Raad van de Europese Unie

Brussel, 6 juni 2025
(OR. en)

9794/25

Interinstitutioneel dossier:
2025/0036(NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

RESULTAAT BESPREKINGEN

van:	het secretariaat-generaal van de Raad
d.d.:	6 juni 2025
aan:	de delegaties
Betreft:	Aanbeveling van de Raad betreffende een EU-blauwdruk voor cybercrisisbeheer - Aanbeveling van de Raad, door de Raad goedgekeurd tijdens zijn zitting van 6 juni 2025

De delegaties vinden in de bijlage de aanbeveling van de Raad die de Raad tijdens zijn zitting van 6 juni 2025 heeft goedgekeurd.

BIJLAGE

AANBEVELING VAN DE RAAD

betreffende een EU-blauwdruk voor cybercrisisbeheer

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name de artikelen 114 en 292,

Gezien het voorstel van de Europese Commissie,

Overwegende hetgeen volgt:

(1) 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 cyberbeveiligingsincidenten en cyberaanvallen. Bovendien uit de toename van geopolitieke spanningen, conflicten en strategische rivaliteit zich in de impact, de omvang en de complexiteit van kwaadwillige cyberactiviteiten. Dergelijke activiteiten kunnen deel uitmaken van hybride campagnes of militaire operaties. Ze kunnen ook rechtstreeks van invloed zijn op de veiligheid, economie en samenleving van de Unie. Daarnaast hebben ze een mogelijk overloopeffect, 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 de responscapaciteit van een getroffen lidstaat te boven gaat of dat een significante impact heeft op meer dan een lidstaat. Afhankelijk van de oorzaak en impact ervan kan een dergelijk incident escaleren en uitgroeien tot een volwaardige crisis die de goede werking van de interne markt aantast of ernstige risico's voor de openbare veiligheid en beveiliging met zich meebrengt voor entiteiten of burgers in verschillende lidstaten of in de hele Unie. Doeltreffend crisisbeheer is essentieel om de economische stabiliteit te handhaven en Europese overheden, kritieke infrastructuur, bedrijven en burgers 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) Gezien de onderlinge afhankelijkheid en verbindingen tussen de ICT-omgevingen van entiteiten van de Unie en de lidstaten, kan een incident in een entiteit van de Unie een cyberbeveiligingsrisico vormen voor de lidstaten en vice versa. Het delen van relevante informatie en de coördinatie met betrekking tot zowel grootschalige cyberbeveiligingsincidenten als ernstige incidenten, zoals gedefinieerd in artikel 3, lid 8, van Verordening (EU, Euratom) 2023/2841[1], is van cruciaal belang in de context van de EU-blauwdruk voor cybercrisisbeheer ("cyberblauwdruk").

[1] 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).

(4) Wat betreft de coördinatie van en respons op crises waarvoor de geïntegreerde EU-regeling politieke crisisrespons (IPCR) uit hoofde van Uitvoeringsbesluit (EU) 2018/1993 van de Raad[2] ("IPCR-regeling") is geactiveerd, moet de cyberblauwdruk de IPCR-regeling volledig in acht nemen. De politieke en strategische coördinatie zou plaatsvinden in het kader van de IPCR. De IPCR-regeling is het instrument voor horizontale coördinatie en respons op het politieke niveau van de Unie. Overeenkomstig de IPCR-regeling wordt het besluit om de regeling te activeren of te deactiveren genomen door het voorzitterschap van de Raad van de Europese Unie. Door de diensten van de Commissie en de Europese Dienst voor extern optreden (EDEO) opgestelde verslagen over geïntegreerde situatiekennis en -analyse (ISAA) ondersteunen de werkzaamheden van de IPCR, zowel in de modus informatiedelen als in de modus volledige activering.

(5) De lidstaten dragen de primaire verantwoordelijkheid voor het beheer van cyberbeveiligingsincidenten en cybercrises. Het potentieel grensoverschrijdende en sectoroverschrijdende karakter van cyberbeveiligingsincidenten vereist echter 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. Cybercrisisbeheer gedurende de volledige levenscyclus omvat paraatheid en gedeeld situationeel bewustzijn om te anticiperen op grootschalige cyberbeveiligingsincidenten, de nodige detectievermogens om de nodige respons- en herstelinstrumenten ter mitigatie en indamming van grootschalige cyberbeveiligingsincidenten vast te stellen, en reactievermogens om verdere incidenten te ontmoedigen en te voorkomen.

[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).

(6) In Aanbeveling (EU) 2017/1584 van de Commissie inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises[3] zijn de doelstellingen en vormen van samenwerking tussen de lidstaten en entiteiten van de Unie bij hun respons op grootschalige cyberbeveiligingsincidenten en cybercrises vastgelegd. In de aanbeveling zijn de betrokken actoren op technisch, operationeel en politiek niveau in kaart gebracht en wordt uitgelegd hoe ze in de bestaande mechanismen voor crisisbeheer van de Unie, zoals de IPCR-regeling, 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. Deze aanbeveling bouwt voort op die kernbeginselen en is bedoeld om Aanbeveling (EU) 2017/1584 te vervangen en een nieuw Uniekader voor cyberbeveiligingscrisisbeheer vast te stellen.

(7) Sommige in deze aanbeveling gebruikte definities zijn gebaseerd op definities en termen die in Richtlijn (EU) 2022/2555[4] worden gebruikt. Het toepassingsgebied van deze aanbeveling verschilt echter van dat van Richtlijn (EU) 2022/2555. Deze aanbeveling bevat het Uniekader voor cybercrisisbeheer in het kader van de algemene paraatheid van de EU voor grootschalige cyberbeveiligingsincidenten en cybercrises die het gevolg zijn van dergelijke incidenten, ongeacht welke sector of entiteit wordt getroffen. Voor zover mogelijk zijn de definities gebaseerd op die van Richtlijn (EU) 2022/2555.

---

[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).

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

(8) Het is nodig de cyberblauwdruk te actualiseren teneinde duidelijke en toegankelijke richtsnoeren te verstrekken waarin wordt toegelicht wat een grootschalig cyberbeveiligingsincident of een cybercrisis op Unieniveau is, hoe het kader voor crisisbeheer wordt getriggerd, wat de rol van relevante netwerken, actoren en mechanismen op Unieniveau is, en hoe de interactie tussen deze actoren en mechanismen gedurende de hele levenscyclus van een cybercrisis verloopt. De cyberblauwdruk heeft tot doel het bredere kader van de civiel-militaire betrekkingen van de EU in de context van cybercrisisbeheer te ondersteunen, onder meer tegen de achtergrond van de verdieping van de betrekkingen tussen de EU en de NAVO, waar mogelijk onder meer door middel van inclusieve, wederkerige en niet-discriminerende verbeterde mechanismen voor informatie-uitwisseling bij cybercrisisbeheer.

(9) Het sectoroverschrijdend crisisbeheer op Unieniveau moet worden versterkt om een geïntegreerde crisisrespons mogelijk te maken, met name in gevallen waarin grootschalige cyberbeveiligingsincidenten en cybercrises gevolgen hebben in de echte wereld. Deze aanbeveling vormt een aanvulling op de IPCR-regeling en andere crisisbeheermechanismen 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), dat in het kader van het UCPM is opgericht bij Besluit nr. 1313/2013/EU van het Europees Parlement en de Raad betreffende een Uniemechanisme voor civiele bescherming[5] ("UCPM-besluit"), het crisisresponsmechanisme van de EDEO (CRM), alsook andere processen, zoals die welke zijn beschreven in het EU-instrumentarium voor cyberdiplomatie[6], de toolbox tegen hybride dreigingen[7] en het herziene EU-protocol voor de bestrijding van hybride bedreigingen[8]. Zij vormt ook een aanvulling op en moet aansluiten bij Aanbeveling (EU) 2024/4371 van de Raad betreffende een blauwdruk om de respons op Unieniveau op verstoringen van kritieke infrastructuur van aanzienlijk grensoverschrijdend belang te coördineren[9] ("EU-blauwdruk voor kritieke infrastructuur"), die betrekking heeft op fysieke, niet-cybergerelateerde weerbaarheid en tot doel heeft de coördinatie van de respons op Unieniveau op dit gebied te verbeteren.

---

5 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).

6 Conclusies van de Raad over een kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten (doc. 9916/17).

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

8 Gezamenlijk werkdocument – EU-protocol voor de bestrijding van hybride bedreigingen (SWD(2023) 116 final).

9 PB C, C/2024/4371, 5.7.2024.

(10) Het Europees netwerk van verbindingsorganisaties voor cybercrises ("EU-CyCLONe") is het netwerk voor de coördinatie van het beheer van grootschalige cyberbeveiligings-incidenten en -crises op operationeel niveau, ook in het geval van sectoroverschrijdende grootschalige cyberbeveiligingsincidenten en cybercrises. Om de bestaande kaders niet verder te compliceren, moet worden vermeden dat sectorale structuren worden opgezet waarvan de taken overlappen met die van EU-CyCLONe. EU-CyCLONe moet ook van de sectoren operationele informatie over cyberbeveiliging ontvangen, en input leveren voor het politieke niveau.

(11) De lidstaten worden aangemoedigd ten volle gebruik te maken van de door relevante programma's van de Unie beschikbaar gestelde financiële middelen voor cyberbeveiliging. Er moet voor worden gezorgd dat deze programma's zo weinig mogelijk administratieve lasten met zich meebrengen voor aanvragers van financiering en dat de deelname van de lidstaten aan deze programma's wordt vergemakkelijkt, door toepasselijke richtsnoeren te verstrekken over haalbare opties voor financiële steun.

(12) Deze aanbeveling draagt bij tot bredere paraatheidsacties die nodig zijn voor de Unie in het licht van sectoroverschrijdende crises, in overeenstemming met de beginselen die zijn vastgelegd in de EU-strategie voor een paraatheidsunie, namelijk een integrerende, alle risico's omvattende overheids- en maatschappijbrede aanpak, met name voor het vergroten van het risico- en dreigingsbewustzijn en het verbeteren van de sectoroverschrijdende crisisrespons,

HEEFT DE VOLGENDE AANBEVELING VASTGESTELD:

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

Doel en toepassingsgebied

1) Deze aanbeveling betreffende een EU-blauwdruk voor cybercrisisbeheer ("cyberblauwdruk") bevat het Uniekader voor cybercrisisbeheer in de context van de algemene paraatheid van de EU voor grootschalige cyberbeveiligingsincidenten en cybercrises. Het kader geeft de rol weer van zowel de lidstaten als de instellingen, organen en instanties van de Unie ("entiteiten van de Unie") binnen hun respectieve bevoegdheden, met volledige inachtneming van de nationale wetten en interne regels, om te zorgen voor een alomvattend en gecoördineerd optreden op Unieniveau.

2) De cyberblauwdruk zou moeten worden toegepast in samenhang met de EU-blauwdruk voor kritieke infrastructuur, met name in het geval van incidenten die zowel de fysieke weerbaarheid als de cyberbeveiliging van kritieke infrastructuur aantasten[10].

3) De cyberblauwdruk biedt richtsnoeren voor de respons op grootschalige cyberbeveiligings-incidenten of cybercrises, en zou moeten worden gebruikt in aanvulling op alle toepasselijke sectorale responsmechanismen, zoals die welke zijn opgenomen in bijlage II. Betrokken belanghebbenden op het gebied van cyberbeveiliging zouden moeten helpen bij de verwezenlijking van de doelstellingen van die sectorale mechanismen, zowel op nationaal als op Unieniveau.

4) In het geval van een EU-brede sectoroverschrijdende crisis met cyberaspecten waarvoor de IPCR wordt geactiveerd, zou de coördinatie van de respons op het politieke niveau van de Unie moeten worden uitgevoerd door de Raad, aan de hand van de IPCR-regeling. Wanneer de IPCR is geactiveerd, zouden maatregelen in het kader van de cyberblauwdruk de respons van de EU op politiek niveau moeten ondersteunen met specifieke hulp op het gebied van cyberbeveiliging.

