Raad van de
Europese Unie

Brussel, 7 september 2023
(OR. en)

12485/23
ADD 1

Interinstitutioneel dossier:
2023/0318(NLE)

PROCIV 57	**ATO 48**
ENV 925	**CSC 408**
JAI 1084	**ECOFIN 839**
SAN 494	**CSCI 149**
COSI 140	**DATAPROTECT 216**
CHIMIE 85	**MI 698**
ENFOPOL 356	**CODEC 1500**
RECH 380	**COPS 418**
CT 133	**JAIEX 46**
DENLEG 38	**COPEN 292**
COTER 153	**IND 441**
RELEX 987	**POLMIL 221**
ENER 467	**IPCR 55**
HYBRID 53	**DIGIT 160**
TRANS 329	**DISINFO 62**
CYBER 203	**CSDP/PSDC 608**
TELECOM 251	**MARE 18**
ESPACE 45	**POLMAR 47**

BEGELEIDENDE NOTA

van:	de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur
ingekomen:	6 september 2023
aan:	mevrouw Thérèse BLANCHET, secretaris-generaal van de Raad van de Europese Unie
nr. Comdoc.:	COM(2023) 526 final
Betreft:	BIJLAGE bij het voorstel voor een AANBEVELING VAN DE RAAD betreffende een blauwdruk om de respons op verstoringen van kritieke infrastructuur van aanzienlijk grensoverschrijdend belang op Unieniveau te coördineren

Hierbij gaat voor de delegaties document COM(2023) 526 final.

Bijlage: COM(2023) 526 final

EUROPESE
COMMISSIE

Brussel, 6.9.2023
COM(2023) 526 final

ANNEX

BIJLAGE

bij

Voorstel voor een AANBEVELING VAN DE RAAD

betreffende een blauwdruk om de respons op verstoringen van kritieke infrastructuur van aanzienlijk grensoverschrijdend belang op Unieniveau te coördineren

BIJLAGE

In deze bijlage wordt ingegaan op de beginselen, de doelstellingen, de belangrijkste actoren en de werking van een blauwdruk voor de coördinatie van de respons op significante incidenten in kritieke infrastructuur ("blauwdruk voor kritieke infrastructuur"), en op de wisselwerking met bestaande crisisresponsmechanismen. Beoogd wordt de samenwerking tussen de lidstaten en de betrokken instellingen, organen, instanties en agentschappen van de Unie bij dergelijke incidenten overeenkomstig de toepasselijke voorschriften en procedures te verbeteren. Deze blauwdruk heeft geen enkele invloed op de rol en het functioneren van andere regelingen.

DEEL I: DOELSTELLINGEN, BEGINSELEN, ACTOREN EN ANDERE INSTRUMENTEN

1. Doelstellingen

De blauwdruk voor kritieke infrastructuur is gericht op het bereiken van de volgende drie hoofddoelstellingen bij een respons op een significant incident in kritieke infrastructuur:

(a) **Gedeeld situationeel bewustzijn**: een goed inzicht in het significante incident in kritieke infrastructuur, en in de oorsprong en de mogelijke gevolgen van het incident voor alle betrokken belanghebbenden op operationeel en strategisch/politiek niveau is essentieel voor een passende gecoördineerde respons.

(b) **Gecoördineerde publieke communicatie**: dit helpt om de negatieve gevolgen van een significant incident in kritieke infrastructuur te reduceren en om discrepanties in de berichten die in en tussen de lidstaten aan het publiek worden overgebracht, tot een minimum te beperken. Duidelijke publieke communicatie is ook belangrijk om de gevolgen van desinformatie te beperken.

(c) **Doeltreffende respons**: door de respons van de lidstaten en de samenwerking tussen de lidstaten en met de betrokken instellingen, organen, instanties en agentschappen van de Unie te versterken, kunnen de gevolgen van een significant incident in kritieke infrastructuur beter worden gereduceerd en essentiële diensten sneller worden hersteld op een manier die de kwetsbaarheid voor verdere significante incidenten tot een minimum beperkt.

2. Beginselen

Evenredigheid

Incidenten die kritieke infrastructuur en/of de verlening van essentiële diensten verstoren, blijven vaak onder de drempel voor significante incidenten in kritieke infrastructuur als gespecificeerd in punt 2 van deze aanbeveling. Dergelijke incidenten kunnen in beginsel dan ook doeltreffend op nationaal niveau worden aangepakt. Daarom is de toepassing van de blauwdruk voor kritieke infrastructuur beperkt tot significante incidenten in kritieke infrastructuur.

Subsidiariteit

De verantwoordelijkheid voor de respons op verstoringen van een kritieke infrastructuur of van de essentiële diensten die door kritieke entiteiten worden verleend, ligt overeenkomstig het Unierecht in de eerste plaats bij de lidstaten. In geval van een significant incident in kritieke infrastructuur van aanzienlijk grensoverschrijdend belang is er echter een belangrijke aanvullende rol weggelegd voor de betrokken instellingen, organen, instanties en agentschappen van de Unie en de Europese Dienst voor extern optreden ("EDEO"), aangezien

een dergelijk incident gevolgen kan hebben voor meerdere of zelfs alle economische sectoren op de interne markt, voor het leven van de burgers die in de Unie wonen, voor de veiligheid en voor de internationale betrekkingen van de Unie.

