EUROPA-
KOMMISSIONEN

Bruxelles, den 24.2.2025
COM(2025) 66 final

2025/0036 (NLE)

Forslag til

RÅDETS HENSTILLING

om en EU-plan for cyberkrisestyring

BEGRUNDELSE

1. BAGGRUND FOR FORSLAGET

• Forslagets begrundelse og formål

I Rådets konklusioner om fremtiden for cybersikkerhed af 22. maj 2024 hed det bl.a. følgende:

> *"[Rådet] opfordrer Kommissionen til hurtigt at evaluere den nuværende plan for cybersikkerhed og på dette grundlag foreslå en revideret plan for cybersikkerhed i form af en henstilling fra Rådet, der vil behandle de nuværende udfordringer og det komplekse cybertrusselsbillede, styrke eksisterende netværk, forbedre samarbejdet og nedbryde siloer mellem organisationer ved først og fremmest at anvende eksisterende strukturer til dette formål. Desuden bør den reviderede plan bygge på gennemprøvede vejledende principper for samarbejde (proportionalitet, subsidiaritet, komplementaritet og fortrolig behandling af oplysninger) og udvide dem til hele krisestyringens livscyklus og bør bidrage til at tilpasse og forbedre sikker kommunikation på cybersikkerhedsområdet. Det bør sikres, at den reviderede plan er forenelig med eksisterende rammer såsom IPCR, EU's cyberdiplomatiske værktøjskasse, den hybride EU-værktøjskasse, beredskabsprotokollen om retshåndhævelse (LERP), nye rammer såsom planen for kritisk infrastruktur, sektorspecifikke procedurer og overordnede krisestyringsstrukturer i EU-enheder, herunder også den højtstående repræsentant og Europol. I denne reviderede plan bør Kommissionens, den højtstående repræsentants og ENISA's rolle i overensstemmelse med deres kompetencer navnlig fokusere på at støtte horisontal koordinering."*

Formålet med dette udkast til Rådets henstilling om EU's plan for cyberkrisestyring (cyberplanen) er på en klar, enkel og tilgængelig måde at præsentere Den Europæiske Unions (EU's) ramme for cyberkrisestyring. Dette bør gøre det muligt for relevante EU-aktører (dvs. individuelle enheder og netværk af enheder på EU-plan) at forstå, hvordan de kan interagere og gøre bedst mulig brug af de tilgængelige mekanismer i hele krisestyringens livscyklus. Den har til formål at forklare, hvad en cyberkrise er, og hvad der udløser en cyberkrisemekanisme på EU-plan. Den forklarer anvendelsen af tilgængelige mekanismer såsom beredskabsmekanismen for cybersikkerhed, herunder EU's cybersikkerhedsreserve, til at forberede, hvordan man håndterer, reagerer på og kommer på fode igen efter en krise som følge af en omfattende cybersikkerhedshændelse. Den har endvidere til formål at fremme et mere struktureret samarbejde mellem civile og militære aktører, herunder samarbejde med Den Nordatlantiske Traktats Organisation (NATO), eftersom en omfattende cyberhændelse, der påvirker Unionens civile infrastruktur, som militæret er afhængigt af, også kan aktivere NATO's reaktionsmekanismer.

Cyberplanen er et ikkebindende instrument, der omhandler specifikke foranstaltninger for relevante aktører i en cyberkrise, og som kan øge den overordnede effektivitet af rammen for cyberkrisestyring. Den ajourfører den plan, der er fastsat i Kommissionens henstilling (EU) 2017/1584 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser, og den bygger på resultaterne og erfaringerne fra øvelser på EU-plan, siden henstillingen blev vedtaget. Den er en del af bredere politiske prioriteter inden for beredskab og sikkerhed.

Som defineret i direktiv (EU) 2022/2555 (NIS 2-direktivet) er en omfattende cybersikkerhedshændelse en hændelse, der forårsager en forstyrrelse, der overstiger en medlemsstats kapacitet til at reagere på den, eller som har en betydelig indvirkning på mindst to medlemsstater. En sådan hændelse kan alt efter årsag og virkning eskalere og udvikle sig til fuldgyldige kriser, der 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.

- **Sammenhæng med de gældende regler på samme område**

Forslaget er i overensstemmelse med relevante EU-instrumenter på cybersikkerhedsområdet, navnlig NIS 2-direktivet og forordning (EU) 2023/2841 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i Unionens institutioner, organer, kontorer og agenturer. Den er også i overensstemmelse med rammerne for EU-civilbeskyttelsesmekanismen, der blev oprettet ved Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU, gennemførelsesafgørelse (EU) 2018/1993 om EU's integrerede ordninger for politisk kriserespons (IPCR) og sektorspecifikke instrumenter til situationsbevidsthed og krisestyring, herunder i elsektoren.

- **Sammenhæng med Unionens politik på andre områder**

Cyberplanen supplerer og er i overensstemmelse med Rådets nyligt vedtagne henstilling om en plan for koordinering af reaktionen på EU-plan på forstyrrelser af kritisk infrastruktur af væsentlig grænseoverskridende relevans, da sidstnævnte omfatter forstyrrelser i forbindelse med ikkecyberrelateret fysisk modstandsdygtighed. Den hænger tæt sammen med krisestyringsmekanismerne og -værktøjerne under den fælles udenrigs- og sikkerhedspolitik (FUSP) og den fælles sikkerheds- og forsvarspolitik (FSFP), som fastsat i Rådets strategiske kompas for sikkerhed og forsvar. Desuden kan EU-initiativer til bekæmpelse af cyberkriminalitet støtte de mål, der forfølges med denne henstilling.

2. RETSGRUNDLAG, NÆRHEDSPRINCIPPET OG PROPORTIONALITETSPRINCIPPET

- **Retsgrundlag**

Forslaget er baseret på artikel 292 i TEUF, som fastsætter de relevante regler for vedtagelse af henstillinger.

Forslaget vil supplere hele den lovgivningsmæssige ramme for cybersikkerhed, der er fastsat på EU-plan. Forslaget omhandler ikke håndtering af større hændelser, der påvirker EU-enheder som omhandlet i forordning 2023/2841, der er vedtaget på grundlag af artikel 298 i TEUF. Det omhandler imidlertid udveksling af oplysninger mellem EU-enheder og medlemsstater, herunder bestemmelserne i forordning 2023/2841 om, at Kommissionens repræsentant i Det Interinstitutionelle Råd for Cybersikkerhed (IICB) skal være kontaktpunkt for at lette IICB's deling af relevante oplysninger i forbindelse med større hændelser med Det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser, EU-CyCLONe, som et bidrag til den fælles situationsbevidsthed.

