EUROPESE
COMMISSIE

Brussel, 24.2.2025
COM(2025) 66 final

2025/0036 (NLE)

Voorstel voor een

AANBEVELING VAN DE RAAD

voor een EU-blauwdruk voor cyberbeveiligingscrisisbeheer

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

• Motivering en doel van het voorstel

De Raad riep in zijn conclusies over de toekomst van cyberbeveiliging van 22 mei 2024

> *"de Commissie op de huidige blauwdruk voor cyberbeveiliging snel te evalueren en op basis daarvan een herziene blauwdruk voor cyberbeveiliging voor te stellen in de vorm van een aanbeveling van de Raad waarin de huidige uitdagingen en het complexe cyberdreigingslandschap worden behandeld, bestaande netwerken worden versterkt, de samenwerking wordt geïntensiveerd en de muren tussen organisaties worden geslecht, waarbij in de eerste plaats van bestaande structuren wordt gebruikgemaakt. Voorts moet de herziene blauwdruk gebaseerd worden op beproefde leidende samenwerkingsbeginselen (evenredigheid, subsidiariteit, complementariteit en vertrouwelijkheid van informatie) en deze uitbreiden naar de hele levenscyclus van crisisbeheersing, alsook bijdragen tot onderlinge afstemming en verbetering van de beveiligde communicatie op het gebied van cyberbeveiliging. De herziene blauwdruk moet gegarandeerd verenigbaar zijn met bestaande kaders, zoals de IPCR, het EU-instrumentarium voor cyberdiplomatie, de EU-toolbox tegen hybride dreigingen, het crisisresponsprotocol van de rechtshandhavingsinstanties (Law Enforcement Emergency Response Protocol – LERP), opkomende kaders zoals de blauwdruk voor kritieke infrastructuur, sectorale procedures en algemene crisisbeheersingsstructuren binnen entiteiten van de Unie, waarbij ook de hoge vertegenwoordiger en Europol betrokken zijn. In deze herziene blauwdruk moet de rol van de Commissie, de hoge vertegenwoordiger en Enisa, in overeenstemming met hun respectieve bevoegdheden, met name gericht zijn op ondersteuning van horizontale coördinatie".*

Deze ontwerpaanbeveling van de Raad betreffende de blauwdruk van de Unie voor cyberbeveiligingscrisisbeheer (de "cyberblauwdruk") heeft tot doel op duidelijke, eenvoudige en toegankelijke wijze het kader van de Europese Unie (EU) voor cyberbeveiligingscrisisbeheer te presenteren. Dit moet relevante actoren van de Unie (d.w.z. individuele entiteiten en netwerken van entiteiten op Unieniveau) in staat stellen te begrijpen hoe ze met elkaar kunnen interageren en optimaal gebruik kunnen maken van de beschikbare mechanismen gedurende de volledige levenscyclus van crisisbeheer. Ze beoogt uit te leggen wat een cybercrisis is en waardoor een cybercrisismechanisme op Unieniveau wordt getriggerd. Ze licht het gebruik toe van beschikbare mechanismen zoals het noodmechanisme voor cyberbeveiliging, waaronder de EU-cyberbeveiligingsreserve, bij de voorbereiding van het beheer van, de respons op en het herstel van een crisis die het gevolg is van een grootschalig cyberbeveiligingsincident. Voorts wil ze een meer gestructureerde samenwerking tussen civiele en militaire actoren bevorderen, met inbegrip van samenwerking met de Noord-Atlantische Verdragsorganisatie (NAVO), aangezien een grootschalig cyberincident met gevolgen voor civiele infrastructuur van de Unie waarvan de strijdkrachten afhankelijk zijn mogelijk ook responsmechanismen van de NAVO in werking doet treden.

De cyberblauwdruk is een niet-bindend instrument waarin specifieke acties voor relevante actoren in een cybercrisis worden vastgesteld en dat de algehele doeltreffendheid van het kader voor cybercrisisbeheer kan vergroten. Hij actualiseert de blauwdruk in Aanbeveling (EU) 2017/1584 van de Commissie inzake een gecoördineerde respons op grootschalige cyberbeveiligingsincidenten en -crises, en houdt rekening met de resultaten van en de lessen die zijn getrokken uit oefeningen op Unieniveau sinds de vaststelling van die aanbeveling. Hij maakt deel uit van bredere politieke prioriteiten op het gebied van paraatheid en beveiliging.

Overeenkomstig Richtlijn (EU) 2022/2555 (de "NIS 2-richtlijn") is een "grootschalig cyberbeveiligingsincident" een incident dat leidt tot een verstoringsniveau dat te groot is om door een getroffen lidstaat alleen te worden verholpen of dat significante gevolgen heeft voor ten minste twee lidstaten. Afhankelijk van zijn oorzaak en impact kan een dergelijk incident escaleren en een volwaardige crisis worden die gevolgen heeft voor de goede werking van de interne markt of ernstige risico's voor de openbare veiligheid en beveiliging met zich meebrengt voor entiteiten of burgers in verschillende lidstaten of in de Unie als geheel.

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

Het voorstel is in overeenstemming met de relevante instrumenten van de Unie op cyberbeveiligingsgebied, met name de NIS 2-richtlijn en Verordening (EU) 2023/2841 tot vaststelling van maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie. Het is ook in overeenstemming met het kader van het Uniemechanisme voor civiele bescherming (UCPM), dat is ingesteld bij Besluit 1313/2013/EU van het Europees Parlement en de Raad, Uitvoeringsbesluit (EU) 2018/1993 inzake de geïntegreerde EU-regeling politieke crisisrespons (IPCR), en sectorale instrumenten voor situationeel bewustzijn en crisisbeheer, onder meer in de elektriciteitssector.

- **Verenigbaarheid met andere beleidsterreinen van de Unie**

De cyberblauwdruk vormt een aanvulling op en is in overeenstemming met de onlangs vastgestelde aanbeveling van de Raad betreffende een blauwdruk om de respons op verstoringen van kritieke infrastructuur van aanzienlijk grensoverschrijdend belang op Unieniveau te coördineren, aangezien deze laatste betrekking heeft op verstoringen in verband met fysieke niet-cyberweerbaarheid. Hij staat in nauwe wisselwerking met de crisisbeheermechanismen en -instrumenten van het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB) en het gemeenschappelijk veiligheids- en defensiebeleid (GVDB), zoals uiteengezet in het strategisch kompas voor veiligheid en defensie van de Raad. Voorts kunnen initiatieven van de Unie ter bestrijding van cybercriminaliteit de doelstellingen van deze aanbeveling ondersteunen.

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

- **Rechtsgrondslag**

Het voorstel is gebaseerd op artikel 292 VWEU, waarin de regels voor de vaststelling van aanbevelingen zijn vastgelegd.

Het voorstel vormt een aanvulling op het gehele wetgevingskader inzake cyberbeveiliging dat op Unieniveau is vastgesteld. Het voorstel heeft geen betrekking op het beheer van ernstige incidenten die gevolgen hebben voor entiteiten van de Unie in de zin van Verordening (EU) 2023/2841, die is vastgesteld op basis van artikel 298 VWEU. Het heeft echter wel betrekking op informatie-uitwisseling tussen entiteiten van de Unie en de lidstaten, met inbegrip van de bepalingen van Verordening (EU) 2023/2841 voor de vertegenwoordiger van de Commissie in de interinstitutionele raad voor cyberbeveiliging (IICB) als contactpunt om het voor de IICB gemakkelijker te maken informatie met betrekking tot ernstige incidenten te delen met het Europees netwerk van verbindingsorganisaties voor cybercrises EU-CyCLONe, als bijdrage aan het gedeeld situationeel bewustzijn.

- **Subsidiariteit (bij niet-exclusieve bevoegdheid)**

Hoewel het reageren op verstoringen van kritieke infrastructuur of van de diensten die worden verleend door essentiële en belangrijke entiteiten eerst en vooral de verantwoordelijkheid van

de lidstaten is, kunnen bepaalde kwaadwillige grensoverschrijdende cyberactiviteiten kritieke informatie-infrastructuren waarvan de goede werking van de interne markt afhankelijk is, verstoren en beschadigen. Daarom speelt de Unie een belangrijke rol in geval van een significant incident of een crisis. Een dergelijke verstoring kan meerdere of zelfs alle onderdelen van de economische bedrijvigheid binnen de eengemaakte markt raken, en kan gevolgen voor de veiligheid en de internationale betrekkingen van de Unie hebben. Om de werking van de interne markt veilig te stellen, is coördinatie op Unieniveau in geval van verstoringen van kritieke infrastructuur met een aanzienlijk grensoverschrijdend effect niet alleen passend, maar ook noodzakelijk. Gecoördineerde respons op Unieniveau zal de respons van de lidstaten op de verstoring ondersteunen door middel van gedeeld situationeel bewustzijn, gecoördineerde publiekscommunicatie en het mitigeren van de gevolgen van de verstoring voor de interne markt.