Complementariteit

De blauwdruk voor kritieke infrastructuur houdt rekening met en is in overeenstemming met de werking van bestaande crisisbeheersingsmechanismen op Unieniveau, namelijk de regelingen van de Raad voor de geïntegreerde EU-regeling politieke crisisrespons ("IPCR"), het interne crisiscoördinatieproces van de Commissie ARGUS, het Uniemechanisme voor civiele bescherming ("UCPM"), ondersteund door het Coördinatiecentrum voor respons in noodsituaties ("ERCC"), en het crisisresponsmechanisme van de EDEO. De blauwdruk is ook gebaseerd op sectorale regelingen, waaronder de bepalingen voor gecoördineerd beheer van grootschalige cyberbeveiligingsincidenten waarin Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad[1] voorziet, en het kader dat is vastgesteld in de blauwdruk voor een gecoördineerde respons op grootschalige grensoverschrijdende cyberincidenten en -crises ("cyberblauwdruk")[2], het netwerk van vervoerscontactpunten[3] en het Europees crisiscoördinatiecentrum voor de luchtvaart[4].

Bovendien bouwt de blauwdruk voor kritieke infrastructuur voort op en moet hij worden toegepast in overeenstemming met de structuren en mechanismen die zijn ingesteld bij Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad[5], met name wat betreft de samenwerking tussen bevoegde autoriteiten en met de Commissie en in de Groep voor de weerbaarheid van kritieke entiteiten. Verder wordt in de blauwdruk rekening gehouden met de verantwoordelijkheden van de betrokken instellingen, organen, instanties en agentschappen van de Unie uit hoofde van het voor hen geldende rechtskader. De crisisresponsactiviteiten voor kritieke infrastructuur vormen een aanvulling op andere crisisbeheersingsmechanismen op Unie-, nationaal en sectoraal niveau die de multisectorale coördinatie ondersteunen.

Vertrouwelijkheid van informatie

In de blauwdruk voor kritieke infrastructuur wordt rekening gehouden met het belang van het waarborgen van de vertrouwelijkheid van gerubriceerde en gevoelige niet-gerubriceerde informatie met betrekking tot kritieke infrastructuur en kritieke entiteiten.

3. Relevante actoren

De lidstaten en de betrokken instellingen, organen, instanties en agentschappen van de Unie als bedoeld in de punten a) tot en met e), bepalen overeenkomstig de voor hen geldende voorschriften en procedures de relevante actor(en) voor elk significant incident in kritieke infrastructuur, afhankelijk van de getroffen sector(en) en het soort incident.

---

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

[2] 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).

[3] Mededeling van de Commissie – Een noodplan voor vervoer (COM(2022) 211 final).

[4] Vastgesteld op grond van artikel 19 van Uitvoeringsverordening (EU) 2019/123 van de Commissie van 24 januari 2019 tot vaststelling van nadere regels voor de uitvoering van de netwerkfuncties voor luchtverkeersbeheer.

[5] Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (PB L 333 van 27.12.2022, blz. 164).

a) Lidstaten

- bevoegde autoriteiten (bv. autoriteiten die verantwoordelijk zijn voor kritieke infrastructuur, betrokken sectorale autoriteiten, overeenkomstig artikel 9, lid 2, van Richtlijn (EU) 2022/2557 aangewezen of opgerichte centrale contactpunten, overeenkomstig artikel 9, lid 1, van Richtlijn (EU) 2022/2557 aangewezen of opgerichte autoriteiten);

- in voorkomend geval, het Europees netwerk van verbindingsorganisaties voor cybercrises ("EU-CyCLONe") als bedoeld in artikel 16 van Richtlijn (EU) 2022/2555;

- de samenwerkingsgroep als bedoeld in artikel 14 van Richtlijn (EU) 2022/2555;

- in voorkomend geval, andere belanghebbenden, waaronder entiteiten of personen uit de particuliere sector, zoals exploitanten van kritieke infrastructuur, waaronder die welke als kritieke entiteiten zijn geïdentificeerd;

- ministers bevoegd voor de weerbaarheid van kritieke infrastructuur en/of minister(s) bevoegd voor de zwaarst door het betrokken significante incident in kritieke infrastructuur getroffen sector(en).

b) De Raad

- het roterende voorzitterschap;

- de relevante werkgroepen, zoals de werkgroep civiele bescherming, waaronder de subgroep weerbaarheid van kritieke entiteiten PROCIV-CER en de voorzitter(s) van de relevante werkgroep(en), afhankelijk van de getroffen sector(en) en de aard van het incident, zoals de Horizontale Groep cybervraagstukken en de Horizontale Groep versterking van weerbaarheid en bestrijding van hybride bedreigingen;

- Coreper, het Politiek en Veiligheidscomité en IPCR, alle ondersteund door het secretariaat-generaal van de Raad.

c) de Commissie, waaronder deskundigengroepen van de Commissie

- de aangewezen leidende dienst (afhankelijk van de getroffen sector), ondersteund door het ERCC als het 24/7 operationele centrum voor het beheer van crisisrespons en het directoraat-generaal Migratie en Binnenlandse Zaken als de ter zake bevoegde dienst alsook, in geval van een sectoroverschrijdend incident, het directoraat-generaal Migratie en Binnenlandse Zaken en andere relevante diensten van de Commissie;

- het directoraat-generaal Communicatie en de dienst van de woordvoerder;

- het directoraat-generaal HERA– de Europese Autoriteit voor paraatheid en respons inzake noodsituaties op gezondheidsgebied;