- **Nærhedsprincippet (for områder, der ikke er omfattet af enekompetence)**

Reaktion på forstyrrelser af kritisk infrastruktur eller af de tjenester, der leveres af væsentlige og vigtige enheder, er først og fremmest medlemsstaternes ansvar, men visse ondsindede cyberaktiviteter af grænseoverskridende karakter kan forstyrre og skade kritiske informationsinfrastrukturer, som er nødvendige for, at det indre marked kan fungere korrekt. Unionen spiller således en vigtig rolle i tilfælde af en væsentlig hændelse eller krise. En sådan forstyrrelse kan påvirke flere eller endda alle dele af den økonomiske aktivitet i det indre marked, og det kan påvirke Unionens sikkerhed og internationale forbindelser. Med henblik på at sikre det indre markeds funktion er koordinering på EU-plan i tilfælde af forstyrrelser af kritisk infrastruktur med betydelige grænseoverskridende virkninger ikke blot

hensigtsmæssig, men også nødvendig. Koordinerede reaktioner på EU-plan vil støtte medlemsstaternes reaktioner på forstyrrelserne gennem fælles situationsbevidsthed, koordineret offentlig kommunikation og afbødning af konsekvenserne af forstyrrelserne på det indre marked.

- **Proportionalitetsprincippet**

Dette forslag er i overensstemmelse med proportionalitetsprincippet, jf. artikel 5, stk. 4, i traktaten om Den Europæiske Union. Hverken indholdet i eller udformningen af dette forslag til Rådets henstilling går videre, end hvad der er nødvendigt for at nå dets mål. De foreslåede foranstaltninger står i et rimeligt forhold til de forfulgte mål, som fokuserer på at sikre en koordineret EU-styring af cyberkriser.

- **Valg af retsakt**

Med henblik på at nå de ovenfor nævnte mål indeholder TEUF bestemmelser, navnlig artikel 292, om, at Rådet kan vedtage henstillinger efter forslag fra Kommissionen. I overensstemmelse med artikel 288 i TEUF er henstillinger ikke bindende. En henstilling fra Rådet er et hensigtsmæssigt instrument i dette tilfælde, da den signalerer medlemsstaternes engagement i de foranstaltninger, der indgår heri, og udgør et stærkt grundlag for samarbejde om koordinering af håndteringen af væsentlige cybersikkerhedshændelser og -kriser. På denne måde vil den foreslåede henstilling supplere den bindende retlige ramme (navnlig NIS 2-direktivet).

3. RESULTATER AF EFTERFØLGENDE EVALUERINGER, HØRINGER AF INTERESSENTER OG KONSEKVENSANALYSER

- **Høringer af interessenter**

I forbindelse med udarbejdelsen af dette forslag gennemførte Kommissionen høringer om revisionen af cyberplanen og opfordrede medlemsstaterne og relevante EU-enheder til at give input. Den tog hensyn til de synspunkter, som medlemsstaternes eksperter og ENISA gav udtryk for på den workshop, som Kommissionen og Polen afholdt i fællesskab den 5. september 2024 i Karpacz.

Kommissionen hørte medlemsstaternes repræsentanter i CSIRT-netværket, EU-CyCLONe og NIS-samarbejdsgruppen på møder i september 2024 og opfordrede til indsendelse af skriftlige bidrag.

Kommissionen fremlagde og indsamlede feedback fra Rådet under to særlige drøftelser i Den Horisontale Gruppe vedrørende Cyberspørgsmål, der blev afholdt i oktober og november 2024.

Kommissionen hørte repræsentanter for den private sektor samt medlemsstaterne, Tjenesten for EU's Optræden Udadtil (EU-Udenrigstjenesten) og ENISA på en workshop, som Polens faste repræsentation ved EU var vært for i Bruxelles i november 2024.

Kommissionen hørte relevante EU-enheder, nemlig EU-Udenrigstjenesten, ENISA, Europol og CERT-EU, herunder gennem drøftelser på højt plan på cyberkrisetaskforcens[1] møder i juli og november 2024.

[1] En uformel gruppe bestående af Kommissionens tjenestegrene og andre EU-tjenester.

Der blev opnået enighed om behovet for et ajourført, klart, enkelt og operationelt dokument, der giver de relevante aktører en forståelse af rammen for cyberkrisestyring, og hvordan de bruger de tilgængelige mekanismer effektivt. Der var også enighed om behovet for at undgå overlapning af instrumenter og gøre god brug af eksisterende mekanismer på EU-plan til koordinering, informationsudveksling og reaktion uden at skabe nye strukturer eller gribe ind i de interne standardprocedurer for eksisterende netværk og eksisterende sektorspecifikke mekanismer.

2025/0036 (NLE)

Forslag til

RÅDETS HENSTILLING

om en EU-plan for cyberkrisestyring

RÅDET FOR DEN EUROPÆISKE UNION,

som henviser til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 292,

som henviser til forslag fra Europa-Kommissionen, og

som tager følgende i betragtning:

(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 cyberhændelser 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 flerdimensionelle hybride trusler 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, der 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 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. Effektiv krisestyring er afgørende for at opretholde den økonomiske stabilitet og beskytte europæiske regeringer, kritisk infrastruktur, borgere og virksomheder samt bidrage til international sikkerhed og stabilitet i cyberspace. Cyberkrisestyring er derfor en integreret del af EU's overordnede krisestyringsramme.

(3) I overensstemmelse med procedurerne i Rådets gennemførelsesafgørelse (EU) 2018/1993[2] træffes en afgørelse om at aktivere og deaktivere EU's integrerede ordninger for politisk kriserespons (IPCR) af formandskabet for Rådet, som (medmindre solidaritetsbestemmelsen er blevet påberåbt) hører de berørte medlemsstater, Kommissionen og den højtstående repræsentant (HR). Desuden kan Generalsekretariatet for Rådet, Kommissionens tjenestegrene og EU-Udenrigstjenesten i henhold til IPCR-procedurerne også i samråd med formandskabet træffe afgørelse om at aktivere IPCR i informationsudvekslingsfunktion. Drøftelserne

[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, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

inden for rammerne af IPCR bygger på rapporter om integreret situationsbevidsthed og analyse udarbejdet af Kommissionens tjenestegrene og Tjenesten for EU's Optræden Udadtil ("EU-Udenrigstjenesten").

