Rådet for
Den Europæiske Union

Bruxelles, den 6. juni 2025
(OR. en)

9794/25

Interinstitutionel sag:
2025/0036(NLE)

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

RESULTAT AF DRØFTELSERNE

fra:	Generalsekretariatet for Rådet
dato:	6. juni 2025
til:	delegationerne
Vedr.:	Rådets henstilling om en EU-plan for cyberkrisestyring –– Rådets henstilling som godkendt af Rådet på samlingen den 6. juni 2025

Vedlagt følger til delegationerne Rådets henstilling som godkendt af Rådet på samlingen den 6. juni 2025.

BILAG

RÅDETS HENSTILLING

om en EU-plan for cyberkrisestyring

RÅDET FOR DEN EUROPÆISKE UNION HAR –

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 114 og 292,

under henvisning til forslag fra Europa-Kommissionen, og

ud fra følgende betragtninger:

(1) Digital teknologi og global konnektivitet er rygraden i Unionens økonomiske vækst, konkurrenceevne og omdannelsen af kritisk infrastruktur. En sammenkoblet og stadig mere digital økonomi øger imidlertid også risikoen for cybersikkerhedshændelser og cyberangreb. Desuden afspejles stigende geopolitiske spændinger, konflikter og strategisk rivalisering i virkningen, omfanget og kompleksiteten af ondsindede cyberaktiviteter. Sådanne aktiviteter kan udgøre en del af hybride kampagner eller militære operationer. De kan også påvirke Unionens sikkerhed, økonomi og samfund direkte. Desuden har de afsmittende potentiale, navnlig når disse aktiviteter er rettet mod internationale strategiske partnerlande såsom kandidatlande eller nabolande.

(2) En omfattende cybersikkerhedshændelse kan forårsage en forstyrrelse på et niveau, som overstiger en medlemsstats kapacitet til at reagere på den, eller som har en betydelig indvirkning på mere end én medlemsstat. En sådan hændelse kan alt efter årsag og virkning eskalere og udvikle sig til en fuldgyldig krise, der påvirker det indre markeds korrekte funktion eller udgør alvorlige risici for den offentlige sikkerhed for enheder eller borgere i flere medlemsstater eller for Unionen som helhed. Effektiv krisestyring er afgørende for at opretholde den økonomiske stabilitet og beskytte europæiske regeringer, kritisk infrastruktur, virksomheder og borgere samt bidrage til international sikkerhed og stabilitet i cyberspace. Cyberkrisestyring er derfor en integreret del af EU's overordnede krisestyringsramme.

(3) I betragtning af den indbyrdes afhængighed og de indbyrdes forbindelser mellem EU-enhedernes og medlemsstaternes IKT-miljøer kan en hændelse i en EU-enhed udgøre en cybersikkerhedsrisiko for medlemsstaterne og omvendt. Udveksling af relevante oplysninger og koordinering vedrørende både omfattende cybersikkerhedshændelser og større hændelser som defineret i artikel 3, nr. 8, i forordning (EU, Euratom) 2023/2841[1] er afgørende i forbindelse med EU-planen for cyberkrisestyring ("cyberplanen").

[1] Europa-Parlamentets og Rådets forordning (EU, Euratom) 2023/2841 af 13. december 2023 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i Unionens institutioner, organer, kontorer og agenturer (EUT L, 2023/2841, 18.12.2023, s. 1).

(4) I tilfælde af en krise, hvor EU's integrerede ordninger for politisk kriserespons ("IPCR") i henhold til Rådets gennemførelsesafgørelse (EU) 2018/1993[2] ("IPCR-ordninger") er blevet aktiveret, bør cyberplanen fuldt ud respektere IPCR-ordningerne for koordination og respons. Den politiske og strategiske koordination vil ske i IPCR. IPCR-ordningerne er værktøjet til horisontal koordination og respons på Unionens politiske plan. I henhold til IPCR-ordningerne træffes afgørelsen om at aktivere eller deaktivere IPCR af formandskabet for Rådet for Den Europæiske Union. Rapporter om integreret situationsbevidsthed og analyse ("ISAA"), der er udarbejdet af Kommissionens tjenestegrene og Tjenesten for EU's Optræden Udadtil ("EU-Udenrigstjenesten"), understøtter IPCR's arbejde i både dens informationsudvekslingsfunktion og dens fulde aktiveringsfunktion.

(5) Medlemsstaterne har det primære ansvar for styringen af cybersikkerhedshændelser og cyberkriser. Cybersikkerhedshændelsers potentielle grænseoverskridende og tværsektorielle karakter kræver imidlertid, at medlemsstaterne og de relevante EU-enheder samarbejder på teknisk, operationelt og politisk plan for at koordinere effektivt i hele Unionen. Cyberkrisestyring i hele livscyklussen omfatter beredskab og fælles situationsbevidsthed for at foregribe omfattende cybersikkerhedshændelser, den nødvendige detektionskapacitet til at identificere de nødvendige respons- og genopretningsværktøjer til at afbøde og inddæmme omfattende cybersikkerhedshændelser samt reaktionskapacitet til at afværge og forebygge yderligere hændelser.

[2] Rådets gennemførelsesafgørelse (EU) 2018/1993 af 11. december 2018 om EU's integrerede ordninger for politisk kriserespons (EUT L 320 af 17.12.2018, s. 28).

(6) Kommissionens henstilling (EU) 2017/1584[3] om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser fastlægger målene og formerne for samarbejde mellem medlemsstaterne og EU-enhederne ved reaktion på væsentlige cybersikkerhedshændelser og cyberkriser. Den kortlagde de relevante aktører på teknisk, operationelt og politisk niveau og forklarede, hvordan de var integreret i Unionens eksisterende krisestyringsmekanismer, såsom IPCR-ordningerne. De centrale principper i henstilling (EU) 2017/1584 er fortsat gyldige, nemlig nærhedsprincippet, komplementaritet og fortrolig behandling af oplysninger samt tilgangen på tre niveauer (teknisk, operationelt og politisk). Nærværende henstilling bygger på disse centrale principper og har til formål at erstatte henstilling (EU) 2017/1584 og fastlægge en ny EU-ramme for cyberkrisestyring.

(7) Visse definitioner, der anvendes i denne henstilling, er baseret på definitioner og udtryk, der anvendes i direktiv (EU) 2022/2555[4]. Denne henstillings anvendelsesområde adskiller sig dog fra anvendelsesområdet for direktiv (EU) 2022/2555. I denne henstilling fastlægges EU-rammen for cyberkrisestyring inden for rammerne af EU's overordnede beredskab over for omfattende cybersikkerhedshændelser og cyberkriser, der opstår som følge af sådanne hændelser – uanset hvilken sektor eller enhed der er berørt. Definitionerne er så vidt muligt baseret på definitionerne i direktiv (EU) 2022/2555.

---

[3] Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (EUT L 239 af 19.9.2017, s. 36).

[4] Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333 af 27.12.2022, s. 80).

(8) En ajourført cyberplan er nødvendig for at give klar og tilgængelig vejledning, der forklarer, hvad en omfattende cybersikkerhedshændelse eller en cyberkrise på EU-plan er, hvordan krisestyringsrammen udløses, og hvilke roller relevante netværk, aktører og mekanismer på EU-plan spiller, samt hvad samspillet mellem disse aktører og mekanismer i hele cyberkrisens livscyklus er. Cyberplanen har til formål at støtte den bredere ramme for EU's civil-militære forbindelser i forbindelse med cyberkrisestyring, herunder på baggrund af en uddybning af forbindelserne mellem EU og NATO, hvis det er muligt, bl.a. gennem inklusive, gensidige og ikkediskriminerende forbedrede informationsudvekslingsmekanismer inden for cyberkrisestyring.

(9) Den tværsektorielle krisestyring på EU-plan bør styrkes for at give mulighed for en integreret kriserespons, navnlig i tilfælde, hvor omfattende cybersikkerhedshændelser og kriser har fysiske konsekvenser. Denne henstilling supplerer IPCR-ordningerne og Unionens øvrige krisestyringsmekanismer, herunder Kommissionens overordnede hurtige varslingssystem, ARGUS, EU-civilbeskyttelsesmekanismen, der støttes af Katastrofeberedskabskoordinationscentret ("ERCC"), der blev oprettet i henhold til Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU om en EU-civilbeskyttelsesmekanisme[5] ("afgørelsen om EU-civilbeskyttelsesmekanismen"), EU-Udenrigstjenestens krisereaktionsmekanisme, samt andre processer såsom dem, der er beskrevet i EU's cyberdiplomatiske værktøjskasse[6], den hybride værktøjskasse[7] og i den reviderede EU-protokol for imødegåelse af hybride trusler[8]. Den supplerer og bør også være i overensstemmelse med Rådets henstilling (EU) 2024/4371 om en plan for koordinering af reaktionen på EU-plan på forstyrrelser af kritisk infrastruktur af væsentlig grænseoverskridende relevans[9] ("EU-planen for kritisk infrastruktur"), som omfatter ikkecyberrelateret fysisk modstandsdygtighed, og som har til formål at forbedre koordineringen af reaktionen på EU-plan på dette område.

---

5 Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU af 17. december 2013 om en EU-civilbeskyttelsesmekanisme (EUT L 347 af 20.12.2013, s. 924).

6 Rådets konklusioner om en ramme for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter (9916/17).

7 Rådets konklusioner om en ramme for en koordineret EU-reaktion på hybride kampagner, 22.6.2022.

8 Joint Staff Working Document – EU Protocol for countering hybrid threats (SWD(2023) 116 final).

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

(10) Det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser ("EU-CyCLONe") er netværket til koordination af styringen af omfattende cybersikkerhedshændelser og kriser på operationelt plan, også i tilfælde af tværsektorielle omfattende cybersikkerhedshændelser og cyberkriser. For ikke at komplicere de eksisterende rammer yderligere bør det undgås at oprette sektorspecifikke strukturer, der overlapper EU-CyCLONes opgaver. EU-CyCLONe bør også modtage operationelle cybersikkerhedsrelaterede oplysninger fra sektorerne og bidrage til det politiske niveau.

(11) Medlemsstaterne tilskyndes til at gøre fuld brug af de finansielle ressourcer, der er til rådighed til cybersikkerhed fra relevante EU-programmer. Det bør sikres, at disse programmer pålægger ansøgere om finansiering minimale administrative byrder, og at medlemsstaternes deltagelse i disse programmer lettes ved ydelse af relevant vejledning om holdbare finansielle støttemuligheder.

(12) Denne henstilling bidrager til bredere beredskabsforanstaltninger, der er nødvendige for, at Unionen kan tackle tværsektorielle kriser, i overensstemmelse med principperne i EU-strategien for en beredskabsunion, nemlig en integreret tilgang, der omfatter alle farer og inddrager alle myndigheder og hele samfundet, navnlig med hensyn til at øge bevidstheden om risici og trusler og tværsektoriel kriserespons –

VEDTAGET DENNE HENSTILING:

I: Formål, anvendelsesområde og vejledende principper for EU's ramme for cyberkrisestyring

Formål og anvendelsesområde

1) I denne henstilling om en EU-plan for cyberkrisestyring ("cyberplan") fastlægges EU-rammen for cyberkrisestyring inden for rammerne af EU's overordnede beredskab over for omfattende cybersikkerhedshændelser og cyberkriser. Rammen afspejler den rolle, som både medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer ("EU-enheder") spiller inden for deres respektive beføjelser under fuld overholdelse af nationale love og interne regler for at sikre en omfattende og koordineret indsats på EU-plan.

2) Cyberplanen bør anvendes i overensstemmelse med EU-planen for kritisk infrastruktur, navnlig hvis hændelser påvirker både den fysiske modstandsdygtighed og cybersikkerheden i forbindelse med kritisk infrastruktur[10].

3) Cyberplanen indeholder retningslinjer for reaktionen på omfattende cybersikkerhedshændelser eller cyberkriser, og den bør anvendes som supplement til alle relevante sektorspecifikke reaktionsmekanismer såsom dem, der er opført i bilag II. Relevante interessenter inden for cybersikkerhed bør hjælpe og bistå med at nå målene for disse sektorspecifikke mekanismer, både på nationalt plan og EU-plan.

