Europeiska unionens råd

Bryssel den 6 juni 2025
(OR. en)

9794/25

Interinstitutionellt ärende:
2025/0036(NLE)

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

LÄGESRAPPORT

från:	Rådets generalsekretariat
av den:	6 juni 2025
till:	Delegationerna
Ärende:	Rådets rekommendation om en EU-plan för hantering av cybersäkerhetskriser – Rådets rekommendation som godkändes av rådet vid mötet den 6 juni 2025

För delegationerna bifogas rådets rekommendation, som godkändes av rådet vid mötet den 6 juni 2025.

BILAGA

RÅDETS REKOMMENDATION

om en EU-plan för hantering av cyberkriser

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA REKOMMENDATION

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artiklarna 114 och 292,

med beaktande av Europeiska kommissionens förslag, och

av följande skäl:

(1) Digital teknik och global konnektivitet är ryggraden i unionens ekonomiska tillväxt och konkurrenskraft och i omställningen av kritisk infrastruktur. En sammanlänkad och alltmer digital ekonomi ökar dock också risken för cybersäkerhetsincidenter och cyberattacker. Växande geopolitiska spänningar, konflikter och strategisk rivalitet återspeglas dessutom i den skadliga cyberverksamhetens effekter, volym och grad av sofistikering. Sådan verksamhet kan utgöra en del av hybridkampanjer eller militära operationer. Den kan också direkt påverka unionens säkerhet, ekonomi och samhälle. Den har dessutom potential till spridningseffekter, särskilt när den riktar sig mot internationella strategiska partnerländer såsom kandidatländer eller grannländer.

(2) En storskalig cybersäkerhetsincident kan orsaka störningar som är så omfattande att den berörda medlemsstaten inte kan hantera dem eller som har en betydande påverkan på fler än en medlemsstat. Beroende på orsak och inverkan kan en sådan incident eskalera och förvandlas till en fullt utvecklad kris som hindrar den inre marknaden från att fungera korrekt eller som allvarligt hotar den allmänna tryggheten och säkerheten för entiteter eller medborgare i flera medlemsstater eller i unionen som helhet. Effektiv krishantering är avgörande för att upprätthålla ekonomisk stabilitet och skydda europeiska förvaltningar, kritisk infrastruktur, företag och medborgare samt bidra till internationell säkerhet och stabilitet i cyberrymden. Hantering av cyberkriser är därmed en integrerad del av EU:s övergripande krishanteringsram.

(3) Med tanke på att unionsentiteternas IKT-miljöer är sammankopplade med medlemsstaternas IKT-miljöer och att dessa är ömsesidigt beroende av varandra, kan en incident hos en unionsentitet utgöra en cybersäkerhetsrisk för medlemsstaterna och vice versa. Utbyte av relevant information och samordning med avseende på både storskaliga cybersäkerhetsincidenter och större incidenter enligt definitionen i artikel 3.8 i förordning (EU, Euratom) 2023/2841[1] är avgörande för EU-planen för hantering av cyberkriser (*cyberplanen*).

[1] Europaparlamentets och rådets förordning (EU, Euratom) 2023/2841 av den 13 december 2023 om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer (OJ L, 2023/2841, 18.12.2023, s. 1).

(4) I händelse av en kris för vilken EU-arrangemangen för integrerad politisk krishantering (*IPCR*) enligt rådets genomförandebeslut (EU) 2018/1993[2] (*IPCR-arrangemang*) har aktiverats bör cyberplanen fullt ut respektera IPCR-arrangemangen vad gäller samordning och insatser. Den politiska och strategiska samordningen bör ske inom ramen för IPCR. IPCR-arrangemangen är ett verktyg för horisontell samordning och horisontella insatser på unionspolitisk nivå. I enlighet med IPCR-arrangemangen fattas beslutet om att aktivera eller avaktivera IPCR av ordförandeskapet för Europeiska unionens råd. Rapporter om integrerad situationsmedvetenhet och analys (*ISAA-rapporter*) som utarbetas av kommissionens avdelningar och Europeiska utrikestjänsten (*utrikestjänsten*) bidrar till IPCR-arbetet, både i dess läge för informationsutbyte och dess lägen för full aktivering.