(4) Selv om medlemsstaterne har det primære ansvar for styringen af nationale cyberkriser, kræver cybersikkerhedshændelsers potentielle grænseoverskridende og tværsektorielle karakter, at medlemsstaterne og de relevante EU-enheder samarbejder på teknisk, operationelt og politisk plan for at koordinere effektivt i hele Unionen. Samtidig er kriserespons og genopretning dyrt for de berørte enheder og sektorer. Krisestyring i hele livscyklussen omfatter derfor beredskab og fælles situationsbevidsthed for at foregribe cybersikkerhedshændelser, den nødvendige detektionskapacitet til at opdage dem samt de nødvendige respons- og genopretningsværktøjer til at afbøde, afværge og inddæmme cybersikkerhedshændelser.

(5) Kommissionens henstilling (EU) 2017/1584[3] om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser fastsætter målene og metoderne for samarbejde mellem medlemsstaterne og EU-enhederne om at reagere på væsentlige cybersikkerhedshændelser og -kriser. Den kortlagde de relevante aktører på teknisk, operationelt og politisk niveau og forklarede, hvordan de var integreret i Unionens bredere krisestyring, 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).

(6) 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[4], Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[5], Kommissionens gennemførelsesforordning 2024/2690[6], Europa-Parlamentets og Rådets forordning (EU, Euratom) 2023/2841[7], Europa-Parlamentets og Rådets forordning (EU)

---

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

4 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).

5 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).

6 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).

7 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).

2021/887[8], Europa-Parlamentets og Rådets forordning (EU) 2024/2847[9], og Europa-Parlamentets og Rådets forordning (EU) 2025/38 ("forordningen om cybersolidaritet")[10]. De specifikke sektorspecifikke cybersikkerhedskriseforanstaltninger omfatter Kommissionens delegerede forordning (EU) 2024/1366[11] og den kommende ramme for koordinering af systemiske cyberhændelser (EU-SCICF) inden for rammerne af Europa-Parlamentets og Rådets forordning (EU) 2022/2554[12]. Direktiv 2013/40[13] 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[14], vil, når de er gennemført, i væsentlig grad lette retshåndhævelsesindsatsen på dette område. EU's cyberforsvarspolitik[15] skitserer rollerne for et operationelt 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 kriseresponsmekanismer 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"[16] indeholder bestemmelser om samarbejde mellem relevante aktører, hvis en hændelse påvirker både fysiske aspekter af og cybersikkerheden i forbindelse med kritisk infrastruktur.

---

8 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).

9 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).

10 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).

11 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).

12 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).

13 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).

14 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).

15 JOIN(2022) 49 final.

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

(7) På EU-plan omfatter de relevante aktører med ansvar for cyberkrisestyring Kommissionen, EU-Udenrigstjenesten, herunder den fælles efterretningsanalysekapacitet (SIAC), Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), Cybersikkerhedstjenesten for Unionens Institutioner, Organer, Kontorer og Agenturer (CERT-EU), Europol gennem sit Europæiske Center til Bekæmpelse af Cyberkriminalitet (EC3), Det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser (EU-CyCLONe), netværket af enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), EU-Satellitcentret (SATCEN), Galileosikkerhedsovervågningscentret og Unionens netværk af delegationer. Disse EU-aktører bør sammen fastlægge samarbejdsområder og bidrage til gennemførelsen af Unionens ramme for cyberkrisestyring i overensstemmelse med deres beføjelser i henhold til gældende lovgivning.

(8) En ajourført henstilling om en plan for cybersikkerhed ("cyberplanen") er nødvendig for at give klar og tilgængelig vejledning, der forklarer, hvad en cyberkrise på EU-plan er, hvordan krisestyringsrammen udløses, og hvilke roller relevante aktører og mekanismer på EU-plan spiller, samt samspillet mellem disse aktører og mekanismer i hele cyberkrisens livscyklus. Cyberplanen skal ses i en bredere sammenhæng med de civil-militære forbindelser og forbindelserne mellem EU og NATO.

(9) Denne henstilling supplerer de integrerede ordninger for politisk kriserespons (IPCR) og Unionens bredere krisemekanismer, herunder Kommissionens overordnede hurtige varslingssystem ARGUS, EU-civilbeskyttelsesmekanismen, der støttes af Katastrofeberedskabskoordinationscentret (ERCC), EU-Udenrigstjenestens krisereaktionsmekanisme (CRM), samt andre processer såsom dem, der er beskrevet i den hybride EU-værktøjskasse[17] og i den reviderede EU-protokol for imødegåelse af hybride trusler. Den supplerer og bør også være i overensstemmelse med Rådets henstilling om en plan for koordinering af en reaktion på EU-plan på forstyrrelser af kritisk infrastruktur af væsentlig grænseoverskridende relevans ("planen for kritisk infrastruktur"), som omfatter ikkecyberrelateret fysisk modstandsdygtighed, og som har til formål at forbedre koordineringen af indsatsen på EU-plan på dette område.

(10) En omfattende og integreret tilgang til krisestyring bør fremmes på tværs af alle sektorer og forvaltningsniveauer. Den tværsektorielle krisestyring på EU-plan bør styrkes for at give mulighed for en integreret kriserespons, navnlig i tilfælde, hvor cyberhændelser har reelle konsekvenser. Hvis cybersikkerhedshændelser er en del af en bredere hybrid kampagne eller krise, bør de relevante aktører støtte bestræbelserne på at udvikle et ensartet situationsbillede på tværs af flere sektorer og områder. Henstillingen bidrager til bredere beredskabsforanstaltninger, der er nødvendige for Unionen over for flerdimensionelle hybride trusler [i overensstemmelse med principperne i strategien for en beredskabsunion].

(11) Sikkerheden i kritisk digital infrastruktur er afgørende for modstandsdygtigheden i Unionens økonomi, samfund og forsvar. Enheder, der er omfattet af anvendelsesområdet for direktiv (EU) 2022/2555, herunder dem, der leverer undersøiske kommunikationskabler, skal træffe foranstaltninger til at beskytte den fysiske og miljømæssige sikkerhed i net- og informationssystemer baseret på en tilgang, der omfatter alle farer, såsom systemsvigt, menneskelige fejl, ondsindede handlinger eller naturfænomener. Desuden bør disse enheder indberette hændelser, herunder hændelser i forbindelse med undersøiske kommunikationskabler, til

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

CSIRT'erne eller, hvor det er relevant, til den kompetente myndighed. Selv om de grundlæggende principper, der ligger til grund for cyberplanen, er relevante for sikkerheden for undersøiske kabler, er mekanismerne deri ikke tilstrækkeligt omfattende til at dække hele cyklussen for modstandsdygtighed over for kriser. Dens særlige karakter kræver en samordnet og skræddersyet indsats for at imødekomme behovene for integreret trusselsovervågning og situationsbevidsthed for havområderne omkring EU, strategiske investeringer for at opbygge reserver og en fælles europæisk tilgang til at øge reparations- og genopretningskapaciteten. EU-strategien for maritim sikkerhed omfatter foranstaltninger til forbedring af cybersikkerheden på det maritime område og til forbedring af overvågningen og beskyttelsen af kritisk maritim infrastruktur, herunder undersøiske kabler. I forbindelse med krisestyring på EU-plan kunne man overveje et specifikt netværk af nationale kontaktpunkter og tætte civil-militære interaktioner, herunder med NATO.