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

Leidende beginselen

5) De volgende leidende beginselen zijn van toepassing op cybercrisisbeheer op Unieniveau:

a) *evenredigheid*: de meeste cyberbeveiligingsincidenten die de lidstaten treffen zijn kleiner dan wat als een grootschalig cyberbeveiligingsincident of een cybercrisis op nationaal of Unieniveau kan worden beschouwd. In het geval van cyberbeveiligings-incidenten en -dreigingen werken de lidstaten samen en wisselen zij op vrijwillige en regelmatige basis informatie uit binnen het netwerk van "computer security incident response teams" ("CSIRT-netwerk") en EU-CyCLONe, in overeenstemming met de operationele standaardprocedures van de netwerken;

b) *subsidiariteit:* het is in de eerste plaats de verantwoordelijkheid van de lidstaten om, indien ze door een cyberbeveiligingsincident, een grootschalig cyberbeveiligings-incident of een cybercrisis worden getroffen, daarop te reageren en herstelmaatregelen te treffen. Gelet op mogelijke grensoverschrijdende effecten zouden de Raad, de Commissie, de hoge vertegenwoordiger, het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), de cyberbeveiligingsdienst voor de instellingen, organen en instanties van de Unie (CERT-EU), Europol en alle andere betrokken entiteiten van de Unie gedurende de gehele levenscyclus van de crisis moeten samenwerken. Deze rol vloeit voort uit het recht van de Unie en weerspiegelt de wijze waarop grootschalige cyberbeveiligingsincidenten en cybercrises gevolgen kunnen hebben voor een of meer economische sectoren in de eengemaakte markt, voor de beveiliging en de internationale betrekkingen van de Unie en voor de entiteiten van de Unie zelf;

c) *complementariteit*: in deze aanbeveling wordt ten volle rekening gehouden met de in bijlage II vermelde bestaande crisisbeheermechanismen op Unieniveau, met name de IPCR-regeling, Argus en het CRM van de EDEO. In deze aanbeveling wordt rekening gehouden met de mandaten van het CSIRT-netwerk en EU-CyCLONe, alsook met Verordening (EU, Euratom) 2023/2841. Wanneer de IPCR wordt geactiveerd, zouden de werkzaamheden van de betrokken netwerken, entiteiten en geactiveerde sectorale mechanismen moeten worden voortgezet en input moeten leveren voor en ondersteuning bieden aan de politieke en strategische coördinatie in het kader van de IPCR;

d) *vertrouwelijkheid van informatie*: alle uitwisselingen van informatie in de context van deze aanbeveling zouden moeten voldoen aan de toepasselijke regels inzake beveiliging en bescherming van persoonsgegevens. In voorkomend geval zou moet rekening moeten worden gehouden met informele niet-openbaarmakings-overeenkomsten, zoals het verkeerslichtprotocol voor de etikettering van gevoelige informatie. Voor de uitwisseling van gerubriceerde informatie zouden, ongeacht de toegepaste rubriceringsregeling, de bestaande bindende regels en overeenkomsten inzake de verwerking van gerubriceerde informatie moeten worden gehanteerd naast de beschikbare officieel erkende instrumenten.

6) Overeenkomstig de bovengenoemde leidende beginselen 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. Deze samenwerking, in het kader van de cyberblauwdruk, wordt bevorderd door de uitvoering van de artikelen 22 en 23 van Verordening (EU, Euratom) 2023/2841. Met name het cybercrisisbeheersplan dat is vastgesteld op basis van artikel 23 van Verordening (EU, Euratom) 2023/2841 draagt bij tot de regelmatige uitwisseling van relevante informatie tussen entiteiten van de Unie en met de lidstaten, en bevat een regeling voor de coördinatie en informatiestroom tussen entiteiten van de Unie.

II: Definities

7) Voor de toepassing van deze cyberblauwdruk wordt verstaan onder:

a) “incident”: een gebeurtenis die 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, in gevaar brengt;

b) “significant incident”: een incident dat:

a. een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit heeft veroorzaakt of kan veroorzaken;

b. andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken;

c) “grootschalig cyberbeveiligingsincident”: een incident dat leidt tot een verstoringsniveau dat de responscapaciteit van een getroffen lidstaat te boven gaat of dat een significante impact heeft op ten minste twee lidstaten;

d) “cybercrisis”: een grootschalig cyberbeveiligingsincident dat is geëscaleerd tot een volwaardige crisis waardoor de goede werking van de interne markt wordt verhinderd of ernstige risico’s voor de openbare veiligheid en beveiliging ontstaan voor entiteiten of burgers in verschillende lidstaten of in de hele Unie.

III: Nationale structuren en verantwoordelijkheden voor cybercrisisbeheer

8) Het is in de eerste plaats de verantwoordelijkheid van de lidstaten om te reageren als ze door grootschalige cyberbeveiligingsincidenten of cybercrises worden getroffen. Elke lidstaat heeft overeenkomstig Richtlijn (EU) 2022/2555 een of meer cybercrisisbeheerautoriteiten en een of meer CSIRT’s.

9) Via Richtlijn (EU) 2022/2555 en andere wetgevings- en niet-wetgevingsinstrumenten op het gebied van cyberbeveiliging hebben de lidstaten hun cyberbeveiligingskaders op elkaar afgestemd door minimumvoorschriften vast te stellen voor de werking van het gecoördineerde regelgevingskader, mechanismen vast te stellen voor een doeltreffende samenwerking tussen de verantwoordelijke autoriteiten in elke lidstaat, en te voorzien in doeltreffende voorzieningen en handhavingsmaatregelen, die essentieel zijn voor de doeltreffende handhaving van deze verplichtingen.

10) Overeenkomstig artikel 9, lid 4, van Richtlijn (EU) 2022/2555 zou elke lidstaat een nationaal plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons moeten vaststellen. Zo'n plan omvat onder meer nationale paraatheidsmaatregelen, cybercrisisbeheerprocedures en nationale procedures en regelingen tussen nationale autoriteiten en instanties om de effectieve deelname van de lidstaat aan het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en cybercrises op Unieniveau en de ondersteuning daarvan te waarborgen. De cybercrisisbeheerprocedures omvatten ook bepalingen over de integratie ervan in het algemene nationale crisisbeheerkader en in de informatie-uitwisselingskanalen.

11) Overeenkomstig artikel 9, lid 1, van Richtlijn (EU) 2022/2555 zouden de lidstaten moeten zorgen voor samenhang met de bestaande kaders voor algemene nationale crisisbeheersing. In geval van activering van de IPCR zouden de nationale crisisbeheerautoriteiten, om de IPCR te informeren, input moeten verzamelen van de cybercrisisbeheerautoriteiten en nationale sectorale crisismechanismen.

12) Overeenkomstig artikel 9, lid 5, van Richtlijn (EU) 2022/2555 zou EU-CyCLONe, op verzoek van een betrokken lidstaat, informatie moeten uitwisselen over de relevante delen van de nationale plannen voor grootschalige cyberbeveiligingsincidenten en crisisrespons, met name over de bepalingen om de effectieve deelname aan het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en cybercrises op Unieniveau en de ondersteuning daarvan te waarborgen, teneinde beste praktijken uit te wisselen en na te gaan of het algemene kader in de praktijk zou werken.

13) EU-CyCLONe en de interinstitutionele raad voor cyberbeveiliging (IICB) worden verzocht in voorkomend geval van gedachten te wisselen over de samenhang van het door de IICB overeenkomstig artikel 23 van Verordening (EU, Euratom) 2023/2841 opgestelde crisisbeheersplan met de nationale plannen voor grootschalige cyberbeveiligingsincidenten en crisisrespons.

14) EU-CyCLONe zou, met de steun van Enisa als secretariaat, een actuele lijst van nationale cybercrisisbeheerautoriteiten moeten bijhouden met contactgegevens van functionarissen en leidinggevenden van EU-CyCLONe, en deze lijst ter beschikking moeten stellen van de leden van EU-CyCLONe.

IV: Belangrijkste netwerken en actoren in het EU-ecosysteem voor cybercrisisbeheer

15) Het CSIRT-netwerk is het belangrijkste technische netwerk voor de uitwisseling van relevante informatie over incidenten, met name binnen het toepassingsgebied van deze aanbeveling, overeenkomstig de relevante taken die zijn beschreven in artikel 15, lid 3, van Richtlijn (EU) 2022/2555. Het draagt bij tot het opbouwen van vertrouwen en bevordert een snelle en effectieve operationele samenwerking tussen de lidstaten. De voorzitter van het CSIRT-netwerk kan als waarnemer deelnemen aan de IICB.

16) CERT-EU is de cyberbeveiligingsdienst voor alle entiteiten van de Unie. CERT-EU treedt overeenkomstig artikel 13 van Verordening (EU, Euratom) 2023/2841 op als knooppunt voor informatie-uitwisseling inzake cyberbeveiliging en responscoördinatie bij incidenten voor entiteiten van de Unie. CERT-EU is lid van het CSIRT-netwerk en ondersteunt de Commissie in EU-CyCLONe. CERT-EU opereert op technisch niveau en is verantwoordelijk voor de coördinatie van het beheer van ernstige incidenten die gevolgen hebben voor entiteiten van de Unie.

17) EU-CyCLONe werkt als bemiddelaar tussen het technische en het politieke niveau, met name tijdens grootschalige cyberbeveiligingsincidenten en cybercrises. Het ondersteunt het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en cybercrises op operationeel niveau en zorgt voor een regelmatige uitwisseling van relevante informatie tussen de lidstaten en de instellingen, organen en instanties van de Unie overeenkomstig artikel 16 van Richtlijn (EU) 2022/2555. De voorzitter van EU-CyCLONe kan als waarnemer deelnemen aan de IICB.

18) Enisa is het agentschap van de Unie dat de krachtens Verordening (EU) 2019/881[11] toegewezen taken uitvoert met het oog op het bereiken van een hoog gezamenlijk niveau van cyberbeveiliging in de hele Unie, onder meer door de lidstaten en de instellingen, organen en instanties van de Unie actief te ondersteunen. Enisa verzorgt onder meer het secretariaat voor het CSIRT-netwerk en EU-CyCLONe en diensten voor situationeel bewustzijn, en helpt de lidstaten door regelmatig cyberbeveiligingsoefeningen op Unieniveau te organiseren. Overeenkomstig Richtlijn (EU) 2022/2555 en Verordening (EU) 2024/2847[12] ontvangt Enisa informatie over significante grensoverschrijdende incidenten en actief uitgebuite kwetsbaarheden en incidenten die gevolgen hebben voor digitale producten.

19) De Raad van de Europese Unie ("de Raad") is, uit hoofde van artikel 16 van het Verdrag betreffende de Europese Unie (VEU), de instelling met beleidsbepalende en coördinerende taken en is belast met de IPCR, die betrekking heeft op coördinatie en respons op het politieke niveau van de Unie. De Raad werkt via Raadsformaties, het Comité van permanente vertegenwoordigers en de bevoegde voorbereidende instanties van de Raad, met name de Horizontale Groep cybervraagstukken (HWPCI), en, in voorkomend geval, de IPCR-regeling.

---

[11] 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).

[12] 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).

20) Als instelling die het algemeen belang van de Unie bevordert en daartoe passende initiatieven neemt en de toepassing van de Verdragen en van de door de instellingen uit hoofde van artikel 17 VEU vastgestelde maatregelen waarborgt, is de Commissie verantwoordelijk voor een bepaalde algemene paraatheid op Unieniveau en bepaalde acties op het gebied van situationeel bewustzijn, waaronder het beheer van het ERCC en het gemeenschappelijk noodcommunicatie- en informatiesysteem (Cecis), in overeenstemming met het UCPM-besluit. De Commissie faciliteert de samenhang en coördinatie tussen gerelateerde operationele crisisresponsacties op Unieniveau. Zij wordt geraadpleegd over besluiten om de IPCR te activeren of te deactiveren. De diensten van de Commissie stellen samen met de EDEO de ISAA-verslagen op. De Commissie is lid van EU-CyCLONe in gevallen waarin een mogelijk of lopend grootschalig cyberbeveiligingsincident significante gevolgen heeft of dreigt te hebben voor diensten en activiteiten die binnen het toepassingsgebied van Richtlijn (EU) 2022/2555 vallen. In andere gevallen is zij waarnemer. Voor EU-CyCLONe is zij tevens het contactpunt in de IICB. Ook is zij waarnemer in het CSIRT-netwerk.