- **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 daarvan te verwezenlijken. De voorgestelde acties zijn evenredig met de nagestreefde doelstellingen, die gericht zijn op een gecoördineerd beheer van cybercrises door de Unie.

- **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. Overeenkomstig artikel 288 VWEU zijn aanbevelingen niet bindend. Een aanbeveling van de Raad is in dit geval een passend instrument, aangezien het de gehechtheid van de lidstaten aan de daarin opgenomen maatregel aangeeft en een sterke basis legt voor samenwerking bij de coördinatie van het beheer van grootschalige cyberbeveiligingsincidenten en -crises. Op die manier vormt de voorgestelde aanbeveling een aanvulling op het bindende rechtskader (met name de NIS 2-richtlijn).

3. EVALUATIE, RAADPLEGING VAN BELANGHEBBENDEN EN EFFECTBEOORDELING

- **Raadpleging van belanghebbenden**

Bij de ontwikkeling van dit voorstel heeft de Commissie overleg gepleegd over de herziening van de cyberblauwdruk en heeft zij de lidstaten en betrokken entiteiten van de Unie om input verzocht. Zij heeft rekening gehouden met de standpunten die door de deskundigen van de lidstaten en Enisa naar voren zijn gebracht tijdens een op 5 september 2024 gezamenlijk door de Commissie en Polen georganiseerde workshop in Karpacz.

De Commissie heeft tijdens vergaderingen in september 2024 vertegenwoordigers van de lidstaten geraadpleegd in het CSIRT-netwerk, EU-CyCLONe en de NIS-samenwerkingsgroep en heeft schriftelijke bijdragen ingewacht.

De Commissie heeft het voorstel gepresenteerd en feedback van de Raad verzameld tijdens twee specifieke besprekingen in de Horizontale Groep cybervraagstukken in oktober en november 2024.

De Commissie heeft vertegenwoordigers van de particuliere sector, de lidstaten, de Europese Dienst voor extern optreden (EDEO) en Enisa geraadpleegd tijdens een workshop die in

november 2024 in Brussel werd georganiseerd door de permanente vertegenwoordiging van Polen bij de EU.

De Commissie heeft betrokken entiteiten van de Unie geraadpleegd, namelijk de EDEO, Enisa, Europol en CERT-EU, onder meer via besprekingen op hoog niveau tijdens de vergaderingen van de taskforce voor cybercrises[1] in juli en november 2024.

Er is consensus ontstaan over de noodzaak van een actueel, duidelijk, eenvoudig en operationeel document dat de betrokken actoren in staat stelt het kader voor cybercrisisbeheer te begrijpen en de beschikbare mechanismen doeltreffend te gebruiken. Er bestond ook consensus over de noodzaak om overlapping van instrumenten te voorkomen en goed gebruik te maken van de bestaande mechanismen op Unieniveau voor coördinatie, informatie-uitwisseling en respons, zonder nieuwe structuren te creëren of de interne standaardprocedures van bestaande netwerken en bestaande sectorale mechanismen te verstoren.

[1] Een informele groep bestaande uit diensten van de Commissie en andere EU-diensten.

2025/0036 (NLE)

Voorstel voor een

AANBEVELING VAN DE RAAD

voor een EU-blauwdruk voor cyberbeveiligingscrisisbeheer

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 292,

Gezien het voorstel van de Europese Commissie,

Overwegende hetgeen volgt:

(1) Digitale technologie en mondiale connectiviteit vormen de ruggengraat van de economische groei en het concurrentievermogen van de Unie en van de transformatie van kritieke infrastructuur. Door een onderling verbonden en steeds digitalere economie vergroot echter ook het risico op cyberincidenten en cyberaanvallen. Bovendien weerspiegelt de toename van geopolitieke spanningen, conflicten en strategische rivaliteit zich in de impact, de omvang en de gesofisticeerdheid van kwaadwillige cyberactiviteiten. Dergelijke activiteiten kunnen deel uitmaken van multidimensionale hybride dreigingen of militaire operaties. Ze kunnen ook rechtstreeks van invloed zijn op de veiligheid, de economie en de samenleving van de Unie. Daarnaast hebben ze een spill-overpotentieel, met name als die activiteiten gericht zijn tegen internationale strategische partnerlanden zoals kandidaat-lidstaten of buurlanden.

(2) Een grootschalig cyberbeveiligingsincident kan leiden tot een verstoringsniveau dat te groot is om door een getroffen lidstaat alleen te worden verholpen of dat een significante impact heeft op meer dan een lidstaat. Afhankelijk van zijn oorzaak en impact kan een dergelijk incident escaleren en een volwaardige crisis worden die gevolgen heeft voor de goede werking van de interne markt of ernstige risico's voor de openbare veiligheid en beveiliging met zich meebrengt voor entiteiten of burgers in verschillende lidstaten of in de Unie als geheel. Doeltreffend crisisbeheer is essentieel om de economische stabiliteit te handhaven en Europese overheden, kritieke infrastructuur, burgers en bedrijven te beschermen, en om bij te dragen tot de internationale veiligheid en stabiliteit in cyberspace. Cybercrisisbeheer is dan ook een integrerend deel van het overkoepelende EU-kader voor crisisbeheer.

(3) Overeenkomstig de in Uitvoeringsbesluit (EU) 2018/1993 van de Raad[2] vastgestelde procedures wordt een besluit tot activering en deactivering van de geïntegreerde EU-regeling politieke crisisrespons (IPCR) genomen door het voorzitterschap van de Raad, dat (behalve wanneer de solidariteitsclausule is ingeroepen) de getroffen lidstaten, de Commissie en de hoge vertegenwoordiger (HV) raadpleegt. Volgens de

[2] Uitvoeringsbesluit (EU) 2018/1993 van de Raad van 11 december 2018 inzake de geïntegreerde EU-regeling politieke crisisrespons (PB L 320 van 17.12.2018, blz. 28, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

IPCR-procedures kunnen het secretariaat-generaal van de Raad, de diensten van de Commissie en de EDEO daarnaast ook overeenkomen de IPCR in de modus informatiedelen te activeren, in overleg met het voorzitterschap. De besprekingen in het kader van de IPCR gaan uit van verslagen over geïntegreerde situatiekennis en -analyse van de diensten van de Commissie en de Europese Dienst voor extern optreden (EDEO).

(4) Hoewel het beheer van nationale cybercrises een primaire verantwoordelijkheid van de lidstaten is, vereist het potentieel grensoverschrijdende en sectoroverschrijdende karakter van cyberbeveiligingsincidenten dat de lidstaten en de betrokken entiteiten van de Unie op technisch, operationeel en politiek niveau samenwerken met het oog op doeltreffende coördinatie in de hele Unie. Tegelijk zijn crisisrespons en -herstel duur voor de getroffen entiteiten en sectoren. Crisisbeheer gedurende de volledige levenscyclus omvat daarom paraatheid en gedeeld situationeel bewustzijn om te anticiperen op cyberbeveiligingsincidenten, de nodige detectiecapaciteiten om cyberincidenten te identificeren en de nodige respons- en herstelinstrumenten ter mitigatie, afschrikking en indamming van cyberbeveiligingsincidenten.

(5) In Aanbeveling (EU) 2017/1584 van de Commissie[3] inzake een gecoördineerde respons op grootschalige cyberbeveiligingsincidenten en -crises zijn de doelstellingen en vormen van samenwerking tussen de lidstaten en entiteiten van de Unie in reactie op grootschalige cyberincidenten en -crises vastgesteld. In de aanbeveling werden de betrokken actoren op technisch, operationeel en politiek niveau in kaart gebracht en werd uitgelegd hoe ze in het bredere crisisbeheer van de Unie, zoals de IPCR, zijn geïntegreerd. De in Aanbeveling (EU) 2017/1584 neergelegde kernbeginselen, namelijk subsidiariteit, complementariteit en vertrouwelijkheid van informatie, alsook de aanpak op drie niveaus (technisch, operationeel en politiek), blijven geldig.