- de Groep voor de weerbaarheid van kritieke entiteiten, voorgezeten door een vertegenwoordiger van de Commissie (directoraat-generaal Migratie en Binnenlandse Zaken), opgericht bij Richtlijn (EU) 2022/2557, en, in voorkomend geval, andere relevante deskundigengroepen en comités;

- het ERCC, dat in het kader van het UCPM is opgericht bij Besluit nr. 1313/2013/EU van het Europees Parlement en de Raad[6] (het 24/7 operationele centrum voor noodsituaties in het kader van het UCPM, ondergebracht bij het directoraat-generaal Europese Civiele Bescherming en Humanitaire Hulp);

- de samenwerkingsgroep als bedoeld in artikel 14 van Richtlijn (EU) 2022/2555;

- het centrum voor situationeel bewustzijn en analyse op het gebied van cyberveiligheid (Cyber Situational Awareness and Analysis Centre);

- het Gezondheidsbeveiligingscomité, als bedoeld in artikel 4 van Verordening (EU) 2022/2371[7];

- het secretariaat-generaal van de Commissie (ARGUS-secretariaat) en de (adjunct-) secretaris-generaal (ARGUS-proces), directoraat-generaal Personele Middelen (directoraat Veiligheid);

- andere relevante deskundigengroepen van de Commissie die de Commissie bijstaan bij de coördinatie van maatregelen in een nood- of crisissituatie;

- andere netwerken voor crisisbeheersing, ook sectoraal (bv. het netwerk van contactpunten voor vervoer dat wordt beheerd door het directoraat-generaal Mobiliteit en Vervoer, de interinstitutionele Cyber Crisis Task Force[8], de Europese crisiscoördinatiecel voor de luchtvaart);

- de voorzitter en/of de bevoegde vicevoorzitter/commissaris.

d) EDEO

- gezamenlijke capaciteit op het gebied van inlichtingenanalyse (“SIAC”), bestaande uit het Inlichtingen- en situatiecentrum van de EU (“EU-Intcen”) en het directoraat Inlichtingen van de Militaire Staf van de EU (“EUMS INT”);

- Centrum voor Crisisrespons (‘‘CRC’’);

- de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid/vicevoorzitter van de Commissie.

e) Relevante organen en instanties van de Unie en relevante agentschappen van de Unie, afhankelijk van de getroffen sector(en)[9].

---

[6] 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).

[7] Verordening (EU) 2022/2371 van het Europees Parlement en de Raad van 23 november 2022 inzake ernstige grensoverschrijdende gezondheidsbedreigingen en tot intrekking van Besluit nr. 1082/2013/EU (PB L 314 van 6.12.2022, blz. 26).

[8] Een informele groep met relevante diensten van de Commissie, de EDEO, het Agentschap voor cyberbeveiliging van de Europese Unie (Enisa), CERT-EU en Europol, onder gezamenlijk voorzitterschap van het directoraat-generaal Communicatienetwerken, Inhoud en Technologie en de EDEO.

[9] Zoals Europol; voor vervoer: het Agentschap van de Europese Unie voor de veiligheid van de luchtvaart (EASA), het Europees Agentschap voor maritieme veiligheid (EMSA), het Spoorwegbureau van de Europese Unie (ERA); op gezondheidsgebied: het Europees Centrum voor ziektepreventie en -bestrijding (ECDC) en het Europees Geneesmiddelenbureau (EMA); voor energie: het Agentschap voor de samenwerking tussen energieregulators (ACER); voor ruimte: het Agentschap van de Europese Unie voor het ruimtevaartprogramma (EUSPA); voor de levensmiddelensector: de Europese Autoriteit voor voedselveiligheid (EFSA); op maritiem gebied: het Europees Bureau voor visserijcontrole (EBVC/EFCA); voor cyberincidenten:

4. Wisselwerking met andere relevante crisisbeheersingsmechanismen en -instrumenten

De blauwdruk voor kritieke infrastructuur is een flexibel instrument waarmee verschillende maatregelen in kaart worden gebracht die gedeeltelijk of volledig kunnen worden genomen met behulp van verschillende bestaande regelingen, afhankelijk van de aard en de ernst van het significante incident in kritieke infrastructuur en de behoefte aan operationele en strategische/politieke coördinatie.

a) Het EU-protocol voor de bestrijding van hybride bedreigingen[10] (''EU-protocol'')

Het EU-protocol geeft een overzicht van processen en instrumenten voor gebruik bij hybride bedreigingen[11] of campagnes.

In geval van een significant incident in kritieke infrastructuur met een hybride dimensie is het EU-protocol in voorkomend geval van toepassing in aanvulling op de blauwdruk voor kritieke infrastructuur, bijvoorbeeld wat betreft specifieke informatie, analyse of communicatie over hybride aspecten van het significante incident in kritieke infrastructuur en wat betreft samenwerking met externe partners.

b) De blauwdruk voor een gecoördineerde respons op grootschalige grensoverschrijdende cyberbeveiligingsincidenten en -crises

Deze cyberblauwdruk is van toepassing op grootschalige grensoverschrijdende incidenten die verstoringen veroorzaken die te groot zijn om door een getroffen lidstaat alleen te worden verholpen of die zodanig verstrekkende en significante technisch of politiek relevante gevolgen hebben voor twee of meer lidstaten of EU-instellingen dat tijdige beleidscoördinatie en respons op het politieke niveau van de Unie vereist zijn.