21) De hoge vertegenwoordiger voor buitenlandse zaken en veiligheidsbeleid (de hoge vertegenwoordiger) voert, met hulp van de EDEO, het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB) van de Unie en doet voorstellen om bij te dragen tot de ontwikkeling van dat beleid, met inbegrip van het gemeenschappelijk veiligheids- en defensiebeleid (GVDB). Dit omvat diplomatieke, inlichtingen- en militaire structuren en mechanismen, met name de gezamenlijke capaciteit op het gebied van inlichtingenanalyse (SIAC) als centraal contactpunt voor de inlichtingen van de lidstaten, de Militaire Staf van de EU (EUMS) als bron van militaire expertise, het EU-instrumentarium voor cyberdiplomatie en het netwerk van EU-delegaties, die vanuit een externe dimensie kunnen bijdragen aan crisisbeheer. De EDEO stelt ook samen met de Commissie de ISAA-verslagen op.

22) In bijlage II staan de rollen en bevoegdheden van de relevante actoren op Unieniveau met betrekking tot cybercrisisbeheer, met inbegrip van de belangrijkste netwerken en actoren.

V: Voorbereiding op een grootschalig cyberbeveiligingsincident of een cybercrisis

Dreigingslandschap

23) De lidstaten en de betrokken entiteiten van de Unie zouden de nodige maatregelen moeten nemen om het situationeel bewustzijn te vergroten, in het besef dat het dreigingslandschap en het incidentspecifieke situationeel bewustzijn verschillende werkwijzen vereisen. De lidstaten en de betrokken entiteiten van de Unie zouden moeten samenwerken op basis van geverifieerde, betrouwbare gegevens, onder meer over trends op het gebied van incidenten, tactieken, technieken en procedures, en actief uitgebuite kwetsbaarheden.

24) Bij het delen van informatie op EU-niveau 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.

25) Om het gedeeld situationeel bewustzijn te vergroten en het gemakkelijker te maken de EU-impact te beoordelen, zouden EU-CyCLONe en het CSIRT-netwerk met steun van Enisa gebruik moeten maken van intern overeengekomen rapportagemechanismen om een EU-overzicht van technische en operationele activiteiten op te stellen op basis van de op nationaal niveau verzamelde informatie.

26) EU-CyCLONe en het CSIRT-netwerk zouden:

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

b) een klimaat van vertrouwen tussen hun leden en tussen de netwerken moeten blijven opbouwen;

c) ten volle gebruik moeten maken van de beschikbare instrumenten voor informatie-uitwisseling, met steun van Enisa, moeten nadenken over hoe deze instrumenten kunnen worden verbeterd en de interoperabiliteit tussen de netwerken moeten waarborgen.

27) EU-CyCLONe, het CSIRT-netwerk en de IICB zouden moeten samenwerken om een doeltreffende uitwisseling van relevante informatie te waarborgen.

28) Als secretariaat voor het CSIRT-netwerk en EU-CyCLONe speelt Enisa een centrale rol bij het ondersteunen van de lidstaten en de instellingen, organen en instanties van de Unie om een gemeenschappelijk situationeel bewustzijn van de EU tot stand te brengen op technisch en operationeel niveau ter ondersteuning van de voorbereiding op grootschalige cyberbeveiligingsincidenten en cybercrises.

29) Overeenkomstig Richtlijn (EU) 2022/2555 en Verordening (EU) 2019/881 zouden de lidstaten en de betrokken entiteiten van de Unie moeten samenwerken met de particuliere sector, met inbegrip van opensourcegemeenschappen en -fabrikanten, om de informatie-uitwisseling te verbeteren. Enisa zou in dit verband met name gebruik moeten maken van zijn partnerschapsprogramma. Daarnaast kunnen de lidstaten en de betrokken entiteiten van de Unie ook voortbouwen op bestaande centra voor informatie-uitwisseling en -analyse (ISAC's) op EU- en nationaal niveau, om de cyberbeveiligingscapaciteit te vergroten en te reageren op cyberbeveiligingsincidenten, onder meer door middel van gezamenlijke vergaderingen van de particuliere sector met EU-CyCLONe of het CSIRT-netwerk.

30) Om de informatie-uitwisseling binnen en tussen de netwerken te verbeteren en de wederzijdse verwachtingen voor die uitwisseling te verduidelijken, zou EU-CyCLONe, met de steun van Enisa als secretariaat en na raadpleging van het CSIRT-netwerk en de NIS-samenwerkingsgroep, binnen 24 maanden na de aanneming van deze aanbeveling overeenstemming moeten bereiken over een gemeenschappelijke, op elkaar afgestemde taxonomie van de ernst van incidenten. Deze taxonomie zou een vergelijking mogelijk moeten maken van de ernst van incidenten in de lidstaten door rekening te houden met de gevolgen voor de dienstverlening, het aantal getroffen entiteiten en hun respectieve relevantie, de gevolgen voor andere diensten en infrastructuur, alsook de financiële, reputationele en politieke schade die is toegebracht. De taxonomie zou moeten voortbouwen op relevante bestaande schalen of taxonomieën, zoals de referentietaxonomie voor de classificatie van incidenten.

Technisch niveau

31) Het CSIRT-netwerk is het platform voor technische samenwerking en informatie-uitwisseling tussen alle lidstaten en via CERT-EU met de entiteiten van de Unie.

32) Overeenkomstig Richtlijn (EU) 2022/2555 heeft elk CSIRT tot taak cyberdreigingen, kwetsbaarheden en incidenten op nationaal niveau te monitoren en te analyseren. De CSIRT's zouden, zowel binnen het CSIRT-netwerk als bilateraal, relevante informatie moeten uitwisselen over incidenten, bijna-incidenten, cyberdreigingen, risico's en kwetsbaarheden om tot een gedeeld situationeel bewustzijn te komen.

33) Om de operationele samenwerking op Unieniveau te verbeteren, zou het CSIRT-netwerk moeten overwegen om organen en agentschappen van de Unie die betrokken zijn bij het cyberbeveiligingsbeleid, zoals Europol, uit te nodigen om deel te nemen aan zijn werkzaamheden.

34) Overeenkomstig Verordening (EU, Euratom) 2023/2841 zou CERT-EU informatie over cyberdreigingen, kwetsbaarheden en incidenten in niet-gerubriceerde ICT-infrastructuur moeten verzamelen, beheren, analyseren en delen met de instellingen, organen en instanties van de Unie en, indien nodig, specifieke voorstellen moeten doen aan de IICB voor richtsnoeren en aanbevelingen aan de instellingen, organen en instanties van de Unie. CERT-EU zou moeten samenwerken en informatie moeten uitwisselen met tegenhangers van de lidstaten, onder meer via het CSIRT-netwerk.

Operationeel niveau

35) Overeenkomstig Richtlijn (EU) 2022/2555 zou EU-CyCLONe moeten fungeren als platform voor samenwerking tussen de cybercrisisbeheerautoriteiten van de lidstaten en via de Commissie met de betrokken entiteiten van de Unie, met als doel het niveau van paraatheid bij het beheer van grootschalige cyberbeveiligingsincidenten en cybercrises te verhogen en een gedeeld situationeel bewustzijn voor grootschalige cyberbeveiligingsincidenten en cybercrises te ontwikkelen.

36) Overeenkomstig Richtlijn (EU) 2022/2555 en Verordening (EU) 2024/2847 ontvangt Enisa informatie over significante grensoverschrijdende incidenten en actief uitgebuite kwetsbaarheden en incidenten die gevolgen hebben voor digitale producten. Enisa, zou, in zijn rol als secretariaat, het CSIRT-netwerk en EU-CyCLONe moeten adviseren met als doel de netwerken te helpen bepalen of er verdere maatregelen moeten worden genomen, en bij te dragen aan het gedeelde situationele bewustzijn.

Politiek niveau

37) De lidstaten en de betrokken entiteiten van de Unie zouden toezicht moeten houden op internationale ontwikkelingen die van invloed zijn op cyberbeveiliging (met inbegrip van cyberdreigingen, hybride dreigingen en buitenlandse informatiemanipulatie en inmenging (FIMI), waaronder desinformatie, indien relevant). Er moet rekening worden gehouden met initiatieven als de technische situatieverslagen inzake de EU-cyberbeveiliging, analyses van de SIAC en andere relevante producten die gespecialiseerde inzichten verschaffen.

38) De hoge vertegenwoordiger zou de lidstaten moeten blijven informeren over en betrekken bij de diplomatieke inspanningen van de Unie in verband met cyberdreigingen, met name die waarbij overheidsactoren betrokken zijn, de betrekkingen met derde landen en internationale organisaties, waaronder de NAVO, en de uitvoering van diplomatieke maatregelen, met inbegrip van beperkende maatregelen.

39) Het voorzitterschap van de Raad van de Europese Unie kan een monitoringpagina op het IPCR-webplatform opzetten waar de lidstaten en de EU-instellingen en -organen informatie kunnen uitwisselen over een eventuele crisis.

Gemeenschappelijke oefeningen

40) De Commissie zou, in coördinatie met de hoge vertegenwoordiger, met steun van Enisa, en na raadpleging van EU-CyCLONe en het CSIRT-netwerk, een efficiënt doorlopend jaarprogramma van cyberoefeningen moeten opstellen om zich voor te bereiden op cybercrises en de organisatorische efficiëntie te vergroten. In het doorlopende programma van cyberoefeningen zou rekening moeten worden gehouden met oefeningen van het UCPM en andere oefeningen in het kader van crisisresponsmechanismen op Unieniveau, met inbegrip van de oefening die is beschreven in de EU-blauwdruk voor kritieke infrastructuur. Het eerste doorlopende programma zou binnen twaalf maanden na de goedkeuring van de cyberblauwdruk moeten worden ontwikkeld en de daaropvolgende programma's zouden elk jaar uiterlijk op 31 maart moeten worden voltooid. Het doorlopende programma zou ter informatie aan de Raad moeten worden voorgelegd.

41) Het doorlopende programma zou ook betrekking moeten hebben op oefeningen die zijn ontwikkeld aan de hand van de scenario's voor gecoördineerde risicobeoordelingen van de EU. Het zou oefeningen moeten omvatten waarbij alle relevante actoren betrokken zijn, met name de particuliere sector en de NAVO.

42) Enisa zou, in zijn rol van secretariaat van het CSIRT-netwerk en EU-CyCLONe, moeten zorgen voor het systematisch verzamelen van lessen die uit oefeningen zijn getrokken, alsook voor het in kaart brengen van de daaruit voortvloeiende acties en het voorstellen van manieren voor de uitvoering ervan, om de doeltreffende uitvoering en het positieve effect ervan op de gemeenschappelijke veerkracht van de EU, met inbegrip van de respectieve operationele standaardprocedures, te waarborgen.

43) Alle actoren en netwerken zouden de coördinatie in geval van een grootschalig cyberbeveiligingsincident of een cybercrisis moeten verbeteren op basis van de lessen die uit de oefeningen zijn getrokken. Met name zouden EU-CyCLONe en het CSIRT-netwerk de tijdens de oefeningen vastgestelde problemen moeten aanpakken om de coördinatie te verbeteren, met name de problemen met betrekking tot de samenwerking tussen de netwerken, en zouden zij, indien nodig, de operationele standaardprocedures snel moeten aanpassen.

44) De NIS-samenwerkingsgroep zou het CSIRT-netwerk, EU-CyCLONe en Enisa moeten uitnodigen om de uit de oefeningen getrokken lessen, alsook de daaruit voortvloeiende acties en de voorgestelde wijze van uitvoering ervan, te presenteren.

45) De Raad kan de voorzitters van het CSIRT-netwerk, EU-CyCLONe, de NIS-samenwerkingsgroep en Enisa verzoeken om uiteen te zetten hoe de uit de oefeningen getrokken lessen zijn toegepast.

46) Enisa wordt verzocht om, in samenwerking met de Commissie en de hoge vertegenwoordiger, tijdens de volgende Cyber Europe-oefening een oefening te organiseren om de cyberblauwdruk te testen. Alle relevante actoren, met inbegrip van het politieke niveau, moeten bij die oefening worden betrokken. Enisa wordt verzocht de betrokkenheid van het politieke niveau te coördineren met het voorzitterschap van de Raad van de Europese Unie. Ook de particuliere sector en de NAVO kunnen bij de oefening worden betrokken.