4) I tilfælde af en EU-dækkende tværsektoriel krise med cyberaspekter, hvor IPCR bliver aktiveret, bør Rådet koordinere reaktionen på Unionens politiske plan ved hjælp af IPCR-ordningerne. Når IPCR er blevet aktiveret, bør foranstaltninger i henhold til cyberplanen støtte EU's reaktion på politisk plan og yde specifik støtte til cybersikkerhed.

[10] EU-planen for kritisk infrastruktur indeholder yderligere oplysninger om koordinering i sådanne tilfælde i bilagets del I, afdeling 4.

Vejledende principper

5) Følgende vejledende principper gælder for cyberkrisestyring på EU-plan:

a) *Proportionalitetsprincippet*: De fleste cybersikkerhedshændelser, der påvirker medlemsstaterne, ligger under tærsklen for, hvad der kan betragtes som en omfattende cybersikkerhedshændelse eller cyberkrise på nationalt plan eller EU-plan. I tilfælde af cybersikkerhedshændelser og -trusler samarbejder og udveksler medlemsstaterne frivilligt og regelmæssigt informationer inden for netværket af enheder, der håndterer IT-sikkerhedshændelser, ("CSIRT-netværket"), og EU-CyCLONe i overensstemmelse med netværkenes operative standardprocedurer ("SOP'er").

b) *Nærhedsprincippet*: Medlemsstaterne har det primære ansvar for at reagere og afhjælpe i tilfælde af en cybersikkerhedshændelse, en omfattende cybersikkerhedshændelse eller en cyberkrise, der påvirker dem. I betragtning af potentielle grænseoverskridende virkninger bør Rådet, Kommissionen, den højtstående repræsentant, Den Europæiske Unions Agentur for Cybersikkerhed ("ENISA"), Cybersikkerhedstjenesten for Unionens Institutioner, Organer, Kontorer og Agenturer ("CERT-EU"), Europol og alle andre relevante EU-enheder samarbejde gennem hele krisens livscyklus. Disse roller stammer fra EU-retten og afspejler, hvordan omfattende cybersikkerhedshændelser og cyberkriser påvirker en eller flere dele af den økonomiske aktivitet i det indre marked, Unionens sikkerhed og internationale forbindelser samt EU-enhederne selv.

c) *Komplementaritet*: Denne henstilling tager fuldt ud hensyn til eksisterende krisestyringsmekanismer på EU-plan, der er opført i bilag II, navnlig IPCR-ordningerne, ARGUS og EU-Udenrigstjenestens krisereaktionsmekanisme. Denne henstilling tager hensyn til mandaterne for CSIRT-netværket og EU-CyCLONe samt forordning (EU, Euratom) 2023/2841. Hvis IPCR aktiveres, bør arbejdet i relevante netværk, enheder og aktiverede sektorspecifikke mekanismer fortsætte og bør indgå i og støtte den politiske og strategiske koordinering, der finder sted i IPCR.

d) *Fortrolig behandling af oplysninger*: Al informationsudveksling inden for rammerne af denne henstilling bør overholde de gældende regler om sikkerhed og beskyttelse af personoplysninger. Uformelle hemmeligholdelsesaftaler, f.eks. Traffic Light Protocol om mærkning af følsomme oplysninger, bør tages i betragtning, når det er relevant. For udveksling af klassificerede oplysninger bør der uanset det anvendte klassifikationssystem anvendes eksisterende bindende regler og aftaler om behandling af klassificerede oplysninger sideløbende med tilgængelige akkrediterede værktøjer.

6) I overensstemmelse med ovenstående vejledende principper bør medlemsstaterne og EU-enhederne uddybe deres samarbejde om cyberkrisestyring, fremme gensidig tillid og bygge på eksisterende netværk og mekanismer. Dette samarbejde inden for rammerne af cyberplanen drager fordel af gennemførelsen af artikel 22 og 23 i forordning (EU, Euratom) 2023/2841. Navnlig den cyberkrisestyringsplan, der er udarbejdet på grundlag af artikel 23 i forordning (EU, Euratom) 2023/2841, bidrager bl.a. til regelmæssig udveksling af relevante oplysninger mellem EU-enheder og med medlemsstaterne og fastlægger ordninger for koordinering og informationsstrømme mellem EU-enhederne.

II: Definitioner

7) I denne cyberplan forstås ved:

a) "hændelse": en begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare

b) "væsentlig hændelse": en hændelse, der

a. har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed

b. har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade

c) "omfattende cybersikkerhedshændelse": en hændelse, der forårsager en forstyrrelse på et niveau, som overstiger en medlemsstats kapacitet til at reagere på den, eller som har en betydelig indvirkning på mindst to medlemsstater

d) "cyberkrise": en omfattende cybersikkerhedshændelse, der eskalerede til en fuldgyldig krise, som forhindrer det indre markeds korrekte funktion eller udgør alvorlige risici for den offentlige sikkerhed for enheder eller borgere i flere medlemsstater eller for Unionen som helhed.

III: Nationale cyberkrisestyringsstrukturer og -ansvarsområder

8) Medlemsstaterne har det primære ansvar for at reagere i tilfælde af omfattende cybersikkerhedshændelser eller cyberkriser, der påvirker dem. Hver medlemsstat har i overensstemmelse med direktiv (EU) 2022/2555 en eller flere cyberkrisestyringsmyndigheder samt en eller flere CSIRT'er.

9) Gennem vedtagelsen af direktiv (EU) 2022/2555 og andre lovgivningsmæssige og ikkelovgivningsmæssige instrumenter vedrørende cybersikkerhed har medlemsstaterne tilpasset deres rammer for cybersikkerhed ved at fastsætte minimumsregler for, hvordan den koordinerede reguleringsramme fungerer, fastlægge mekanismer for effektivt samarbejde mellem de ansvarlige myndigheder i hver medlemsstat og tilvejebringe effektive retsmidler og håndhævelsesforanstaltninger, der er afgørende for effektiv håndhævelse af disse forpligtelser.

10) I overensstemmelse med artikel 9, stk. 4, i direktiv (EU) 2022/2555 bør medlemsstaterne vedtage nationale beredskabsplaner for omfattende cybersikkerhedshændelser og kriser. Disse planer omfatter bl.a. nationale beredskabsforanstaltninger, cyberkrisestyringsprocedurer og nationale procedurer og ordninger mellem nationale myndigheder og organer for at sikre deres effektive deltagelse i og støtte til den koordinerede håndtering af omfattende cybersikkerhedshændelser og cyberkriser på EU-plan. Cyberkrisestyringsprocedurerne omfatter også bestemmelser om deres integration i den generelle nationale krisestyringsramme og kanalerne for udveksling af oplysninger.

11) I overensstemmelse med artikel 9, stk. 1, i direktiv (EU) 2022/2555 bør medlemsstaterne sikre sammenhængen med de eksisterende rammer for generel national krisestyring. I tilfælde af aktivering af IPCR bør de nationale krisestyringsmyndigheder med henblik på at informere IPCR indsamle input fra cyberkrisestyringsmyndighederne og de nationale sektorspecifikke krisemekanismer.

12) I overensstemmelse med artikel 9, stk. 5, i direktiv (EU) 2022/2555 bør EU-CyCLONe efter anmodning fra en berørt medlemsstat udveksle oplysninger om de relevante dele af de nationale beredskabsplaner for omfattende cybersikkerhedshændelser og kriser, navnlig om de bestemmelser, der skal sikre effektiv deltagelse i og støtte til den koordinerede håndtering af omfattende cybersikkerhedshændelser og cyberkriser på EU-plan, med henblik på at udveksle bedste praksis og overveje, om den overordnede ramme vil fungere i praksis.

13) EU-CyCLONe og Det Interinstitutionelle Råd for Cybersikkerhed ("IICB") opfordres til, hvor det er relevant, at udveksle oplysninger om sammenhængen mellem den krisestyringsplan, der er udarbejdet af IICB i overensstemmelse med artikel 23 i forordning (EU, Euratom) 2023/2841, og nationale beredskabsplaner for omfattende cybersikkerhedshændelser og kriser.

14) EU-CyCLONe bør med støtte fra ENISA som sekretariat føre en ajourført liste over nationale cyberkrisestyringsmyndigheder med kontaktoplysninger på EU-CyCLONe's medarbejdere og ledere og stille den til rådighed for EU-CyCLONe's medlemmer.

IV: De vigtigste netværk og aktører i EU's økosystem for cyberkrisestyring

15) CSIRT-netværket er det vigtigste tekniske netværk til udveksling af relevante oplysninger om hændelser, navnlig inden for denne henstillings anvendelsesområde, i overensstemmelse med de relevante opgaver, der er beskrevet i artikel 15, stk. 3, i direktiv (EU) 2022/2555. Det bidrager til skabelsen af tillid mellem medlemsstaterne og fremmer hurtigt og effektivt operationelt samarbejde mellem medlemsstaterne. Formanden for CSIRT-netværket kan deltage som observatør i IICB.

16) CERT-EU er cybersikkerhedstjenesten for alle EU-enheder. CERT-EU fungerer som knudepunkt for udveksling af oplysninger vedrørende cybersikkerhed og for koordinering af reaktionen på hændelser for EU-enheder i overensstemmelse med artikel 13 i forordning (EU) 2023/2841. CERT-EU er medlem af CSIRT-netværket og støtter Kommissionen i EU-CyCLONe. CERT-EU opererer på teknisk plan og er ansvarlig for at koordinere håndteringen af større hændelser, der påvirker EU-enheder.

17) EU-CyCLONe fungerer som en formidler mellem det tekniske og politiske niveau, navnlig under omfattende cybersikkerhedshændelser og cyberkriser. Det støtter den koordinerede håndtering af omfattende cybersikkerhedshændelser og cyberkriser på operationelt plan og sikrer regelmæssig udveksling af relevant information mellem medlemsstaterne og EU-institutioner, -organer, -kontorer og-agenturer i overensstemmelse med artikel 16 i direktiv (EU) 2022/2555. Formanden for EU-CyCLONe kan deltage som observatør i IICB.

18) ENISA er det EU-agentur, der udfører de opgaver, det tillægges i henhold til forordning (EU) 2019/881[11], med det formål at opnå et højt fælles cybersikkerhedsniveau i hele Unionen, herunder ved aktivt at støtte medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer. ENISA varetager bl.a. sekretariatsfunktionen for CSIRT-netværket og EU-CyCLONe, leverer situationsbevidsthedstjenester og bistår medlemsstaterne ved regelmæssigt at tilrettelægge cybersikkerhedsøvelser på EU-plan. I overensstemmelse med direktiv (EU) 2022/2555 og forordning (EU) 2024/2847[12] modtager ENISA oplysninger om væsentlige grænseoverskridende hændelser og aktivt udnyttede sårbarheder og hændelser, der påvirker digitale produkter.

19) Rådet for Den Europæiske Union ("Rådet") er institutionen med politikformulerende og koordinerende funktioner i henhold til artikel 16 i traktaten om Den Europæiske Union (TEU) og har fået overdraget ansvaret for IPCR, som vedrører koordination og respons på Unionens politiske niveau. Rådet arbejder gennem rådssammensætninger, De Faste Repræsentanters Komité og relevante forberedende organer i Rådet, navnlig Den Horisontale Gruppe vedrørende Cyberspørgsmål ("Cybergruppen"), samt, hvor det er relevant, IPCR-ordningerne.

---

[11] Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15).

[12] Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) nr. 168/2013 og (EU) 2019/1020 og direktiv (EU) 2020/1828 (forordningen om cyberrobusthed) (EUT L, 2024/2847, 20.11.2024, s. 1).

20) Kommissionen er som den institution, der fremmer Unionens almene interesser og tager passende initiativer med henblik herpå samt drager omsorg for gennemførelsen af traktaterne og af de foranstaltninger, der vedtages af institutionerne i henhold til artikel 17 i TEU, ansvarlig for visse generelle beredskabsforanstaltninger på EU-plan og visse foranstaltninger vedrørende situationsbevidsthed, herunder forvaltningen af ERCC og det fælles varslings- og informationssystem ("CECIS"), i overensstemmelse med afgørelsen om EU-civilbeskyttelsesmekanismen. Den fremmer sammenhæng og koordinering mellem relaterede kriseberedskabsforanstaltninger på EU-plan på operationelt plan. Den høres om beslutninger om at aktivere eller deaktivere IPCR. Kommissionens tjenestegrene udarbejder sammen med EU-Udenrigstjenesten ISAA-rapporterne. Den er medlem af EU-CyCLONe i tilfælde, hvor en potentiel eller igangværende omfattende cybersikkerhedshændelse har eller sandsynligvis vil have en betydelig indvirkning på tjenester og aktiviteter, der er omfattet af anvendelsesområdet for direktiv (EU) 2022/2555, og er observatør i andre tilfælde. Den er kontaktpunktet i IICB til EU-CyCLONe. Den er observatør i CSIRT-netværket.

