[23].

[23] COM(2020) 595 final.

(10) De NIS-samenwerkingsgroep, die haar taken moet uitvoeren overeenkomstig artikel 11 van Richtlijn (EU) 2016/1148 en vervolgens artikel 14 van de NIS2-richtlijn, wordt uitgenodigd om, met de steun van de Commissie en Enisa, prioriteit te geven aan haar werkzaamheden op het gebied van de beveiliging van de sectoren digitale infrastructuur en ruimtevaart, onder meer door met betrekking tot onderzeese communicatiekabels op basis van een op alle gevaren gebaseerde aanpak beleidsrichtsnoeren en methodologieën en maatregelen voor het beheer van cyberbeveiligingsrisico's op te stellen, in afwachting van de inwerkingtreding van de NIS2-richtlijn, en door ter attentie van exploitanten in de ruimtevaartsector richtsnoeren inzake maatregelen voor het beheer van cyberbeveiligingsrisico's te ontwikkelen die de grondinfrastructuur voor het ondersteunen van de verlening van vanuit de ruimte opererende diensten veerkrachtiger maken.

(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, met name 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 dringend werk moeten maken van de uitvoering van de in de EU-toolbox inzake 5G-cyberbeveiliging[24] aanbevolen maatregelen. Lidstaten die nog geen beperkingen ten aanzien van aanbieders met een hoog risico hebben ingevoerd, zouden dit onverwijld moeten doen, aangezien elke vertraging de netwerken in de Unie kwetsbaarder kan maken. Zij zouden ook de fysieke en niet-fysieke bescherming van kritieke en gevoelige delen van de 5G-netwerken moeten versterken, onder meer door middel van strikte toegangscontroles. Daarnaast zouden de lidstaten in samenwerking met de Commissie moeten beoordelen of aanvullende maatregelen, onder meer in de vorm van juridisch bindende vereisten op het niveau van de Unie, nodig zijn om een consistent niveau van beveiliging en veerkracht van de 5G-netwerken te waarborgen.

(13) De lidstaten zouden de komende netcode inzake cyberbeveiligingsaspecten van grensoverschrijdende elektriciteitsstromen zo spoedig mogelijk moeten uitvoeren, voortbouwend op de ervaring die is opgedaan met de uitvoering van de NIS-richtlijn en de relevante richtsnoeren van de NIS-samenwerkingsgroep, met name het door die groep opgestelde referentiedocument over beveiligingsmaatregelen voor aanbieders van essentiële diensten.

(14) De lidstaten zouden het gebruik van Galileo en/of Copernicus voor bewakingsdoeleinden moeten ontwikkelen en relevante informatie moeten delen met de deskundigen overeenkomstig punt 15. Met het oog op het monitoren van kritieke infrastructuur en het ondersteunen van crisisrespons zou goed gebruik moeten worden gemaakt van de capaciteiten voor satellietcommunicatie voor overheidsgebruik (GOVSATCOM) in het kader van het ruimtevaartprogramma van de Unie.

[24] 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

Acties op het niveau van de Unie

(15) De Commissie is voornemens om ter bevordering van de fysieke niet-cyberveerkracht van entiteiten die kritieke infrastructuur exploiteren, de samenwerking tussen deskundigen van de lidstaten te versterken, met name door:

(a) voorbereidingen te treffen voor de ontwikkeling en bevordering van gemeenschappelijke instrumenten ter ondersteuning van de lidstaten bij het vergroten van die veerkracht, onder meer aan de hand van methodologieën en risicoscenario's;

(b) ondersteuning te verlenen voor de ontwikkeling van gemeenschappelijke beginselen voor de uitvoering van de in punt 6 bedoelde stresstests door de lidstaten, te beginnen met tests gericht op door de mens veroorzaakte risico's in de energiesector en vervolgens in andere belangrijke sectoren, zoals digitale infrastructuur, vervoer en ruimtevaart; andere significante risico's en gevaren aan te pakken; en, in voorkomend geval, ondersteuning en advies inzake de uitvoering van dergelijke stresstests te verstrekken;

(c) een beveiligd platform te bieden voor het verzamelen, inventariseren en uitwisselen van beste praktijken, lessen uit nationale ervaringen en andere informatie met betrekking tot die veerkracht, onder meer over het uitvoeren van die stresstests en het omzetten van de resultaten daarvan in protocollen en noodplannen.

Bij de werkzaamheden van die deskundigen zou bijzondere aandacht moeten worden besteed aan sectoroverschrijdende afhankelijkheden en entiteiten die kritieke infrastructuur met grensoverschrijdende relevantie exploiteren, en deze werkzaamheden zouden moet worden voortgezet door de Groep voor de veerkracht van kritieke entiteiten, zodra deze is ingesteld.