In geval van een significant incident in kritieke infrastructuur dat samenvalt met of verband lijkt te houden met een grootschalig cyberbeveiligingsincident, voorzien de desbetreffende werkgroepen van de Raad in passende coördinatie op operationeel niveau, bijvoorbeeld met EU-CyCLONe of door middel van een gezamenlijke vergadering van de Groep voor de weerbaarheid van kritieke entiteiten en de samenwerkingsgroep. De coördinatie heeft tot doel te bepalen welke actor(en), instrument(en) of mechanisme(n) op de meest doeltreffende wijze kunnen bijdragen aan de respons op het significante incident in kritieke infrastructuur, waarbij overlapping en parallelle werkzaamheden worden voorkomen.

c) Uniemechanisme voor civiele bescherming en het Coördinatiecentrum voor respons in noodsituaties

Overeenkomstig Besluit nr. 1313/2013/EU betreffende een Uniemechanisme voor civiele bescherming heeft het ERCC, het 24/7 operationele centrum van de Commissie voor het beheer van crisisrespons, de leiding over operationele responsmaatregelen in het kader van het UCPM bij door de natuur of door de mens veroorzaakte rampen of dreigende rampen (waaronder die waarbij kritieke infrastructuur wordt verstoord). In dergelijke gevallen kan het ERCC zorgen voor vroegtijdige waarschuwing, melding en analyse, voor ondersteuning van

---

het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), Computer Security Incident Response Teams (CSIRT's), het computercrisisresponsteam voor de instellingen, organen en instanties van de Europese Unie (CERT-EU).

[10] Joint Staff Working Document - EU Protocol for countering hybrid threats (SWD(2023) 116 final).

[11] Onder hybride bedreigingen wordt verstaan een combinatie van dwingende en ontregelende activiteit en conventionele en onconventionele methoden, die op een gecoördineerde manier kunnen worden gebruikt door zowel statelijke als niet-statelijke actoren om specifieke doelstellingen te bereiken, maar waarbij nog geen sprake is van formeel verklaarde oorlogsvoering.

de informatie-uitwisseling en, in geval van activering van het UCPM door een lidstaat, voor de inzet van operationele bijstand en deskundigen in de getroffen gebieden. Bovendien kan het ERCC de sectorale en sectoroverschrijdende coördinatie vergemakkelijken, zowel op Unieniveau als tussen de Unie en de betrokken nationale autoriteiten, waaronder de autoriteiten die verantwoordelijk zijn voor civiele bescherming en de weerbaarheid van kritieke infrastructuur.

d) Andere sectorale of sectoroverschrijdende mechanismen en instrumenten

De blauwdruk voor kritieke infrastructuur vormt geen overlapping met andere sectorale of sectoroverschrijdende crisisbeheersingsinstrumenten of coördinatiemechanismen. Indien er in de getroffen sector reeds dergelijke instrumenten of mechanismen bestaan, kan de blauwdruk voor kritieke infrastructuur, binnen het toepassingsgebied ervan, worden gebruikt als een aanvulling op de sectorale of sectoroverschrijdende instrumenten of mechanismen, zonder deze evenwel te vervangen. Om overlapping te voorkomen, zou de nodige coördinatie tussen de verschillende actoren moeten plaatsvinden. Dit kan bijvoorbeeld gebeuren in het kader van het interne crisiscoördinatieproces ARGUS van de Commissie, met ondersteuning van het ERCC, en/of in het kader van de coördinatievergaderingen van het IPCR.

DEEL II: INFORMATIE-UITWISSELING EN GECOÖRDINEERDE RESPONS

De hieronder beschreven maatregelen bestaan uit vormen van samenwerking, met name informatie-uitwisseling, gecoördineerde communicatie en respons. Deze structuur stemt overeen met de modaliteiten van het crisiscoördinatiemechanisme IPCR van de Raad en in de structuur is rekening gehouden met de mogelijkheid dat gebruik wordt gemaakt van de reeds op EU-niveau bestaande crisiscoördinatiemechanismen. De structuur toont hoe deze vormen van samenwerking, als ze worden gebruikt, zouden worden geïntegreerd. De meeste van deze maatregelen kunnen echter ook zelfstandig worden uitgevoerd: ze hangen niet af van het gebruik van dat mechanisme, maar vullen het eerder aan. De maatregelen worden in chronologische volgorde gepresenteerd, rekening houdend met de mogelijkheid dat in geval van een grootschalige crisis waarbij sprake is van een significant incident in kritieke infrastructuur, verschillende maatregelen tegelijkertijd en doorlopend worden uitgevoerd.

1. INFORMATIE-UITWISSELING

(a) Op operationeel niveau

De lidstaten die door het significante incident in kritieke infrastructuur worden getroffen, passen hun eigen noodmaatregelen toe, zorgen voor coördinatie met de betrokken nationale crisisbeheersingsmechanismen en voor de inschakeling van alle betrokken nationale, regionale en lokale actoren, in voorkomend geval.