(12) Kriseberedskab kræver en omfattende risikovurdering af alle farer og trusler i betragtning af konvergensen mellem EU's økonomiske og sikkerhedsmæssige interesser. En fælles EU-situationsbevidsthed blandt medlemsstaterne og EU-enhederne, der fremmes ved at nå til enighed om et fælles klassificeringssystem og sikre kommunikationskanaler, bør muliggøre en koordineret og informeret reaktion på potentielle og omfattende cybersikkerhedshændelser samt afskrækkelse af vedholdende trusselsaktører. Med udgangspunkt i need-to-know-princippet og i betragtning af betydningen af tillid til informationsudvekslingen kan grupper af medlemsstater i forskellige konfigurationer og, hvor det er relevant, relevante EU-enheder eventuelt samarbejde og dele oplysninger, der er relevante for håndteringen af cyberhændelser. Hvis medlemsstater og EU-enheder deler oplysninger om trusler, risici og manglende modenhed, bør det være muligt at fastsætte de rette prioriteter for sunde investeringer og konkrete tiltag, der vil føre til bedre cyberrobusthed.

(13) I overensstemmelse med artikel 6 i forordning (EU) 2019/881 udarbejder ENISA i tæt samarbejde med medlemsstaterne en regelmæssig tilbundsgående teknisk EU-cybersikkerhedsrapport om hændelser og cybertrusler. Denne rapport benævnes EU's fælles cybervurderingsrapport (EU-JCAR) og udarbejdes sammen med Europol/EC3 og CERT-EU med henblik på at styrke Unionens beredskab, da den tilvejebringer situationsbevidsthed på grundlag af en analyse af hændelser og cybertrusler.

(14) Central kritisk infrastruktur såsom energi, transport, digital infrastruktur, sundhed og finansielle tjenester samt de sikkerhedsløsninger, der anvendes til at beskytte den, drives normalt af private virksomheder. Beskyttelse af denne infrastruktur mod omfattende cyberhændelser kræver et tæt samarbejde mellem offentlige og private enheder, herunder producenter og open source-udviklere, bygget på tillid og klare og dedikerede procedurer for informationsudveksling, formidling og koordinering af indsatsen.

(15) Cyberøvelser på EU-plan er et yderst effektivt redskab til at teste procedurer og samarbejdsmekanismer og dermed styrke beredskabet. Da øvelserne er ressourcekrævende, skal øvelsesdagsordenen være så strømlinet og konsolideret som muligt og tage hensyn til de scenarier, der er udviklet i EU-koordinerede risikovurderinger og andre relevante initiativer.

(16) De digitale infrastrukturer i Europa har mange dybt forankrede tekniske afhængigheder. Disse bør håndteres for at sikre driftskontinuitet i en krise. Dette vedrører f.eks. domænenavnesystemet (DNS), som er en afgørende komponent, der understøtter internettets drift. DNS-resolvere er afgørende for at få adgang til

internettet, herunder under en større cyberkrise, da de oversætter internetdomænenavne til IP-adresser. Direktiv (EU) 2022/2555 tilskynder relevante interessenter til at vedtage en diversificeringsstrategi for DNS-oversættelser. Det tilskynder også medlemsstaterne til at fremme udviklingen og anvendelsen af en offentlig og sikker europæisk DNS-oversættelsestjeneste som en central foranstaltning til at sikre kriseberedskab og modstandsdygtighed.

(17) For at øge modstandsdygtigheden af andre kritiske komponenter, såsom routingsystemet, og sikre deres funktionalitet under større cyberkriser, er det desuden afgørende at implementere tilsvarende bedste praksis og de seneste tilgængelige standarder rettidigt. Gennemførelsesforordning (EU) 2024/2690 giver derfor mandat til at oprette et multiinteressentforum for at udpege de bedste tilgængelige standarder og implementeringsteknikker for væsentlige cybersikkerhedselementer og tilskynder til deltagelse fra relevante enheder.

(18) En koordineret tilgang er nødvendig for at opdage ondsindet aktivitet i de stadig mere komplekse globale forsyningskæder, der kan have en indvirkning på EU-plan. Dette er navnlig relevant på områder, hvor Unionen er afhængig af teknologi fra højrisikoleverandører, der er underlagt et tredjelands jurisdiktion, som kræver, at oplysninger om software- eller hardwaresårbarheder indberettes til myndighederne, inden de vides at blive udnyttet. Statsstøttede aktører kan også placere sig i kritisk infrastruktur med den hensigt at forårsage forstyrrelser på et senere tidspunkt, f.eks. under en konflikt. Dette er vanskeligt at opdage ved hjælp af traditionelle metoder, da trusselsaktører skjuler deres aktiviteter ved at blande sig med legitim trafik og anvende de såkaldte "living off the land"-teknikker, som bruger legitime værktøjer og processer til at skjule ondsindede aktiviteter. Det samme gælder for tredjelande, hvor trusselsaktører, der opererer fra disse lande, ifølge offentlige erklæringer fra Unionen eller dens medlemsstater har udført ondsindede cyberaktiviteter mod Unionen. Forsyningskæderne bør blive mere modstandsdygtige og diversificerede, samtidig med at der anvendes et fælles udgangspunkt for beredskab.

(19) På teknisk plan spiller CSIRT'er, retshåndhævende myndigheder samt de nationale og grænseoverskridende cyberknudepunkter (cyberknudepunkter), der skal oprettes i henhold til forordning (EU) 2025/38, en afgørende rolle i at opdage hændelser, cybertrusler og sårbarheder og støtte den tekniske ansvarsfordeling og genopretning efter cyberangreb. Effektive proceduremæssige ordninger for samarbejde mellem CSIRT-netværket og EU-CyCLONe, som krævet i direktiv (EU) 2022/2555, er afgørende. Den europæiske varslingsmekanisme for cybersikkerhed har til formål at støtte udviklingen af avanceret kapacitet for Unionen med henblik på at forbedre detektions-, analyse- og databehandlingskapaciteten i forbindelse med cybertrusler og forebyggelse af hændelser i Unionen.