(16) De lidstaten zouden ten volle moeten deelnemen aan de in punt 15 bedoelde versterkte samenwerking, onder meer door contactpunten met relevante expertise aan te wijzen en door ervaringen uit te wisselen over de methodologieën die worden gebruikt voor de stresstests en de protocollen en noodplannen die op basis daarvan worden ontwikkeld. Bij de uitwisseling van informatie zouden de vertrouwelijkheid van die informatie en de veiligheids- en commerciële belangen van de kritieke entiteiten gewaarborgd moeten worden, en zou de veiligheid van de lidstaten in acht moeten worden genomen. Dit houdt niet in dat informatie wordt verstrekt waarvan de bekendmaking strijdig is met de wezenlijke belangen van de lidstaten inzake nationale veiligheid, openbare veiligheid of defensie.

(17) De Commissie zal de lidstaten ondersteunen door instrumenten voor risicobeoordelingen te verstrekken, alsook handleidingen en richtsnoeren, onder meer een handboek over de bescherming van kritieke infrastructuur en openbare ruimten tegen onbemande luchtvaartuigsystemen. De EDEO wordt uitgenodigd om, met name via het EU-Inlichtingen- en situatiecentrum en de EU-Fusiecel voor analyse van hybride dreigingen, briefings te houden over de dreigingen voor kritieke infrastructuur in de EU, teneinde het situationeel bewustzijn te verbeteren.

(18) De Commissie zal ondersteuning verlenen om ervoor te zorgen dat de resultaten van projecten die betrekking hebben op de veerkracht van entiteiten die kritieke infrastructuur exploiteren, en die worden gefinancierd in het kader van de onderzoeks- en innovatieprogramma's van de Unie, worden benut. De Commissie is voornemens om de financiering voor deze veerkracht te verhogen, met inachtneming van de grenzen van de begroting die in het meerjarig financieel kader 2021-2027 aan Horizon Europa is toegewezen. Dit zou het mogelijk moeten maken de huidige en

toekomstige uitdagingen op dit gebied, zoals het klimaatbestendig maken van kritieke infrastructuur, aan te pakken zonder afbreuk te doen aan de financiering van andere activiteiten op het gebied van onderzoek en innovatie inzake civiele veiligheid in het kader van Horizon Europa. De Commissie zal ook haar inspanningen voor de verspreiding van de resultaten van relevante, door de Unie gefinancierde onderzoeksprojecten opvoeren.

(19) De NIS-samenwerkingsgroep wordt uitgenodigd om, in samenwerking met de Commissie en de hoge vertegenwoordiger, overeenkomstig hun respectieve taken en verantwoordelijkheden uit hoofde van het Unierecht, intensiever samen te werken met relevante netwerken en civiele en militaire organen bij het uitvoeren van risicobeoordelingen en het opzetten van risicoscenario's inzake cyberbeveiliging, die in een eerste fase gericht zijn op energie-, communicatie-, vervoers- en ruimtevaartinfrastructuur en de onderlinge afhankelijkheden tussen sectoren en lidstaten. Bij deze exercitie zou rekening moeten worden gehouden met de betrokken risico's voor de fysieke infrastructuur waarvan deze sectoren gebruikmaken. De risicobeoordelingen en scenario's zouden regelmatig moeten worden uitgevoerd en zouden de in deze sectoren bestaande of geplande risicobeoordelingen moeten aanvullen en verder ontwikkelen zonder deze evenwel te overlappen. Ze zouden als input moeten dienen voor discussies over de wijze waarop de algehele veerkracht van entiteiten die kritieke infrastructuur exploiteren, kan worden versterkt en kwetsbaarheden kunnen worden aangepakt.

(20) De Commissie zal haar activiteiten ter ondersteuning van de paraatheid van de lidstaten, alsook haar respons op grootschalige cyberincidenten versnellen. Zij zal met name:

(a) in aanvulling op relevante risicobeoordelingen in het kader van netwerk- en informatiebeveiliging, een uitgebreide studie uitvoeren waarin de onderzeese kabelinfrastructuur die de lidstaten met elkaar en Europa met de wereld verbindt, wordt geïnventariseerd en in kaart gebracht, onder meer met betrekking tot capaciteiten en reserves, kwetsbaarheden, risico's voor de beschikbaarheid van diensten en risicobeperking. De bevindingen zouden met de lidstaten moeten worden gedeeld;

(b) de paraatheid van de lidstaten en de instellingen, organen en instanties van de EU voor een respons op grootschalige cyberincidenten ondersteunen.