Waar dit relevant is voor bijstand op het gebied van civiele bescherming, wordt de coördinatie tussen de lidstaten en met de Commissie verzorgd door het ERCC in het kader van het UCPM.

i) Informatie-uitwisseling en melding door de nationale bevoegde autoriteiten

De voor kritieke infrastructuur bevoegde nationale autoriteiten van de door het significante incident in kritieke infrastructuur getroffen lidstaten nemen de verplichtingen op het gebied van melding en informatieverstrekking overeenkomstig artikel 15 van Richtlijn (EU) 2022/2557 in acht en stellen bovendien het roterende voorzitterschap van de Raad en de Commissie via hun centrale contactpunten onverwijld in kennis van de relevante informatie die zij van de exploitant(en) van de kritieke infrastructuur, van kritieke entiteiten of uit andere

bronnen hebben ontvangen, alsook van informatie over de crisisbeheersingsmechanismen die in werking zijn gesteld. Wat de Commissie betreft, zorgt het ERCC 24/7 voor operationeel contact en operationele capaciteit en voor realtime coördinatie, monitoring en ondersteuning bij de respons op noodsituaties op Unieniveau en staat het ten dienste van de lidstaten en de Commissie als het operationele centrum voor crisisrespons ter bevordering van een sectoroverschrijdende aanpak van rampenbeheersing.

Deze informatie-uitwisseling heeft betrekking op de aard van het significante incident in kritieke infrastructuur, de oorzaak ervan, de geconstateerde of geschatte gevolgen van de verstoring voor de kritieke infrastructuur en voor de verlening van essentiële diensten, de sector- en grensoverschrijdende gevolgen van het incident en de beperkingsmaatregelen die op nationaal niveau of met andere betrokken lidstaten en de Commissie reeds zijn genomen of gepland zijn in het kader van bestaande regelingen, bijvoorbeeld de regelingen voor informatie-uitwisseling op grond van de artikelen 9 en 15 van Richtlijn (EU) 2022/2557. Deze melding wordt gedaan zonder dat daarvoor wordt geput uit de middelen waarover de kritieke infrastructuur of, in sommige gevallen, de kritieke entiteit of de lidstaat beschikt voor het uitvoeren van activiteiten die verband houden met het aanpakken van incidenten – wat de prioriteit moet blijven.

Met het oog op de follow-up brengen het ERCC of de in kennis gestelde diensten van de Commissie die bevoegd zijn voor de sector(en) waarin het significante incident in kritieke infrastructuur zich heeft voorgedaan, het contactpunt bij het directoraat-generaal Migratie en Binnenlandse Zaken en het secretariaat-generaal van de Commissie op de hoogte. Ondertussen begint het ERCC, als dat nog niet begonnen is, met het monitoren van de gebeurtenissen, in het bijzonder in gevallen waarin het UCPM door een of meer van de getroffen lidstaten is geactiveerd.

Als de informatie relevant kan zijn met het oog op cyberbeveiliging of verband kan houden met een cyberbeveiligingsincident, deelt de Commissie de relevante informatie met EU-CyCLONe.

In geval van cyberincidenten en incidenten die negatieve gevolgen hebben voor kritieke entiteiten, dienen de in Richtlijn (EU) 2022/2557 bedoelde nationale bevoegde autoriteiten onverwijld samen te werken en informatie uit te wisselen met de in Richtlijn (EU) 2022/2555 bedoelde bevoegde autoriteiten, onder meer met betrekking tot de door kritieke entiteiten genomen cyberbeveiligingsmaatregelen en fysieke maatregelen.

Wat maritieme aangelegenheden betreft, overwegen de nationale bevoegde autoriteiten de mogelijkheid om gebruik te maken van de gemeenschappelijke gegevensuitwisselingsstructuur (Common Information Sharing Environment, “CISE”), zodat zonder onnodige vertraging informatie kan worden uitgewisseld.

ii) Organisatie van deskundigenbijeenkomsten

De Commissie roept zo snel mogelijk de Groep voor de weerbaarheid van kritieke entiteiten bijeen met het oog op het vergemakkelijken van de uitwisseling van relevante informatie over het incident (aard, oorzaak, gevolgen en sector- en grensoverschrijdende gevolgen) en over de responsmaatregelen (zoals beperkingsmaatregelen en technische ondersteuning voor de getroffen lidstaten) tussen de voor kritieke infrastructuur bevoegde nationale autoriteiten en de betrokken instellingen, organen, instanties en agentschappen van de Unie. Afhankelijk van het zwaartepunt van het incident worden de betrokken diensten van de Commissie nauw betrokken bij vergaderingen van de Groep voor de weerbaarheid van kritieke entiteiten, zodat informatie die via bestaande sectorale instrumenten is verzameld, kan worden uitgewisseld. In geval van incidenten waarbij zowel cyberbeveiligingsaspecten als fysieke niet-cybergebonden

aspecten een rol spelen, zorgen de relevante diensten van de Commissie, CERT-EU en de EDEO, waar relevant, voor kennisgeving aan en raadpleging van de Cyber Crisis Task Force en de voorzitters van de in artikel 14 van Richtlijn (EU) 2022/2555 bedoelde samenwerkingsgroep en, in voorkomend geval, van EU-CyCLONe met betrekking tot de behoefte aan coördinatieactiviteiten. In overleg met de respectievelijke voorzitters kan de Commissie (het directoraat-generaal Migratie en Binnenlandse Zaken en het directoraat-generaal Communicatienetwerken, Inhoud en Technologie) een gezamenlijke vergadering van de Groep voor de weerbaarheid van kritieke entiteiten en de samenwerkingsgroep voorstellen om tot een gedeeld situationeel bewustzijn te komen en de respectievelijke responsmaatregelen te coördineren.

In geval van een significant sectoroverschrijdend incident in kritieke infrastructuur waarvoor gevolgenbeheersing op Unieniveau vereist is of kan zijn, kan de Commissie sectoroverschrijdende coördinatievergaderingen met alle relevante belanghebbenden beleggen.