21) Den højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik (den højtstående repræsentant) varetager med bistand fra EU-Udenrigstjenesten Unionens fælles udenrigs- og sikkerhedspolitik ("FUSP") og bidrager med sine forslag til udarbejdelsen af denne politik, herunder den fælles sikkerheds- og forsvarspolitik ("FSFP"). Dette omfatter diplomatiske, efterretningsmæssige og militære strukturer og mekanismer, navnlig den fælles efterretningsanalysekapacitet ("SIAC") som det centrale kontaktpunkt for medlemsstaternes efterretninger, EU's Militærstab ("EUMS") som kilden til militær ekspertise, EU's cyberdiplomatiske værktøjskasse samt netværket af EU-delegationer, der kan bidrage til ekstern krisestyring. EU-Udenrigstjenesten udarbejder også ISAA-rapporterne sammen med Kommissionen.

22) I bilag II beskrives roller og kompetencer for de relevante aktører på EU-plan i forbindelse med cyberkrisestyring, herunder de vigtigste netværk og aktører.

V: Forberedelse til omfattende cybersikkerhedshændelser og en cyberkrise

Trusselsbillede

23) Medlemsstaterne og de relevante EU-enheder bør træffe de nødvendige foranstaltninger for at øge situationsbevidstheden i erkendelse af, at trusselsbilledet og hændelsesspecifik situationsbevidsthed kræver forskellige fremgangsmåder. Medlemsstaterne og relevante EU-enheder bør samarbejde på grundlag af verificerede, pålidelige data, herunder tendenser inden for hændelser, taktikker, teknikker og procedurer, og aktivt udnyttede sårbarheder.

24) Når medlemsstaterne udveksler oplysninger på EU-plan, bør de gøre fuld brug af de eksisterende platforme for teknisk og operationelt samarbejde, f.eks. dem, der anvendes af CSIRT-netværket og EU-CyCLONe.

25) For at øge den fælles situationsbevidsthed og lette vurderingen af EU's indvirkning bør EU-CyCLONe og CSIRT-netværket med støtte fra ENISA anvende en internt aftalt rapporteringsmekanisme til at udarbejde en EU-oversigt over tekniske og operationelle aktiviteter baseret på de oplysninger, der er indsamlet på nationalt plan.

26) EU-CyCLONe og CSIRT-netværket bør:

a) samarbejde om at forbedre informationsudvekslingen mellem det tekniske og operationelle niveau og situationsbevidstheden som helhed

b) fortsætte med at opbygge et tillidsbaseret klima mellem deres medlemmer og mellem netværkene

c) gøre fuld brug af de tilgængelige værktøjer til informationsudveksling med støtte fra ENISA, overveje, hvordan disse værktøjer kan forbedres, og sikre interoperabilitet mellem netværkene.

27) EU-CyCLONe, CSIRT-netværket og IICB bør samarbejde om at sikre effektiv udveksling af relevante oplysninger.

28) ENISA spiller som sekretariat for CSIRT-netværket og EU-CyCLONe en central rolle med hensyn til at støtte medlemsstaterne og Unionens institutioner, organer og agenturer i at opnå en fælles EU-situationsbevidsthed på det tekniske og operationelle plan for at støtte forberedelsen til omfattende cybersikkerhedshændelser og kriser.

29) I overensstemmelse med direktiv (EU) 2022/2555 og forordning (EU) 2019/881 bør medlemsstaterne og relevante EU-enheder koordinere med den private sektor, herunder open source-fællesskaber og -producenter, for at forbedre informationsudvekslingen. ENISA bør navnlig anvende sit partnerskabsprogram i denne henseende. Desuden kan medlemsstaterne og relevante EU-enheder også bygge videre på eksisterende informationsudvekslings- og analysecentre ("ISAC'er") på EU-plan og nationalt plan for at øge cybersikkerhedskapaciteten og reagere på cybersikkerhedshændelser, herunder gennem den private sektors fælles møder med EU- CyCLONe eller CSIRT-netværket.

30) For at forbedre informationsudvekslingen inden for og mellem netværkene og for at præcisere de gensidige forventninger til en sådan udveksling bør EU-CyCLONe med støtte fra ENISA som sekretariat og efter høring af CSIRT-netværket og NIS-samarbejdsgruppen senest 24 måneder efter vedtagelsen af denne henstilling nå til enighed om en fælles tilpasset taksonomi for alvorsgrader af hændelser. Denne taksonomi bør gøre det muligt at sammenligne alvoren af hændelser på tværs af medlemsstaterne ved at tage hensyn til indvirkningen på leveringen af tjenester, antallet af berørte enheder og deres respektive relevans, indvirkningen på andre tjenester og infrastrukturer samt den økonomiske, omdømmemæssige og politiske skade, der påføres. Den bør bygge på relevante eksisterende skalaer eller taksonomier såsom Reference Incident Classification Taxonomy.

Teknisk plan

31) CSIRT-netværket er platformen for teknisk samarbejde og informationsudveksling mellem alle medlemsstaterne og gennem CERT-EU med EU-enhederne.

32) I overensstemmelse med direktiv (EU) 2022/2555 har hver CSIRT til opgave at overvåge og analysere cybertrusler, sårbarheder og hændelser på nationalt plan. CSIRT'er bør både inden for CSIRT-netværket og bilateralt udveksle relevante oplysninger om hændelser, nærvedhændelser, cybertrusler, risici og sårbarheder for at opnå en fælles situationsbevidsthed.

33) For at styrke det operationelle samarbejde på EU-plan bør CSIRT-netværket overveje at indbyde EU-organer og -agenturer, der er involveret i cybersikkerhedspolitikken, såsom Europol, til at deltage i sit arbejde.

34) I overensstemmelse med forordning (EU) 2023/2841 bør CERT-EU indsamle, forvalte, analysere og dele oplysninger med Unionens institutioner, organer, kontorer og agenturer om cybertrusler, sårbarheder og hændelser i uklassificeret IKT-infrastruktur og om nødvendigt udstede specifikke forslag til IICB om retningslinjer og henstillinger til Unionens institutioner, organer, kontorer og agenturer. CERT-EU bør samarbejde og udveksle oplysninger med medlemsstatsmodparter, herunder ved hjælp af CSIRT-netværket.

Operationelt plan

35) I overensstemmelse med direktiv (EU) 2022/2555 bør EU-CyCLONe fungere som en platform for samarbejde mellem medlemsstaternes cyberkrisestyringsmyndigheder og gennem Kommissionen med de relevante EU-enheder med det formål at øge beredskabsniveauet i forbindelse med håndtering af omfattende cybersikkerhedshændelser og cyberkriser og udvikle en fælles situationsbevidsthed om omfattende cybersikkerhedshændelser og cyberkriser.

36) I overensstemmelse med direktiv (EU) 2022/2555 og forordning (EU) 2024/2847 modtager ENISA oplysninger om væsentlige grænseoverskridende hændelser og aktivt udnyttede sårbarheder og hændelser, der påvirker digitale produkter. ENISA, der fungerer som sekretariat, bør rådgive CSIRT-netværket og EU-CyCLONe med det formål at støtte netværkene i at afgøre, om der bør træffes yderligere foranstaltninger, og for at bidrage til den fælles situationsbevidsthed.

Politisk plan

37) Medlemsstaterne og relevante EU-enheder bør overvåge den internationale udvikling, der påvirker cybersikkerheden (herunder cybertrusler, hybride trusler og udenlandsk informationsmanipulation og indblanding ("FIMI"), herunder desinformation, hvor det er relevant). Initiativer såsom de fælles cybervurderingsrapporter ("JCAR"), analyser fra SIAC og andre relevante produkter, der giver en særlig indsigt, bør tages i betragtning.

38) Den højtstående repræsentant bør fortsat informere og inddrage medlemsstaterne i Unionens diplomatiske indsats i forbindelse med cybertrusler, navnlig dem, der involverer statslige aktører, samarbejdet med tredjelande og internationale organisationer, herunder NATO, og gennemførelsen af diplomatiske foranstaltninger, herunder restriktive foranstaltninger.

39) Formandskabet for Rådet for Den Europæiske Union kan oprette en overvågningsside på IPCR-webplatformen, hvor medlemsstaterne og EU's institutioner og organer kan udveksle oplysninger om en krise, der muligvis er under udvikling.

Fælles øvelser

40) Kommissionen bør i koordinering med den højtstående repræsentant med støtte fra ENISA og efter høring af EU-CyCLONe og CSIRT-netværket udarbejde et effektivt årligt rullende program for cyberøvelser for at forberede sig på cyberkriser og forbedre den organisatoriske effektivitet. Det rullende program for cyberøvelser bør tage hensyn til øvelser i EU-civilbeskyttelsesmekanismen og i andre kriseresponsmekanismer på EU-plan, herunder den øvelse, der er skitseret i EU-planen for kritisk infrastruktur. Det første rullende program bør udvikles inden for 12 måneder efter vedtagelsen af cyberplanen, og efterfølgende programmer skal være færdiggjort senest den 31. marts hvert år. Det rullende program bør forelægges Rådet til orientering.

41) Det rullende program bør også omfatte øvelser, der er udviklet ved hjælp af EU-koordinerede risikovurderingsscenarier. Den bør omfatte øvelser, der involverer alle relevante aktører, navnlig den private sektor og NATO.

42) ENISA bør i sin rolle som sekretariat for CSIRT-netværket og EU-CyCLONe sikre systematisk indsamling af erfaringer fra øvelserne samt identificering af de deraf følgende foranstaltninger og forslag til, hvordan de kan gennemføres, for at sikre, at de gennemføres effektivt og har en positiv indvirkning på EU's fælles modstandsdygtighed, herunder de respektive SOP'er.

43) Alle aktører og netværk bør forbedre koordineringen i tilfælde af en omfattende cybersikkerhedshændelse eller cyberkrise på grundlag af erfaringerne fra øvelserne. Navnlig bør EU-CyCLONe og CSIRT-netværket tage fat på de udfordringer, der er identificeret under øvelserne for at forbedre koordineringen, især dem, der vedrører samarbejdet mellem netværkene, og om nødvendigt hurtigt tilpasse SOP'erne.

44) NIS-samarbejdsgruppen bør opfordre CSIRT-netværket, EU-CyCLONe og ENISA til at fremlægge erfaringerne fra øvelserne og samt identifikationen af og forslagene til, hvordan de deraf følgende foranstaltninger kan gennemføres.

45) Rådet kan opfordre formændene for CSIRT-netværket, EU-CyCLONe, NIS-samarbejdsgruppen og ENISA til at redegøre for, hvordan erfaringerne fra øvelserne er blevet gennemført.

46) ENISA opfordres til i samarbejde med Kommissionen og den højtstående repræsentant at tilrettelægge en øvelse for at teste cyberplanen under den næste Cyber Europe-øvelse. Øvelsen bør involvere alle relevante aktører, herunder det politiske niveau. ENISA opfordres til at koordinere inddragelsen af det politiske niveau med formandskabet for Rådet for Den Europæiske Union. Øvelsen kan også omfatte den private sektor og NATO.

VI: Opdagelse af en hændelse, der kan eskalere til en omfattende cybersikkerhedshændelse eller cyberkrise

47) I overensstemmelse med deres respektive mandater og på grundlag af en tilgang, der omfatter alle farer, bør alle aktører bidrage med oplysninger om en potentiel omfattende cybersikkerhedshændelse eller cyberkrise, til relevante netværk.

48) Hvis grænseoverskridende cyberknudepunkter indhenter oplysninger om en mulig eller igangværende omfattende cybersikkerhedshændelse, bør de i overensstemmelse med forordning (EU) 2025/38[13] og med henblik på fælles situationsbevidsthed sikre, at der uden unødig forsinkelse gives relevante oplysninger til medlemsstaternes myndigheder og Kommissionen via EU-CyCLONe og CSIRT-netværket.