VI: Detectie van een incident dat zou kunnen escaleren naar een grootschalig cyberbeveligingsincident of een cybercrisis

47) In overeenstemming met hun respectieve mandaten en op basis van de alle gevaren omvattende aanpak zouden alle actoren informatie die op een potentieel grootschalig cyberbeveiligingsincident of een potentiële cybercrisis wijst, aan de relevante netwerken moeten doorgeven.

48) Overeenkomstig Verordening (EU) 2025/38[13] zouden landsgrensoverschrijdende cyberhubs die informatie verkrijgen over een mogelijk of lopend grootschalig cyberbeveiligingsincident, er ten behoeve van een gemeenschappelijk situationeel bewustzijn voor moeten zorgen dat relevante informatie onverwijld aan de autoriteiten van de lidstaten en de Commissie wordt verstrekt via EU-CyCLONe en het CSIRT-netwerk.

[13] 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).

49) Wanneer een significant incident wordt waargenomen kan het, met name wanneer het onmiddellijke gevolgen heeft, worden gemeld aan of opgespoord door een CSIRT dan wel de cybercrisisbeheerautoriteiten of andere sectorale autoriteiten van de lidstaten. De lidstaten worden aangemoedigd informatie over zo'n incident uit te wisselen binnen de netwerken, die zouden moeten overwegen om passende maatregelen te nemen. Het CSIRT-netwerk en EU-CyCLONe kunnen onafhankelijk van elkaar worden geactiveerd, afhankelijk van de aard van het incident en de vereiste respons. Beide netwerken worden echter aangemoedigd om op basis van overeengekomen procedurele regelingen met elkaar te blijven samenwerken. Het besluit om een netwerk te activeren berust uitsluitend bij elk respectief netwerk zelf en wordt genomen op onafhankelijke wijze.

50) Het CSIRT-netwerk zou EU-CyCLONe moeten adviseren over de vraag of een waargenomen cyberbeveiligingsincident kan worden beschouwd als een potentieel of lopend grootschalig cyberbeveiligingsincident.

51) Overeenkomstig Richtlijn (EU) 2022/2555 zouden het CSIRT-netwerk en EU-CyCLONe onverwijld procedurele regelingen moeten overeenkomen in het geval van een potentieel of lopend grootschalig cyberbeveiligingsincident om te zorgen voor technische en operationele coördinatie en tijdige en relevante informatie op politiek niveau.

VII: Reageren op een grootschalig cyberbeveiligingsincident of een cybercrisis op Unieniveau

Respons op een grootschalig cyberbeveiligingsincident of een cybercrisis waarvoor de IPCR niet is geactiveerd in volledige modus

52) Een doeltreffende respons op grootschalige cyberbeveiligingsincidenten of cybercrises op EU-niveau vereist doeltreffende samenwerking op technisch, operationeel en politiek vlak met een overheidsbrede aanpak, waar mogelijk met inbegrip van rechtshandhaving.

53) Op elk niveau zouden de betrokken actoren specifieke activiteiten moeten uitvoeren om een gedeeld situationeel bewustzijn en een gecoördineerde respons te bewerkstelligen. Deze maatregelen zullen ervoor zorgen dat informatie op geordende en doeltreffende wijze wordt verspreid.

54) De respons zou in verhouding moeten staan tot de impact van het grootschalige cyberbeveiligingsincident of de cybercrisis. Overeenkomstig Richtlijn (EU) 2022/2555 zouden de cybercrisisbeheerautoriteiten van de lidstaten moeten zorgen voor samenhang en onderlinge afstemming op nationaal niveau tussen de sectorale reacties op de cybercrisis.

55) Bij een grootschalig cyberbeveiligingsincident of een cybercrisis zouden alle actoren en netwerken in nauwe onderlinge afstemming als volgt moeten reageren:

a) op technisch niveau:

i. De getroffen lidstaten en hun CSIRT's zouden moeten samenwerken met de getroffen entiteiten bij de respons op incidenten en de verlening van bijstand, indien van toepassing.

ii. De CSIRT's zouden via het CSIRT-netwerk moeten samenwerken en relevante technische informatie over het incident moeten delen. De CSIRT's werken samen bij de analyse van de beschikbare technische artefacten en andere technische informatie in verband met het incident teneinde de oorzaak ervan te achterhalen en mogelijke technische mitigatiemaatregelen te bepalen.

iii. De CSIRT's en de cybercrisisbeheerautoriteiten van de lidstaten worden aangemoedigd om het binnen het CSIRT-netwerk of EU-CyCLONe te melden als zij kennis krijgen van een significant incident.

iv. Het CSIRT-netwerk zou, met de steun van Enisa, de door de CSIRT's verstrekte nationale verslagen moeten bundelen en die aan EU-CyCLONe voorleggen.

v. Indien een cyberbeveiligingsincident zou kunnen escaleren naar een grootschalig cyberbeveiligingsincident of een cybercrisis, zou het CSIRT-netwerk de nodige informatie moeten delen met EU-CyCLONe. EU-CyCLONe zou deze informatie moeten gebruiken om de Raad te informeren.

vi. Het CSIRT-netwerk zou nauw contact moeten onderhouden met Europol om ervoor te zorgen dat relevante technische informatie wordt gedeeld. Het CSIRT-netwerk en Europol zouden in geval van een grootschalig cyberbeveiligingsincident indien nodig contactpunten moeten instellen om de informatie-uitwisseling beter te laten verlopen.

b) op operationeel niveau:

i. De lidstaten zouden de impact van het incident op nationaal niveau moeten beperken door de nodige maatregelen te nemen.

ii. Het CSIRT-netwerk zou EU-CyCLONe technische beoordelingen van de lopende incidenten moeten verstrekken, die EU-CyCLONe kan gebruiken.

iii. EU-CyCLONe zou de gevolgen en de impact van relevante grootschalige cyberbeveiligingsincidenten en cybercrises moeten beoordelen en mogelijke mitigatiemaatregelen moeten voorstellen, en zou de gecoördineerde beheersing van grootschalige cyberbeveiligingsincidenten en cybercrises en de besluitvorming op politiek niveau moeten ondersteunen.

iv. Indien een grootschalig cyberbeveiligingsincident met sectoroverschrijdende gevolgen de activering van responsmaatregelen op Unieniveau vereist, met name een van de in bijlage II vermelde horizontale en sectorale crisisbeheermechanismen op Unieniveau,

(a) dan kunnen bepaalde actoren, afhankelijk van het soort sectorale crisisbeheermechanisme op Unieniveau, vragen om de activering van dat mechanisme.

(b) Indien een dergelijk sectoraal mechanisme wordt geactiveerd, krijgen de sectorale entiteiten ondersteuning van andere betrokken entiteiten bij het beperken van de gevolgen van het incident.

(c) De Commissie zou het voor de contactpunten voor de in bijlage II opgenomen horizontale en sectorale crisismechanismen op Unieniveau en EU-CyCLONe eenvoudiger moeten maken om informatie aan elkaar door te geven, en zou een geïntegreerde sectoroverschrijdende analyse moeten uitvoeren en opties voor een geschikt geïntegreerd responsplan moeten voorstellen.

(d) De Commissie zou, in voorkomend geval via EU-CyCLONe en in samenwerking met de hoge vertegenwoordiger, ervoor moeten zorgen dat de operationele maatregelen op EU-niveau op cybergebied consistent zijn met en aansluiten op de gerelateerde responsacties op Unieniveau, met name in verband met verzoeken om bijstand via het UCPM.

(e) Indien een IPCR-monitoringspagina is opgezet met informatie over het incident, zouden de gevolgen ervan en de genomen maatregelen ook via het IPCR-webplatform moeten worden gedeeld tussen de lidstaten en entiteiten van de Unie.

v. De lidstaten kunnen overeenkomstig artikel 15 van Verordening (EU) 2025/38 verzoeken om diensten uit de EU-cyberbeveiligingsreserve. Onverminderd eventuele toekomstige uitvoeringshandelingen uit hoofde van die verordening zouden de diensten uit de EU-cyberbeveiligingsreserve binnen 24 uur na het verzoek moeten worden ingezet.

c) op politiek niveau:

i. De Raad kan om briefings verzoeken van de belangrijkste betrokkenen, met name de Commissie, de hoge vertegenwoordiger en EU-CyCLONe, teneinde op politiek en strategisch niveau passend te kunnen reageren.

ii. De Raad, gesteund door de Commissie en de hoge vertegenwoordiger, kan bepalen welke maatregelen geschikt zijn om te reageren op het grootschalige cyberbeveiligingsincident, met inbegrip van de mogelijke diplomatieke reacties overeenkomstig hoofdstuk IX.

iii. De lidstaten kunnen extra cybercrisisbeheermechanismen of -instrumenten activeren, afhankelijk van de aard en de impact van het incident.

iv. Wanneer de IPCR in de modus informatiedelen in werking wordt gesteld, wordt het ISAA-ondersteuningsvermogen geactiveerd, waardoor er meer informatie wordt uitgewisseld via het IPCR-webplatform en er gezorgd wordt voor een gedeeld situatiebeeld. De situatieverslagen van EU-CyCLONe en het CSIRT-netwerk zouden de belangrijkste instrumenten moeten blijven om het gemeenschappelijk situationeel bewustzijn te verwoorden op respectievelijk operationeel en technisch niveau. Deze verslagen kunnen als input dienen voor de ISAA-rapporten.

v. In geval van een incident dat de activering van responsacties op Unieniveau vereist, met name de in bijlage II vermelde relevante horizontale en sectorale crisisbeheermechanismen op Unieniveau, zou de Raad, in samenwerking met de Commissie en de hoge vertegenwoordiger, moeten zorgen voor samenhang en onderlinge afstemming tussen de respons op de cybercrisis en de daarmee verband houdende responsacties op Unieniveau.

vi. Indien wordt verzocht om relevante mechanismen, met name de diensten van de cyberbeveiligingsreserve, zouden de diensten van de Commissie en, in voorkomend geval, de EDEO, alsook de betrokken Raadsinstanties, met name de HWPCI en de Horizontale Groep versterking van weerbaarheid en bestrijding van hybride bedreigingen (HWP-ERCHT), naargelang het geval, met elkaar moeten overleggen over het ontwerp en de uitvoering van maatregelen, en het passende besluitvormingsproces met aanvullende maatregelen, en dit in lijn met de toolbox tegen hybride dreigingen[14] in het geval van kwaadwillige cyberactiviteiten die deel uitmaken van een bredere hybride campagne.

Respons op een grootschalig cyberbeveiligingsincident of een cybercrisis waarvoor de IPCR is geactiveerd in volledige modus

56) De stappen in het deel "*Respons op een grootschalig cyberbeveiligingsincident of een cybercrisis waarvoor de IPCR niet is geactiveerd in volledige modus*" hierboven zouden moeten worden uitgevoerd.

57) Wanneer de IPCR in volledige modus wordt geactiveerd, waarborgen de ISAA-rapporten een gemeenschappelijk situationeel bewustzijn op politiek niveau. De situatieverslagen van EU-CyCLONe en het CSIRT-netwerk zouden de belangrijkste instrumenten moeten blijven om het gemeenschappelijk situationeel bewustzijn te verwoorden op respectievelijk operationeel en technisch niveau. Deze verslagen kunnen als input dienen voor de ISAA-rapporten.

58) In het geval van een grootschalig cyberbeveiligingsincident of een cybercrisis die leidt tot de activering van de IPCR in volledige modus, zouden alle actoren in nauwe onderlinge afstemming moeten reageren met een overheidsbrede aanpak, en wel als volgt:

a) De coördinatie van de respons op het politieke niveau van de Unie wordt uitgevoerd door de Raad via de IPCR-regeling.

---

14 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.

b) EU-CyCLONe verstrekt, in samenwerking met het CSIRT-netwerk, duidelijke informatie aan het politieke niveau over de impact en de mogelijke gevolgen van het incident en over de respons- en herstelmaatregelen, onder meer door bij te dragen aan de ISAA-rapporten.

c) Naast het ISAA-vermogen roept het voorzitterschap van de Raad van de Europese Unie IPCR-rondetafels bijeen om politieke en strategische coördinatie van de EU-respons mogelijk te maken, waarbij de acties in het kader van de cyberblauwdruk en de werkzaamheden van relevante sectorale mechanismen input leveren aan de IPCR-werkzaamheden. Via de rondetafels kunnen bovendien specifieke lacunes in de respons in kaart worden gebracht en specifieke EU-actoren worden uitgenodigd om deze te verhelpen en tijdens toekomstige rondetafels verslag hierover uit te brengen, ter ondersteuning van de politieke en strategische coördinatie in de IPCR.

d) Het voorzitterschap van de Raad van de Europese Unie bekijkt of EU-CyCLONe moet worden uitgenodigd op bepaalde vergaderingen, met inbegrip van rondetafels in het kader van de IPCR-regeling en andere relevante Raadszittingen.

e) De crisisbeheerautoriteiten van de lidstaten moeten zorgen voor samenhang en onderlinge afstemming tussen de sectorale reacties op de cybercrisis die worden ondersteund door de cybercrisisbeheerautoriteiten.

f) De mogelijke diplomatieke reacties worden overwogen en uitgevoerd overeenkomstig hoofdstuk IX.