Indien een significant incident in kritieke infrastructuur ook gevolgen heeft voor een derde land, pleegt de Commissie overleg met de bevoegde autoriteit van het getroffen derde land en kan zij deze autoriteit uitnodigen voor een vergadering van de Groep voor de weerbaarheid van kritieke entiteiten.

iii) Ondersteuning door de Commissie en agentschappen van de Unie

Waar relevant en in overeenstemming met zijn mandaat presenteert Europol een verslag over de stand van zaken in de Unie op het gebied van incidenten. Andere agentschappen van de Unie stellen hun "toezichthoudende" directoraten-generaal, waar relevant en in overeenstemming met hun mandaat, in kennis van relevante informatie die bijdraagt aan het situationeel bewustzijn of de gecoördineerde respons op het significante incident in kritieke infrastructuur, en die directoraten-generaal brengen op hun beurt verslag uit aan de Commissie (directoraat-generaal Migratie en Binnenlandse Zaken, in zijn hoedanigheid van voorzitter van de Groep voor de weerbaarheid van kritieke entiteiten).

De Commissie kan een bijdrage aan het situationeel bewustzijn leveren door gebruik te maken van de middelen van het ruimtevaartprogramma van de Unie[12], zoals Copernicus, Galileo en Egnos, waar relevant en in overeenstemming met het toepasselijke rechtskader.

(b) Op strategisch niveau

i) Opstellen van verslagen inzake situationeel bewustzijn

De Commissie stelt een verslag inzake situationeel bewustzijn op basis van de informatie die de nationale bevoegde autoriteiten in een vergadering van de Groep voor de weerbaarheid van kritieke entiteiten of in gezamenlijke vergaderingen met betrokken diensten, deskundigengroepen of netwerken meedelen, en op basis van andere beschikbare informatie.

In dit verslag wordt, waar relevant, rekening gehouden met de resultaten van de desbetreffende risicobeoordelingen, evaluaties en scenario's die vanuit het oogpunt van cyberbeveiliging worden opgesteld op EU-niveau, onder meer door de Commissie, de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid en de samenwerkingsgroep.

[12] 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).

In geval van activering van het IPCR kan dit verslag bijdragen aan de geïntegreerde situatiekennis- en -analyse ("ISAA") van de diensten van de Commissie en de EDEO.

SIAC presenteert, waar relevant, een actuele, op inlichtingen gebaseerde beoordeling van het incident.

ii) Activering van de crisiscoördinatiemechanismen van de Unie en gebruik van de instrumenten van de Unie

Het ERCC begint met het bieden van ondersteuning met het oog op het situationeel bewustzijn rond het incident, waar dat relevant is, met name als de gebeurtenis aanleiding geeft tot activering van het UCPM[13]. Daarnaast kunnen getroffen lidstaten satellietbeelden van hun grondgebied opvragen via de dienst van Copernicus voor het beheer van noodsituaties.

Wanneer het passend wordt geacht om in de hele Commissie informatie te delen met de EDEO en de betrokken agentschappen van de Unie, activeert het leidende directoraat-generaal of directoraat-generaal Migratie en Binnenlandse Zaken, in coördinatie met het secretariaat-generaal, het interne crisiscoördinatieproces ARGUS fase I van de Commissie door een event te openen op de IT-tool ARGUS.

Het roterende voorzitterschap van de Raad van de Unie kan de IPCR-regelingen activeren in de informatie-uitwisselingsmodus, wat inhoudt dat de Commissie en de EDEO in voorkomend geval ISAA-verslagen kunnen opstellen met bijdragen van nationale bevoegde autoriteiten en andere bronnen. Zelfs zonder activering van het IPCR kan onder bepaalde voorwaarden een monitoringpagina op het IPCR-webplatform worden geïnitieerd door het roterende voorzitterschap van de Raad of door de Commissie.

In voorkomend geval kunnen nog andere (sectorale) crisisbeheersingsmechanismen en -instrumenten van de Unie worden geactiveerd volgens de respectievelijke procedures. De Commissie zorgt voor coördinatie tussen deze mechanismen en instrumenten.

Indien het fysieke incident samenvalt met of verband lijkt te houden met een grootschalig cyberbeveiligingsincident, zoals gedefinieerd in artikel 6, punt 7, van Richtlijn (EU) 2022/2555, kan het roterende voorzitterschap van de Raad aan de hand van de cyberblauwdruk voorzien in passende coördinatie op operationeel niveau, waarbij onder andere EU-CyCLONe en de Groep voor de weerbaarheid van kritieke entiteiten worden betrokken.

iii) Coördinatie van publieke communicatie

De lidstaten die getroffen zijn door het significante incident in kritieke infrastructuur, coördineren hun publieke communicatie over de crisis zoveel mogelijk, met inachtneming van de nationale bevoegdheid op dit gebied. Het crisiscommunicatienetwerk van het IPCR kan hierbij in voorkomend geval worden betrokken.

Op basis van het gedeeld situationeel bewustzijn verlenen de Groep voor de weerbaarheid van kritieke entiteiten en de getroffen lidstaten in voorkomend geval ondersteuning bij de formulering van onderling afgesproken materiaal voor publieke communicatie.

[13] Zoals de publicatie van producten voor mediamonitoring, berichten op het gebied van civiele bescherming, analytische briefings, ECHO Daily Maps, ECHO Daily Flashes en andere op maat gemaakte producten.