[13] Europa-Parlamentets og Rådets forordning (EU) 2025/38 af 19. december 2024 om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser og om ændring af forordning (EU) 2021/694 (forordning om cybersolidaritet) (EUT L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

49) Hvis der observeres en væsentlig hændelse, der navnlig har en øjeblikkelig virkning, kan den indberettes til eller opdages af en CSIRT samt af medlemsstaternes cyberkrisestyringsmyndigheder eller andre sektormyndigheder. Medlemsstaterne tilskyndes til at udveksle oplysninger om en sådan hændelse inden for netværkene, som bør overveje at træffe passende foranstaltninger. CSIRT-netværket og EU-CyCLONe kan aktiveres hver for sig afhængigt af hændelsens art og den påkrævede reaktion. Begge netværk tilskyndes imidlertid til at fortsætte det indbyrdes samarbejde på grundlag af aftalte proceduremæssige ordninger. Beslutningen om aktivering træffes ene og alene og uden indblanding af hvert af de respektive netværk.

50) CSIRT-netværket bør rådgive EU-CyCLONe om, hvorvidt en observeret cybersikkerhedshændelse kan betragtes som en potentiel eller igangværende omfattende cybersikkerhedshændelse.

51) Som angivet i direktiv (EU) 2022/2555 bør CSIRT-netværket og EU-CyCLONe straks fastlægge proceduremæssige ordninger i tilfælde af en potentiel eller igangværende omfattende cybersikkerhedshændelse for at sikre teknisk-operationel koordinering og rettidige og relevante oplysninger til det politiske niveau.

VII: Reaktion på en omfattende cybersikkerhedshændelse eller cyberkrise på EU-plan

Reaktion på en omfattende cybersikkerhedshændelse eller cyberkrise, hvor IPCR ikke aktiveres i fuld aktiveringsfunktion

52) En effektiv reaktion på omfattende cybersikkerhedshændelser eller cyberkriser på EU-plan afhænger af et effektivt teknisk, operationelt og politisk samarbejde i en tilgang, der omfatter alle myndigheder, herunder så vidt muligt retshåndhævelse.

53) På hvert plan bør de involverede aktører udføre specifikke aktiviteter for at opnå fælles situationsbevidsthed og en koordineret reaktion. Sådanne foranstaltninger skal sikre en velordnet og effektiv formidling af oplysninger.

54) Reaktionen bør være passende i forhold til virkningen af den omfattende cybersikkerhedshændelse eller cyberkrise. I overensstemmelse med direktiv (EU) 2022/2555 bør medlemsstaternes cyberkrisestyringsmyndigheder sikre national sammenhæng og koordinering mellem de sektorspecifikke reaktioner på cyberkrisen.

55) I tilfælde af en omfattende cybersikkerhedshændelse eller en cyberkrise bør alle aktører og netværk reagere i tæt koordinering som følger:

a) På teknisk plan:

i. De berørte medlemsstater og deres CSIRT'er bør samarbejde med de berørte enheder om at reagere på hændelser og yde bistand, hvor det er relevant.

ii. CSIRT'erne bør samarbejde gennem CSIRT-netværket om at dele relevante tekniske oplysninger om hændelsen. CSIRT'erne samarbejder i deres bestræbelser på at analysere de tilgængelige tekniske artefakter og andre tekniske oplysninger vedrørende hændelsen med henblik på at fastslå årsagen og mulige tekniske afhjælpende foranstaltninger.

iii. Når en CSIRT eller en medlemsstats cyberkrisestyringsmyndighed bliver opmærksom på en væsentlig hændelse, tilskyndes de til at give besked inden for CSIRT-netværket eller EU-CyCLONe.

iv. CSIRT-netværket bør med støtte fra ENISA udarbejde en samling af nationale rapporter indsendt af CSIRT'er, som bør forelægges for EU-CyCLONe.

v. Når en cybersikkerhedshændelse har potentiale til at eskalere til en omfattende cybersikkerhedshændelse eller en cyberkrise, bør CSIRT-netværket udveksle relevante oplysninger med EU-CyCLONe. EU-CyCLONe bør anvende disse oplysninger til at orientere Rådet.

vi. CSIRT-netværket bør være i tæt kontakt med Europol for at sikre udveksling af relevante tekniske oplysninger. CSIRT-netværket og Europol bør oprette kontaktpunkter for at forbedre informationsudvekslingen, når det er relevant i tilfælde af en omfattende cybersikkerhedshændelse.

b) På operationelt plan:

i. Medlemsstaterne bør afbøde hændelsens virkninger på nationalt plan ved hjælp af passende foranstaltninger.

ii. CSIRT-netværket bør give EU-CyCLONe tekniske vurderinger af de igangværende hændelser, som kan anvendes af EU-CyCLONe.

iii. EU-CyCLONe bør vurdere konsekvenserne og virkningerne af relevante omfattende cybersikkerhedshændelser og cyberkriser og foreslå mulige afbødende foranstaltninger og støtte den koordinerede håndtering af omfattende cybersikkerhedshændelser og cyberkriser samt støtte beslutningstagningen på politisk plan.

iv. Hvis en omfattende cybersikkerhedshændelse med tværsektoriel indvirkning kræver aktivering af indsatsforanstaltninger på EU-plan, navnlig relevante horisontale og sektorspecifikke krisestyringsmekanismer på EU-plan, der er opført i bilag II,

a) kan de relevante aktører afhængigt af typen af sektorspecifikke krisestyringsmekanismer på EU-plan opfordre til aktivering af nævnte mekanisme

b) støtter de relevante enheder sektorenhederne med at afbøde virkningerne af hændelsen i tilfælde af aktivering af en sådan sektorspecifik mekanisme

c) bør Kommissionen lette formidlingen af de nødvendige oplysninger mellem kontaktpunkterne for de relevante horisontale og sektorspecifikke krisemekanismer på EU-plan, der er opført i bilag II, og EU-CyCLONe, og bør ligeledes foretage en integreret tværsektoriel analyse og foreslå muligheder for en passende integreret beredskabsplan

d) bør Kommissionen gennem EU-CyCLONe, hvor det er relevant, i samarbejde med den højtstående repræsentant sikre sammenhæng og koordinering på EU-plan af de operationelle foranstaltninger på cyberområdet med relaterede indsatsforanstaltninger på EU-plan, navnlig i forbindelse med anmodninger om bistand gennem EU-civilbeskyttelsesmekanismen

e) bør oplysninger om hændelsen, dens virkninger og trufne foranstaltninger, hvis der er oprettet en IPCR-overvågningsside, også udveksles mellem medlemsstaterne og EU-enhederne via IPCR-webplatformen

v. Medlemsstaterne kan anmode om tjenester fra EU's cybersikkerhedsreserve i overensstemmelse med artikel 15 i forordning (EU) 2025/38. Med forbehold af eventuelle fremtidige gennemførelsesretsakter i henhold til nævnte forordning bør tjenester i EU's cybersikkerhedsreserve indsættes senest 24 timer efter anmodningen.

c) På politisk plan:

i. Rådet kan anmode om briefinger fra de vigtigste interessenter, navnlig Kommissionen, den højtstående repræsentant og EU-CyCLONe, med henblik på at gennemføre en passende politisk og strategisk reaktion.

ii. Rådet kan med støtte fra Kommissionen og den højtstående repræsentant træffe afgørelse om passende foranstaltninger til at reagere på den omfattende cybersikkerhedshændelse, herunder eventuelle diplomatiske reaktioner i overensstemmelse med kapitel IX.

iii. Medlemsstaterne kan aktivere yderligere cyberkrisestyringsmekanismer eller -instrumenter afhængigt af hændelsens art og virkning.

iv. Når IPCR aktiveres i informationsudvekslingsfunktion, aktiveres ISAA-støttekapaciteten, hvilket øger informationsudvekslingen via IPCR-webplatformen og sikrer et fælles situationsoverblik. Situationsrapporterne fra EU-CyCLONe og CSIRT-netværket bør fortsat være de vigtigste instrumenter, der præsenterer den fælles situationsbevidsthed på henholdsvis det operationelle og det tekniske plan. Disse rapporter kan danne grundlag for ISAA-rapporterne.

v. I tilfælde af en hændelse, der kræver aktivering af indsatsforanstaltninger på EU-plan, navnlig relevante horisontale og sektorspecifikke krisestyringsmekanismer på EU-plan, der er opført i bilag II, bør Rådet i samarbejde med Kommissionen og den højtstående repræsentant sikre sammenhæng og koordinering mellem reaktionerne på cyberkrisen og relaterede indsatsforanstaltninger på EU-plan.

vi. Hvis der anmodes om relevante mekanismer, navnlig cybersikkerhedsreservens tjenester, bør Kommissionens tjenestegrene og, hvor det er relevant, EU-Udenrigstjenesten samt relevante rådsorganer, navnlig Cybergruppen og Den Horisontale Gruppe vedrørende Styrkelse af Modstandsdygtighed og Imødegåelse af Hybride Trusler ("HWP ERCHT"), alt efter hvad der er relevant, koordinere udformningen og gennemførelsen af foranstaltninger samt den passende beslutningsproces for yderligere foranstaltninger i overensstemmelse med den hybride værktøjskasse[14] i tilfælde af ondsindede cyberaktiviteter, der er en del af en bredere hybrid kampagne.

Reaktion på en omfattende cybersikkerhedshændelse eller cyberkrise, hvor IPCR aktiveres i fuld aktiveringsfunktion

56) De trin, der er anført i afsnittet "*Reaktion på en omfattende cybersikkerhedshændelse eller cyberkrise, hvor IPCR ikke aktiveres i fuld aktiveringsfunktion*" ovenfor, bør gennemføres.

57) Når IPCR aktiveres i fuld aktiveringsfunktion, tjener ISAA-rapporterne til at sikre fælles situationsbevidsthed på politisk plan. Situationsrapporterne fra EU-CyCLONe og CSIRT-netværket bør fortsat være de vigtigste instrumenter, der præsenterer den fælles situationsbevidsthed på henholdsvis det operationelle og det tekniske plan. Disse rapporter kan danne grundlag for ISAA-rapporterne.

58) I tilfælde af en omfattende cybersikkerhedshændelse eller cyberkrise, der resulterer i aktivering af IPCR i fuld aktiveringsfunktion, bør alle aktører reagere i tæt koordinering i en tilgang, der omfatter alle myndigheder, som følger:

a) Koordinering af reaktionen på Unionens politiske plan varetages af Rådet med anvendelse af IPCR-ordningerne.

[14] Den hybride værktøjskasse er en ramme for en koordineret reaktion på hybride kampagner, der påvirker EU og medlemsstaterne, og som f.eks. omfatter forebyggende, samarbejdsmæssige, stabilitetsmæssige, restriktive foranstaltninger og genopretningsforanstaltninger og støtter solidaritet og gensidig bistand.

b) EU-CyCLONe bør i samarbejde med CSIRT-netværket give klare oplysninger til det politiske niveau om hændelsens virkninger, mulige konsekvenser og reaktions- og afhjælpningsforanstaltninger, herunder ved at bidrage til ISAA-rapporterne.

c) Ud over ISAA-kapaciteten vil formandskabet for Rådet for Den Europæiske Union indkalde til IPCR-rundbordsdiskussioner for at muliggøre politisk og strategisk koordinering af EU's reaktion med tiltag inden for rammerne af cyberplanen og arbejdet i relevante sektorspecifikke mekanismer, der bidrager til IPCR's arbejde. Rundbordsdiskussionerne kan desuden afdække nogle specifikke mangler i reaktionen og tilskynde til, at specifikke EU-aktører afhjælper dem og melder tilbage ved fremtidige rundbordsdiskussioner for at støtte den politiske og strategiske koordinering i IPCR.

d) Formandskabet for Rådet for Den Europæiske Union bør overveje at indbyde EU-CyCLONe til relevante møder, herunder rundbordsdiskussioner under IPCR-ordningerne og andre relevante rådsmøder.

e) Medlemsstaternes krisestyringsmyndigheder bør sikre sammenhæng og koordinering mellem de sektorspecifikke reaktioner på cyberkrisen med støtte fra cyberkrisestyringsmyndigheder.

f) De mulige diplomatiske reaktioner bør overvejes og gennemføres i overensstemmelse med kapitel IX.