(6) Sinds 2017 heeft de Unie haar cyberbeveiligingskader uitgebouwd via verschillende instrumenten die bepalingen bevatten met betrekking tot cyberbeveiligingscrisisbeheer: Verordening (EU) 2019/881 van het Europees Parlement en de Raad[4], Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad[5], Uitvoeringsverordening (EU) 2024/2690 van de Commissie[6], Verordening

---

3 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, ELI: http://data.europa.eu/eli/reco/2017/1584/oj).

4 Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

5 Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972, en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PB L 333 van 27.12.2022, blz. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

6 Uitvoeringsverordening (EU) 2024/2690 van de Commissie van 17 oktober 2024 tot vaststelling van regels voor de toepassing van Richtlijn (EU) 2022/2555 wat betreft de technische en methodologische vereisten van de maatregelen voor het beheer van cyberbeveiligingsrisico's en nadere specificatie van de gevallen waarin een incident als significant wordt beschouwd met betrekking tot DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, aanbieders van

(EU, Euratom) 2023/2841 van het Europees Parlement en de Raad[7], Verordening (EU) 2021/887 van het Europees Parlement en de Raad[8], Verordening (EU) 2024/2847 van het Europees Parlement en de Raad[9], en Verordening (EU) 2025/38 van het Europees Parlement en de Raad ("verordening cybersolidariteit")[10]. Specifieke sectorale cyberbeveiligingscrisismaatregelen zijn onder meer Gedelegeerde Verordening (EU) 2024/1366 van de Commissie[11] en het aanstaande coördinatiekader voor systemische cyberincidenten (EU-SCICF) in het kader van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad[12]. Richtlijn 2013/40[13] bevat de referentie voor de definitie van strafbare activiteiten in verband met cyberaanvallen, en de regels van de Unie inzake grensoverschrijdende toegang tot elektronisch bewijsmateriaal, met name Verordening (EU) 2023/1543 van het Europees Parlement en de Raad[14], zullen, zodra ze ten uitvoer zijn gelegd, de rechtshandhaving op dit gebied aanzienlijk faciliteren. "Het EU-beleid op het gebied van cyberdefensie"[15] schetst de rol van een EU-netwerk voor militaire computercrisisresponsteams (Micnet) en de conferentie van EU-cybercommandanten, en beoogt de oprichting van een EU-coördinatiecentrum voor cyberdefensie (EUCDCC). In bepaalde kritieke sectoren in de bijlagen I en II bij

---

onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten, en verleners van vertrouwensdiensten (PB L, 2024/2690, 18.10.2024).

7 Verordening (EU, Euratom) 2023/2841 van het Europees Parlement en de Raad van 13 december 2023 tot vaststelling van maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie (PB L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

8 Verordening (EU) 2021/887 van het Europees Parlement en de Raad van 20 mei 2021 tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra (PB L 202 van 8.6.2021, blz. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

9 Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Verordening cyberweerbaarheid) (PB L, 2024/2847, 20.11. 2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

10 Verordening (EU) 2025/38 van het Europees Parlement en de Raad van 19 december 2024 tot vaststelling van maatregelen ter versterking van de solidariteit en de capaciteit in de Unie om cyberdreigingen en -incidenten op te sporen, zich erop voor te bereiden en erop te reageren en tot wijziging van Verordening (EU) 2021/694 (verordening cybersolidariteit) (PB L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

11 Gedelegeerde Verordening (EU) 2024/1366 van de Commissie van 11 maart 2024 tot aanvulling van Verordening (EU) 2019/943 van het Europees Parlement en de Raad door middel van de vaststelling van een netcode inzake sectorspecifieke regels voor met cyberbeveiliging samenhangende aspecten van grensoverschrijdende elektriciteitsstromen (PB L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

12 Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (PB L 333 van 27.12.2022, blz. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

13 Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad (PB L 218 van 14.8.2013, blz. 8, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

14 Verordening (EU) 2023/1543 van het Europees Parlement en de Raad van 12 juli 2023 betreffende het Europees verstrekkingsbevel en het Europees bewaringsbevel voor elektronisch bewijsmateriaal in strafzaken en de tenuitvoerlegging van vrijheidsstraffen als gevolg van een strafprocedure, en Richtlijn (EU) 2023/1544 van het Europees Parlement en de Raad van 12 juli 2023 tot vaststelling van geharmoniseerde regels inzake de aanwijzing van aangewezen vestigingen en de aanstelling van wettelijke vertegenwoordigers ten behoeve van de vergaring van elektronisch bewijsmateriaal in strafprocedures (PB L 191 van 28.7.2023, blz. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

15 JOIN(2022) 49 final.

Richtlijn (EU) 2022/2555 bestaan er andere niet-cybergerelateerde mechanismen voor situationeel bewustzijn en crisisrespons. De aanbeveling van de Raad betreffende een blauwdruk om de respons op Unieniveau op verstoringen van kritieke infrastructuur van aanzienlijk grensoverschrijdend belang te coördineren[16] voorziet in samenwerking tussen relevante actoren wanneer een incident gevolgen heeft voor zowel fysieke aspecten als de cyberbeveiliging van kritieke infrastructuur.

(7) Op het niveau van de Unie zijn de actoren met taken op het gebied van cybercrisisbeheer de Commissie, de EDEO, met inbegrip van de gezamenlijke capaciteit op het gebied van inlichtingenanalyse (SIAC), het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), de cyberbeveiligingsdienst voor de instellingen, organen en instanties van de Unie (CERT-EU), Europol via zijn Europees Centrum voor de bestrijding van cybercriminaliteit (EC3), het Europees netwerk van verbindingsfunctionarissen voor cybercrisisbeheer (EU-CyCLONe), het netwerk van Computer Security Incident Response Teams (CSIRT's), het Satellietcentrum van de EU (Satcen), het Galileo-centrum voor beveiligingscontrole en het netwerk van delegaties van de Unie. Deze actoren van de Unie moeten samen de gebieden voor samenwerking bepalen en bijdragen tot de uitvoering van het kader voor cybercrisisbeheer van de Unie, overeenkomstig hun bevoegdheden uit hoofde van het toepasselijk recht.

(8) Een geactualiseerde aanbeveling met een blauwdruk voor cyberbeveiliging ("cyberblauwdruk") is nodig om duidelijke en toegankelijke richtsnoeren te verstrekken waarin wordt toegelicht wat een cybercrisis op Unieniveau is, hoe het kader voor crisisbeheer wordt getriggerd, wat de rol van relevante actoren en mechanismen op Unieniveau is, en hoe de interactie tussen deze actoren en mechanismen gedurende de gehele levenscyclus van een cybercrisis verloopt. De cyberblauwdruk moet worden gezien in de bredere context van de civiel-militaire betrekkingen en de betrekkingen tussen de EU en de NAVO.

(9) Deze aanbeveling vormt een aanvulling op de regeling inzake een geïntegreerde politieke crisisrespons (IPCR) en bredere crisismechanismen van de Unie, waaronder het algemeen systeem voor vroegtijdige waarschuwing Argus van de Commissie, het Uniemechanisme voor civiele bescherming (UCPM), dat wordt ondersteund door het Coördinatiecentrum voor respons in noodsituaties (ERCC), het crisisresponsmechanisme van de Europese Dienst voor extern optreden (CRM), alsook andere processen, zoals die welke worden beschreven in de EU-toolbox tegen hybride dreigingen[17] en in het herziene EU-protocol voor de bestrijding van hybride bedreigingen. Ze vormt ook een aanvulling op en moet coherent zijn met de aanbeveling van de Raad betreffende een blauwdruk om de respons op Unieniveau op verstoringen van kritieke infrastructuur van aanzienlijk grensoverschrijdend belang te coördineren ("blauwdruk voor kritieke infrastructuur"), die betrekking heeft op fysieke niet-cyberweerbaarheid en tot doel heeft de coördinatie van de respons op Unieniveau op dit gebied te verbeteren.

(10) Een omvattende en geïntegreerde aanpak van crisisbeheer moet in alle sectoren en op alle bestuursniveaus worden bevorderd. Sectoroverschrijdend crisisbeheer op Unieniveau moet worden versterkt om een geïntegreerde crisisrespons mogelijk te

[16] PB C, C/2024/4371, 5.7.2024.

[17] Conclusies van de Raad over een kader voor een gecoördineerde EU-respons op hybride campagnes, 22 juni 2022.

maken, met name in gevallen waarin cyberincidenten gevolgen hebben in de echte wereld. Wanneer cyberbeveiligingsincidenten deel uitmaken van een bredere hybride campagne of crisis, moeten de relevante actoren inspanningen ondersteunen om een geünificeerd situatiebeeld te ontwikkelen over verschillende sectoren en domeinen heen. De aanbeveling draagt bij tot bredere paraatheidsacties die de Unie nodig heeft in het licht van multidimensionale hybride dreigingen [in lijn met de in de strategie voor een paraatheidsunie vastgelegde beginselen].