(20) Med hensyn til øjeblikkelig reaktion omfatter de mekanismer, der er til rådighed for medlemsstaterne, EU's cybersikkerhedsreserve og foranstaltninger til støtte for gensidig bistand, der er oprettet i henhold til forordning (EU) 2025/38, EU-hybridberedskabshold og PESCO's cyberberedskabshold (CRRT'er) samt mekanismer til støtte for NATO-allierede. Desuden støtter EU's beredskabsprotokol om retshåndhævelse (LEERP) EU's 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 efterforskningen, herunder konfliktløsning på retshåndhævelsesniveau og koordinering med ikkeretshåndhævende partnere. Opnåelse af et klart billede af, hvilke reaktionsmuligheder der er tilgængelige i tilfælde

af cyberhændelser og hybride aktiviteter, og hvordan de anvendes, kan sikre en effektiv ressourceallokering og forhindre dobbeltarbejde. I henhold til forordning (EU) 2025/38 skal medlemsstaterne derfor underrette CSIRT-netværket og EU-CyCLONe, når de anmoder om støtte fra EU's cybersikkerhedsreserve.

(21) Effektiv bekæmpelse af cyberkriminalitet er afgørende for cybersikkerhed. Afskrækkelse kan ikke opnås gennem modstandsdygtighed alene, men kræver også identifikation, retsforfølgning og reaktion over for lovovertrædere. Samarbejde gennem tilpassede tekniske systemer og platforme og udveksling af relevante oplysninger mellem cybersikkerhedsaktører, cyberdiplomatiske enheder og retshåndhævende myndigheder er derfor afgørende for at sikre en omfattende forståelse af trusselsbilledet og være i stand til at reagere på en sammenhængende og koordineret måde.

(22) Kriser skaber usikkerhed, som modstandere nemt kan udnytte til at sprede desinformation og så mistillid. For at imødegå dette er det vigtigt med en klar og sammenhængende offentlig kommunikation om situationen, og hvilke skridt der tages for at afhjælpe den. En koordineret strategisk kommunikation kan også støtte diplomatiske tiltag over for vedvarende trusselsaktører og udviklingen af en fortælling om trusler mod Unionen, dens afskrækkende foranstaltninger og behovet for at fremme ansvarlig statslig adfærd i cyberspace.

(23) For at sikre en effektiv krisestyring er det nødvendigt at finde frem til fælles sikre kommunikationsløsninger på cyberområdet og gennemføre dem i hele Unionen, herunder om nødvendigt med henblik på udveksling af EU's klassificerede oplysninger. Efter anmodning fra Rådet kortlagde Kommissionen og andre relevante EU-enheder eksisterende sikre kommunikationsværktøjer og fremlagde resultaterne i december 2022. Der er flere af de eksisterende særskilte tiltag fra EU-enhedernes side for at opbygge sikker kommunikationskapacitet i en krise, der kræver bedre koordinering og udnyttelse. Dette omfatter oprettelsen af et EU-system for kritisk kommunikation (EUCCS) for at øge den offentlige kommunikationsinfrastrukturs modstandsdygtighed over for ondsindet indblanding og forbedre det daglige operationelle samarbejde, herunder på tværs af grænser.

(24) Unionens sikkerhedsmiljø kræver en tilgang til civilt og militært beredskab og parathed, der omfatter alle farer og inddrager alle myndigheder og hele samfundet. Militære organer er afhængige af kritisk civil infrastruktur såsom kommunikation, energi, sundhed, transport og logistik. I overensstemmelse hermed og som understreget i EU's cyberforsvarspolitik[18] kræver EU's cybersikkerhed større samarbejde og synergier mellem civile og militære netværks beredskabs- og indsatskapacitet, herunder i tilfælde af et væbnet angreb. Cybersikkerhedsaktører bør samarbejde på tværs af institutionelle og operationelle siloer for at foregribe og imødegå truslen om multisektorielle og flerdimensionelle forstyrrelser i overensstemmelse med principperne[, der skal integreres] i strategien for en beredskabsunion. Desuden spiller ondsindet cyberaktivitet en stadig større rolle i bredere hybride kampagner mod Unionen, dens medlemsstater og strategiske partnere. Der er derfor behov for et stærkere samarbejde mellem Unionen og NATO.

(25) På det militære område udgør det fremtidige EU-Koordinationscenter for Cyberforsvar og den fælles efterretningsanalysekapacitet (SIAC) inden for Tjenesten for EU's Optræden Udadtil, det operationelle netværk for militære IT-beredskabsenheder

[18] EU's cyberforsvarspolitik, JOIN(2022) 49 final.

(MICNET) og EU's konference for cyberøverstbefalende, der støttes af Det Europæiske Forsvarsagentur (EDA), samt relevante projekter under det permanente strukturerede samarbejde (PESCO) vigtige aktører og initiativer til koordinering og samarbejde om beredskab med henblik på opdagelse, afskrækkelse af og forsvar mod og genopretning efter cybertrusler, der påvirker Unionen og medlemsstaterne. Der bør derfor tilskyndes til samarbejde mellem civile og militære aktører såsom samarbejdet mellem EU-CyCLONe og EU's konference for cyberøverstbefalende samt det potentielle samarbejde mellem MICNET og CSIRT-netværket.

(26) Samarbejde med strategiske internationale partnerlande og organisationer uden for Unionen styrker Unionens cybersikkerhedskapacitet. Ved at fremme internationalt samarbejde kan Unionen og dens partnere sikre fælles situationsbevidsthed og sammenhæng i cyberkrisestyringen og en robust sikkerhedsstatus og dermed bidrage til et globalt, åbent, stabilt, sikkert og modstandsdygtigt cyberspace. Dette samarbejde bør være baseret på tillid og det fælles mål om at beskytte kritisk infrastruktur og væsentlige tjenester mod cybertrusler, herunder ved at fremme ansvarlig statslig adfærd i cyberspace baseret på De Forenede Nationers (FN's) rammer og ved at holde trusselsaktører ansvarlige for deres uansvarlige og ulovlige adfærd i cyberspace. Cyberdiplomatiske foranstaltninger bidrager til afskrækkelse af og reaktion på ondsindede cyberaktiviteter og sikrer koordinering og samarbejde med strategiske internationale partnerlande.

HENSTILLER:

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

(1) I denne henstilling fastlægges EU-rammen for cyberkrisestyring inden for rammerne af EU's overordnede beredskab over for flerdimensionelle hybride trusler. Hvordan en hændelse kan eskalere til en omfattende hændelse og derefter til en krise på EU-plan, illustreres og sammenfattes i bilag 1, herunder når en sådan hændelse falder sammen med andre hybride trusler, der kræver interaktion mellem de nødvendige reaktioner. Rammen for cyberkrisestyring bør gøre det muligt for relevante aktører på EU-plan, herunder enheder og netværk, at forstå, hvordan de kan interagere og gøre bedst mulig brug af de eksisterende mekanismer, der er opført i bilag II, i hele krisestyringens livscyklus. Den indeholder desuden anbefalinger til disse aktører på EU-plan til, hvordan de eksisterende mekanismers effektivitet kan forbedres.