VIII: Offentlig kommunikationsindsats

59) Selv om kommunikation til befolkningen i en enkelt medlemsstat om en igangværende omfattende cybersikkerhedshændelse eller cyberkrise, herunder som led i bevidstgørelse, som er en national kompetence, bør medlemsstaterne, Kommissionen og den højtstående repræsentant sigte mod at koordinere deres offentlige kommunikation i videst muligt omfang. Det uformelle IPCR-krisekommunikationsnetværk kan inddrages, hvis det er relevant.

60) Med henblik på at forberede sig på omfattende cybersikkerhedshændelser og cyberkriser opfordres medlemsstaterne og, hvor det er relevant, Kommissionen og CERT-EU til at udveksle oplysninger om deres kommunikationsindsats inden for EU-CyCLONe og CSIRT-netværket, herunder bedste praksis, såsom rådgivningsmateriale eller oplysningskampagner. ENISA bør stille værktøjer til rådighed, der støtter en sådan udveksling og sikrer let adgang.

61) I tilfælde af en omfattende cybersikkerhedshændelse eller cyberkrise opfordres medlemsstaterne til inden for EU-CyCLONe at udveksle oplysninger om deres offentlige kommunikationsindsats for at opbygge en fælles bevidsthed og koordinere tiltagene. EU-CyCLONe kan på eget initiativ eller efter anmodning fra Rådet dele en oversigt over sådanne tilgange med Rådet.

IX: Diplomatisk reaktion og samarbejde med strategiske partnere

62) Den højtstående repræsentant bør i tæt samarbejde med Kommissionen og andre relevante EU-enheder:

a) støtte beslutningstagningen i Rådet, herunder gennem analyser, rapporter og forslag, om anvendelsen af mulige foranstaltninger som led i EU's cyberdiplomatiske værktøjskasse. Dette vil gøre det muligt at anvende hele spektret af tilgængelige EU-værktøjer til at forebygge, afværge og reagere på ondsindede cyberaktiviteter, styrke EU's cyberposition og fremme international fred, sikkerhed og stabilitet i cyberspace

b) hvis der identificeres en relevant hændelse, lette formidlingen af nødvendige oplysninger til strategiske partnere, herunder til NATO, når det er relevant

c) styrke koordineringen med strategiske partnere, herunder med NATO, når det er relevant, om reaktionen på ondsindede cyberaktiviteter fra vedholdende trusselsaktørers side, navnlig ved anvendelse af EU's cyberdiplomatiske værktøjskasse, i overensstemmelse med gennemførelsesretningslinjerne.

63) Medlemsstaterne, den højtstående repræsentant, Kommissionen og andre relevante EU-enheder bør samarbejde med strategiske partnere og internationale organisationer om at fremme god praksis og ansvarlig statslig adfærd i cyberspace og sikre en hurtig og koordineret reaktion i tilfælde af potentielle eller omfattende cybersikkerhedshændelser.

64) Samarbejdet mellem Den Europæiske Union og NATO bør foregå i overensstemmelse med de aftalte vejledende principper om inklusivitet, gensidighed og gennemsigtighed og med fuld respekt for Unionens beslutningsautonomi.

65) Kommissionen og den højtstående repræsentant bør under hensyntagen til eksisterende aftaler såsom den tekniske aftale mellem CERT-EU og NATO fra 2016 oprette kontaktpunkter for koordinering med NATO i tilfælde af en cyberkrise for at udveksle nødvendige oplysninger om situationen og anvendelsen af kriseresponsmekanismer for at øge samarbejdet om og effektiviteten af reaktionen. Med henblik herpå bør Unionen undersøge, hvordan informationsudvekslingen med NATO kan forbedres på en inklusiv, gensidig og ikkediskriminerende måde, navnlig ved at sikre værktøjer til sikker kommunikation, samtidig med at der tages hensyn til forskellige medlemsstaters standarder for informationsudveksling.

66) Som led i Unionens rullende program for cyberøvelser, der er omhandlet i kapitel V ovenfor, bør Kommissionens tjenestegrene og EU-Udenrigstjenesten overveje at tilrettelægge en øvelse på personaleniveau med NATO for at afprøve samarbejdet mellem civile og militære enheder i tilfælde af en omfattende cybersikkerhedshændelse eller cyberkrise, hvor medlemsstaterne eller NATO-allierede søger reaktioner på et cyberangreb, der påvirker deres sikkerhed. Øvelsen bør gennemføres på en inklusiv og ikkediskriminerende måde og under fuld overholdelse af de aftalte principper for parametrene for samarbejdet mellem EU og NATO. Øvelsen bør gennemføres inden for rammerne af EU's integrerede resolutionsøvelse (parallel og koordineret øvelse, "PACE"). Alle de nødvendige foranstaltninger bør træffes for at sikre deltagelse af alle de aktører, der er omhandlet i cyberplanen.

67) Fælles cyberøvelser på EU-plan med landene på Vestbalkan, Republikken Moldova, Ukraine samt andre strategiske partnere og ligesindede tredjelande bør også overvejes i samråd med Rådet, Kommissionen og den højtstående repræsentant.

X. Koordinering af cyberkrisestyring med militære aktører på EU-plan

68) Medlemsstaterne bør fortsat styrke samarbejdet mellem civile og militære cyberaktører på nationalt plan.

69) EU-CyCLONe og CSIRT-netværket bør identificere mulige metoder til og procedurer for samarbejde med de relevante militære EU-aktører såsom EU's konference for cyberøverstbefalende og det operationelle netværk for militære IT-beredskabsenheder ("MICNET") for at drage fordel af et fælles militært og civilt perspektiv, navnlig gennem fælles møder. EU-CyCLONe og CSIRT-netværket bør underrette Rådet om de fremskridt, der gøres med hensyn til et sådant samarbejde.

70) Den berørte medlemsstat opfordres til at underrette EU-CyCLONe samt EU-Udenrigstjenesten, hvis der anvendes relevante nationale eller multinationale militære indsatskapaciteter i forbindelse med en omfattende cybersikkerhedshændelse eller cyberkrise, og leveringen af disse oplysninger aftales indbyrdes mellem brugeren og udbyderen af en sådan indsatskapacitet.

71) Som led i Unionens rullende program for cyberøvelser, der er omhandlet i kapitel V ovenfor, bør Kommissionen og den højtstående repræsentant overveje at tilrettelægge en fælles øvelse for at afprøve samarbejdet mellem både civile og militære cyberaktører i tilfælde af en omfattende cybersikkerhedshændelse, der berører medlemsstaterne.

XI: Genopretning efter og erfaringer fra en cyberkrise

72) Medlemsstaterne, relevante EU-enheder og netværk bør samarbejde i genopretningsfasen efter en cyberkrise for at sikre en hurtig genetablering af centrale funktioner. De retshåndhævende myndigheder bør også, hvor det er relevant, inddrages i et sådant samarbejde. I denne fase er samarbejde med den private sektor afgørende, navnlig for at lette genopretningen af data og genindførelsen af systemer. I en effektiv koordinering mellem interessenter bør minimering af forstyrrelser og sikring af driftskontinuitet prioriteres.

73) Medlemsstaterne, relevante EU-enheder og netværk bør arbejde sammen i genopretningsfasen på grundlag af erfaringerne fra tidligere cyberkriser eller håndterede cybersikkerhedshændelser samt hændelsesrapporter, navnlig inden for rammerne af den europæiske mekanisme til gennemgang af cybersikkerhedshændelser, der er oprettet ved forordning (EU) 2025/38.

74) EU-CyCLONe bør fremlægge en omfattende liste over erfaringer fra tidligere cyberkriser eller håndterede cybersikkerhedshændelser og bedste praksis for CSIRT-netværket, NIS-samarbejdsgruppen og Rådet. ENISA bør sikre, at disse erfaringer afspejles korrekt i fremtidige beredskabsaktiviteter og i forbindelse med planlægningen af fremtidige øvelser.

XII: Sikker kommunikation

75) Baseret på kortlægning af eksisterende sikre kommunikationsværktøjer[15] bør Kommissionen inden udgangen af 2026 foreslå et interoperabelt sæt sikre kommunikationsløsninger. Rådet, Kommissionen, den højtstående repræsentant, EU-CyCLONe og CSIRT-netværket bør nå til enighed om dette sæt inden udgangen af 2027. Disse løsninger bør drage fordel af de tiltag inden for sikker kommunikation, som EU-institutionerne kan træffe inden for rammerne af EU-strategien for en beredskabsunion, og bør dække hele spektret af de nødvendige kommunikationsmetoder (tale, data, videokonferencer, meddelelser, samarbejde og dokumentdeling og høring). Løsningerne bør opfylde fælles definerede krav til beskyttelse af følsomme ikkeklassificerede oplysninger. Der bør anvendes løsninger, som er baseret på åben protokol med open source-implementeringer, der egner sig til realtidskommunikation, og som forvaltes af en enhed med hjemsted i EU.

76) EU-CyCLONe og CSIRT-netværket bør med henblik på udveksling af oplysninger, der er klassificeret RESTREINT UE/EU RESTRICTED, om nødvendigt kunne anvende sikre kommunikationskanaler, der er sikret EU's institutioner, organer og agenturer til udveksling af klassificerede informationer indbyrdes og med medlemsstaterne.

[15] WK 862/2023.

77) Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed ("ECCC"), der er oprettet ved forordning (EU) 2021/887[16], bør, uden at det berører den fremtidige flerårige finansielle ramme, overveje finansiering gennem programmet for et digitalt Europa for at bistå medlemsstaterne med at anvende sikre kommunikationsværktøjer. Enhver overlapning af investeringer i interoperable sikre systemer bør undgås.

78) Navnlig bør EU-enheder og medlemsstater udarbejde beredskabsplaner i tilfælde af alvorlige kriser, hvor normale kommunikationskanaler, der er afhængige af internettet eller telekommunikationsnet, afbrydes eller ikke er tilgængelige.

79) Der bør etableres kommunikations- og informationsudvekslingsmekanismer mellem retshåndhævelses- og cybersikkerhedsnetværk, navnlig på teknisk plan, med henblik på en effektiv cyberkriserespons. Disse mekanismer bør respektere hver parts rolle og undgå at forstyrre igangværende operationer og sikre, at kommunikationen bliver overflødig. EU-systemet for kritisk kommunikation ("EUCCS"), der i øjeblikket er under udvikling, kan gavne den fælles indsats med relevante cybersamfund.

XIII: Afsluttende bestemmelser

80) EU-CyCLONe bør i samarbejde med CSIRT-netværket og andre hovedaktører i EU's økosystem for cyberkrisestyring med støtte fra ENISA senest et år efter offentliggørelsen af henstillingen udarbejde detaljerede procesflowdiagrammer, der skitserer informationsstrømmene mellem relevante aktører, beslutningsprocesser og rapporter, der er udarbejdet i forbindelse med håndteringen af omfattende cybersikkerhedshændelser eller cyberkriser som beskrevet i denne henstilling. Flowdiagrammerne bør dække forskellige samarbejdsformer og -lag. De bør ajourføres efter behov.

[16] Europa-Parlamentets og Rådets forordning (EU) 2021/887 af 20. maj 2021 om oprettelse af Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed og Netværket af Nationale Koordinationscentre (EUT L 202 af 8.6.2021, s. 1).

81) For at støtte en effektiv anvendelse af den reviderede cyberplan og på grundlag af erfaringerne fra de fælles cyberøvelser, der gennemføres i henhold hertil, kan Rådet om nødvendigt udarbejde et sæt gennemførelsesretningslinjer. Disse retningslinjer kan omhandle de praktiske udfordringer, der er konstateret under øvelserne, og afhjælpe påviste mangler og manglende forbindelser inden for koordinering, kommunikation og operationel interaktion.