VIII: Publiekscommunicatie

59) De communicatie richting de bevolking van een individuele lidstaat over een lopend grootschalig cyberbeveiligingsincident of een cybercrisis, onder meer als onderdeel van bewustmaking, is een nationale bevoegdheid, maar de lidstaten, de Commissie en de hoge vertegenwoordiger zouden ernaar moeten streven hun publiekscommunicatie zoveel mogelijk op elkaar af te stemmen. In voorkomend geval kan het informele IPCR-netwerk van crisisvoorlichters daarbij worden betrokken.

60) Om zich voor te bereiden op grootschalige cyberbeveiligingsincidenten en cybercrises worden de lidstaten en, in voorkomend geval, de Commissie en CERT-EU verzocht binnen EU-CyCLONe en het CSIRT-netwerk informatie uit te wisselen over hun communicatie-inspanningen, met inbegrip van beste praktijken, zoals adviezen of bewustmakingscampagnes. Enisa zou instrumenten ter beschikking moeten stellen om deze uitwisseling te ondersteunen en zou moeten zorgen voor een gemakkelijke toegang daartoe.

61) In geval van een grootschalig cyberbeveiligingsincident of een cybercrisis worden de lidstaten verzocht binnen EU-CyCLONe informatie te delen over hun inspanningen op het gebied van publiekscommunicatie teneinde een gemeenschappelijk bewustzijn op te bouwen en de acties op elkaar af te stemmen. EU-CyCLONe kan op eigen initiatief of op verzoek van de Raad een overzicht van dergelijke benaderingen delen met de Raad.

IX: Diplomatieke respons en samenwerking met strategische partners

62) De hoge vertegenwoordiger zou het volgende moeten ondernemen, in nauwe samenwerking met de Commissie en andere betrokken entiteiten van de Unie:

a) de besluitvorming binnen de Raad over de toepassing van mogelijke maatregelen uit het EU-instrumentarium voor cyberdiplomatie ondersteunen, onder meer met analyses, rapporten en voorstellen. Dit maakt het mogelijk gebruik te maken van het volledige spectrum van beschikbare instrumenten van de Unie om kwaadwillige cyberactiviteiten te voorkomen, te ontmoedigen en erop te reageren, haar cyberhouding te versterken en internationale vrede, veiligheid en stabiliteit in cyberspace te bevorderen;

b) indien een relevant incident wordt geconstateerd, de nodige uitwisseling van informatie met strategische partners faciliteren, waaronder de NAVO indien relevant;

c) de coördinatie met strategische partners, waaronder de NAVO indien relevant, verbeteren met betrekking tot de respons op kwaadwillige cyberactiviteiten door persistente-dreigingsactoren, met name bij het gebruik van het EU-instrumentarium voor cyberdiplomatie, in lijn met de uitvoeringsrichtsnoeren.

63) De lidstaten, de hoge vertegenwoordiger, de Commissie en andere betrokken 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 respons bij potentiële of grootschalige cyberbeveiligingsincidenten.

64) De samenwerking tussen de Europese Unie en de NAVO zou moeten verlopen conform de overeengekomen leidende beginselen van inclusiviteit, wederkerigheid en transparantie, met volledige inachtneming van de autonome besluitvorming van de Unie.

65) Rekening houdend met bestaande overeenkomsten, zoals de technische overeenkomst tussen CERT-EU en de NAVO van 2016, zouden de Commissie en de hoge vertegenwoordiger in geval van een cybercrisis contactpunten voor coördinatie met de NAVO moeten oprichten om de nodige informatie over de situatie en het gebruik van crisisresponsmechanismen uit te wisselen teneinde de samenwerking bij en de doeltreffendheid van de respons te vergroten. Daartoe zou de Unie moeten nagaan hoe de informatie-uitwisseling met de NAVO op inclusieve, wederkerige en niet-discriminerende wijze kan worden verbeterd, met name door te zorgen voor instrumenten voor beveiligde communicatie, rekening houdend met de normen voor informatie-uitwisseling van de verschillende lidstaten.

66) Als onderdeel van het in hoofdstuk V bedoelde doorlopende Unieprogramma van cyberoefeningen zouden de diensten van de Commissie en de EDEO moeten overwegen een oefening te organiseren met de NAVO, op personeelsniveau, om de samenwerking tussen civiele en militaire entiteiten bij een grootschalig cyberbeveiligingsincident of een cybercrisis waarbij de lidstaten of NAVO-bondgenoten willen reageren op een cyberaanval die hun veiligheid aantast, te testen. De oefening zou op inclusieve en niet-discriminerende wijze moeten worden uitgevoerd, met volledige inachtneming van de overeengekomen beginselen voor de parameters voor de samenwerking tussen de EU en de NAVO. De oefening zou moeten worden uitgevoerd in het kader van de oefening "EU Integrated Resolve" (een parallelle en gecoördineerde oefening, "PACE"). Daarbij zouden alle nodige maatregelen moeten worden genomen om ervoor te zorgen dat alle in de cyberblauwdruk genoemde actoren deelnemen aan de oefening.

67) In overleg met de Raad, de Commissie en de hoge vertegenwoordiger zouden ook gezamenlijke cyberoefeningen op Unieniveau met de landen van de Westelijke Balkan, de Republiek Moldavië, Oekraïne en andere strategische partners en gelijkgestemde derde landen moeten worden overwogen.

X: Coördinatie van cybercrisisbeheer met militaire actoren op EU-niveau

68) De lidstaten zouden de samenwerking tussen civiele en militaire cyberactoren op nationaal niveau moeten blijven versterken.

69) EU-CyCLONe en het CSIRT-netwerk zouden mogelijke manieren en procedures moeten vaststellen om samen te werken met de betrokken militaire actoren van de EU, zoals de conferentie van EU-cybercommandanten en het operationeel netwerk voor militaire computercrisisresponsteams (Micnet), zodat profijt kan worden getrokken van een gezamenlijk militair en civiel perspectief, met name via gezamenlijke vergaderingen. EU-CyCLONe en het CSIRT-netwerk zouden de Raad moeten informeren over de vooruitgang die wordt geboekt met betrekking tot deze samenwerking.

70) De getroffen lidstaat wordt verzocht EU-CyCLONe en de EDEO in te lichten als er relevante nationale of multinationale militaire responsvermogens worden gebruikt bij een grootschalig cyberbeveiligingsincident of een cybercrisis, en de verstrekking van deze informatie overeengekomen is tussen de gebruiker en de aanbieder van dat responsvermogen.

71) Als onderdeel van het in hoofdstuk V bedoelde doorlopende Unieprogramma van cyberoefeningen zouden de Commissie en de hoge vertegenwoordiger moeten overwegen een gezamenlijke oefening te organiseren om de samenwerking tussen zowel civiele als militaire cyberactoren bij een grootschalig cyberbeveiligingsincident dat gevolgen heeft voor de lidstaten te testen.

XI: Herstel en geleerde lessen uit een cybercrisis

72) De lidstaten, de betrokken entiteiten van de Unie en netwerken zouden tijdens de herstelfase na een cybercrisis moeten samenwerken om ervoor te zorgen dat de kernfuncties snel worden hersteld. Bij deze samenwerking moeten, in voorkomend geval, ook de rechtshandhavingsinstanties worden betrokken. In deze fase is samenwerking met de particuliere sector van cruciaal belang, met name om het herstel van gegevens en systemen te faciliteren. Bij een doeltreffende coördinatie tussen belanghebbenden zou prioriteit moeten worden gegeven aan het zoveel mogelijk beperken van de verstoringen en het waarborgen van bedrijfscontinuïteit.

73) De lidstaten en de betrokken entiteiten van de Unie en netwerken zouden in de herstelfase moeten samenwerken op basis van de lessen die zijn getrokken uit cybercrises en beheerde cyberbeveiligingsincidenten uit het verleden en uit incidentenverslagen, met name in de context van het bij Verordening (EU) 2025/38 ingestelde Europees evaluatiemechanisme voor cyberbeveiligingsincidenten.

74) EU-CyCLONe zou het CSIRT-netwerk, de NIS-samenwerkingsgroep en de Raad een uitgebreide lijst van geleerde lessen uit cybercrises en beheerde cyberbeveiligingsincidenten uit het verleden en beste praktijken moeten verstrekken. Enisa zou ervoor moeten zorgen dat deze geleerde lessen naar behoren worden meegenomen in toekomstige paraatheidsactiviteiten en bij het uitwerken van de planning van toekomstige oefeningen.

XII: Beveiligde communicatie

75) Op basis van de inventarisatie van bestaande beveiligde communicatie-instrumenten[15] zou de Commissie uiterlijk eind 2026 een interoperabele reeks beveiligde communicatieoplossingen moeten voorstellen. Uiterlijk eind 2027 zouden de Raad, de Commissie, de hoge vertegenwoordiger, EU-CyCLONe en het CSIRT-netwerk het eens moeten worden over deze reeks. Deze oplossingen zouden moeten teruggrijpen op de acties op het gebied van beveiligde communicatie die de EU-instellingen in het kader van de EU-strategie voor een paraatheidsunie kunnen ondernemen, en zouden communicatieoplossingen moeten omvatten voor alle gebruikte communicatiemiddelen (spraak, gegevens, videoverbinding, berichten, samenwerking en het delen en raadplegen van documenten). De oplossingen zouden moeten voldoen aan gezamenlijk vastgestelde vereisten voor de bescherming van gevoelige niet-gerubriceerde informatie. Er zou gebruik moeten worden gemaakt van oplossingen op basis van een open protocol met opensourcetoepassingen die geschikt zijn voor realtimecommunicatie en die worden beheerd door een in de EU gevestigde entiteit.

76) EU-CyCLONe en het CSIRT-netwerk zouden voor de uitwisseling van als RESTREINT UE/EU RESTRICTED gerubriceerde informatie indien nodig gebruik moeten kunnen maken van beveiligde communicatiekanalen waarin is voorzien voor de instellingen, organen en instanties van de EU om onderling en met de lidstaten gerubriceerde informatie uit te wisselen.

---

[15] Doc. WK 862/2023.

77) Het bij Verordening (EU) 2021/887[16] 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 instrumenten voor beveiligde communicatie. Dubbele investeringen in interoperabele beveiligde systemen moeten worden vermeden.

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

79) Er 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 cybercrisisrespons. Deze mechanismen zouden de rol van elke partij moeten eerbiedigen, inmenging in lopende activiteiten moeten voorkomen en communicatieredundantie moeten waarborgen. Het EU-systeem voor kritieke communicatie (EUCCS) dat momenteel wordt ontwikkeld, kan de gezamenlijke respons met de betrokken cybergemeenschappen ten goede komen.

XIII: Slotbepalingen

80) EU-CyCLONe zou, in samenwerking met het CSIRT-netwerk en andere belangrijke actoren in het EU-ecosysteem voor cybercrisisbeheer en met steun van Enisa, binnen een jaar na de bekendmaking van deze aanbeveling gedetailleerde processtroomdiagrammen moeten ontwikkelen met een overzicht van de informatiestromen tussen de betrokken actoren, de besluitvormingsprocessen en de verslagen die zijn opgesteld tijdens het beheer van grootschalige cyberbeveiligingsincidenten of cybercrises zoals omschreven in deze aanbeveling. De stroomdiagrammen zouden verschillende samenwerkingsvormen en -lagen moeten omvatten. Ze zouden wanneer dat nodig is moeten worden geactualiseerd.

---

[16] 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).