(21) De Commissie zal intensiever werken aan toekomstgerichte anticiperende maatregelen, onder meer binnen het Uniemechanisme voor civiele bescherming, in samenwerking met de lidstaten uit hoofde van de artikelen 6 en 10 van Besluit 1313/2013/EU, en in het kader van noodplannen ter ondersteuning van de operationele paraatheid van het Coördinatiecentrum voor respons in noodsituaties.

De Commissie zal met name het volgende doen:

(a) in het Coördinatiecentrum voor respons in noodsituaties verdere werkzaamheden verrichten op het gebied van anticipatie en sectoroverschrijdende preventie-, paraatheids- en responsplanning om te anticiperen op en voorbereid te zijn op verstoringen in de verlening van essentiële diensten door entiteiten die kritieke infrastructuur exploiteren;

(b) de investeringen verhogen op het gebied van preventiegerichte benaderingen en de paraatheid van de bevolking in geval van dergelijke verstoringen, met bijzondere

aandacht voor chemische, biologische, radiologische en nucleaire stoffen en explosieven of andere opkomende door de mens veroorzaakte dreigingen;

(c) de uitwisseling van relevante kennis en beste praktijken versterken en het ontwerp en de uitvoering van activiteiten voor capaciteitsontwikkeling, zoals opleidingscursussen en oefeningen met de entiteiten die kritieke infrastructuur exploiteren, verbeteren, door gebruik te maken bestaande structuren en expertise, zoals het kennisnetwerk op het gebied van Europese civiele bescherming.

(22) De Commissie zal het gebruik van bewakingsmiddelen van de EU (Copernicus en Galileo) bevorderen teneinde de lidstaten bij het monitoren van kritieke infrastructuur en, in voorkomend geval, de onmiddellijke omgeving van die infrastructuur te ondersteunen, en teneinde steun te verlenen voor andere bewakingsopties waarin het ruimtevaartprogramma van de Unie voorziet.

(23) 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 veerkracht van entiteiten die kritieke infrastructuur exploiteren, met name bijvoorbeeld als volgt:

(a) Europol, op het gebied van informatieverzameling, criminaliteitsanalyse en ondersteuning van onderzoek bij grensoverschrijdende rechtshandhavingsacties;

(b) 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) Euspa, op het gebied van het ruimtevaartprogramma van de Unie;

(d) Enisa, op het gebied van cyberbeveiliging.

HOOFDSTUK III: BETERE RESPONS

Acties op het niveau van de lidstaten

(24) De lidstaten:

(a) zouden hun respons moeten coördineren en zich een overzicht moeten vormen van de sectoroverschrijdende respons op aanzienlijke verstoringen in de verlening van essentiële diensten door entiteiten die kritieke infrastructuur exploiteren – in het kader van de geïntegreerde EU-regeling politieke crisisrespons (IPCR) waar het gaat om kritieke infrastructuur met grensoverschrijdende relevantie, de blauwdruk voor een gecoördineerde respons op grensoverschrijdende grootschalige cyberincidenten en -crises, of het kader voor een gecoördineerde EU-respons op hybride campagnes waar het gaat om een hybride campagne;

(b) zouden de informatie-uitwisseling binnen het Uniemechanisme voor civiele bescherming moeten intensiveren om tot betere vroegtijdige waarschuwing te komen en hun respons op dergelijke aanzienlijke verstoringen in het kader van het mechanisme te coördineren, en zo te zorgen voor een snellere, door de Unie gefaciliteerde reactie wanneer dat nodig is;

(c) zouden hun paraatheid om via het Uniemechanisme voor civiele bescherming op dergelijke aanzienlijke verstoringen te reageren, moeten verhogen, met name wanneer deze verstoringen waarschijnlijk aanzienlijke grensoverschrijdende of zelfs pan-Europese, alsook sectoroverschrijdende gevolgen hebben;

(d) zouden samen met de Commissie moeten 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) zouden entiteiten die kritieke infrastructuur exploiteren alsook relevante nationale autoriteiten moeten uitnodigen om de capaciteit van die entiteiten te versterken zodat de essentiëledienstverlening tot een basisniveau kan worden hersteld;

(f) zouden ervoor moeten zorgen dat, wanneer kritieke infrastructuur moet worden heropgebouwd, de heropgebouwde infrastructuur veerkrachtig genoeg is om alle significante risico's waaraan deze kan worden blootgesteld, te weerstaan, ook in ongunstige klimaatscenario's.

(25) De lidstaten worden uitgenodigd vaart te zetten achter de voorbereidingen voor de omzetting en toepassing van de NIS2-richtlijn, door onmiddellijk te beginnen met het versterken van de capaciteiten van de nationale CSIRT's (Computer Security Incident Response Teams), om rekening te houden met de nieuwe taken van de CSIRT's en met het grotere aantal entiteiten uit nieuwe sectoren, door hun cyberbeveiligingsstrategieën snel bij te werken en door zo spoedig mogelijk nationale plannen voor incidenten en crisisrespons op het gebied van cyberbeveiliging vast te stellen.