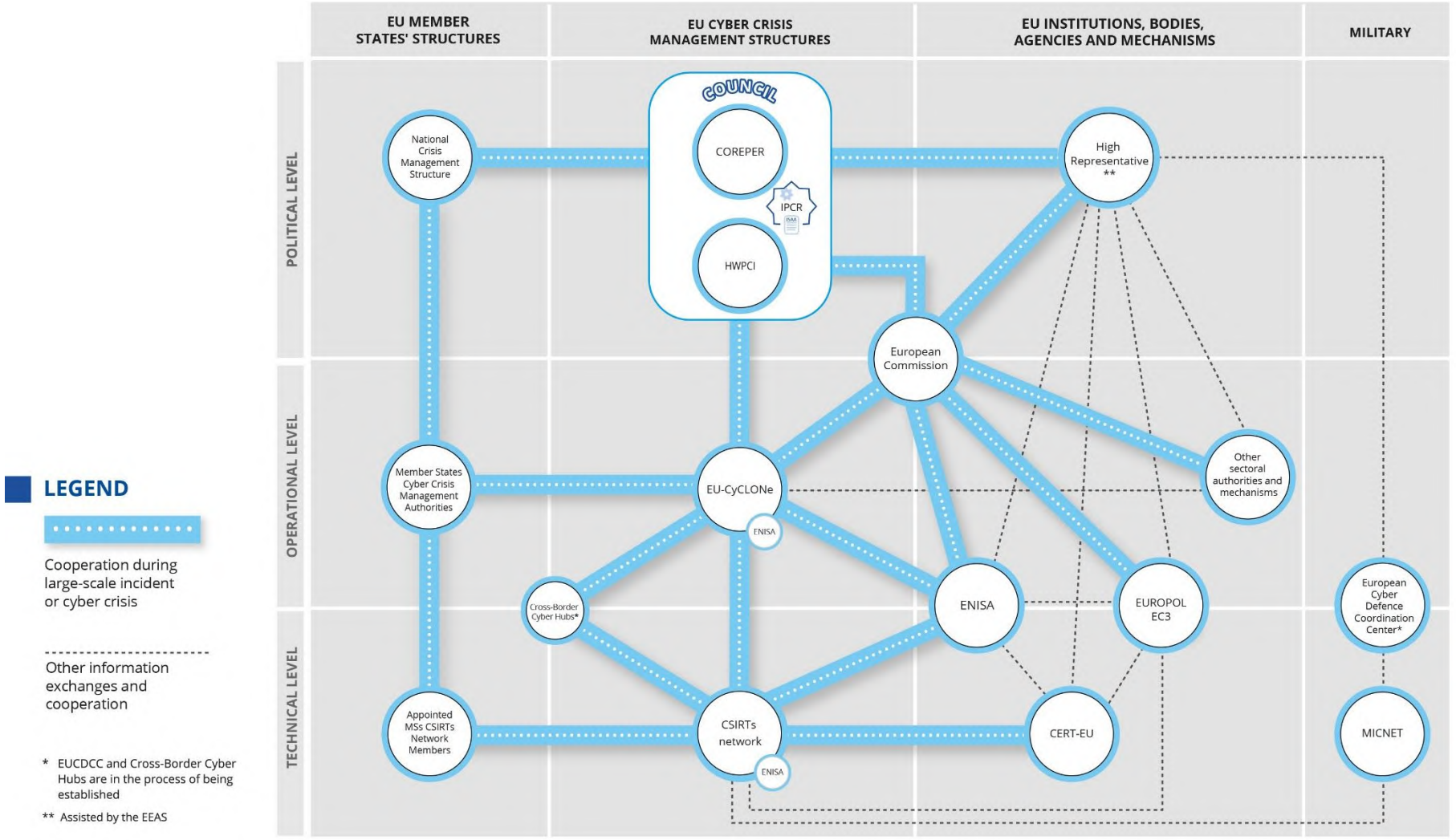
82) Denne henstilling bør revideres af Kommissionen i samarbejde med medlemsstaterne mindst hvert fjerde år efter dens offentliggørelse. Efter hver revision bør Kommissionen offentliggøre en rapport og forelægge den for Rådet. Kommissionen og medlemsstaterne bør navnlig tage hensyn til virkningerne af det skiftende trusselsbillede, resultaterne af fælles øvelser og lovgivningsmæssige ændringer, navnlig eventuelle ændringer som følge af revisionen af forordning (EU) 2019/881.

Udfærdiget i Bruxelles, den […].

På Rådets vegne

Formand

BILAG I – Unionens plan for reaktion på en cybersikkerhedskrise



BILAG II – RELEVANTE AKTØRER PÅ EU-PLAN (ENHEDER OG NETVÆRK) OG KRISESTYRINGSMEKANISMER

(1) Inddragelse af de vigtigste aktører i hele cyberkrisestyringens livscyklus (omfattende cybersikkerhedshændelser og cyberkriser)

	Beredskab	Detektion	Reaktion på en omfattende cybersikkerhedshændelse eller en cyberkrise			Offentlig kommunikation	Genopretning og erfaringer
			på teknisk plan	på operationelt plan	på politisk plan		
Medlemsstater	X	X	X	X	X	X	X
Kommissionen	X			X	X	X	
Den højtstående repræsentant med bistand fra EU-Udenrigstjenesten	X			X	X	X	
Rådet	X				X	X	X
ENISA	X		X	X			
CERT-EU	X	X	X	X		X	X
CSIRT-netværket	X	X	X				X
EU-CyCLONe	X			X	X		X

(2) Roller og kompetencer for de relevante aktører på EU-plan og mekanismer (i alfabetisk rækkefølge) i forbindelse med cyberkrisestyring

Aktør	Niveau	Rolle og kompetence	Henvisning
CERT-EU	Teknisk/ operationelt	Koordinerer kriseреaktionen på teknisk plan og håndteringen af større hændelser, der påvirker EU-enheder. Fører en fortegnelse over disponibel teknisk ekspertise, der vil være brug for i forbindelse med reaktionen på større hændelser, og bistår IICB med at koordinere EU-enhedernes cyberkrisehåndteringsplaner for større hændelser. Medlem af CSIRT-netværket. Støtter Kommissionen i EU-CyCLONe i den koordinerede håndtering af omfattende cybersikkerhedshændelser og kriser. Fungerer som knudepunkt for udveksling af cybersikkerhedsoplysninger og koordinering af reaktionen på hændelser og letter udvekslingen af oplysninger om hændelser, cybertrusler, sårbarheder og	Europa-Parlamentets og Rådets forordning (EU, Euratom) 2023/2841 Forordning (EU) 2025/38

Aktør	Niveau	Rolle og kompetence	Henvisning
		nærvedhændelser mellem EU-enheder og -modparter. Anmoder om indsættelse af EU's cybersikkerhedsreserve på vegne af EU-enheder. Samarbejder med NATO's Center for Cybersikkerhed på baggrund af deres tekniske aftale.	
Rådet for Den Europæiske Union	Politisk	Politikformulerende og koordinerende funktioner. Har fået overdraget ansvaret for IPCR, som vedrører koordination og respons på Unionens politiske niveau.	Artikel 16 i traktaten om Den Europæiske Union
Formandskabet for Rådet for Den Europæiske Union	Politisk	Beslutter (medmindre solidaritetsbestemmelsen er blevet påberåbt i henhold til artikel 222 i traktaten om Den Europæiske Unions funktionsmåde), om IPCR skal aktiveres i samråd med de berørte medlemsstater, alt efter hvad der er relevant, samt Kommissionen og HR.	Artikel 16 i traktaten om Den Europæiske Union Rådets gennemførelsesafgørelse (EU) 2018/1993
Grænseoverskridende cyberknudepunkter	Teknisk	Et grænseoverskridende cyberknudepunkt er en platform for flere lande, som er oprettet i henhold til en skriftlig konsortieaftale, der i en koordineret netværksstruktur	Forordning (EU) 2025/38

Aktør	Niveau	Rolle og kompetence	Henvisning
		samler nationale cyberknudepunkter fra mindst tre medlemsstater, og som er udformet med henblik på at styrke overvågningen, opdagelsen og analysen af cybertrusler og forebygge hændelser og støtte tilvejebringelse af cybermæssige trusselsefterretninger, navnlig gennem udveksling af relevante data og oplysninger, anonymiserede hvor det er hensigtsmæssigt, samt gennem deling af avancerede værktøjer og fælles udvikling af cybermæssige opdagelses-, analyse-, forebyggelses- og beskyttelseskapaciteter i et pålideligt miljø. Samarbejder tæt med CSIRT-netværket om at udveksle oplysninger. Giver oplysninger om en potentiel eller igangværende omfattende cybersikkerhedshændelse til medlemsstaternes myndigheder og Kommissionen gennem EU-CyCLONe og CSIRT-netværket.	

Aktør	Niveau	Rolle og kompetence	Henvisning
CSIRT-netværket	Teknisk	Bidrager til skabelsen af tillid mellem medlemsstaterne og fremmer hurtigt og effektivt operationelt samarbejde mellem medlemsstaterne. Er det vigtigste netværk til udveksling af relevant information om hændelser, nærvedhændelser, cybertrusler, risici og sårbarheder. På anmodning af et medlem, der potentielt er berørt af en hændelse, udveksler og drøfter netværket oplysninger i forbindelse med denne hændelse og tilknyttede cybertrusler. Netværket kan også lette en samordnet reaktion på en hændelse, som er identificeret inden for et anmodende medlems jurisdiktion. Yder bistand til medlemsstaterne i forbindelse med håndteringen af grænseoverskridende hændelser og undersøger yderligere former for samarbejde, herunder gensidig bistand. Modtager oplysninger fra medlemsstaterne vedrørende	Direktiv (EU) 2022/2555 Forordning (EU) 2025/38

Aktør	Niveau	Rolle og kompetence	Henvisning
		deres anmodninger til EU's cybersikkerhedsreserve.	
Konferencen af cyberøverstbefalende		Et forum for cyberøverstbefalende på nationalt plan i medlemsstaterne, hvor de kan samarbejde og udveksle vigtige oplysninger om igangværende cyberspaceoperationer og strategier til afbødning af omfattende cyberhændelser. Den organiseres af det roterende formandskab for Rådet for Den Europæiske Union med støtte fra Det Europæiske Forsvarsagentur (EDA), Tjenesten for EU's Optræden Udadtil (EU-Udenrigstjenesten), herunder EU's Militærstab (EUMS).	Fælles meddelelse om EU's politik for cyberforsvar (2022)
Kommissionen	Operationelt/ politisk	Den Europæiske Unions udøvende organ. Sikrer et velfungerende indre marked. Fremmer sammenhæng og koordinering mellem relaterede kriseberedskabstiltag på EU-plan. Visse generelle beredskabstiltag på EU-plan i henhold til	Artikel 17 i traktaten om Den Europæiske Union Gennemførelsesafgørelse (EU) 2018/1993 Afgørelse nr. 1313/2013/EU

Aktør	Niveau	Rolle og kompetence	Henvisning
		afgørelsen om en EU-civilbeskyttelsesmekanisme, herunder forvaltning af Katastrofeberedskabskoordinationscentret og det fælles varslings- og informationssystem. Observatør i EU-CyCLONe og medlem i tilfælde af en potentiel eller igangværende omfattende hændelse, der har eller sandsynligvis vil have en betydelig indvirkning på tjenester og aktiviteter, der er omfattet af anvendelsesområdet for direktiv (EU) 2022/2555. Observatør i CSIRT-netværket. Overordnet ansvar for gennemførelsen af EU's cybersikkerhedsreserve. Kontaktpunkt i Det Interinstitutionelle Råd for Cybersikkerhed med henblik på udveksling af relevante oplysninger i relation til større hændelser for EU-CyCLONe. Høres af formandskabet for Rådet om beslutninger om at aktivere eller deaktivere IPCR (medmindre solidaritetsbestemmelsen er	Direktiv (EU) 2022/2555 Forordning (EU) 2025/38 Forordning (EU, Euratom) 2023/2841

Aktør	Niveau	Rolle og kompetence	Henvisning
		blevet påberåbt i henhold til artikel 222 i TEUF). Kommissionens tjenestegrene udarbejder sammen med EU-Udenrigstjenesten ISAA-rapporterne.	
Den Europæiske Unions Agentur for Cybersikkerhed (ENISA)	Teknisk/operationelt	Udfører opgaver med det formål at opnå et højt cybersikkerhedsniveau i hele Unionen, herunder ved aktivt at støtte medlemsstaterne og EU-institutionerne. Varetager sekretariatsfunktionen for CSIRT-netværket og EU-CyCLONe. Udarbejder en regelmæssig EU-cybersikkerhedsrapport om hændelser og cybertrusler (med EC3 og CERT-EU og i tæt samarbejde med medlemsstaterne). Bidrager til udviklingen af en fælles reaktion på omfattende grænseoverskridende hændelser eller kriser, især ved: - at samle og analysere rapporter fra nationale kilder	Direktiv (EU) 2022/2555 Forordning (EU) 2019/881 Forordning (EU) 2025/38 Forordning (EU) 2024/2847