(5) Medlemsstaterna har huvudansvaret för hanteringen av cybersäkerhetsincidenter och cyberkriser. Cybersäkerhetsincidenternas potentiella gränsöverskridande och sektorsövergripande karaktär kräver emellertid att medlemsstaterna och de berörda unionsentiteterna samarbetar på teknisk, operativ och politisk nivå för att effektivt samordna sig i hela unionen. Hantering av cyberkriser under hela deras livscykel omfattar beredskap och gemensam situationsmedvetenhet för att förutse storskaliga cybersäkerhetsincidenter, den detektionskapacitet som krävs för att identifiera de reaktions- och återhämtningsverktyg som behövs för att mildra och begränsa storskaliga cybersäkerhetsincidenter samt en insatsförmåga som kan avskräcka från och förebygga ytterligare incidenter.

[2] Rådets genomförandebeslut (EU) 2018/1993 av den 11 december 2018 om EU-arrangemangen för integrerad politisk krishantering (EUT L 320, 17.12.2018, s. 28).

(6) I kommissionens rekommendation (EU) 2017/1584[3] om samordnade insatser vid storskaliga cyberincidenter och cyberkriser fastställs mål för och former av samarbete mellan medlemsstaterna och unionens entiteter vid hantering av storskaliga cybersäkerhetsincidenter och cyberkriser. Där redogörs för de aktörer som berörs på teknisk, operativ och politisk nivå och hur de ingår i unionens befintliga krishanteringsmekanismer, t.ex. IPCR-arrangemangen. De grundläggande principerna i rekommendation (EU) 2017/1584 – subsidiaritet, komplementaritet och konfidentialitet för information – är fortfarande giltiga, liksom uppdelningen i tre nivåer (teknisk, operativ och politisk). Den här rekommendationen bygger på dessa grundläggande principer och är avsedd att ersätta rekommendation (EU) 2017/1584 genom att fastställa en ny unionsram för hantering av cybersäkerhetskriser.

(7) Vissa definitioner som används i den här rekommendationen bygger på definitioner och termer som används i direktiv (EU) 2022/2555[4]. Tillämpningsområdet för den här rekommendationen skiljer sig dock från tillämpningsområdet för direktiv (EU) 2022/2555. I denna rekommendation fastställs unionens ram för cyberkrishantering inom ramen för EU:s övergripande beredskap för storskaliga cybersäkerhetsincidenter och cyberkriser som uppstår till följd av sådana incidenter, oavsett vilken sektor eller enhet som berörs. I möjligaste mån bygger definitionerna på definitionerna i direktiv (EU) 2022/2555.

---

[3] Kommissionens rekommendation (EU) 2017/1584 av den 13 september 2017 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser (EUT L 239, 19.9.2017, s. 36).

[4] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80).

(8) En uppdaterad cyberplan krävs för att tillhandahålla tydlig och tillgänglig vägledning som förklarar vad en storskalig cybersäkerhetsincident eller en cyberkris på unionsnivå är, hur krishanteringsramen utlöses, vilka roller de berörda nätverken, aktörerna och mekanismerna på unionsnivå spelar samt hur dessa aktörer och mekanismer samverkar under cyberkrisens hela livscykel. Syftet med cyberplanen är att stödja den bredare ramen för EU:s civil-militära förbindelser vid cyberkrishantering, bland annat mot bakgrund av de allt närmare förbindelserna mellan EU och Nato, där så är möjligt även genom inkluderande, ömsesidiga och icke-diskriminerande förbättrade mekanismer för informationsutbyte vid cyberkrishantering.

(9) Den sektorsövergripande krishanteringen på unionsnivå bör förbättras för att möjliggöra integrerad krishantering, särskilt när storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser får fysiska konsekvenser. Denna rekommendation kompletterar IPCR-arrangemangen och unionens övriga krishanteringsmekanismer, inbegripet kommissionens allmänna förvarningssystem Argus, unionens civilskyddsmekanism med stöd av Centrumet för samordning av katastrofberedskap (ERCC), som inrättats inom ramen för civilskyddsmekanismen genom Europaparlamentets och rådets beslut nr 1313/2013/EU om en civilskyddsmekanism för unionen[5], utrikestjänstens krishanteringsmekanism samt andra processer, såsom de som beskrivs i EU:s verktygslåda för cyberdiplomati[6], verktygslådan för hantering av hybridhot[7] och i EU:s reviderade protokoll för att motverka hybridhot[8]. Den kompletterar och bör också vara förenlig med rådets rekommendation (EU) 2024/4371 om en plan för samordnade insatser på unionsnivå vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse[9] (*EU-planen för kritisk infrastruktur*), som handlar om fysisk, icke-cyberrelaterad resiliens och syftar till att förbättra samordningen av insatserna på unionsnivå på det här området.