(11) De beveiliging van kritieke digitale infrastructuur is van fundamenteel belang voor de veerkracht van de economie, de samenleving en de defensie van de Unie. Binnen het toepassingsgebied van Richtlijn (EU) 2022/2555 vallende entiteiten, met inbegrip van entiteiten die onderzeese communicatiekabels leveren, moeten maatregelen nemen ter bescherming van de fysieke en de omgevingsbeveiliging van netwerk- en informatiesystemen op basis van een benadering die alle gevaren omvat, zoals systeemstoringen, menselijke fouten, kwaadwillige handelingen of natuurverschijnselen. Daarnaast moeten die entiteiten incidenten, met inbegrip van incidenten in verband met onderzeese communicatiekabels, rapporteren aan de CSIRT's of, indien van toepassing, aan de bevoegde autoriteit. Hoewel de fundamentele beginselen die ten grondslag liggen aan de cyberblauwdruk relevant zijn voor de beveiliging van onderzeese kabels, zijn de mechanismen die erin zijn opgenomen niet uitgebreid genoeg om de volledige cyclus van crisisbestendigheid te bestrijken. De specifieke aard ervan rechtvaardigt een eensgezinde en op maat gesneden inspanning om tegemoet te komen aan de behoefte aan geïntegreerde dreigingssurveillance en situationeel bewustzijn voor de zeebekkens rond de EU, strategische investeringen om redundanties te creëren en een gemeenschappelijke Europese aanpak om de reparatie- en herstelcapaciteiten te versterken. De EU-strategie voor maritieme veiligheid omvat acties om de cyberbeveiliging op maritiem gebied te verbeteren en de surveillance en bescherming van kritieke maritieme infrastructuur, met inbegrip van onderzeese kabels, te verbeteren. Voor crisisbeheer op Unieniveau zou een specifiek netwerk van nationale contactpunten en nauwe civiel-militaire interacties, waaronder met de NAVO, kunnen worden overwogen.

(12) Paraatheid voor een crisis vereist een alle gevaren en alle dreigingen omvattende risicobeoordeling, gezien de convergentie van de economische en veiligheidsbelangen van de EU. Een situationeel bewustzijn van de Unie dat door de lidstaten en entiteiten van de Unie wordt gedeeld en wordt gefaciliteerd door een gemeenschappelijke taxonomie en beveiligde communicatiekanalen overeen te komen, moet een gecoördineerde en geïnformeerde respons op potentiële en grootschalige cyberbeveiligingsincidenten en de afschrikking van persistente-dreigingsactoren mogelijk maken. Op basis van het "need-to-know"-beginsel en rekening houdend met het belang van vertrouwen in informatie-uitwisseling, is het mogelijk dat groepen lidstaten in verschillende samenstelling en, in voorkomend geval, betrokken entiteiten van de Unie willen samenwerken en voor het beheer van cyberincidenten relevante informatie willen uitwisselen. Dat lidstaten en entiteiten van de Unie informatie delen over dreigingen, risico's en maturiteitshiaten moet het mogelijk maken de juiste prioriteiten vast te stellen voor deugdelijke investeringen en concrete acties die tot een betere cyberweerbaarheid zouden leiden.

(13) Overeenkomstig artikel 6 van Verordening (EU) 2019/881 stelt Enisa, in nauwe samenwerking met de lidstaten, regelmatig een grondig technisch situatieverslag inzake de EU-cyberbeveiliging op met betrekking tot incidenten en cyberdreigingen. Dat verslag wordt het gezamenlijk cyberevaluatieverslag van de EU (EU-JCAR)

genoemd en wordt samen met Europol/EC3 en CERT-EU opgesteld met als doel de paraatheid van de Unie te vergroten, aangezien het een situationeel bewustzijn op basis van een analyse van incidenten en cyberdreigingen biedt.

(14) Essentiële kritieke infrastructuur, zoals energie-infrastructuur, vervoersinfrastructuur, digitale infrastructuur en infrastructuur voor gezondheids- of financiële diensten, en de beveiligingsoplossingen ter bescherming daarvan, worden gewoonlijk door particuliere ondernemingen geëxploiteerd. Om deze infrastructuur tegen grootschalige cyberincidenten te beschermen, is nauwe samenwerking nodig tussen publieke en particuliere entiteiten, waaronder fabrikanten en opensourceontwikkelaars, op basis van vertrouwen en duidelijke en specifieke procedures voor de uitwisseling en de verspreiding van informatie en de coördinatie van de respons.

(15) Cyberoefeningen op Unieniveau zijn een zeer doeltreffend instrument om procedures en samenwerkingsmechanismen te testen en zo de paraatheid te vergroten. Aangezien oefeningen veel middelen vergen, moet de oefenagenda zoveel mogelijk worden gestroomlijnd en geconsolideerd en moet rekening worden gehouden met de scenario's die zijn opgesteld in het kader van door de Unie gecoördineerde risicobeoordelingen en andere relevante initiatieven.

(16) Europese digitale infrastructuren kennen veel diep ingebedde technische afhankelijkheden. Die moeten worden aangepakt om de bedrijfscontinuïteit tijdens een crisis te waarborgen. Het gaat bijvoorbeeld om het domeinnaamsysteem (DNS), wat een cruciale component is voor de werking van het internet. DNS-resolvers zijn van essentieel belang voor de toegang tot internet, ook tijdens een grote cybercrisis, aangezien ze internetdomeinnamen vertalen naar IP-adressen. Richtlijn (EU) 2022/2555 moedigt belanghebbenden aan een diversificatiestrategie voor DNS-omzetting vast te stellen. Ze moedigt de lidstaten ook aan de ontwikkeling en het gebruik van een openbare en beveiligde Europese DNS-omzettingsdienst te bevorderen als een belangrijke maatregel ter waarborging van crisisparaatheid en weerbaarheid.

(17) Om de weerbaarheid van andere kritieke componenten, zoals het routeringssysteem, te vergroten en de functionaliteit ervan tijdens grote cybercrises te waarborgen, is het voorts van essentieel belang dat de beste praktijken ter zake en de meest recente beschikbare normen tijdig worden toegepast. Bijgevolg wordt bij Uitvoeringsverordening (EU) 2024/2690 een multistakeholderforum opgericht om de beste beschikbare normen en implementatietechnieken voor essentiële cyberbeveiligingselementen vast te stellen en wordt participatie van relevante entiteiten aangemoedigd.

(18) Voor de doeltreffende detectie van kwaadwillige activiteit in de steeds complexere mondiale toeleveringsketens, met een mogelijk Uniebrede impact, is een gecoördineerde aanpak vereist. Dit is met name relevant voor gebieden waar de Unie afhankelijk is van technologie van leveranciers met een hoog risico die vallen onder de jurisdictie van een derde land dat voorschrijft dat informatie over kwetsbaarheden in software of hardware aan zijn autoriteiten wordt gemeld voordat bekend is dat ze worden uitgebuit. Door staten gesteunde actoren kunnen zich ook in kritieke infrastructuur prepositioneren met de intentie om op een later tijdstip, bijvoorbeeld tijdens een conflict, disruptie te veroorzaken. Dit is moeilijk op te sporen met behulp van traditionele methoden, aangezien dreigingsactoren hun activiteiten verhullen door in legitiem verkeer op te gaan en "living off the land"-technieken te combineren die legitieme instrumenten en processen gebruiken om kwaadwillige activiteiten te

verbergen. Hetzelfde geldt voor derde landen wanneer, volgens publieke verklaringen van de Unie of haar lidstaten, dreigingsactoren die vanaf het grondgebied van die landen opereren, kwaadwillige cyberactiviteiten tegen de Unie ontplooien. Toeleveringsketens moeten weerbaarder en gediversifieerder worden, met behoud van een gemeenschappelijk basisniveau van paraatheid.

(19) Op technisch niveau spelen CSIRT's, rechtshandhavingsinstanties en de uit hoofde van Verordening (EU) 2025/38 op te richten nationale en landsgrensoverschrijdende cyberhubs, een essentiële rol bij het detecteren van incidenten, cyberdreigingen en kwetsbaarheden, het ondersteunen van technische attributies en het herstellen van cyberaanvallen. Doeltreffende procedurele regelingen voor samenwerking tussen het CSIRT-netwerk en EU-CyCLONe, zoals vereist door Richtlijn (EU) 2022/2555, zijn van essentieel belang. Het Europees waarschuwingsmechanisme voor cyberbeveiliging heeft tot doel de ontwikkeling van geavanceerde capaciteiten voor de Unie te ondersteunen om de capaciteiten op het gebied van detectie, analyse en gegevensverwerking met betrekking tot cyberdreigingen en de preventie van incidenten in de Unie te verbeteren.