81) Om de doeltreffende toepassing van de herziene cyberblauwdruk te ondersteunen, en voortbouwend op de ervaring die is opgedaan met de gezamenlijke cyberoefeningen in het kader van die blauwdruk, kan de Raad indien nodig een reeks uitvoeringsrichtsnoeren opstellen. Met deze richtsnoeren zouden de praktische problemen die tijdens de oefeningen aan het licht zijn gekomen, kunnen worden aangepakt, en zouden lacunes en ontbrekende schakels die zijn ontdekt in de coördinatie, communicatie en operationele interactie, kunnen worden verholpen.

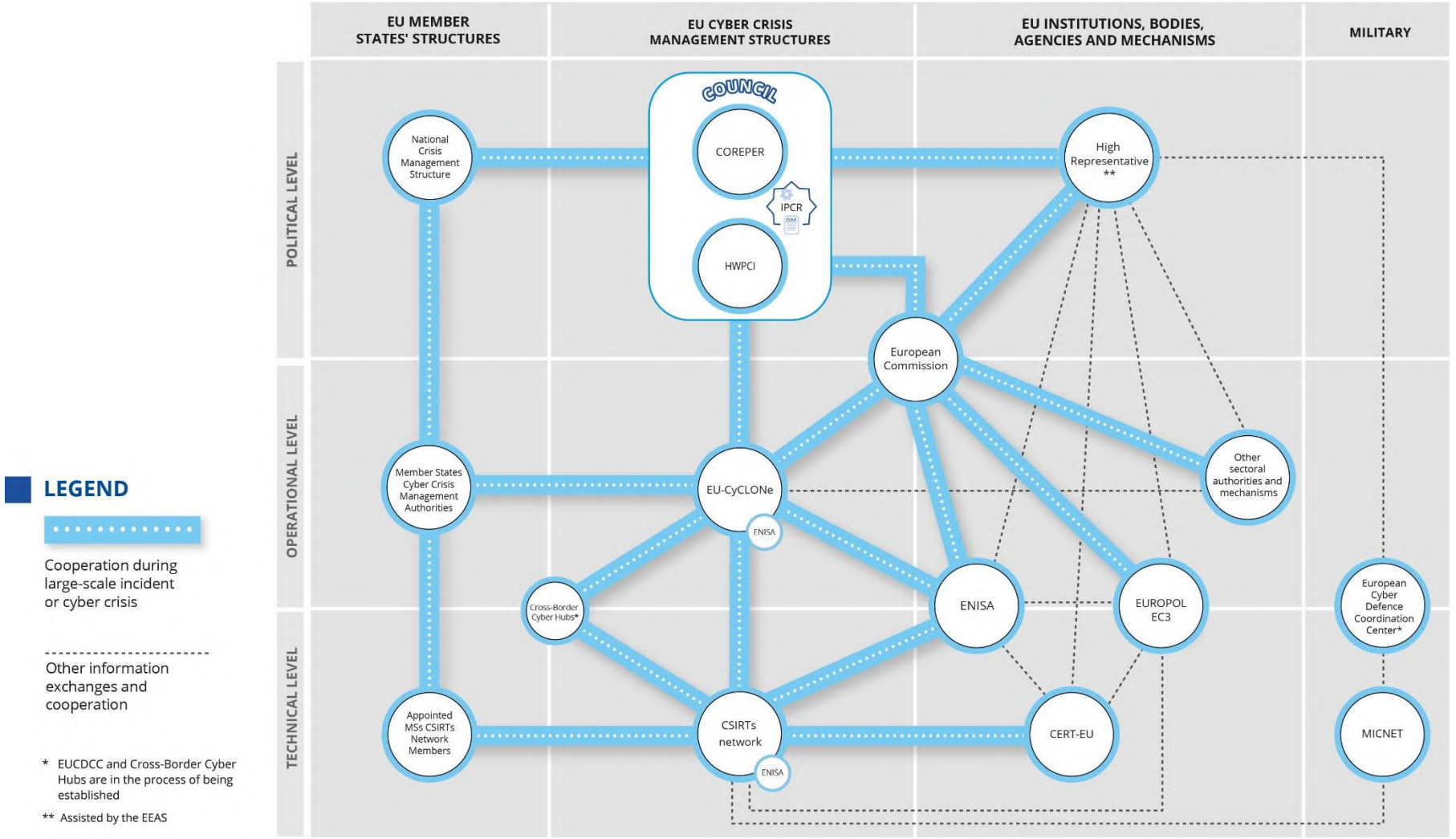
82) Deze aanbeveling zou na de bekendmaking ervan ten minste om de vier jaar door de Commissie moeten worden geëvalueerd, in samenwerking met de lidstaten. Na elke evaluatie zou de Commissie een verslag moeten publiceren en voorleggen aan de Raad. De Commissie en de lidstaten zouden met name rekening moeten houden met de gevolgen van het veranderende dreigingslandschap, de resultaten van gezamenlijke oefeningen en wetswijzigingen, in het bijzonder mogelijke wijzigingen als gevolg van de herziening van Verordening (EU) 2019/881.

Gedaan te Brussel,

Voor de Raad

De voorzitter

BIJLAGE I – Blauwdruk van de Unie voor de respons op een cyberbeveiligingscrisis



BIJLAGE II – RELEVANTE ACTOREN (ENTITEITEN EN NETWERKEN) EN CRISISBEHEERMECHANISMEN OP UNIENIVEAU

(1) Betrokkenheid van de belangrijkste actoren in de levenscyclus van cybercrisisbeheer (grootschalige cyberbeveiligingsincidenten en cybercrises)

	Paraatheid	Detectie	Respons op een grootschalig cyberbeveiligingsincident of een cybercrisis			Publiekscommunicatie	Herstel en geleerde lessen
			Technisch niveau	Operationeel niveau	Politiek niveau		
Lidstaten	X	X	X	X	X	X	X
Commissie	X			X	X	X	
Hoge vertegenwoordiger, bijgestaan door de EDEO	X			X	X	X	
Raad	X				X	X	X
Enisa	X		X	X			
CERT-EU	X	X	X	X		X	X
CSIRT-netwerk	X	X	X				X
EU-CyCLONe	X			X	X		X

(2) Rollen en bevoegdheden van de relevante actoren op Unieniveau (in alfabetische volgorde) met betrekking tot cybercrisisbeheer

Actor	Niveau	Rol en bevoegdheid	Referentie
CERT-EU	Technisch / Operationeel	Coördineert de crisisrespons op technisch niveau en het beheer van ernstige incidenten die gevolgen hebben voor entiteiten van de Unie. Houdt een inventaris bij van de beschikbare technische deskundigheid die nodig is voor de respons op ernstige incidenten, en ondersteunt de interinstitutionele raad voor cyberbeveiliging (IICB) bij de coördinatie van de cybercrisisbeheersplannen van de entiteiten van de Unie voor ernstige incidenten. Lid van het CSIRT-netwerk. Steunt de Commissie binnen EU-CyCLONe bij het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en cybercrises. Fungeert als knooppunt voor informatie-uitwisseling inzake cyberbeveiliging en responscoördinatie bij incidenten, en faciliteert de uitwisseling van informatie over incidenten, cyberdreigingen, kwetsbaarheden en bijna-	Verordening (EU, Euratom) 2023/2841 Verordening (EU) 2025/38

Actor	Niveau	Rol en bevoegdheid	Referentie
		incidenten tussen entiteiten van de Unie en hun tegenhangers. Verzoekt om de inzet van de EU-cyberbeveiligingsreserve namens entiteiten van de Unie. Werkt samen met het NAVO-cyberbeveiligingscentrum op basis van hun technische overeenkomst.	
Raad van de Europese Unie	Politiek	Beleidsvorming en coördinatie. Is belast met de IPCR, die bestaat in coördinatie en respons op het politieke niveau van de Unie.	Artikel 16 van het Verdrag betreffende de Europese Unie
Voorzitterschap van de Raad van de Europese Unie	Politiek	Besluit (behalve wanneer de solidariteitsclausule wordt ingeroepen op grond van artikel 222 van het Verdrag betreffende de werking van de Europese Unie) om de IPCR al dan niet te activeren, waar passend in overleg met de getroffen lidstaten, alsook met de Commissie en de hoge vertegenwoordiger.	Artikel 16 van het Verdrag betreffende de Europese Unie Uitvoeringsbesluit (EU) 2018/1993 van de Raad
Landsgrens-overschrijdende cyberhubs	Technisch	"Landsgrensoverschrijdende cyberhub": een meerlandenplatform, opgericht bij een schriftelijke consortiumovereenkomst, dat nationale cyberhubs uit ten minste drie lidstaten samenbrengt in een	Verordening (EU) 2025/38

Actor	Niveau	Rol en bevoegdheid	Referentie
		gecoördineerde netwerkstructuur, en dat bedoeld is om de monitoring, detectie en analyse van cyberdreigingen te versterken, incidenten te voorkomen en de productie van inlichtingen over cyberdreigingen te ondersteunen, met name door het uitwisselen van relevante en in voorkomend geval, geanonimiseerde gegevens en informatie, het delen van geavanceerde instrumenten en het gezamenlijk ontwikkelen van capaciteit op het gebied van de detectie, analyse en preventie van, alsook de bescherming tegen cyberdreigingen en -incidenten in een betrouwbare omgeving; Werkt nauw samen en deelt informatie met het CSIRT-netwerk. Verstrekt informatie over een potentieel of aan de gang zijnd grootschalig cyberbeveiligingsincident aan de autoriteiten van de lidstaten en de Commissie via EU-CyCLONe en het CSIRT-netwerk.	

Actor	Niveau	Rol en bevoegdheid	Referentie
CSIRT-netwerk	Technisch	Draagt bij tot het opbouwen van vertrouwen en bevordert een snelle operationele samenwerking tussen de lidstaten. Vormt het belangrijkste netwerk voor het uitwisselen van relevante informatie over incidenten, bijna-incidenten, cyberdreigingen, risico's en kwetsbaarheden. Op verzoek van een lid dat mogelijk door een incident wordt getroffen, wisselt het netwerk informatie uit met betrekking tot dat incident en daarmee samenhangende cyberdreigingen en bespreekt het deze. Het netwerk kan ook een gecoördineerde respons faciliteren op een incident dat binnen de jurisdictie van een verzoekend lid is geconstateerd. Verleent bijstand aan de lidstaten bij het beheer van grensoverschrijdende incidenten en onderzoekt verdere vormen van samenwerking, waaronder wederzijdse bijstand.	Richtlijn (EU) 2022/2555 Verordening (EU) 2025/38

Actor	Niveau	Rol en bevoegdheid	Referentie
		Ontvangt informatie van de lidstaten over hun verzoeken aan de EU-cyberbeveiligingsreserve.	
Conferentie van cybercommandanten		Een forum voor nationale cybercommandanten uit de lidstaten om samen te werken en vitale informatie uit te wisselen over lopende cyberspace-operaties en strategieën ter mitigatie van grootschalige cyberincidenten. De conferentie wordt georganiseerd door het roulerende voorzitterschap van de Raad van de Europese Unie, met de steun van het Europees Defensieagentschap (EDA) en de Europese Dienst voor extern optreden (EDEO), met inbegrip van de Militaire Staf van de EU (EUMS).	Gezamenlijke mededeling over het EU-beleid op het gebied van cyberdefensie (2022)
Commissie	Operationeel / Politiek	Uitvoerend orgaan van de Europese Unie. Waarborgt de goede werking van de interne markt. Faciliteert de samenhang en onderlinge afstemming tussen gerelateerde crisisresponsacties op Unieniveau. Verricht bepaalde algemene paraatheidsacties op Unieniveau uit hoofde van het UCPM-besluit, waaronder het	Artikel 17 van het Verdrag betreffende de Europese Unie Uitvoeringsbesluit (EU) 2018/1993 Besluit nr. 1313/2013/EU

Actor	Niveau	Rol en bevoegdheid	Referentie
		beheer van het Coördinatiecentrum voor respons in noodsituaties en het gemeenschappelijk noodcommunicatie- en informatiesysteem. Waarnemer in EU-CyCLONe en lid in geval van een mogelijk of lopend grootschalig incident dat aanzienlijke gevolgen heeft of dreigt te hebben voor diensten en activiteiten die binnen het toepassingsgebied van Richtlijn (EU) 2022/2555 vallen. Waarnemer in het CSIRT-netwerk. Algemene verantwoordelijkheid voor de uitvoering van de EU-cyberbeveiligingsreserve. Contactpunt in de IICB voor de uitwisseling met EU-CyCLONe van relevante informatie over ernstige incidenten. Wordt door het voorzitterschap van de Raad geraadpleegd over besluiten om de IPCR te activeren of te deactiveren (behalve wanneer de solidariteitsclausule op grond van artikel 222 VWEU wordt ingeroepen).	Richtlijn (EU) 2022/2555 Verordening (EU) 2025/38 Verordening (EU, Euratom) 2023/2841