---

5 Europaparlamentets och rådets beslut nr 1313/2013/EU av den 17 december 2013 om en civilskyddsmekanism för unionen (EUT L 347, 20.12.2013, s. 924).

6 Rådets slutsatser om en ram för en gemensam diplomatisk respons från EU mot skadlig it-verksamhet (9916/17).

7 Rådets slutsatser om en ram för en samordnad EU-reaktion på hybridkampanjer, 22 juni 2022.

8 Gemensamt arbetsdokument från kommissionens avdelningar, *EU Protocol for countering hybrid threats* (inte översatt till svenska) (SWD(2023) 116 final).

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

(10) Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) är ett nätverk för samordning av hanteringen av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser på operativ nivå, även vid sektorsövergripande storskaliga cybersäkerhetsincidenter och cyberkriser. För att inte ytterligare komplicera de befintliga ramarna bör man undvika att skapa sektorsspecifika strukturer som överlappar EU-CyCLONes arbetsuppgifter. EU-CyCLONe bör få operativ information om cybersäkerhet även från sektorerna och bidra med underlag på politisk nivå.

(11) Medlemsstaterna uppmanas att fullt ut utnyttja de ekonomiska resurser som finns tillgängliga för cybersäkerhet via berörda unionsprogram. Det bör säkerställas att dessa program medför så små administrativa bördor som möjligt för dem som ansöker om finansiering och att medlemsstaternas medverkan i programmen underlättas genom relevant vägledning om genomförbara alternativ för ekonomiskt stöd.

(12) Rekommendationen bidrar till bredare beredskapsåtgärder som krävs för att unionen ska kunna hantera sektorsövergripande kriser i linje med principerna i EU:s strategi för en beredskapsunion, nämligen en integrerad myndighetsövergripande och samhällsövergripande allriskstrategi, i synnerhet vad gäller att förbättra medvetenheten om risker och hot samt sektorsövergripande krishantering.

HÄRIGENOM REKOMMENDERAS FÖLJANDE.

I: Syfte, tillämpningsområde och vägledande principer för EU:s ram för hantering av cyberkriser

Syfte och tillämpningsområde

1. I den här rekommendationen om en EU-plan för hantering av cyberkriser (*cyberplanen*) fastställs unionens ram för hantering av cyberkriser inom ramen för EU:s övergripande beredskap för storskaliga cybersäkerhetsincidenter och cyberkriser. Ramen återspeglar både medlemsstaternas och unionens institutioners, organs och byråers (*unionsentiteters*) roller inom ramen för deras respektive befogenheter, med full respekt för nationell rätt och interna regler, för att säkerställa övergripande och samordnade åtgärder på unionsnivå.

2. Cyberplanen bör tillämpas i överensstämmelse med EU-planen för kritisk infrastruktur, särskilt när det gäller incidenter som påverkar både den fysiska resiliensen och cybersäkerheten för kritisk infrastruktur[10].

3. Cyberplanen ger vägledning för insatser vid storskaliga cybersäkerhetsincidenter eller cyberkriser, och den bör användas som komplement till alla relevanta sektoriella insatsmekanismer, såsom de som förtecknas i bilaga II. Berörda parter inom cybersäkerhet bör hjälpa till och bistå med att uppnå målen för dessa sektoriella mekanismer, både på nationell nivå och unionsnivå.

4. I händelse av en EU-omfattande sektorsövergripande kris med cyberaspekter för vilken IPCR aktiveras bör samordningen av insatserna på unionspolitisk nivå utföras av rådet med hjälp av IPCR-arrangemangen. När IPCR har aktiverats bör åtgärder inom ramen för cyberplanen stödja EU:s insatser på politisk nivå och ge särskilt stöd i fråga om cybersäkerhet.