(2) Unionen og dens medlemsstater bør følge cyberplanen i forbindelse med håndteringen af en krise, der opstår som følge af en omfattende cybersikkerhedshændelse, som defineret i artikel 6, nr. 7), i direktiv (EU) 2022/2555, som påvirker det indre markeds korrekte funktion eller udgør alvorlige risici for den offentlige sikkerhed for enheder eller borgere i flere medlemsstater eller Unionen som helhed ("cyberkrise").

(3) Når en cybersikkerhedshændelse, der opdages på teknisk plan af en CSIRT eller et cyberknudepunkt, resulterer i en eskalering i henhold til CSIRT-netværkets interne procedurer, bør passende oplysninger deles med EU-CyCLONe i overensstemmelse med relevante proceduremæssige ordninger, hvor det igen bør overvejes, om den udgør en potentiel eller igangværende omfattende hændelse som defineret i artikel 6, nr. 7), i direktiv (EU) 2022/2555. Afgørelsen af, om en cyberkrise eksisterer eller ophører med at eksistere som følge af denne omfattende hændelse, bør foretages i overensstemmelse med gennemførelsesafgørelse (EU) 2018/1993 og særlig artikel 4 og 5 deri.

(4) I overensstemmelse med proportionalitetsprincippet, nærhedsprincippet, komplementariteten og den fortrolige behandling af oplysningerne i bilag III bør medlemsstaterne og EU-enhederne uddybe deres samarbejde om cyberkrisestyring, fremme gensidig tillid og bygge på eksisterende netværk og mekanismer. Cyberplanen griber ikke ind i, hvordan enheder definerer deres interne procedurer, men hver enhed bør klart definere de grænseflader, der anvendes i arbejdet med andre enheder. Disse grænseflader bør aftales i fællesskab mellem de berørte enheder og dokumenteres klart.

(5) Cyberplanen bør anvendes i overensstemmelse med planen for kritisk infrastruktur, navnlig i tilfælde af hændelser, der påvirker både den fysiske modstandsdygtighed og cybersikkerheden i kritisk infrastruktur[19]. Hvis der er sektorspecifikke krisestyringsforanstaltninger, der dækker cybersikkerhedshændelser, bør disse foranstaltninger gennemføres i overensstemmelse med denne henstilling.

II: Forberedelse på en cyberkrise på EU-plan

(a) Situationsbevidsthed og informationsudveksling

(6) Verificerede, pålidelige data, herunder tendenser inden for hændelser, taktikker, teknikker og procedurer, og aktivt udnyttede sårbarheder bør danne grundlag for en fælles situationsbevidsthed blandt medlemsstaterne og EU-enhederne om cybertrusselsbilledet. Denne fælles viden bør anvendes af medlemsstaterne og EU-enhederne til at foregribe, forberede sig på og opdage cyberangreb i overensstemmelse med deres respektive ansvarsområder. Denne fælles situationsbevidsthed bør:

(a) finde anvendelse på alle kritiske sektorer, der er opført i direktiv (EU) 2022/2555, navnlig kommunikation, digital infrastruktur, energi, transport, finans, rummet og sundhed, og bør også finde anvendelse via CERT-EU på EU-enhedernes net og systemer i overensstemmelse med forordning (EU, Euratom) 2023/2841

(b) være baseret på diversificerede og integrerede datasæt af høj kvalitet, der indsamles, behandles og deles i realtid

(c) tages i betragtning i den fælles cybervurderingsrapport (JCAR) og andre relevante produkter

(d) tage hensyn til relaterede hybride trusler, herunder udenlandsk informationsmanipulation og indblanding (FIMI) og desinformation

(e) støtte kortsigtede foranstaltninger og indsatsforanstaltninger samt bidrage til langsigtet politisk planlægning i forbindelse med beredskab og afskrækkelse

(f) [linke til andre risiko- og trusselsvurderinger, der udarbejdes regelmæssigt og styrkes af strategien for en beredskabsunion for at sikre synergier og forenkling af medlemsstaternes rapporteringsforpligtelser.]

(7) EU-CyCLONe og CSIRTs-netværket bør

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

[19] Planen for kritisk infrastruktur indeholder yderligere oplysninger om koordinering i sådanne tilfælde i bilagets del I, afsnit 4.

(b) fortsætte med at opbygge et tillidspræget klima mellem medlemmerne

(c) gøre fuld brug af de tilgængelige værktøjer til informationsdeling.

(8) Medlemsstaterne og relevante EU-enheder bør forbedre metoderne til at koordinere og indgå partnerskaber med den private sektor, herunder open source-fællesskaber og producenter, for at forbedre informationsudvekslingen på grundlag af eksisterende informationsudvekslings- og analysecentre på EU-plan og nationalt plan, for at øge cybersikkerhedskapaciteten og reagere på cybersikkerhedshændelser, herunder gennem rundbordsdrøftelser med EU-CyCLONe og CSIRT-netværket.

(9) Medlemsstaterne og relevante EU-enheder kan med henblik på at fremme samarbejdet og styrke tilliden og på grundlag af ordningerne for udveksling af cybersikkerhedsoplysninger i direktiv (EU) 2022/2555 og bestemmelserne i forordning (EU) 2025/38 om cyberknudepunkter skabe frivillige samarbejdsklynger efter need-to-know-princippet, hvor der er fælles bekymringer, såsom afskrækkelse fra, opdagelse af eller reaktion på en bestemt type trussel, som kun rammer dem. Sådanne klynger bør respektere de relevante aktørers mandat samt allerede etablerede strukturer. Disse samarbejdsklynger kan opfordre EU-enheder til at fremme deres samarbejde, herunder via passende infrastruktur.

(10) Medlemsstaterne bør gennem NIS-samarbejdsgruppen, der er nedsat ved direktiv (EU) 2022/2555, senest 12 måneder efter vedtagelsen af cyberplanen udarbejde en fælles taksonomi med hensyn til cyberkrisestyring samt en vejledning om sikker håndtering og udveksling af oplysninger vedrørende cybersikkerhedshændelser og -kriser, herunder et afsnit om fastlæggelse af fortrolighedsniveauet for disse oplysninger (kategorisering).