Actor	Niveau	Rol en bevoegdheid	Referentie
		De diensten van de Commissie stellen samen met de EDEO de ISAA-verslagen op.	
Agentschap van de Europese Unie voor cyberbeveiliging (Enisa)	Technisch / Operationeel	Voert taken uit met het oog op het bereiken van een hoog niveau van cyberbeveiliging in de hele Unie, onder meer door de lidstaten en de instellingen van de Unie actief te ondersteunen. Verzorgt het secretariaat voor het CSIRT-netwerk en EU-CyCLONe. Stelt regelmatig een technisch situatieverslag inzake EU-cyberbeveiliging op over incidenten en cyberdreigingen (met het EC3 en CERT-EU en in nauwe samenwerking met de lidstaten). Draagt bij tot de ontwikkeling van een gemeenschappelijke respons op grootschalige grensoverschrijdende incidenten of crises, hoofdzakelijk door: - verslagen uit nationale bronnen te bundelen en te analyseren; - de informatiestroom tussen het technische, operationele en politieke niveau te waarborgen; - op verzoek de behandeling van	Richtlijn (EU) 2022/2555 Verordening (EU) 2019/881 Verordening (EU) 2025/38 Verordening (EU) 2024/2847

Actor	Niveau	Rol en bevoegdheid	Referentie
		incidenten te vergemakkelijken; - entiteiten van de Unie te ondersteunen op het gebied van publiekscommunicatie; - de lidstaten op verzoek te ondersteunen op het gebied van publiekscommunicatie; - de responscapaciteit bij incidenten te testen en regelmatig cyberbeveiligings-oefeningen te organiseren. Treedt op als aanbestedende dienst wanneer hij is belast met het geheel of gedeeltelijk operationeel houden en beheren van de EU-cyberbeveiligingsreserve. Organiseert tweejaarlijkse grootschalige omvattende cyberbeveiligingsoefeningen op Unieniveau met technische, operationele of strategische elementen. Stelt in samenwerking met de betrokken lidstaat en andere relevante belanghebbenden een incidentevaluatieverslag op om de oorzaken, gevolgen en beperking van een incident te beoordelen (op verzoek van de Commissie of EU-CyCLONe	

Actor	Niveau	Rol en bevoegdheid	Referentie
		en met goedkeuring van de betrokken lidstaat). Informeert EU-CyCLONe indien informatie die wordt verstrekt in het kader van de rapportageverplichtingen van de verordening cyberweerbaarheid relevant is voor het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en cybercrises op operationeel niveau.	
Europees netwerk van verbindings-organisaties voor cybercrises (EU-CyCLONe)	Operationeel	Ondersteunt het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en cybercrises op operationeel niveau. Waarborgt de regelmatige uitwisseling van relevante informatie tussen de lidstaten en instellingen, organen en instanties van de Unie. Coördineert het beheer van grootschalige cyberbeveiligingsincidenten en cybercrises en ondersteunt de besluitvorming op politiek niveau met betrekking tot dergelijke incidenten en crises. Beoordeelt de gevolgen en de impact van relevante	Richtlijn (EU) 2022/2555 Verordening (EU) 2025/38

Actor	Niveau	Rol en bevoegdheid	Referentie
		grootschalige cyberbeveiligingsincidenten en cybercrises en stelt mogelijke mitigatiemaatregelen voor. Bespreekt op verzoek van een betrokken lidstaat de nationale plannen voor grootschalige cyberbeveiligingsincidenten en crisisrespons. Ontwikkelt, samen met Enisa en de Commissie, het model dat de indiening van verzoeken om steun uit de EU-cyberbeveiligingsreserve moet faciliteren. Ontvangt informatie van de lidstaten over hun verzoeken aan de EU-cyberbeveiligingsreserve. Ontvangt van de grensoverschrijdende cyberhubs of het CSIRT-netwerk informatie over een potentieel of aan de gang zijnd grootschalig cyberbeveiligingsincident.	
Hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid, ondersteund door de	Politiek	Geeft leiding aan en coördineert de inspanningen van de Unie om externe veiligheidsdreigingen op het gebied van hybride en cyberdreigingen aan te pakken.	Besluit 2010/427/EU van de Raad

Actor	Niveau	Rol en bevoegdheid	Referentie
Europese Dienst voor extern optreden		Is verantwoordelijk voor de instrumenten van de Unie voor cyberdiplomatie en cyberdefensie om externe dreigingen te ontmoedigen en erop te reageren, onder meer door gebruik te maken van de instrumentaria voor hybride en cyberdiplomatie van de Unie. Onderhoudt contacten met externe partners, onder meer via de inzet van het GVDB (gemeenschappelijk veiligheids- en defensiebeleid). Zorgt voor paraatheid van de Unie en de lidstaten op het gebied van situationeel bewustzijn en capaciteit om te reageren op hybride en cyberdreigingen, bijvoorbeeld door middel van praktische oefeningen, opleiding en netwerken. Behandelt de veiligheids- en defensie-implicaties van de ruimtemiddelen van de Unie, met name in het kader van het GVDB van de Unie. Ondersteunt de conferentie van EU-cybercommandanten. Ondersteunt het operationeel EU-netwerk voor militaire	

Actor	Niveau	Rol en bevoegdheid	Referentie
		computercrisisresponsteams (Micnet). Wordt door het voorzitterschap van de Raad geraadpleegd over besluiten om de IPCR te activeren of te deactiveren (behalve wanneer de solidariteitsclausule op grond van artikel 222 VWEU wordt ingeroepen). De EDEO stelt, samen met de diensten van de Commissie, de ISAA-verslagen op.	
EU-coördinatiecentrum voor cyberdefensie	Horizontaal	Het oorspronkelijke doel ervan is in de eerste plaats het gedeelde situationeel bewustzijn van de Unie en haar lidstaten over kwaadwillige activiteiten in cyberspace te vergroten, met name wat betreft militaire GVDB-missies en -operaties.	Gezamenlijke mededeling over het EU-beleid op het gebied van cyberdefensie (2022)
Europol	Operationeel	Biedt operationele en technische ondersteuning aan de bevoegde autoriteiten van de lidstaten voor het voorkomen en ontmoedigen van cybercriminaliteit. Verleent de bevoegde autoriteiten van de lidstaten op hun verzoek bijstand bij de respons op cyberaanvallen van vermoedelijk criminele oorsprong.	Verordening (EU) 2016/794, met inbegrip van alle wijzigingen

Actor	Niveau	Rol en bevoegdheid	Referentie
Interinstitutionele raad voor cyberbeveiliging		Stelt een cybercrisisbeheersplan op om op operationeel niveau het gecoördineerde beheer van ernstige incidenten met gevolgen voor entiteiten van de Unie te ondersteunen en bij te dragen tot de regelmatige uitwisseling van relevante informatie. Coördineert de vaststelling van de cybercrisisbeheersplannen door de individuele entiteiten van de Unie. Stelt, op basis van een voorstel van CERT-EU, richtsnoeren of aanbevelingen vast inzake samenwerking op het gebied van de respons op significante incidenten met betrekking tot entiteiten van de Unie.	Verordening (EU, Euratom) 2023/2841
Operationeel netwerk voor militaire computercrisis-responsteams (Micnet)	Technisch	Bevordert een robuustere en beter gecoördineerde respons op cyberdreigingen ten aanzien van defensiesystemen in de Unie, met inbegrip van systemen die worden gebruikt bij militaire GVDB-missies en -operaties; opgericht en ondersteund door het Europees Defensieagentschap.	Gezamenlijke mededeling over cyberdefensie 2022

Actor	Niveau	Rol en bevoegdheid	Referentie
Gezamenlijke capaciteit op het gebied van inlichtingenanalyse (SIAC)		Samengesteld uit 1) het Inlichtingen- en situatiecentrum van de EU (EU-Intcen) en 2) het directoraat Inlichtingen van de Militaire Staf van de EU (EUMS INT) SIAC. Verstrekt strategische inlichtingen over buitenlands beleid, terrorisme en cyber- en hybride dreigingen. Beheert militaire inlichtingen voor GVDB-missies en ondersteunt defensie- en crisisbeheeroperaties van de Unie. Onder het gezag van de hoge vertegenwoordiger.	Artikel 38 en artikelen 42 tot en met 46 van het Verdrag betreffende de Europese Unie

(3) Relevante crisisbeheermechanismen en -platformen op Unieniveau

Mechanisme	Horizontaal/sectoraal/cyber specifiek	Beschrijving	Referentie
Argus	Horizontaal	Het coördinatieproces van de Commissie en het algemene waarschuwingssysteem voor een coherente respons in geval van een grote grensoverschrijdende crisis die actie op EU-niveau vereist. Brengt alle betrokken diensten en kabinetten samen om maatregelen te nemen en deze te coördineren. Stelt de Commissie in staat relevante informatie uit te wisselen over opkomende multisectorale crises of voorzienbare of onmiddellijke dreigingen die optreden op Unieniveau vereisen.	Mededeling COM(2005) 662 van de Commissie
Crisisrespons-centrum van de EDEO (CRC)	Horizontaal	Het centrale toegangspunt voor alle crisisgerelateerde kwesties in de EDEO en de permanente 24/7-crisisresponscapaciteit voor noodsituaties die de veiligheid van het personeel in de EU-delegaties bedreigen en/of in reactie op crises die burgers van de Unie in het buitenland treffen. Het brengt deskundigen op het gebied van beveiliging, consulaire zaken en situationeel bewustzijn samen, en steunt daarbij op toegewijde	Een strategisch kompas voor veiligheid en defensie – Voor een Europese Unie die haar burgers, waarden en belangen beschermt en bijdraagt aan de internationale vrede en veiligheid (21 maart 2022)

Mechanisme	Horizontaal/sectoraal/cyberspecifiek	Beschrijving	Referentie
		professionals ter plaatse in de delegaties van de Unie.	
Blauwdruk voor kritieke infrastructuur	Horizontaal	Coördineert een respons op Unieniveau op verstoringen van kritieke infrastructuur van aanzienlijk grensoverschrijdend belang.	Aanbeveling C/2024/4371 van de Raad
Waarschuwings-systeem voor cyberbeveiliging	Cyberspecifiek	Zorgt voor geavanceerde vermogens van de Unie om de vermogens op het gebied van detectie, analyse en gegevensverwerking met betrekking tot cyberdreigingen en de preventie van incidenten in de Unie te verbeteren.	Verordening (EU) 2025/38
Instrumentarium voor cyberdiplomatie (kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten)	Cyberspecifiek	Maakt een gezamenlijke diplomatieke respons van de Unie op kwaadwillige cyberactiviteiten mogelijk, die bijdraagt tot conflictpreventie, het beperken van cyberbeveiligingsdreigingen en een grotere stabiliteit in de internationale betrekkingen.	Conclusies van de Raad van 19 juni 2017 Herziene uitvoeringsrichtsnoeren 10289/23 van 8 juni 2023
EU-cyberbeveiligings-reserve	Cyberspecifiek	Mobiliseert deskundigen en middelen op het gebied van cyberbeveiliging tijdens crises om de responsinspanningen in de lidstaten en de instellingen, organen of agentschappen van de Unie te ondersteunen.	Verordening (EU) 2025/38