[10] I del I avsnitt 4 i bilagan till EU-planen för kritisk infrastruktur ges en närmare beskrivning av samordningen i sådana fall.

Vägledande principer

5. Följande vägledande principer gäller för cyberkrishantering på unionsnivå:

a) *Proportionalitet*: De flesta cybersäkerhetsincidenter som påverkar medlemsstaterna är inte så omfattande att de betraktas som en storskalig cybersäkerhetsincident eller en cyberkris på nationell nivå eller unionsnivå. Vid cybersäkerhetsincidenter och cybersäkerhetshot samarbetar medlemsstaterna och utbyter frivilligt och regelbundet information inom nätverket för enheter för hantering av it-säkerhetsincidenter (*CSIRT-nätverket*) och EU-CyCLONe, i enlighet med nätverkens standardiserade tillvägagångssätt (SOP).

b) *Subsidiaritet*: Medlemsstaterna har huvudansvaret för insatserna för att hantera och avhjälpa en eventuell cybersäkerhetsincident, en storskalig cybersäkerhetsincident eller en cyberkris som drabbar dem. Med tanke på potentiella gränsöverskridande effekter bör rådet, kommissionen, den höga representanten, Europeiska unionens cybersäkerhetsbyrå (Enisa), cybersäkerhetstjänsten för unionens institutioner, organ och byråer (CERT-EU), Europol och alla andra relevanta unionsentiteter samarbeta under hela krislivscykeln. Deras roller har stöd i unionsrätten och återspeglar hur storskaliga cybersäkerhetsincidenter och cyberkriser påverkar en eller flera branscher på den inre marknaden, unionens säkerhet och internationella förbindelser, liksom unionsentiteterna själva.

c) *Komplementaritet*: Den här rekommendationen beaktar fullt ut befintliga krishanteringsmekanismer på unionsnivå enligt bilaga II, i synnerhet IPCR-arrangemangen, Argus och utrikestjänstens krishanteringsmekanism. Rekommendationen tar hänsyn till CSIRT-nätverkets och EU-CyCLONes mandat samt förordning (EU, Euratom) 2023/2841. Om IPCR aktiveras bör arbetet i relevanta nätverk, entiteter och aktiverade sektoriella mekanismer fortsätta, och det bör bidra med underlag och stöd för den politiska och strategiska samordning som äger rum inom IPCR.

d) *Konfidentialitet för information*: Allt informationsutbyte inom ramen för denna rekommendation bör följa tillämpliga regler om säkerhet och skydd av personuppgifter. Informella avtal om konfidentialitet, såsom Traffic Light Protocol för märkning av känslig information, bör beaktas när så är lämpligt. För utbyte av säkerhetsskyddsklassificerade uppgifter, oavsett vilket klassificeringssystem som tillämpas, bör befintliga bindande regler och avtal om behandling av säkerhetsskyddsklassificerade uppgifter användas tillsammans med tillgängliga ackrediterade verktyg.

6. I enlighet med de ovannämnda vägledande principerna bör medlemsstaterna och unionsentiteterna fördjupa sitt samarbete i fråga om hantering av cyberkriser, främja ömsesidigt förtroende och bygga vidare på befintliga nätverk och mekanismer. Genomförandet av artiklarna 22 och 23 i förordning (EU, Euratom) 2023/2841 gynnar detta samarbete inom ramen för cyberplanen. I synnerhet bidrar den cyberkrishanteringsplan som upprättats på grundval av artikel 23 i förordning (EU, Euratom) 2023/2841 bland annat till det regelbundna utbytet av relevant information mellan unionsentiteter och med medlemsstater, och fastställer arrangemang för samordning och informationsflöde mellan unionsentiteter.

II. Definitioner

7. I denna cyberplan gäller följande definitioner:

a) *incident*: en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem.

b) *betydande incident*: en incident som

a) har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för den berörda entiteten,

b) har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

c) *storskalig cybersäkerhetsincident*: en incident som orsakar störningar som är så omfattande att den berörda medlemsstaten inte kan hantera dem eller som har en betydande påverkan på minst två medlemsstater.

d) *cyberkris*: en storskalig cybersäkerhetsincident som eskalerat till en fullt utvecklad kris som hindrar den inre marknaden från att fungera korrekt eller som allvarligt hotar den allmänna tryggheten och säkerheten för entiteter eller medborgare i flera medlemsstater eller i unionen som helhet.