Acties op het niveau van de Unie

(26) Wat betreft de respons op aanzienlijke verstoringen in de verlening van essentiële diensten door entiteiten die kritieke infrastructuur exploiteren, zou er coördinatie tussen experts van de lidstaten moeten plaatsvinden met betrekking tot de veerkracht van die entiteiten en de respons op dergelijke verstoringen, wat kan bijdragen tot de werking van de geïntegreerde EU-regeling politieke crisisrespons (IPCR).

(27) De Commissie zal nauw met de lidstaten samenwerken aan de verdere ontwikkeling van inzetbare responscapaciteiten voor noodsituaties, met inbegrip van deskundigen en rescEU-voorraden in het kader van het Uniemechanisme voor civiele bescherming, met het oog op een betere operationele paraatheid voor het aanpakken van de onmiddellijke en indirecte gevolgen van aanzienlijke verstoringen in de verlening van essentiële diensten door entiteiten die kritieke infrastructuur exploiteren.

(28) Rekening houdend met het veranderende risicolandschap en in samenwerking met de lidstaten zal de Commissie in het kader van het Uniemechanisme voor civiele bescherming:

(a) de adequaatheid en operationele paraatheid van de bestaande responscapaciteit voortdurend analyseren en testen;

(b) regelmatig evalueren of er behoefte is aan de ontwikkeling van nieuwe responscapaciteiten op EU-niveau via rescEU;

(c) de sectoroverschrijdende samenwerking verder intensiveren om te zorgen voor een adequate respons op EU-niveau, en regelmatig oefeningen organiseren om deze samenwerking te testen;

(d) het Coördinatiecentrum voor respons in noodsituaties (ERCC) verder ontwikkelen tot het sectoroverschrijdende crisiscentrum op EU-niveau voor de coördinatie van steun aan getroffen lidstaten.

(29) De Commissie zal in samenwerking met de hoge vertegenwoordiger, in nauw overleg met de lidstaten en met de steun van de betrokken agentschappen van de Unie een blauwdruk ontwikkelen voor incidenten en crises in verband met kritieke infrastructuur, waarin de doelstellingen en vormen van samenwerking tussen de lidstaten en de instellingen, organen en instanties van de EU bij de respons op incidenten tegen kritieke infrastructuur worden vastgesteld en beschreven, met name wanneer deze een aanzienlijke verstoring van de verlening van essentiële diensten voor de interne markt met zich meebrengen. Wat de coördinatie van de respons betreft, zou in deze blauwdruk gebruik moeten worden gemaakt van de bestaande geïntegreerde EU-regeling politieke crisisrespons (IPCR).

(30) De Commissie zal met belanghebbenden en deskundigen samenwerken aan mogelijke maatregelen voor herstel na incidenten aan onderzeese kabelinfrastructuur (die in samenhang met de in punt 20 a) bedoelde inventarisatiestudie moeten worden gepresenteerd) aan de verdere uitwerking van noodplannen en risicoscenario's, en aan werkzaamheden op het gebied van de rampbestendigheid van de Unie in het kader van het Uniemechanisme voor civiele bescherming.

HOOFDSTUK IV: INTERNATIONALE SAMENWERKING

(31) De Commissie en de hoge vertegenwoordiger zullen, in voorkomend geval en in overeenstemming met hun respectieve taken en verantwoordelijkheden uit hoofde van het Unierecht, ondersteuning verlenen aan partnerlanden om entiteiten die op het grondgebied van die landen kritieke infrastructuur exploiteren, veerkrachtiger te maken.

(32) 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 veerkracht van kritieke infrastructuur versterken via de gestructureerde dialoog tussen de EU en de NAVO over veerkracht, en zullen daartoe een taskforce oprichten.

(33) 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 over een kader voor een gecoördineerde EU-respons op hybride campagnes[25], 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 EU-respons op hybride campagnes en hybride dreigingen, onder meer tegen entiteiten die kritieke infrastructuur exploiteren.

(34) Waar relevant en passend zal de Commissie de deelname van vertegenwoordigers van derde landen in overweging nemen in het kader van de samenwerking en informatie-uitwisseling tussen deskundigen van de lidstaten op het gebied van veerkracht van entiteiten die kritieke infrastructuur exploiteren.

[25] Conclusies van de Raad over een kader voor een gecoördineerde EU-respons op hybride campagnes - Consilium (europa.eu) (niet in het NL)

[…]

Gedaan te Straatsburg,

Voor de Raad
De voorzitter