(20) Wat de onmiddellijke respons betreft, zijn de mechanismen waarover de lidstaten beschikken onder meer de EU-cyberbeveiligingsreserve en acties ter ondersteuning van wederzijdse bijstand uit hoofde van Verordening (EU) 2025/38, teams voor snelle respons op hybride dreigingen en permanente gestructureerde samenwerking (Pesco), snellereactieteams bij cyberbeveiligingsincidenten (CRRT's), alsook mechanismen voor NAVO-bondgenoten. Daarnaast ondersteunt het crisisresponsprotocol van de EU-rechtshandhavingsinstanties (Leerp) de rechtshandhavingsinstanties van de EU bij het bieden van een onmiddellijke respons op grote grensoverschrijdende cyberaanvallen door middel van snelle beoordeling, beveiligde en tijdige uitwisseling van kritieke informatie en doeltreffende coördinatie van de internationale aspecten van hun onderzoeken, met inbegrip van deconflictering op rechtshandhavingsniveau en coördinatie met niet-rechtshandhavingspartners. Door een duidelijk beeld te krijgen van welke responsopties in geval van cyberincidenten en hybride activiteiten beschikbaar zijn en hoe deze worden gebruikt, kan voor een efficiënte toewijzing van middelen worden gezorgd en duplicering worden voorkomen. Dienovereenkomstig zijn de lidstaten op grond van Verordening (EU) 2025/38 verplicht het CSIRT-netwerk en EU-CyCLONe in te lichten wanneer ze om diensten van de EU-cyberbeveiligingsreserve verzoeken.

(21) Doeltreffende bestrijding van cybercriminaliteit is van essentieel belang voor cyberbeveiliging. Afschrikking kan niet worden bereikt door middel van weerbaarheid alleen, maar vereist ook het identificeren en vervolgen van, en optreden tegen overtreders. Samenwerking door middel van aangepaste technische systemen en platforms en uitwisseling van relevante informatie tussen cyberbeveiligingsactoren, cyberdiplomatie-entiteiten en rechtshandhavingsinstanties zijn daarom van essentieel belang om een omvattend begrip van het dreigingslandschap te waarborgen en om op coherente en gecoördineerde wijze te kunnen reageren.

(22) Crises veroorzaken onzekerheid die tegenstanders gemakkelijk kunnen uitbuiten om desinformatie te verspreiden en wantrouwen te zaaien. Essentieel om dit tegen te gaan, is duidelijke en coherente publiekscommunicatie over de situatie en over welke maatregelen worden genomen om ze te verhelpen. Een gecoördineerde strategische communicatie kan ook steun verlenen aan diplomatieke acties ten aanzien van persistente-dreigingsactoren en de ontwikkeling van een narratief over bedreigingen

voor de Unie, haar afschrikkingsacties en de noodzaak om verantwoordelijk staatsgedrag in cyberspace te bevorderen.

(23) Met het oog op een doeltreffend crisisbeheer moeten gemeenschappelijke beveiligde communicatieoplossingen voor het cyberdomein worden vastgesteld en in de hele Unie worden toegepast, inclusief waar nodig voor de uitwisseling van gerubriceerde EU-informatie. Op verzoek van de Raad hebben de Commissie en andere relevante entiteiten van de Unie de bestaande beveiligde communicatie-instrumenten in kaart gebracht en de resultaten in december 2022 gepresenteerd. Er bestaan verschillende afzonderlijke inspanningen van entiteiten van de Unie om in een crisis capaciteiten voor beveiligde communicatie op te bouwen, die een betere coördinatie en hefboomwerking vereisen. Deze omvatten de oprichting van een EU-systeem voor kritieke communicatie (EUCCS) om de weerbaarheid van publieke communicatie-infrastructuur tegen kwaadwillige inmenging te vergroten en de dagelijkse operationele samenwerking, ook over de grenzen heen, te verbeteren.

(24) De beveiligingsomgeving van de Unie vereist een alle gevaren omvattende, overheids- en maatschappijbrede aanpak van civiele en militaire paraatheid en bereidheid. Militaire instanties zijn afhankelijk van kritieke infrastructuur van civiele aard, zoals communicatie-, energie-, gezondheids-, vervoers- en logistieke infrastructuur. Daarom is, zoals ook is benadrukt in de mededeling inzake het EU-beleid op het gebied van cyberdefensie[18], voor de cyberbeveiliging van de EU meer samenwerking en synergie nodig tussen de capaciteiten van civiele en militaire netwerken voor paraatheid en respons, waaronder in het geval van een gewapende aanval. Cyberbeveiligingsactoren moeten over institutionele en operationele eilandjes heen samenwerken om te anticiperen op en het hoofd te bieden aan de dreiging van multisectorale, multidimensionale disruptie, in lijn met de in de strategie voor een paraatheidsunie [te verankeren] beginselen. Voorts speelt kwaadwillige cyberactiviteit een steeds grotere rol in bredere hybride campagnes tegen de Unie, haar lidstaten en strategische partners. Daarom is nauwere samenwerking tussen de Unie en de NAVO nodig.

(25) In de militaire gemeenschap zijn het toekomstige EU-coördinatiecentrum voor cyberdefensie en de gezamenlijke capaciteit op het gebied van inlichtingenanalyse (SIAC) binnen de Europese Dienst voor extern optreden, het operationeel netwerk voor militaire computercrisisresponsteams (Micnet) en de door het Europees Defensieagentschap (EDA) gefaciliteerde conferentie van EU-cybercommandanten, alsook relevante projecten in het kader van de permanente gestructureerde samenwerking (Pesco), belangrijke actoren en initiatieven voor coördinatie en samenwerking op het gebied van paraatheid voor detectie van, afschrikking van, verdediging tegen en herstel van cyberdreigingen die gevolgen hebben voor de Unie en de lidstaten. Daarom moet samenwerking tussen civiele en militaire actoren worden aangemoedigd, zoals de samenwerking tussen EU-CyCLONe en de conferentie van EU-cybercommandanten, alsook de mogelijke samenwerking tussen Micnet en het CSIRT-netwerk.

(26) Samenwerking met strategische internationale partnerlanden en organisaties buiten de Unie versterkt de cyberbeveiligingscapaciteiten van de Unie. Door internationale samenwerking te bevorderen, kunnen de Unie en haar partners zorgen voor een gedeeld situationeel bewustzijn en samenhang op het gebied van cybercrisisbeheer en een robuuste cyberhouding, wat bijdraagt tot een mondiale, open, stabiele, beveiligde

[18] Het EU-beleid op het gebied van cyberdefensie, JOIN(2022) 49 final.

en weerbare cyberspace. Deze samenwerking moet berusten op vertrouwen en het gedeelde doel om kritieke infrastructuur en essentiële diensten te beschermen tegen cyberdreigingen, onder meer door verantwoordelijk staatsgedrag in cyberspace te bevorderen op basis van het kader van de Verenigde Naties en door dreigingsactoren ter verantwoording te roepen voor hun onverantwoordelijke en onrechtmatige gedrag in cyberspace. Cyberdiplomatiemaatregelen dragen bij tot de afschrikking van en respons op kwaadwillige cyberactiviteiten en zorgen voor coördinatie en samenwerking met strategische internationale partnerlanden,

HEEFT DE VOLGENDE AANBEVELING VASTGESTELD:

I: Doel, toepassingsgebied en beginselen van het EU-kader voor cybercrisisbeheer

(1) Deze aanbeveling bevat het Uniekader voor cyberbeveiligingscrisisbeheer in de context van de algemene paraatheid van de EU voor multidimensionale hybride dreigingen. Hoe een incident kan escaleren tot een grootschalig incident en vervolgens tot een crisis op EU-niveau, wordt geïllustreerd en samengevat in bijlage 1, ook wanneer een dergelijk incident gelijktijdig plaatsvindt met andere hybride dreigingen die interactie tussen de vereiste reacties vergen. Het kader voor cybercrisisbeheer zou de relevante actoren op Unieniveau, met inbegrip van entiteiten en netwerken, in staat moeten stellen te begrijpen hoe ze met elkaar kunnen samenwerken en optimaal gebruik kunnen maken van de in bijlage II vermelde bestaande mechanismen gedurende de volledige levenscyclus van het crisisbeheer. Daarnaast worden aan deze actoren op Unieniveau aanbevelingen gedaan over de wijze waarop de doeltreffendheid van de bestaande mechanismen kan worden verbeterd.