Aktør	Niveau	Rolle og kompetence	Henvisning
		- at sikre informationsstrømmen mellem teknisk, operationelt og politisk niveau - på anmodning at lette håndteringen af hændelser - at støtte EU-enheder med hensyn til offentlig kommunikation - på anmodning at støtte medlemsstaterne med hensyn til offentlig kommunikation - at afprøve kapaciteten til at reagere på hændelser og regelmæssigt tilrettelægge cybersikkerhedsøvelser. Fungerer som ordregivende myndighed, hvis det helt eller delvis er overdraget driften og forvaltningen af EU's cybersikkerhedsreserve. Tilrettelægger hvert andet år omfattende cybersikkerhedsøvelser i stor skala på EU-plan med tekniske, operationelle eller strategiske elementer. Udarbejder en rapport om gennemgang af hændelser i samarbejde med den berørte medlemsstat og andre relevante interessenter for at vurdere årsagerne til og konsekvenserne	

Aktør	Niveau	Rolle og kompetence	Henvisning
		og afbødningen af en hændelse (på anmodning af Kommissionen eller EU-CyCLONe og med den berørte medlemsstats godkendelse). Underretter EU-CyCLONe, hvis de oplysninger, der er afgivet i henhold til rapporteringsforpligtelserne i forordningen om cyberrobusthed, er relevante for den koordinerede håndtering af omfattende cybersikkerhedshændelser og kriser på operationelt plan.	
Det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe)	Operationelt	Støtter den koordinerede håndtering af store cybersikkerhedshændelser og kriser på operationelt plan. Sikrer en regelmæssig udveksling af relevante oplysninger mellem medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer. Koordinerer håndteringen af omfattende cybersikkerhedshændelser og kriser og støtter beslutningstagningen på politisk plan i forbindelse med sådanne hændelser og kriser.	Direktiv (EU) 2022/2555 Forordning (EU) 2025/38

Aktør	Niveau	Rolle og kompetence	Henvisning
		Vurderer konsekvenserne og indvirkningen af relevante omfattende cybersikkerhedshændelser og kriser og foreslår mulige afbødende foranstaltninger. Drøfter på anmodning af en berørt medlemsstat nationale beredskabsplaner for omfattende cybersikkerhedshændelser og kriser. Udvikler sammen med ENISA og Kommissionen den skabelon, der skal lette indgivelsen af anmodninger om støtte fra EU's cybersikkerhedsreserve. Modtager oplysninger fra medlemsstaterne vedrørende deres anmodninger til EU's cybersikkerhedsreserve. Modtager oplysninger om en potentiel eller igangværende omfattende cybersikkerhedshændelse fra de grænseoverskridende cyberknudepunkter eller CSIRT-netværket.	
Unionens højtstående repræsentant for udenrigsanliggender	Politisk	Fører an i og koordinerer Unionens indsats for at imødegå eksterne sikkerhedstrusler på	Rådets afgørelse 2010/427/EU

Aktør	Niveau	Rolle og kompetence	Henvisning
og sikkerhedspolitik med bistand fra Tjenesten for EU's Optræden Udadtil		områderne hybride trusler og cybertrusler. Ansvarlig for Unionens cyberdiplomati og cyberforsvarsinstrumenter med henblik på at afskrække fra og reagere på eksterne trusler, herunder ved hjælp af Unionens hybride og cyberdiplomatiske værktøjskasser. Samarbejder med eksterne partnere, også gennem FSFP-engagement. Tilvejebringer Unionens og medlemsstaternes situationsbevidsthed og kapacitet til at reagere på hybride trusler og cybertrusler, f.eks. gennem praktiske øvelser, uddannelse og netværk. Håndterer sikkerheds- og forsvarsmæssige konsekvenser af Unionens rumaktiver, navnlig inden for rammerne af Unionens fælles sikkerheds- og forsvarspolitik (FSFP). Støtter EU's konference for cyberøverstbefalende. Støtter EU's operationelle netværk for militære IT-beredskabsenheder (MICNET).	

Aktør	Niveau	Rolle og kompetence	Henvisning
		Høres af formandskabet for Rådet om beslutninger om at aktivere eller deaktivere IPCR (medmindre solidaritetsbestemmelsen er blevet påberåbt i henhold til artikel 222 i TEUF). EU-Udenrigstjenesten udarbejder sammen med Kommissionens tjenestegrene ISAA-rapporterne.	
EU-Koordinationscentret for Cyberforsvar	Horisontalt	Dets oprindelige mål er primært at øge Unionens og dens medlemsstaters fælles situationsbevidsthed om ondsindede aktiviteter i cyberspace, navnlig i forbindelse med militære FSFP-missioner og -operationer.	Fælles meddelelse om EU's politik for cyberforsvar (2022)
Europol	Operationelt	Yder operationel og teknisk støtte til medlemsstaternes kompetente myndigheder med henblik på forebyggelse af og afskrækkelse fra cyberkriminalitet. Bistår medlemsstaternes kompetente myndigheder på deres anmodning med at reagere på cyberangreb af formodet kriminel oprindelse.	Forordning (EU) 2016/794, herunder alle ændringer

Aktør	Niveau	Rolle og kompetence	Henvisning
Det Interinstitutionelle Råd for Cybersikkerhed		Fastlægger en plan for cyberkrisestyring for på operationelt plan at støtte den koordinerede håndtering af større hændelser, der påvirker EU-enheder, og bidrage til regelmæssig udveksling af relevante oplysninger. Koordinerer vedtagelsen af de enkelte EU-enheders cyberkrisestyringsplaner. Vedtager på grundlag af et CERT-EU-forslag retningslinjer eller henstillinger om samarbejde om reaktion på væsentlige hændelser vedrørende EU-enheder.	Forordning (EU, Euratom) 2023/2841
Det operationelle netværk for militære IT-beredskabsenheder (MICNET)	Teknisk	Fremmer en mere solid og koordineret reaktion på cybertrusler, der påvirker forsvarssystemerne i Unionen, bl.a. de systemer, der anvendes til militære FSFP-missioner og -operationer. Støttet af Det Europæiske Forsvarsagentur.	Fælles meddelelse om cyberforsvar 2022

Aktør	Niveau	Rolle og kompetence	Henvisning
Den fælles efterretningsanalysekapacitet (SIAC)		Består af 1) EU's Efterretnings- og Situationscenter (EU INTCEN) og 2) Efterretningsdirektoratet under EU's Militærstab (EUMS INT) "SIAC". Leverer strategiske efterretninger om udenrigspolitik, terrorisme og hybride trusler og håndterer militære efterretninger til FSFP-missioner og støtter Unionens forsvars- og krisestyringsoperationer. Under den højtstående repræsentants myndighed.	Artikel 38 og 42-46 i traktaten om Den Europæiske Union

(3) Relevante krisestyringsmekanismer og -platforme på EU-plan

Mekanisme	Horisontal/sektorspecifik/cyberspecifik	Beskrivelse	Henvisning
ARGUS	Horisontal	Kommissionens koordinationsproces og overordnede varslingssystem for en sammenhængende indsats i tilfælde af en større grænseoverskridende krise, der kræver en indsats på EU-plan. Den samler alle relevante tjenestegrene og kabinetter til at træffe afgørelse om og koordinere foranstaltninger. Giver Kommissionen mulighed for at udveksle relevante oplysninger om nye multisektorale kriser eller forudseelige eller overhængende trusler, der kræver handling på EU-plan.	Meddelelse fra Kommissionen KOM(2005) 662
EU-Udenrigs-tjenestens kriserespons-center (CRC)	Horisontal	Det fælles kontaktpunkt for alle kriserelaterede spørgsmål i EU-Udenrigstjenesten og den permanente kriseberedskabskapacitet døgnet rundt til nødsituationer, der truer sikkerheden for personalet i EU-delegationerne og/eller som reaktion på kriser, der påvirker EU-borgere i udlandet. Det samler sikkerhedseksperter, konsulære eksperter og eksperter i situationsbevidsthed, samtidig med	Et strategisk kompas for sikkerhed og forsvar – For en Europæisk Union, der beskytter sine borgere, værdier og interesser og bidrager til international fred og sikkerhed (21.3.2022)

Mekanisme	Horisontal/sektorspecifik/cyberspecifik	Beskrivelse	Henvisning
		at der trækkes på engagerede fagfolk på stedet i EU-delegationerne.	
Plan for kritisk infrastruktur	Horisontal	Koordinerer en reaktion på EU-plan på forstyrrelser af kritisk infrastruktur af væsentlig grænseoverskridende relevans.	Rådets henstilling C/2024/4371
Varslings-systemet for cybersikkerhed	Cyberspecifik	Sikrer avanceret EU-kapacitet til at forbedre detektions-, analyse- og databehandlingskapaciteten i forbindelse med cybertrusler og forebyggelse af hændelser i Unionen.	Forordning (EU) 2025/38
Cyberdiplomatisk værktøjskasse (ramme for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter)	Cyberspecifik	Muliggør en fælles diplomatisk reaktion fra Unionens side på ondsindede cyberaktiviteter, der bidrager til forebyggelse af konflikter, afbødning af cybersikkerhedstrusler og øget stabilitet i internationale forbindelser.	Rådets konklusioner af 19. juni 2017 Reviderede gennemførelsesretningslinjer 10289/23 (8.6.2023)
EU's cybersikkerheds-reserve	Cyberspecifik	Mobiliserer cybersikkerhedseksperter og -ressourcer under kriser for at støtte indsatsen i medlemsstaterne og Unionens institutioner, organer eller agenturer	Forordning (EU) 2025/38

Mekanisme	Horisontal/sektorspecifik/cyberspecifik	Beskrivelse	Henvisning
Netregler om sektorspecifikke regler for cybersikkerheds mæssige aspekter af grænseover-skridende elektricitets-strømme	Sektorspecifik	Fastlægger en tilbagevendende proces for cybersikkerhedsrisikovurderinger i elsektoren på EU-plan, medlemsstatsniveau, regionalt plan og enhedsniveau. Indeholder bestemmelser, der er specifikke for krisestyring og samarbejde med CSIRT'er og EU-CyCLONe i tilfælde, hvor en omfattende cybersikkerhedshændelse har indvirkning på andre sektorer, der er afhængige af elforsyningssikkerheden.	Kommissionens delegerede forordning (EU) 2024/1366
Hybrid værktøjskasse	Horisontal	Indeholder et sæt bestemmelser, der skal sikre et overblik over, hvad der er tilgængeligt på EU-plan som reaktion på alle former for hybride trusler, deres koordinerede anvendelse og sammenhæng i tiltagene på tværs af områder. Den hybride værktøjskasse bidrager til at sikre, at beslutningstagningen baseres på en omfattende situationsbevidsthed og de indhøstede erfaringer.	Rådets konklusioner om en ramme for en koordineret EU-reaktion på hybride kampagner (22.6.2022) Gennemførelsesretningslinjer for rammen for en koordineret EU-reaktion på hybride kampagner (14.12.2022)

Mekanisme	Horisontal/sektorspecifik/cyberspecifik	Beskrivelse	Henvisning
Hybridberedskabshold (EU-hybridberedskabshold)	Horisontal	Som led i den hybride EU-værktøjskasse trækker EU-hybridberedskabshold på relevant sektorspecifik civil og militær ekspertise på nationalt plan og EU-plan for at yde skræddersyet og målrettet kortsigtet bistand til medlemsstaterne, missioner og operationer under den fælles sikkerheds- og forsvarspolitik og partnerlande i forbindelse med imødegåelse af hybride trusler og kampagner.	Vejledende ramme for den praktiske oprettelse af EU-hybridberedskabshold (21.5.2024) Operationel vejledning for udsendelse af hybridberedskabshold, godkendt af Coreper den 4. december 2024
IPCR	Horisontal	Støtter en hurtig og koordineret beslutningstagning på EU's politiske niveau i forbindelse med større og komplekse kriser. Beslutningen om at aktivere og deaktivere træffes af formandskabet for Rådet, som (medmindre solidaritetsbestemmelsen er blevet påberåbt) hører de berørte medlemsstater, Kommissionen og HR. GSR, Kommissionens tjenestegrene og EU-Udenrigstjenesten kan også i samråd med formandskabet beslutte	Rådets gennemførelsesafgørelse (EU) 2018/1993