Mechanisme	Horizontaal/sectoraal/cyber specifiek	Beschrijving	Referentie
Netcode voor sectorspecifieke regels voor cyberbeveiligings-aspecten van grens-overschrijdende elektriciteits-stromen	Sectoraal	Stelt een periodiek proces van cyberbeveiligingsrisicobeoordelingen in de elektriciteitssector vast, op Unie-, lidstaat-, regionaal en entiteitsniveau. Bevat bepalingen die specifiek zijn voor crisisbeheer en samenwerking met de CSIRT's en EU-CyCLONe wanneer een grootschalig cyberbeveiligingsincident gevolgen heeft voor andere sectoren die afhankelijk zijn van de elektriciteitsvoorzieningszekerheid.	Gedelegeerde Verordening (EU) 2024/1366 van de Commissie
Toolbox tegen hybride dreigingen	Horizontaal	Bevat een reeks bepalingen om te zorgen voor een overzicht van wat op EU-niveau beschikbaar is als reactie op alle soorten hybride dreigingen, het gecoördineerde gebruik ervan en het waarborgen van de samenhang van onze acties op verschillende domeinen. De toolbox tegen hybride dreigingen helpt zorgen voor besluitvorming op basis van een omvattend situationeel bewustzijn en van de geleerde lessen.	Conclusies van de Raad over een kader voor een gecoördineerde EU-respons op hybride campagnes, 22 juni 2022 Uitvoeringsrichtsnoeren voor het kader voor een gecoördineerde EU-respons op hybride campagnes, 14 december 2022

Mechanisme	Horizontaal/sectoraal/cyber specifiek	Beschrijving	Referentie
Teams voor snelle reactie op hybride dreigingen (EU-HRRT's)	Horizontaal	Als onderdeel van de EU-toolbox tegen hybride dreigingen maken de EU-teams voor snelle reactie op hybride dreigingen gebruik van relevante sectorale nationale en EU-expertise op civiel en militair gebied om gerichte kortetermijnbijstand op maat te verlenen aan lidstaten, missies en operaties in het kader van het gemeenschappelijk veiligheids- en defensiebeleid, en partnerlanden bij de bestrijding van hybride dreigingen en campagnes.	Richtinggevend kader voor de praktische oprichting van de EU-teams voor snelle reactie op hybride dreigingen (21 mei 2024) Operationele richtsnoeren voor de inzet van teams voor snelle reactie op hybride dreigingen, goedgekeurd door het Coreper op 4 december 2024
IPCR	Horizontaal	Steunt snelle en gecoördineerde politieke besluitvorming op Unieniveau met betrekking tot grote en complexe crises. Het besluit tot activering en deactivering wordt genomen door het voorzitterschap van de Raad, dat de getroffen lidstaten, de Commissie en de HV raadpleegt (behalve wanneer de solidariteitsclausule is ingeroepen). Het SGR, de diensten van de Commissie en de EDEO kunnen ook, in overleg met het voorzitterschap, overeenkomen de	Uitvoeringsbesluit (EU) 2018/1993 van de Raad

Mechanisme	Horizontaal/sectoraal/cyber specifiek	Beschrijving	Referentie
		IPCR-regeling te activeren in de modus informatiedelen. De door de diensten van de Commissie en de EDEO voorbereide ISAA-rapporten vormen een uitgangspunt voor de werkzaamheden van de IPCR. Deze rapporten berusten op relevante informatie en analysen die zijn verstrekt door de lidstaten (bijvoorbeeld de bevoegde nationale crisiscentra) en door de betrokken agentschappen en organen van de Unie.	
EU Law Enforcement Emergency Response Protocol (EU-crisisrespons-protocol van de rechtshandhavings-instanties)	Horizontaal	Een instrument om de rechtshandhavingsinstanties van de Unie te ondersteunen bij het onmiddellijk reageren op grote grensoverschrijdende cyberaanvallen door middel van snelle beoordeling, de beveiligde en tijdige uitwisseling van kritieke informatie en doeltreffende coördinatie van de internationale aspecten van hun onderzoeken.	Conclusies van de Raad (26 juni 2018) over gecoördineerde EU-respons op grootschalige cyberincidenten en -crises
Snellereactieteams bij cyberincidenten (CRRT) van Pesco	Cyberspecifiek	De CRRT's van Pesco zijn een gezamenlijk ontwikkeld civiel-militair cyberdefensievermogen van de EU-lidstaten om snel te reageren	Artikel 42, lid 6, en artikel 46 van en protocol nr. 10 bij het

Mechanisme	Horizontaal/sectoraal/cyber specifiek	Beschrijving	Referentie
		op cyberincidenten en cybercrises en ook preventief actie te ondernemen, zoals kwetsbaarheidsbeoordelingen en verkiezingsmonitoring. De CRRT's van Pesco hebben tot taak om, op verzoek, cyberondersteuning te verlenen aan de EU-lidstaten, EU-instellingen, -organen en -instanties, militaire GVDB-missies en -operaties van de EU, alsook partnerlanden.	Verdrag betreffende de Europese Unie

Architectuur voor respons op ruimtedreigingen (STRA)	Sectoraal (Ruimtedreigingen, met inbegrip van cyber-gerelateerde dreigingen)	Architectuur voor respons op ruimtedreigingen (STRA) inzake de taken die de Raad en de hoge vertegenwoordiger moeten uitoefenen om een bedreiging af te wenden die voortvloeit uit de stationering, de exploitatie of het gebruik van de systemen die zijn opgezet en de diensten die worden verleend in het kader van het ruimtevaartprogramma van de Unie.	Besluit (GBVB) 2021/698 van de Raad
Coördinatiekader met betrekking tot systemische cyberincidenten (EU-SCICF)	Sectoraal	Er wordt gewerkt aan een kader voor communicatie en coördinatie dat potentiële systemische cybergebeurtenissen in de financiële sector aanpakt en beheert. Het zal voortbouwen op een van de beoogde rollen van de Europese toezichthoudende autoriteiten (ETA's) in het kader van Verordening (EU) 2022/2554, namelijk om geleidelijk een doeltreffende gecoördineerde respons op Unieniveau mogelijk te maken bij een ernstig grensoverschrijdend ICT-incident of een daarmee verband houdende dreiging die mogelijk een systemisch effect zal hebben op de financiële sector van de Unie in zijn geheel.	Aanbeveling van het Europees Comité voor systeemrisico's van 2 december 2021 inzake een pan-Europees coördinatiekader voor de betrokken autoriteiten met betrekking tot systemische cyberincidenten (ESRB/2021/17)
Uniemechanisme voor civiele	Horizontaal	Zorgt voor samenwerking op het gebied van civiele bescherming om	Besluit nr. 1313/2013/EU

bescherming (UCPM)		de preventie, paraatheid en respons bij rampen te verbeteren.	
CISE – gemeenschappelijke gegevens-uitwisselings-structuur	Specifiek maritiem, voor zeven sectoren	CISE is een netwerk dat systemen van EU/EER-autoriteiten met verantwoordelijkheden op het gebied van maritieme bewaking met elkaar verbindt. CISE maakt het mogelijk om over grenzen en verschillende sectoren heen relevante informatie op een naadloze en geautomatiseerde wijze uit te wisselen.	Een strategisch kompas voor veiligheid en defensie – Voor een Europese Unie die haar burgers, waarden en belangen beschermt en bijdraagt aan de internationale vrede en veiligheid (21 maart 2022)

(4) Zeer kritieke sectoren en andere kritieke sectoren in het kader van Richtlijn (EU) 2022/2555 en sectorale crisismechanismen op Unieniveau (indien van toepassing)		
Sectoren	**Deelsector**	**Toepasselijke sectorale crisismechanismen**
Energie	Elektriciteit	Coördinatiegroep voor elektriciteit
	Stadsverwarming en -koeling	N.v.t.
	Aardolie	Coördinatiegroep voor aardolie EU-Groep van autoriteiten voor offshore olie- en gasactiviteiten (EUOAG)
	Aardgas	Coördinatiegroep voor gas
	Waterstof	N.v.t.
Vervoer	Lucht	Europees crisiscoördinatiecentrum voor de luchtvaart (EACCC)
	Spoor	N.v.t.
	Water	Europees Bureau voor visserijcontrole (EBVC) SafeSeaNet (SSN) Geïntegreerde maritieme diensten (IMS) Datacentrum voor identificatie en volgen van schepen op lange afstand (LRIT) Diensten voor maritieme bijstand van EMSA

	Weg	N.v.t.
	Horizontaal	Netwerk van nationale contactpunten voor vervoer, opgericht bij het noodplan voor vervoer (COM(2022) 211)
Bankwezen		EU-SCICF
Infrastructuur voor de financiële markt		EU-SCICF Europees financieel stabilisatiemechanisme

Volksgezondheid		Systeem voor vroegtijdige waarschuwing en reactie (EWRS) Snellewaarschuwingssysteem voor weefsels en cellen en voor bloedbestanddelen (RATC/RAB) van het Centrum voor het beheer van crisissituaties op het gebied van de volksgezondheid (Health Emergency Operations Facility – HEOF) Kader voor noodsituaties op het gebied van de volksgezondheid Snellewaarschuwingssysteem voor chemische incidenten (Raschem) Europees surveillanceportaal inzake overdraagbare ziekten Paraatheid en respons inzake noodsituaties op gezondheidsgebied (HERA) Medisch informatiesysteem (MediSys) Uitvoerende stuurgroep inzake tekorten aan medische hulpmiddelen (MDSSG) Snellewaarschuwingssysteem voor geneesmiddelenbewaking EU-taskforce voor gezondheid (EUHTF) Gezondheidsbeveiligingscomité
Drinkwater		N.v.t.

Afvalwater		N.v.t.
Digitale infrastructuur		N.v.t.
Beheer van ICT-diensten		N.v.t.
Openbaar bestuur		N.v.t.
Ruimte		Architectuur voor respons op ruimtedreigingen (STRA)
Post- en koeriersdiensten		N.v.t.
Afvalstoffenbeheer		N.v.t.
Vervaardiging, productie en distributie van chemische stoffen		Snellewaarschuwingssysteem voor chemische incidenten (Raschem)

Productie, verwerking en distributie van levensmiddelen		Europees systeem voor gewasmonitoring Detectie van mondiale hotspots van landbouwproductieanomalieën (ASAP) Europees netwerk van fytosanitaire informatiesystemen (Europhyt) Veterinair noodteam van de EU (EUVET) Systeem voor snelle waarschuwingen voor levensmiddelen en diervoeders (RASFF) Europees mechanisme voor paraatheid en respons bij voedselzekerheidscrises (EFSCM) Verordening inzake noodsituaties op de interne markt en veerkracht van de interne markt (Imera)
Maakindustrie	Medische hulpmiddelen	N.v.t.
	Informaticaproducten, elektronische en optische producten	N.v.t.
	Machines, apparaten en werktuigen	N.v.t.
	Vervaardiging van motorvoertuigen, aanhangers en opleggers	N.v.t.
	Vervaardiging van andere transportmiddelen	N.v.t.

Digitale aanbieders		N.v.t.
Onderzoek		N.v.t.

BIJLAGE III – EU-kader voor cyberbeveiligingscrisisbeheer en bijbehorende instrumenten

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[1],
- Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad[2],
- Uitvoeringsverordening (EU) 2024/2690 van de Commissie[3], Verordening (EU, Euratom) 2023/2841 van het Europees Parlement en de Raad[4],
- Verordening (EU) 2021/887 van het Europees Parlement en de Raad[5],
- Verordening (EU) 2024/2847 van het Europees Parlement en de Raad[6], en
- Verordening (EU) 2025/38 van het Europees Parlement en de Raad ("verordening cybersolidariteit")[7].

Specifieke sectorale cyberbeveiligingscrisismaatregelen zijn onder meer Gedelegeerde Verordening (EU) 2024/1366 van de Commissie[8] en het aanstaande coördinatiekader met betrekking tot systemische cyberincidenten (EU-SCICF) in het kader van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad[9].

Richtlijn 2013/40/EU[10] is 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[11], zullen, zodra ze ten uitvoer zijn gelegd, de rechtshandhaving op dit gebied aanzienlijk faciliteren.

"Het EU-beleid op het gebied van cyberdefensie"[12] schetst de rol van een operationeel 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 die zijn opgenomen in de bijlagen I en II bij 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[13] voorziet in samenwerking tussen relevante actoren wanneer een incident gevolgen heeft voor zowel de fysieke aspecten als de cyberbeveiliging van kritieke infrastructuur.

[1] 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 (cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

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

[3] 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 onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten, en verleners van vertrouwensdiensten (PB L, 2024/2690, 18.10.2024). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] 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).

[5] 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).

[6] 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).

[7] 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).

[8] 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).

[9] 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).

[10] 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).

[11] 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).

[12] JOIN(2022) 49 final. https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52022JC0049

[13] *PB C, C/2024/4371, 5.7.2024.* https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:C_202404371