(2) De Unie en haar lidstaten zouden de cyberblauwdruk moeten volgen bij het beheer van een crisis als gevolg van een grootschalig cyberbeveiligingsincident, zoals gedefinieerd in artikel 6, punt 7, van Richtlijn (EU) 2022/2555, dat gevolgen heeft voor de goede werking van de interne markt of ernstige risico's met zich meebrengt voor entiteiten of burgers in verschillende lidstaten of de Unie als geheel ("cybercrisis").

(3) Wanneer een cyberbeveiligingsincident, dat op technisch niveau door een CSIRT of een cyberhub is gedetecteerd, leidt tot opschaling in het kader van de interne procedures van het CSIRT-netwerk, zou overeenkomstig de relevante procedurele regelingen passende informatie moeten worden gedeeld met EU-CyCLONe, dat op zijn beurt zou moeten nagaan of het een potentieel of aan de gang zijnd grootschalig incident zoals gedefinieerd in artikel 6, punt 7, van Richtlijn (EU) 2022/2555 betreft. De vaststelling of er als gevolg van dit grootschalige incident een cybercrisis bestaat of ophoudt te bestaan, zou moeten gebeuren overeenkomstig Uitvoeringsbesluit (EU) 2018/1993, en met name de artikelen 4 en 5.

(4) Overeenkomstig de beginselen van proportionaliteit, subsidiariteit, complementariteit en vertrouwelijkheid van informatie van bijlage III zouden de lidstaten en de entiteiten van de Unie hun samenwerking op het gebied van cybercrisisbeheer moeten verdiepen door wederzijds vertrouwen te bevorderen en voort te bouwen op bestaande netwerken en mechanismen. Hoewel de cyberblauwdruk geen invloed heeft op de wijze waarop entiteiten hun interne procedures bepalen, zou elke entiteit duidelijk de interfaces moeten bepalen om met andere entiteiten samen te werken. Deze interfaces zouden door de betrokken entiteiten gezamenlijk moeten worden overeengekomen en duidelijk moeten worden gedocumenteerd.

(5) De cyberblauwdruk zou moeten worden toegepast in samenhang met de blauwdruk voor kritieke infrastructuur, met name in het geval van incidenten die gevolgen hebben voor zowel de fysieke weerbaarheid als de cyberbeveiliging van kritieke infrastructuur[19]. Wanneer er sectorspecifieke crisisbeheersmaatregelen zijn die betrekking hebben op cyberbeveiligingsincidenten, zouden die maatregelen moeten worden uitgevoerd op een met deze aanbeveling strokende wijze.

II: Voorbereiding op een cybercrisis op Unieniveau

(a) Situationeel bewustzijn en delen van informatie

(6) Geverifieerde, betrouwbare gegevens, met inbegrip van trends in incidenten, tactieken, technieken en procedures, en actief uitgebuite kwetsbaarheden zouden de basis moeten vormen voor een gemeenschappelijk situationeel bewustzijn van het cyberdreigingslandschap onder de lidstaten en entiteiten van de Unie. Deze gedeelde kennis zou door de lidstaten en de entiteiten van de Unie moeten worden gebruikt om te anticiperen op cyberaanvallen, zich erop voor te bereiden en ze te detecteren, in lijn met hun respectieve bevoegdheidsgebieden. Dit gemeenschappelijk situationeel bewustzijn zou:

(a) van toepassing moeten zijn op alle in Richtlijn (EU) 2022/2555 vermelde kritieke sectoren, met name communicatie, digitale infrastructuur, energie, vervoer, financiën, ruimtevaart en gezondheidzorg, en zou ook, via CERT-EU, van toepassing moeten zijn op de netwerken en systemen van entiteiten van de Unie overeenkomstig Verordening (EU, Euratom) 2023/2841;

(b) moeten berusten op gediversifieerde en geïntegreerde datasets van hoge kwaliteit die in realtime worden verzameld, verwerkt en gedeeld;

(c) in aanmerking moeten worden genomen in het gezamenlijk cyberevaluatieverslag (JCAR) en andere relevante producten;

(d) rekening moeten houden met gerelateerde hybride dreigingen, inclusief buitenlandse informatiemanipulatie en inmenging (FIMI) en desinformatie;

(e) kortetermijnacties en responsmaatregelen moeten ondersteunen en bijdragen aan langetermijnbeleidsplanning in de context van paraatheid en afschrikking;

(f) [link naar andere risico- en dreigingsbeoordelingen die regelmatig worden opgesteld en versterkt door de strategie voor een paraatheidsunie om synergieën en vereenvoudiging van de rapportageverplichtingen voor de lidstaten te waarborgen.]

(7) EU-CyCLONe en het CSIRT-netwerk zouden:

(a) moeten samenwerken om het delen van informatie tussen het technische en operationele niveau en het situationeel bewustzijn als geheel te verbeteren;

(b) een klimaat van vertrouwen tussen de leden moeten blijven scheppen;

(c) ten volle gebruik moeten maken van de beschikbare instrumenten voor het delen van informatie.

(8) De lidstaten en de relevante entiteiten van de Unie zouden de mogelijkheden moeten verbeteren voor coördinatie en het sluiten van partnerschappen met de particuliere

[19] . In deel I, afdeling 4, van de bijlage bij de blauwdruk voor kritieke infrastructuur wordt de coördinatie in dergelijke gevallen nader toegelicht.

sector, onder meer met opensourcegemeenschappen en fabrikanten, voor het delen van informatie op EU- en nationaal niveau, via bestaande centra voor informatie-uitwisseling en -analyse, en voor het vergroten van de cyberbeveiligingscapaciteit voor de respons op cyberbeveiligingsincidenten, onder meer via rondetafelgesprekken met EU-CyCLONe en het CSIRT-netwerk.

(9) De lidstaten en de relevante entiteiten van de Unie zouden ervoor kunnen kiezen om, met het oog op het bevorderen van de samenwerking en het versterken van het vertrouwen, en voortbouwend op de informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging van Richtlijn (EU) 2022/2555 en de bepalingen van Verordening (EU) 2025/38 met betrekking tot cyberhubs, vrijwillige samenwerkingsclusters op een "need-to-know"-basis op te zetten wanneer er gemeenschappelijke zorgen bestaan, zoals afschrikking van, detectie van, of respons op een bepaald soort dreiging waarmee zij in het bijzonder worden geconfronteerd. Dergelijke clusters zouden het mandaat van de relevante actoren en reeds bestaande structuren moeten eerbiedigen. Die samenwerkingsclusters zouden de entiteiten van de Unie kunnen oproepen om hun samenwerking te faciliteren, onder meer via passende infrastructuur.

(10) De lidstaten zouden, via de bij Richtlijn (EU) 2022/2555 opgerichte NIS-samenwerkingsgroep, binnen twaalf maanden na de vaststelling van de cyberblauwdruk een gemeenschappelijke taxonomie met betrekking tot cybercrisisbeheer moeten ontwikkelen en richtsnoeren moeten verstrekken voor de beveiligde verwerking en uitwisseling van informatie in verband met cyberbeveiligingsincidenten en -crises, met inbegrip van een deel dat gewijd is aan het bepalen van het vertrouwelijkheidsniveau van deze informatie (rubricering).

(11) Bij het bepalen van het vertrouwelijkheidsniveau voor de beschikbare informatie zouden de lidstaten en de relevante entiteiten van de Unie rekening moeten houden met de mogelijke impact die overrubricering kan hebben op de vrijwillige uitwisseling van informatie en het tot stand brengen van een gemeenschappelijk situationeel bewustzijn. Bij het delen van niet-gerubriceerde informatie zouden de lidstaten ten volle gebruik moeten maken van de bestaande platforms voor technische en operationele samenwerking, zoals die welke door het CSIRT-netwerk en EU-CyCLONe worden gebruikt.

b) Gemeenschappelijke oefeningen

(12) De lidstaten en de relevante entiteiten van de Unie zouden een efficiënte continue cyclus van cyberoefeningen moeten ontwikkelen om zich op cybercrises voor te bereiden en de organisatorische efficiëntie te vergroten. Deze oefeningen zouden moeten uitgaan van de scenario's die zijn ontwikkeld op basis van door de EU gecoördineerde risicobeoordelingen, inclusief die met betrekking tot multisectorale crises. De continue cyclus van cyberoefeningen zou rekening moeten houden met het Uniemechanisme voor civiele bescherming en andere crisisresponsmechanismen op Unieniveau. Hij moet ervoor zorgen dat de lessen die uit de oefeningen zijn getrokken, daadwerkelijk worden geïmplementeerd.