Europol en andere relevante agentschappen van de Unie coördineren hun publieke communicatieactiviteiten met de dienst van de woordvoerder van de Commissie, op basis van het gedeeld situationeel bewustzijn.

Als het significante incident in kritieke infrastructuur een externe of hybride dimensie heeft of raakt aan het gemeenschappelijk veiligheids- en defensiebeleid, wordt de publieke communicatie gecoördineerd met de EDEO en de dienst van de woordvoerder van de Commissie, overeenkomstig het EU-protocol voor de bestrijding van hybride bedreigingen[14].

2. RESPONS (MET DOORLOPENDE MAATREGELEN ZOALS BESCHREVEN ONDER INFORMATIE-UITWISSELING EN AANVULLENDE MAATREGELEN OP STRATEGISCH/POLITIEK NIVEAU)

(a) Op strategisch niveau

i) Doorlopende opstelling van situatieverslagen

De Werkgroep Civiele Bescherming – Weerbaarheid van kritieke entiteiten (PROCIV-CER) van de Raad wordt op de hoogte gesteld van het opstellen van een politiek/strategisch situatieverslag (bv. het ISAA-verslag in geval van activering van het IPCR of het door de Commissie opgestelde verslag inzake het gedeeld situationeel bewustzijn) en zorgt voor de voorbereiding van het Coreper, indien dit nog niet is bijeengeroepen, of de vergadering van het Politiek en Veiligheidscomité, in voorkomend geval.

SIAC intensiveert het contact met de inlichtingendiensten van de lidstaten, verzamelt de uit alle bronnen afkomstige informatie en bereidt een analyse en beoordeling van het incident voor, evenals, zo nodig, regelmatige updates.

ii) Volledige activering van de crisiscoördinatiemechanismen van de Unie en gebruik van de instrumenten van de Unie

Indien de voorzitter van de Commissie het interne crisiscoördinatieproces van de Commissie ARGUS fase II activeert, worden op korte termijn een of meer vergaderingen van het crisiscoördinatiecomité, met deelname van de relevante diensten en agentschappen van de Commissie en, waar relevant, de EDEO, belegd om alle aspecten van het significante incident in kritieke infrastructuur te coördineren.

Als het voorzitterschap van de Raad het IPCR volledig activeert:

- belegt het roterende voorzitterschap van de Raad tijdig een informele rondetafelbijeenkomst met de betrokken nationale, Europese en internationale actoren, waar de vertegenwoordiger van de Commissie in zijn hoedanigheid van voorzitter van de groep voor de weerbaarheid van kritieke entiteiten (directoraat-generaal Migratie en Binnenlandse Zaken) verslag kan uitbrengen over de eerdere vergadering(en) van de groep – in voorkomend geval ook bijgewoond door andere diensten van de Commissie en de EDEO.

- kunnen SIAC en de betrokken agentschappen van de Unie worden uitgenodigd om tijdens deze vergadering een stand van zaken te geven over het significante incident in kritieke infrastructuur.

De dienst die de leiding heeft over de ISAA-rapportage (de leidende dienst van de Commissie of de EDEO) stelt het ISAA-verslag op aan de hand van bijdragen van de betrokken diensten van de Commissie, de betrokken instanties, organen en agentschappen van de Unie en de

[14] Joint Staff Working Document - EU Protocol for countering hybrid threats (SWD(2023) 116 final).

nationale bevoegde autoriteiten. De lidstaten worden uitgenodigd om via het IPCR-webplatform input voor de ISAA-verslagen te leveren.

In geval van een significant incident in kritieke infrastructuur dat relevant is voor de internationale veiligheid, kunnen de diensten van de Commissie en de EDEO een vergadering in het kader van de gestructureerde EU-NAVO-dialoog over veerkracht bijeenroepen om bij te dragen aan een gedeeld situationeel bewustzijn en de uitwisseling van informatie over de maatregelen die respectievelijk door de Unie en de NAVO zijn genomen.

iii) Publieke communicatie

De Raad stelt gemeenschappelijke berichten voor publieke communicatie op. Het informele netwerk van crisisvoorlichters dat in het kader van het IPCR is opgericht, kan daarbij ondersteuning verlenen. In voorkomend geval stelt de dienst van de woordvoerder van de Commissie ook berichten voor publieke communicatie op.

Als het significante incident in kritieke infrastructuur een externe of hybride dimensie heeft of raakt aan het gemeenschappelijk veiligheids- en defensiebeleid, wordt de publieke communicatie gecoördineerd met de EDEO en de dienst van de woordvoerder van de Commissie.

iv) Ondersteuning van lidstaten en doeltreffende respons

Het roterende voorzitterschap kan een vergadering van PROCIV-CER bijeenroepen om de activiteiten in het kader van het IPCR te ondersteunen, indien dit wordt geactiveerd.

De lidstaten die door het significante incident in kritieke infrastructuur worden getroffen, kunnen via de Groep voor de weerbaarheid van kritieke entiteiten verzoeken om technische bijstand van andere lidstaten of betrokken instellingen, organen en agentschappen van de Unie, bijvoorbeeld in de vorm van specifieke deskundigheid om de negatieve gevolgen van het significante incident in kritieke infrastructuur te beperken.