(11) Ved fastlæggelsen af fortrolighedsniveauet for de tilgængelige oplysninger bør medlemsstaterne og relevante EU-enheder tage hensyn til den potentielle indvirkning, som overklassificering kan have på frivillig udveksling af oplysninger og opnåelse af en fælles situationsbevidsthed. Når medlemsstaterne udveksler ikkeklassificerede oplysninger, 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.

b) Fælles øvelser

(12) Medlemsstaterne og relevante EU-enheder bør udvikle en effektiv rullende cyklus af cyberøvelser for at forberede sig på cyberkriser og styrke den organisatoriske effektivitet. Disse øvelser bør baseres på de scenarier, der er udviklet på grundlag af EU-koordinerede risikovurderinger, herunder dem, der vedrører tværsektorielle kriser. Den rullende cyklus af cyberøvelser bør tage hensyn til EU-civilbeskyttelsesmekanismen og andre kriseresponsmekanismer på EU-plan. Den bør sikre, at erfaringerne fra øvelserne føres ud i praksis.

(13) Relevante EU-aktører kan gennemføre mindre øvelser for at teste deres interaktioner og grænseflader i tilfælde af eskalerende cyberhændelser.

(14) Kommissionens tjenestegrene, EU-Udenrigstjenesten og ENISA opfordres til at tilrettelægge en øvelse for at teste cyberplanen inden for 18 måneder efter vedtagelsen af cyberplanen med inddragelse af alle relevante aktører, herunder den private sektor.

c) DNS-oversættelseskapacitet

(15) Medlemsstaterne, relevante EU-enheder samt private enheder såsom operatører af kritisk infrastruktur bør styrke deres diversificeringsstrategi for DNS-oversættelse (domænenavnsystem), herunder anvendelsen af mindst én EU-baseret DNS-infrastruktur såsom DNS4EU for at sikre pålidelig DNS-oversættelse under større kriser. ENISA og EU-CyCLONe bør udvikle og levere failover i nødsituationer, der skitserer trinnene for at skifte til EU-baseret DNS-infrastruktur, hvis andre DNS-tjenester svigter, og dermed sikre kontinuitet i kritiske tjenester under en krise.

(16) Desuden bør nationale cyberknudepunkter og grænseoverskridende cyberknudepunkter dele relevante oplysninger om trusler med sådanne EU-baserede DNS-infrastrukturer for at støtte dem i at yde et højt beskyttelsesniveau mod EU-specifikke trusler og dermed yderligere øge kapaciteten til at opdage og afbøde EU-specifikke trusler.

(17) For generelt at styrke sikkerheden og tilgængeligheden af kritisk internetinfrastruktur, også under kriser, bør medlemsstaterne aktivt fremme deltagelsen af alle relevante interessenter – herunder dem, der ikke er direkte omfattet af NIS2-gennemførelsesretsakten – i det bemyndigede multiinteressentforum, der har til opgave at finde de bedste tilgængelige standarder og implementeringsteknikker for vigtige netsikkerhedsforanstaltninger. Desuden bør medlemsstaterne overveje at deltage i forummet og selv vedtage de anbefalede retningslinjer.

d) Ressourcer

(18) Medlemsstaterne bør gøre fuld brug af de finansielle ressourcer, der er til rådighed til cybersikkerhed fra relevante EU-programmer.

III: Opdagelse af en hændelse, der kan eskalere til en cyberkrise

(19) Cyberhændelser bliver mere og mere komplekse, og det bliver stadig sværere at opdage dem, og derfor bør både offentlige og private enheder indføre trusselsbaserede detektionsstrategier på tværs af deres digitale infrastrukturer for at identificere mulig prædeployering, der efterfølgende kan udnyttes til afbrydelsesformål. Når der identificeres skjulte operationer, bør enheder proaktivt dele relevante oplysninger med deres partnere i god tid, inden situationer eskalerer til kriser.

(20) Alle aktører bør i overensstemmelse med deres respektive mandater og på grundlag af en tilgang, der omfatter alle farer, bidrage med oplysninger, der peger mod en potentiel cyberkrise, til relevante netværk.

(21) CSIRT-netværket og EU-CyCLONe bør 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.

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

(23) De grænseoverskridende cyberknudepunkter, der allerede er oprettet eller skal oprettes i henhold til forordning (EU) 2025/38, bør bidrage med relevante oplysninger til mekanismerne på EU-plan i tilfælde af en potentiel eller igangværende omfattende cybersikkerhedshændelse baseret på tilgangen, der omfatter alle farer, herunder fysisk skade på kritisk infrastruktur, som

kompromitterer 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.

(24) Hvis der konstateres en potentiel eller omfattende cybersikkerhedshændelse med indvirkning på flere sektorer:

(a) bør Kommissionen fremme 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

(b) bør de relevante EU-enheder støtte EU-CyCLONe i vurderingen af konsekvenserne for sektorer og befolkningen.

IV: Reaktion på en cyberkrise på EU-plan

(25) I tilfælde af en cyberkrise, der er konstateret under IPCR, bør alle aktører sikre tæt koordinering med andre enheder, der reagerer på bredere hybride trusler i en tilgang, der omfatter alle myndigheder, som følger:

(a) Den eller de berørte medlemsstater og CSIRT-netværket bør samarbejde om hurtigt at genoprette kompromitterede systemer og sikre minimale driftsforstyrrelser.

(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 rapporten om integreret situationsbevidsthed og analyse (ISAA) under IPCR-ordningerne.

(c) Kommissionen bør i samarbejde med den højtstående repræsentant, hvor det er relevant, sikre sammenhæng og koordinering mellem reaktionerne på krisen og relaterede indsatsforanstaltninger på EU-plan, navnlig relevante sektorspecifikke krisestyringsmekanismer på EU-plan, der er opført i bilag 2, og i forbindelse med anmodningen om bistand gennem EU-civilbeskyttelsesmekanismen.

(d) Rådets formandskab bør overveje at indbyde formanden for EU-CyCLONe til uformelle rundbordsmøder og andre relevante rådsmøder under IPCR-ordningerne.

(e) Rådet bør med støtte fra EU-CyCLONe og relevante EU-enheder koordinere indsatsen for offentlig kommunikation, herunder for at sikre, at krisesituationen ikke anvendes til at sprede unøjagtige oplysninger.

(f) Den højtstående repræsentant bør i tæt samarbejde med Kommissionen og andre relevante EU-enheder støtte beslutningstagningen i Rådet, herunder gennem analyser og rapporter, om anvendelsen af mulige foranstaltninger som led i den 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 sikkerhedsstatus og fremme international fred, sikkerhed og stabilitet i cyberspace.

(g) Kommissionen, den højtstående repræsentant og medlemsstaterne bør også udnytte økonomiske værktøjer såsom handelsforbud mere effektivt for bedre at forebygge, afværge og reagere på vedvarende ondsindede cyberaktiviteter fra statslige aktørers side.