(13) Relevante Unieactoren kunnen kleinere oefeningen uitvoeren om hun interacties en interfaces te testen in geval van escalerende cyberincidenten.

(14) De diensten van de Commissie, de EDEO en Enisa worden verzocht binnen 18 maanden na de vaststelling van de cyberblauwdruk een oefening te organiseren om

de cyberblauwdruk te testen, waarbij alle relevante actoren, waaronder de particuliere sector, worden betrokken.

c) DNS-omzettingscapaciteiten

(15) De lidstaten, relevante entiteiten van de Unie en particuliere entiteiten zoals exploitanten van kritieke infrastructuur zouden hun diversificatiestrategie voor DNS-omzetting moeten versterken, met inbegrip van het gebruik van ten minste één in de Unie gevestigde DNS-infrastructuur zoals DNS4EU om betrouwbare DNS-omzetting te waarborgen tijdens een grote crisis. Enisa en EU-CyCLONe zouden richtsnoeren voor failover in noodgevallen moeten ontwikkelen en beschikbaar moeten stellen, waarin ze de stappen beschrijven om op in de Unie gevestigde DNS-infrastructuur over te schakelen indien andere DNS-diensten falen, zodat de continuïteit van kritieke diensten tijdens een crisis wordt gewaarborgd.

(16) Daarnaast zouden nationale cyberhubs en landsgrensoverschrijdende cyberhubs relevante informatie over dreigingen moeten delen met dergelijke in de Unie gevestigde DNS-infrastructuren om ze te ondersteunen bij het bieden van een hoog niveau van bescherming tegen Uniespecifieke dreigingen en zo de capaciteiten voor het detecteren en mitigeren van Uniespecifieke dreigingen verder te vergroten.

(17) Om de beveiliging en de beschikbaarheid van kritieke internetinfrastructuur in het algemeen te versterken, ook tijdens crises, zouden de lidstaten actief de deelname moeten bevorderen van alle relevante belanghebbenden — met inbegrip van de belanghebbenden die niet rechtstreeks onder de NIS 2-uitvoeringshandeling vallen — in het gemandateerde multistakeholderforum dat tot taak heeft de beste beschikbare normen en implementatietechnieken voor cruciale netwerkbeveiligingsmaatregelen vast te stellen. Bovendien zouden de lidstaten moeten overwegen zelf aan het forum deel te nemen en de aanbevolen richtsnoeren over te nemen.

d) Middelen

(18) De lidstaten zouden ten volle gebruik moeten maken van de financiële middelen die beschikbaar zijn voor cyberbeveiliging in het kader van relevante programma's van de Unie.

III: Detectie van een incident dat tot een cybercrisis zou kunnen escaleren

(19) Om de escalerende complexiteit van cyberincidenten en de toenemende uitdagingen bij de detectie ervan aan te pakken, zouden zowel publieke als particuliere entiteiten in hun digitale infrastructuur dreigingsgebaseerde detectiestrategieën moeten implementeren ter opsporing van mogelijke prepositionering die later voor disruptiedoeleinden zou kunnen worden gebruikt. Wanneer geheime operaties aan het licht komen, zouden entiteiten relevante informatie proactief met hun partners moeten delen, geruime tijd voordat situaties tot crises escaleren.

(20) Alle actoren zouden, in overeenstemming met hun respectieve mandaten en op basis van de alle gevaren omvattende aanpak, informatie die op een potentiële cybercrisis wijst, aan de relevante netwerken moeten doorgeven.

(21) Het CSIRT-netwerk en EU-CyCLONe zouden procedurele regelingen moeten vaststellen in het geval van een potentieel of aan de gang zijnd grootschalig cyberbeveiligingsincident, om te zorgen voor technische en operationele coördinatie en tijdige en relevante informatie op politiek niveau.

(22) Het CSIRT-netwerk zou EU-CyCLONe moeten adviseren over de vraag of een waargenomen cyberbeveiligingsincident kan worden beschouwd als een potentieel of aan de gang zijnd grootschalig incident.

(23) De grensoverschrijdende cyberhubs, die reeds zijn opgericht of moeten worden opgericht uit hoofde van Verordening (EU) 2025/38, zouden met relevante informatie moeten bijdragen aan de mechanismen op Unienvieau in geval van een potentieel of aan de gang zijnd grootschalig cyberbeveiligingsincident op basis van de alle gevaren omvattende aanpak, met inbegrip van fysieke schade aan kritieke infrastructuur die afbreuk doet aan de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen.

(24) Wanneer een potentieel of grootschalig cyberbeveiligingsincident met een multisectorale impact wordt gedetecteerd:

(a) zou de Commissie de noodzakelijke informatiestroom tussen contactpunten voor de in bijlage II vermelde relevante horizontale en sectorale crisismechanismen op Unieniveau en EU-CyCLONe moeten faciliteren;

(b) zouden relevante entiteiten van de Unie EU-CyCLONe moeten ondersteunen bij het beoordelen van de gevolgen voor sectoren en de bevolking.

IV: Reageren op een cybercrisis op Unieniveau

(25) In geval van een in het kader van de IPCR vastgestelde cybercrisis, zouden alle actoren in nauwe samenwerking met andere entiteiten die reageren op bredere hybride dreigingen, als volgt moeten reageren in het kader van een overheidsbrede aanpak:

(a) de getroffen lidstaat of de getroffen lidstaten en het CSIRT-netwerk zouden moeten samenwerken om getroffen systemen snel te herstellen, om een zo klein mogelijke operationele verstoring te waarborgen;

(b) EU-CyCLONe zou, in samenwerking met het CSIRT-netwerk, het politieke niveau duidelijke informatie moeten verstrekken over de impact en de mogelijke gevolgen van het incident en over de respons- en herstelmaatregelen, onder meer door bij te dragen aan het verslag over geïntegreerde situatiekennis en -analyse (ISAA) in het kader van de IPCR-regeling;

(c) de Commissie zou, in voorkomend geval in samenwerking met de hoge vertegenwoordiger, moeten zorgen voor samenhang en coördinatie tussen de respons op de crisis en de gerelateerde responsacties op Unieniveau, met name de in bijlage 2 vermelde relevante sectorale crisisbeheermechanismen op Unieniveau, en met betrekking tot het verzoeken om bijstand via het Uniemechanisme voor civiele bescherming;

(d) het voorzitterschap van de Raad zou moeten overwegen de voorzitter van EU-CyCLONe uit te nodigen voor informele rondetafelbijeenkomsten en andere relevante Raadszittingen in het kader van de IPCR-regeling;

(e) de Raad zou, ondersteund door EU-CyCLONe en relevante entiteiten van de Unie, de inspanningen op het gebied van publiekscommunicatie moeten coördineren, onder meer om ervoor te zorgen dat de crisissituatie niet wordt gebruikt om onjuiste informatie te verspreiden;

(f) de hoge vertegenwoordiger zou, in nauwe samenwerking met de Commissie en andere relevante entiteiten van de Unie, de besluitvorming in de Raad moeten ondersteunen, onder meer door middel van analysen en verslagen over het gebruik van mogelijke maatregelen als onderdeel van het instrumentarium voor cyberdiplomatie. Dit maakt het mogelijk gebruik te maken van het volledige spectrum van beschikbare instrumenten van de Unie om kwaadwillige cyberactiviteiten te voorkomen, af te schrikken en erop te reageren, haar cyberhouding te versterken en internationale vrede, veiligheid en stabiliteit in cyberspace te bevorderen;

(g) de Commissie, de hoge vertegenwoordiger en de lidstaten zouden ook economische instrumenten zoals handelsverboden effectiever moeten benutten om persistente kwaadwillige cyberactiviteiten van statelijke actoren beter te voorkomen, af te schrikken en erop te reageren.