De lidstaten die door het significante incident in kritieke infrastructuur worden getroffen, kunnen ook verzoeken om technische en/of financiële bijstand van de Commissie of de relevante agentschappen van de Unie. In coördinatie met de betrokken agentschappen van de Unie gaat de Commissie na welke steun zij kan verlenen, activeert zij in voorkomend geval technische beperkingsmaatregelen op Unieniveau in overeenstemming met hun respectievelijke procedures en coördineert zij de technische capaciteit die nodig is om de gevolgen van het significante incident in kritieke infrastructuur tegen te houden of te beperken.

Met name in het kader van het UCPM kunnen de getroffen landen om bijstand verzoeken via het gemeenschappelijk noodcommunicatie- en informatiesysteem (“Cecis”), waarna het ERCC de verlening van bijstand door de lidstaten en de aan het UCPM deelnemende landen zou coördineren, alsook via “rescEU”.

In het kader van hun respectievelijke mandaat en op verzoek verlenen Europol en de andere betrokken agentschappen van de Unie de lidstaten die door een significant incident in kritieke infrastructuur worden getroffen, ondersteuning bij het onderzoek naar het incident.

(b) Op politiek niveau

Het voorzitterschap van de Raad zou zich kunnen buigen over de noodzaak IPCR-rondetafelconferenties, vergaderingen van werkgroepen van de Raad, het Coreper, de Raad van Ministers en/of topontmoetingen bijeen te roepen om van gedachten te wisselen over de mogelijke oorsprong en de verwachte gevolgen van het significante incident in kritieke infrastructuur voor de lidstaten en de Unie, overeenstemming te bereiken over

gemeenschappelijke richtsnoeren en de nodige maatregelen vast te stellen om de door het significante incident in kritieke infrastructuur getroffen lidstaten te steunen en de gevolgen van het incident te beperken.

Diagram 1: Schematisch overzicht van de blauwdruk voor kritieke infrastructuur

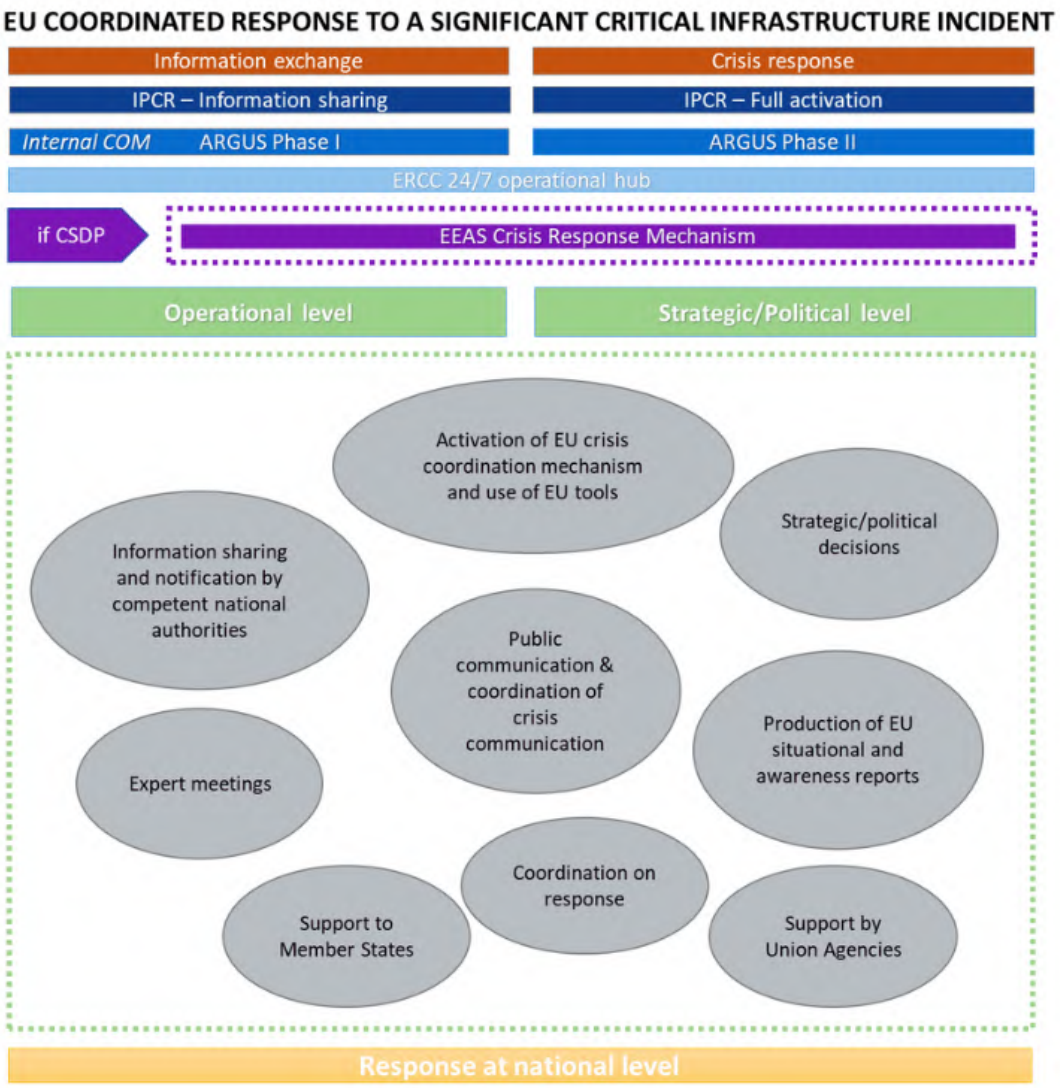

Diagram 2: Besluitvorming in het kader van de blauwdruk voor kritieke infrastructuur