(26) Hvis en bruger af de tjenester, der leveres af EU's cybersikkerhedsreserve[20], anmoder om tjenester fra EU's cybersikkerhedsreserve i overensstemmelse med artikel 15 i forordning (EU) 2025/38 og med forbehold af eventuelle fremtidige gennemførelsesretsakter i henhold til nævnte forordning, gælder følgende:

(a) Tjenesterne bør leveres inden for 24 timer efter anmodningen.

(b) Kommissionen og den højtstående repræsentant bør sikre koordinering med yderligere foranstaltninger i overensstemmelse med den hybride værktøjskasse[21] i tilfælde af ondsindede cyberaktiviteter, der er en del af en bredere hybrid kampagne.

(c) I tilfælde af ondsindet cyberaktivitet med en militær dimension bør den anmodende medlemsstat underrette Unionens konference af cyberøverstbefalende om sin anmodning.

(27) I tilfælde af en omfattende cybersikkerhedshændelse, der påvirker den korrekte funktion af rumtjenester, der er afgørende for Unionens eller dens medlemsstaters sikkerhed, bør EU-CyCLONe underrette den højtstående repræsentant med henblik på at koordinere en eventuel reaktion med den struktur for reaktion på rumtrusler, der er oprettet i overensstemmelse med Rådets afgørelse (FUSP) 2021/698.

V: Genopretning efter en cyberkrise

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

VI: Sikker kommunikation

(29) Baseret på kortlægning af eksisterende sikre kommunikationsværktøjer[22] bør Kommissionen, den højtstående repræsentant, EU-CyCLONe, CSIRT-netværket og relevante EU-enheder inden udgangen af 2026 nå til enighed om et interoperabelt sæt sikre kommunikationsløsninger for relevante EU-aktører. Disse løsninger bør dække hele spektret af de nødvendige kommunikationsmetoder (tale, data, videokonferencer (VTC), meddelelser, samarbejde og dokumentdeling og høring). Løsningerne bør afspejle centrale principper såsom Unionens sikkerhedsinteresser, teknologisk suverænitet og fortrolighed samt funktioner såsom anvendelighed, indbygget sikkerhed, certificering foretaget af europæiske informationssikkerhedsorganer, end-to-end-kryptering, autentifikation, tilgængelighed og post-kvantekryptografi. Løsningerne bør opfylde fælles definerede krav til beskyttelse af følsomme ikkeklassificerede oplysninger og omfatte værktøjer til udveksling af RESTREINT UE/EU RESTRICTED-oplysninger.

---

20 EU's cybersikkerhedsreserve er en mekanisme, der består af tjenester fra betroede udbydere af administrerede sikkerhedstjenester, der leveres på anmodning til støtte for indsatsen og iværksættelse af de indledende genopretningsforanstaltninger i tilfælde af væsentlige cybersikkerhedshændelser, omfattende cybersikkerhedshændelser eller cybersikkerhedshændelser svarende til omfattende cybersikkerhedshændelser, der påvirker medlemsstaterne, EU's institutioner, organer eller agenturer eller tredjelande, der er associeret til programmet for et digitalt Europa.

21 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.

22 HWPCI WK 862/23.

(30) På dette grundlag bør aktører på EU-plan anvende løsninger baseret på Matrix-protokollen til realtidskommunikation. Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed (ECCC), der er oprettet ved forordning (EU) 2021/887, 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 disse værktøjer.

(31) 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.

(32) På mellemlang sigt bør der etableres kommunikations- og informationsudvekslingsmekanismer mellem retshåndhævelses- og cybersikkerhedsnetværk, navnlig på teknisk plan, med henblik på en effektiv kriserespons. Disse mekanismer bør respektere hver parts rolle og undgå at forstyrre igangværende operationer. Kommissionen samarbejder med medlemsstaterne om at oprette EU-systemet for kritisk kommunikation (EUCCS), som senest i 2030 bør forbinde kommunikationsnetværkene for retshåndhævelse og civilbeskyttelse i hele Schengenområdet, således at kritisk kommunikationsudstyr kan anvendes på andre medlemsstaters område. EUCCS kan derfor også gavne den fælles indsats med relevante cybersamfund. Dette system bør omfatte backup-kommunikation gennem f.eks. satellitkommunikation.

VII: Koordinering af cyberkriser med militære aktører

(33) EU-CyCLONe og EU's konference for cyberøverstbefalende, MICNET og CSIRT-netværket samt et fremtidigt EU-Koordinationscenter for Cyberforsvar og dets civile EU-modparter bør samarbejde om at udvikle fælles situationsbevidsthed mellem civile og militære aktører.

(34) Unionen bør under hensyntagen til eksisterende aftaler såsom den tekniske aftale mellem CERT-EU og NATO fra 2016 bestræbe sig på at oprette kontaktpunkter for koordinering med NATO i tilfælde af en cyberkrise for at udveksle nødvendige oplysninger om situationen og anvendelsen af kriseresponsmekanismer. Med henblik herpå bør Unionen undersøge, hvordan kapaciteten til informationsudveksling med NATO kan forbedres, herunder gennem mulige sammenkoblinger mellem deres respektive kommunikations- og informationssystemer.

(35) Hvis en medlemsstat i forbindelse med en cybersikkerhedshændelse anvender relevante forsvarsinitiativer såsom PESCO's CRRT'er eller andre relevante initiativer såsom EU-hybridberedskabshold (HRRT'er), bør den underrette EU-CyCLONe samt EU's konference for cyberøverstbefalende.

VIII: Samarbejde med strategiske partnere

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

(a) hvis der identificeres en relevant hændelse, lette formidlingen af nødvendige oplysninger til strategiske partnere

(b) styrke koordineringen med strategiske partnere om reaktionen på vedvarende ondsindede cyberaktiviteter fra vedvarende trusselsaktørers side, navnlig ved anvendelse af den cyberdiplomatiske værktøjskasse, i overensstemmelse med gennemførelsesretningslinjerne.

(37) 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 cyberhændelser.

(38) Som led i den rullende øvelsescyklus, der er omhandlet i afsnit II ovenfor, bør Kommissionens tjenestegrene og EU-Udenrigstjenesten overveje at tilrettelægge en fælles personaleøvelse for at afprøve samarbejdet mellem både civile og militære komponenter i tilfælde af en omfattende cyberhændelse, der berører EU-medlemsstater og NATO-allierede, herunder når NATO-traktatens artikel 4 eller 5 udløses eller sandsynligvis vil blive udløst.

(39) I betragtning af kandidatlandenes udsatte position og potentialet for cyberhændelser i Unionens naboskabsområde, bør fælles øvelser med deltagelse af kandidatlande overvejes.

Udfærdiget i Bruxelles, den .

På Rådets vegne

Formand