Mekanisme	Horisontal/sektorspecifik/cyberspecifik	Beskrivelse	Henvisning
		at aktivere IPCR i informationsudvekslingsfunktion. ICPR's arbejde er baseret på ISAA-rapporter, der er udarbejdet af Kommissionens tjenestegrene og EU-Udenrigstjenesten. Sådanne rapporter baseres på relevante oplysninger og analyser fra medlemsstaterne (eksempelvis fra relevante nationale krisecentre) og fra de relevante EU-agenturer og -organer.	
EU's beredskabs-protokol om retshåndhævelse	Horisontal	Et redskab til at støtte Unionens retshåndhævende myndigheder i at reagere øjeblikkeligt på større grænseoverskridende cyberangreb gennem hurtig vurdering, sikker og rettidig udveksling af kritiske oplysninger og effektiv koordinering af de internationale aspekter af deres efterforskning.	Rådets konklusioner (26.6.2018) om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser
PESCO's EU-hybridberedskabshold (CRRT)	Cyberspecifik	PESCO's CRRT'er er en civil-militær cyberforsvarskapacitet, som EU's medlemsstater har udviklet i fællesskab, til hurtigt at reagere på cyberhændelser og cyberkriser samt	Artikel 42, stk. 6, artikel 46 og protokol nr. 10 til traktaten om

Mekanisme	Horisontal/sektorspecifik/cyberspecifik	Beskrivelse	Henvisning
		udføre forebyggende foranstaltninger såsom sårbarhedsvurderinger og valgovervågning. Missionen for PESCO's CRRT'er er på anmodning at yde cyberstøtte til EU's medlemsstater, EU's institutioner, organer og agenturer, EU's militære FSFP-missioner og -operationer samt partnerlande.	Den Europæiske Union

Strukturen for reaktion på rumtrusler (Space Threat Response Architecture, STRA)	Sektorspecifik (rumtrusler, herunder cyberrelaterede)	Strukturen for reaktion på rumtrusler (STRA) for så vidt angår det ansvar, der skal udøves af Rådet og den højtstående repræsentant for at afværge en trussel, der opstår som følge af indførelsen, driften eller anvendelsen af de systemer, der er oprettet, og de tjenester, der leveres under Unionens rumprogram	Rådets afgørelse (FUSP) 2021/698
Rammen for koordinering af systemiske cyberhændelser (EU-SCICF)	Sektorspecifik	En ramme under udvikling til kommunikation og koordinering, som håndterer og styrer potentielle systemiske cyberhændelser i den finansielle sektor. Den vil bygge på en af de europæiske tilsynsmyndigheders (ESA'ers) planlagte roller i henhold til forordning (EU) 2022/2554 med hensyn til gradvist at muliggøre en effektiv koordineret reaktion på EU-plan i tilfælde af en større grænseoverskridende hændelse vedrørende informations- og kommunikationsteknologi (IKT) eller en dermed forbundet trussel, der har en systemisk indvirkning på Unionens finansielle sektor som helhed.	Det Europæiske Udvalg for Systemiske Risicis henstilling af 2. december 2021 om en paneuropæisk ramme for relevante myndigheders koordinering i tilfælde af systemiske cyberhændelser (ESRB/2021/17)
EU-civilbeskyttelses-mekanismen	Horisontal	Sikrer samarbejde om civilbeskyttelse for at forbedre katastrofeforebyggelsen, -beredskabet og -indsatsen.	Afgørelse nr. 1313/2013/EU

CISE – Den fælles ramme for informationsudveksling	Specifikt maritimt område, der dækker syv sektorer	CISE er et netværk, der forbinder systemer hos EU/EØS-myndigheder med ansvar for havovervågning. CISE muliggør udveksling af relevante oplysninger på tværs af grænser og forskellige sektorer på en problemfri og automatiseret måde.	Et strategisk kompas for sikkerhed og forsvar – For en Europæisk Union, der beskytter sine borgere, værdier og interesser og bidrager til international fred og sikkerhed (21.3.2022)

(4) Sektorer af særligt kritisk betydning og andre kritiske sektorer i henhold til direktiv (EU) 2022/2555 og sektorspecifikke krisemekanismer på EU-plan (hvor det er relevant)		
Sektor	**Delsektor**	**Gældende sektorspecifikke krisemekanismer**
Energi	Elektricitet	Elektricitetskoordinationsgruppen
	Fjernvarme og fjernkøling	Ikke relevant
	Olie	Oliekoordinationsgruppen Den Europæiske Unions Myndighedsgruppe for Offshore Olie- og Gasaktiviteter (EUOAG)
	Gas	Gaskoordinationsgruppen
	Brint	Ikke relevant
Transport	Luft	Krisekoordineringscellen for europæisk luftfart (EACCC)
	Jernbane	Ikke relevant
	Vand	EU-Fiskerikontrolagenturet (EFCA) SafeSeaNet (SSN) Integrerede maritime tjenester (IMS) Det Europæiske Datacenter for Identifikation og Sporing af Skibe på Lang Afstand (LRIT) EMSA's søfartsstøttetjenester

	Vejtransport	Ikke relevant
	Horisontal	Netværket af kontaktpunkter inden for transport, der er oprettet ved beredskabsplanen for transport (COM(2022) 211)
Bankvirksomhed		EU-SCICF
Finansielle markedsinfrastrukturer		EU-SCICF Den europæiske finansielle stabiliseringsmekanisme

Sundhed		Systemet for tidlig varsling og reaktion (EWRS) Sundhedskrisekoordinationscentret (HEOF) Hurtigt varslingssystem for vævs-, celle- og blodkomponenter (RATC/RAB) Ramme for folkesundhedsmæssige krisesituationer Systemet for hurtig varsling om kemiske hændelser (RASCHEM) Den europæiske overvågningsportal for smitsomme sygdomme Kriseberedskab og -indsats på Sundhedsområdet (HERA) Medicinsk sundhedsefterretningssystem (MedIsys) Højtstående Styringsgruppe vedrørende Medicinsk Udstyr (MDSSG) Hurtig varsling om lægemiddelovervågning EU-sundhedstaskforce (EUHTF) Udvalget for Sundhedssikkerhed
Drikkevand		Ikke relevant

Spildevand		Ikke relevant
Digital infrastruktur		Ikke relevant
Forvaltning af IKT-tjenester		Ikke relevant
Offentlig administration		Ikke relevant
Rummet		Strukturen for reaktion på rumtrusler (Space Threat Response Architecture, STRA)
Post- og kurertjenester		Ikke relevant
Affaldshåndtering		Ikke relevant
Fremstilling, produktion og distribution af kemikalier		Systemet for hurtig varsling om kemiske hændelser (RASCHEM)

Produktion, tilvirkning og distribution af fødevarer		Global anomalidetektionshotspot for landbrugsproduktion (ASAP) Det europæiske netværk af plantesundhedsinformationssystemer (EUROPHYT) EU's veterinærberedskabsteam (EUVET) Det hurtige varslingssystem for fødevarer og foder (RASFF) Europæisk kriseberedskabs- og indsatsmekanisme for fødevaresikkerhed (EFSCM) Forordningen om nødsituationer for det indre marked og det indre markeds modstandsdygtighed (IMERA)
Fremstilling	Medicinsk udstyr	Ikke relevant
	Computere og elektroniske og optiske produkter	Ikke relevant
	Maskiner og udstyr	Ikke relevant
	Fremstilling af motorkøretøjer, påhængsvogne og sættevogne	Ikke relevant
	Fremstilling af andre transportmidler	Ikke relevant

Digitale udbydere		Ikke relevant
Forskning		Ikke relevant

BILAG III – EU's ramme for håndtering af cybersikkerhedskriser og tilhørende instrumenter

Siden 2017 har Unionen udviklet sin ramme for cybersikkerhed gennem flere instrumenter, der indeholder bestemmelser, som er relevante for styring af cybersikkerhedskriser:

- Europa-Parlamentets og Rådets forordning (EU) 2019/881[1]
- Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[2]
- Kommissionens gennemførelsesforordning (EU) 2024/2690[3], Europa-Parlamentets og Rådets forordning (EU, Euratom) 2023/2841[4]
- Europa-Parlamentets og Rådets forordning (EU) 2021/887[5]
- Europa-Parlamentets og Rådets forordning (EU) 2024/2847[6] og
- Europa-Parlamentets og Rådets forordning (EU) 2025/38 (forordningen om cybersolidaritet)[7].

De specifikke sektorspecifikke cybersikkerhedskriseforanstaltninger omfatter Kommissionens delegerede forordning (EU) 2024/1366[8] og den kommende ramme for koordinering af systemiske cyberhændelser (EU-SCICF) inden for rammerne af Europa-Parlamentets og Rådets forordning (EU) 2022/2554[9].

Direktiv (EU) 2013/40[10] indeholder referencen til definitionen af kriminelle aktiviteter i forbindelse med cyberangreb, og EU-reglerne om grænseoverskridende adgang til elektronisk bevismateriale, navnlig Europa-Parlamentets og Rådets forordning (EU) 2023/1543[11], vil, når de er gennemført, i væsentlig grad lette retshåndhævelsesindsatsen på dette område.

EU's politik for cyberforsvar[12] skitserer rollerne for EU's operationelle netværk for militære IT-beredskabsenheder (MICNET) og EU's konference for cyberøverstbefalende og indeholder bestemmelser om oprettelse af EU-Koordinationscentret for Cyberforsvar (EUCDCC).

Der findes andre ikkecyberrelaterede situationsbevidstheds- og krisereaktionsmekanismer i nogle af de kritiske sektorer, der er opført i bilag I og II til direktiv (EU) 2022/2555.

Rådets henstilling om en plan for koordinering af reaktionen på EU-plan på forstyrrelser af kritisk infrastruktur af væsentlig grænseoverskridende relevans[13] indeholder bestemmelser om samarbejde mellem relevante aktører, hvis en hændelse påvirker både fysiske aspekter af og cybersikkerheden i forbindelse med kritisk infrastruktur.

[1] Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[2] Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333 af 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] Kommissionens gennemførelsesforordning (EU) 2024/2690 af 17. oktober 2024 om regler for anvendelsen af direktiv (EU) 2022/2555 for så vidt angår tekniske og metodologiske krav til foranstaltninger til styring af cybersikkerhedsrisici og yderligere præcisering af de tilfælde, hvor en hændelse anses for at være væsentlig for så vidt angår DNS-tjenesteudbydere, topdomænenavneadministratorer og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester og af tillidstjenester (EUT L, 2024/2690, 18.10.2024). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] Europa-Parlamentets og Rådets forordning (EU, Euratom) 2023/2841 af 13. december 2023 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i Unionens institutioner, organer, kontorer og agenturer (EUT L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

[5] Europa-Parlamentets og Rådets forordning (EU) 2021/887 af 20. maj 2021 om oprettelse af Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed og Netværket af Nationale Koordinationscentre (EUT L 202 af 8.6.2021, s. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[6] Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) nr. 168/2013 og (EU) 2019/1020 og direktiv (EU) 2020/1828 (forordningen om cyberrobusthed) (EUT L, 2024/2847, 20.11. 2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Europa-Parlamentets og Rådets forordning (EU) 2025/38 af 19. december 2024 om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybertrusler og -hændelser og om ændring af forordning (EU) 2021/694 (forordning om cybersolidaritet) (EUT L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] Kommissionens delegerede forordning (EU) 2024/1366 af 11. marts 2024 om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) 2019/943 for så vidt angår fastsættelse af netregler om sektorspecifikke regler for cybersikkerhedsmæssige aspekter af grænseoverskridende elektricitetsstrømme (EUT L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 af 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (EUT L 218 af 14.8.2013, s. 8, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Europa-Parlamentets og Rådets forordning (EU) 2023/1543 af 12. juli 2023 om europæiske editionskendelser og europæiske sikringskendelser om elektronisk bevismateriale i straffesager og om fuldbyrdelse af frihedsstraffe idømt som led i en straffesag og Europa-Parlamentets og Rådets direktiv (EU) 2023/1544 af 12. juli 2023 om harmoniserede regler for udpegning af bestemte forretningssteder og udpegning af retlige repræsentanter med henblik på indsamling af elektronisk bevismateriale i straffesager (EUT L 191 af 28.7.2023, s. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

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

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