(26) Wanneer een gebruiker van de door de EU-cyberbeveiligingsreserve[20] verleende diensten overeenkomstig artikel 15 van Verordening (EU) 2025/38 om diensten uit de EU-cyberbeveiligingsreserve verzoekt, en onverminderd toekomstige uitvoeringshandelingen uit hoofde van die verordening:

(a) zouden de diensten binnen 24 uur na het verzoek moeten worden geleverd;

(b) zouden de Commissie en de hoge vertegenwoordiger moeten zorgen voor coördinatie met aanvullende maatregelen, in lijn met de toolbox tegen hybride dreigingen[21] in het geval van kwaadwillige cyberactiviteiten die deel uitmaken van een bredere hybride campagne;

(c) zou, in het geval van kwaadwillige cyberactiviteit met een militaire dimensie, de verzoekende lidstaat de conferentie van cybercommandanten van de Unie in kennis moeten stellen van zijn verzoek.

(27) In geval van een grootschalig cyberbeveiligingsincident dat gevolgen heeft voor de goede werking van ruimtediensten die essentieel zijn voor de veiligheid van de Unie of haar lidstaten, zou EU-CyCLONe de hoge vertegenwoordiger daarvan in kennis moeten stellen met het oog op de coördinatie van een mogelijke respons met de overeenkomstig Besluit (GBVB) 2021/698 van de Raad vastgestelde architectuur voor respons op ruimtedreigingen.

V: Herstel van een cybercrisis

(28) De lidstaten, relevante entiteiten en netwerken van de Unie zouden in de herstelfase moeten samenwerken op basis van de lessen die zijn getrokken uit de oefeningen die hebben plaatsgevonden alsook uit incidentenverslagen, met name in de context van het bij Verordening (EU) 2025/38 ingestelde Europees mechanisme voor de evaluatie van cyberbeveiligingsincidenten.

---

[20] De EU-cyberbeveiligingsreserve is een uit diensten van betrouwbare aanbieders van beheerde beveiligingsdiensten bestaand mechanisme om, op verzoek, de respons te ondersteunen en herstelacties te initiëren in geval van significante cyberbeveiligingsincidenten, grootschalige cyberbeveiligingsincidenten of aan grootschalige cyberbeveiligingsincidenten gelijkwaardige incidenten die gevolgen hebben voor de lidstaten, de instellingen, organen of instanties van de Unie of met het programma Digitaal Europa geassocieerde derde landen.

[21] De toolbox tegen hybride dreigingen is een kader voor een gecoördineerde respons op hybride campagnes die de EU en haar lidstaten treffen, dat bijvoorbeeld preventieve, coöperatieve, stabiliteits-, restrictieve en herstelmaatregelen omvat en solidariteit en wederzijdse bijstand ondersteunt.

VI: Beveiligde communicatie

(29) Op basis van het in kaart brengen van bestaande instrumenten voor beveiligde communicatie[22] zouden de Commissie, de hoge vertegenwoordiger, EU-CyCLONe, het CSIRT-netwerk en relevante entiteiten van de Unie uiterlijk eind 2026 overeenstemming moeten bereiken over een interoperabele reeks oplossingen voor beveiligde communicatie voor relevante actoren van de Unie. Deze oplossingen zouden betrekking moeten hebben op alle vereiste communicatiemiddelen (spraak, data, videoteleconferentie (VTC), berichtenverkeer, samenwerking en het delen en raadplegen van documenten). De oplossingen zouden kernbeginselen moeten weerspiegelen zoals veiligheidsbelangen van de Unie, technologische soevereiniteit en vertrouwelijkheid, alsook kenmerken zoals bruikbaarheid, beveiliging door ontwerp, certificering door Europese informatiebeveiligingsinstanties, end-to-endencryptie, authenticatie, beschikbaarheid en post-kwantumcryptografie. De oplossingen zouden moeten voldoen aan gezamenlijk vastgestelde vereisten voor de bescherming van gevoelige niet-gerubriceerde informatie en instrumenten moeten omvatten voor de uitwisseling van RESTREINT UE/EU RESTRICTED-informatie.

(30) Op basis hiervan zouden actoren op Unieniveau gebruik moeten maken van oplossingen op basis van het Matrix-protocol voor realtimecommunicatie. Het bij Verordening (EU) 2021/887 opgerichte Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging (ECCC) zou, onverminderd het toekomstige meerjarig financieel kader, financiering via het programma Digitaal Europa moeten overwegen om de lidstaten bij te staan bij de uitrol van deze instrumenten.

(31) De EU-entiteiten en de lidstaten zouden met name noodmaatregelen moeten ontwikkelen voor ernstige crises wanneer normale communicatiekanalen die gebruikmaken van internet of telecommunicatienetwerken worden verstoord of niet beschikbaar zijn.

(32) Op middellange termijn zouden mechanismen voor communicatie en informatie-uitwisseling tussen rechtshandhavings- en cyberbeveiligingsnetwerken, met name op technisch niveau, moeten worden opgezet met het oog op een doeltreffende crisisrespons. Deze mechanismen zouden de rol van elke partij moeten eerbiedigen en inmenging in lopende activiteiten moeten voorkomen. De Commissie werkt samen met de lidstaten aan de oprichting van het Europees systeem voor kritieke communicatie (EUCCS), dat tegen 2030 de communicatienetwerken voor rechtshandhaving en civiele bescherming in het hele Schengengebied met elkaar zou moeten verbinden, zodat kritieke communicatieapparatuur op het grondgebied van andere lidstaten kan worden gebruikt. EUCCS kan daarom ook de gezamenlijke respons met relevante cybergemeenschappen ten goede komen. Dit systeem zou back-upcommunicatie moeten omvatten, bijvoorbeeld via satellietcommunicatie.

VII: Coördinatie van cybercrises met militaire actoren

(33) EU-CyCLONe en de conferentie van EU-cybercommandanten, Micnet en het CSIRT-netwerk, alsook een toekomstig EU-coördinatiecentrum voor cyberdefensie, en zijn civiele tegenhangers in de Unie, zouden moeten samenwerken om een gemeenschappelijk situationeel bewustzijn tussen civiele en militaire actoren te ontwikkelen.

[22] HWPCI WK 862/23.

(34) Rekening houdend met bestaande overeenkomsten, zoals de technische overeenkomst tussen CERT-EU en de NAVO van 2016, zou de Unie ernaar moeten streven in geval van een cybercrisis contactpunten voor coördinatie met de NAVO op te richten om de nodige informatie over de situatie en het gebruik van crisisresponsmechanismen uit te wisselen. Daartoe zou de Unie moeten nagaan hoe de capaciteiten voor informatie-uitwisseling met de NAVO kunnen worden verbeterd, onder meer door middel van mogelijke koppelingen tussen hun respectieve communicatie- en informatiesystemen.

(35) Wanneer een lidstaat in de context van een cyberbeveiligingsincident gebruikmaakt van relevante defensie-initiatieven, zoals de CRRT's van Pesco of andere relevante initiatieven, zoals de snellereactieteams van de Unie tegen hybride dreigingen (HRRT's), zou hij EU-CyCLONe en de EU-conferentie van cybercommandanten daarvan in kennis moeten stellen.

VIII: Samenwerking met strategische partners

(36) De hoge vertegenwoordiger zou, in nauwe samenwerking met de Commissie en andere relevante entiteiten van de Unie:

(a) indien een relevant incident wordt geconstateerd, de nodige informatiestroom met strategische partners moeten faciliteren;

(b) de coördinatie met strategische partners moeten verbeteren met betrekking tot de respons op aanhoudende kwaadwillige cyberactiviteiten door persistente-dreigingsactoren, met name bij het gebruik van het instrumentarium voor cyberdiplomatie, in lijn met de uitvoeringsrichtsnoeren ervan.

(37) De lidstaten, de hoge vertegenwoordiger, de Commissie en andere relevante entiteiten van de Unie zouden moeten samenwerken met strategische partners en internationale organisaties om goede praktijken en verantwoordelijk staatsgedrag in cyberspace te bevorderen en te zorgen voor een snelle en gecoördineerde reactie in geval van potentiële of grootschalige cyberincidenten.

(38) In het kader van de in deel II hierboven bedoelde continue cyclus van oefeningen zouden de diensten van de Commissie en de EDEO moeten overwegen een gezamenlijke personeelsoefening te organiseren om de samenwerking tussen zowel civiele als militaire componenten te testen in het geval van een grootschalig cyberincident dat lidstaten van de Unie en NAVO-bondgenoten treft, ook wanneer artikel 4 of artikel 5 van het NAVO-verdrag in werking wordt gesteld of waarschijnlijk in werking zal worden gesteld.

(39) Gezien de blootstelling van kandidaat-lidstaten en het potentieel van cyberincidenten die plaatsvinden in de nabuurschap van de Unie, zouden gezamenlijke oefeningen met kandidaat-lidstaten moeten worden overwogen.

Gedaan te Brussel,

Voor de Raad

De voorzitter