III: Nationella strukturer och ansvarsområden för cyberkrishantering

8. Medlemsstaterna har huvudansvaret för insatserna i händelse av storskaliga cybersäkerhetsincidenter eller cyberkriser som drabbar dem. Varje medlemsstat har, i enlighet med direktiv (EU) 2022/2555, en eller flera cyberkrishanteringsmyndigheter samt en eller flera CSIRT-enheter.

9. Genom antagandet av direktiv (EU) 2022/2555 och andra lagstiftningsinstrument och andra instrument på cybersäkerhetsområdet har medlemsstaterna anpassat sina ramverk för cybersäkerhet genom att fastställa minimiregler för ett fungerande samordnat regelverk, genom att fastställa mekanismer för effektivt samarbete mellan de ansvariga myndigheterna i varje medlemsstat och genom att föreskriva effektiva rättsmedel och efterlevnadskontrollåtgärder, vilket är centralt för att upprätthålla en effektiv kontroll av att dessa skyldigheter efterlevs.

10. I enlighet med artikel 9.4 i direktiv (EU) 2022/2555 bör medlemsstaterna anta nationella planer för hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Dessa planer omfattar bland annat nationella beredskapsåtgärder, förfaranden för hantering av cyberkriser och nationella förfaranden och arrangemang mellan nationella myndigheter och organ för att säkerställa att de på ett ändamålsenligt sätt kan delta i och stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och cyberkriser på unionsnivå. Cyberkrishanteringsförfarandena innefattar även bestämmelser om dessas integrering i den allmänna nationella ramen för krishantering och kanaler för informationsutbyte.

11. I enlighet med artikel 9.1 i direktiv (EU) 2022/2555 ska medlemsstaterna säkerställa samstämmighet med befintliga ramar för allmän nationell krishantering. Vid aktivering av IPCR bör de nationella krishanteringsmyndigheterna i syfte att informera IPCR samla in synpunkter från cyberkrishanteringsmyndigheterna och nationella sektorsspecifika krismekanismer.

12. I enlighet med artikel 9.5 i direktiv (EU) 2022/2555 bör EU-CyCLONe, på begäran av en berörd medlemsstat, utbyta information om relevanta delar av nationella planer för hanteringen av storskaliga cybersäkerhetsincidenter och kriser, särskilt om bestämmelserna för att säkerställa ett ändamålsenligt deltagande i och stöd till en samordnad hantering av storskaliga cybersäkerhetsincidenter och cyberkriser på unionsnivå, i syfte att utbyta bästa praxis och överväga om den övergripande ramen skulle fungera i praktiken.

13. EU-CyCLONe och den interinstitutionella cybersäkerhetsstyrelsen uppmanas att vid behov utbyta information om samstämmigheten mellan den krishanteringsplan som cybersäkerhetsstyrelsen upprättar i enlighet med artikel 23 i förordning (EU, Euratom) 2023/2841 och de nationella planerna för hanteringen av storskaliga cybersäkerhetsincidenter och kriser.

14. EU-CyCLONe bör, med stöd av Enisa som sekretariat, upprätthålla en aktuell förteckning över nationella cyberkrishanteringsmyndigheter med kontaktuppgifter till EU-CyCLONes tjänstemän och chefer, och göra den tillgänglig för EU-CyCLONes medlemmar.

IV: Huvudsakliga nätverk och aktörer i EU:s ekosystem för hantering av cyberkriser

15. CSIRT-nätverket är det huvudsakliga tekniska nätverket för utbyte av relevant information om incidenter, särskilt inom tillämpningsområdet för denna rekommendation, i enlighet med de relevanta uppgifter som beskrivs i artikel 15.3 i direktiv (EU) 2022/2555. Det bidrar till uppbyggandet av förtroende och tillit och främjar ett snabbt och ändamålsenligt operativt samarbete mellan medlemsstaterna. Ordföranden för CSIRT-nätverket får delta som observatör i den interinstitutionella cybersäkerhetsstyrelsen.

16. CERT-EU är alla unionsentiteters cybersäkerhetstjänst. CERT-EU fungerar som unionsentiteternas nav för utbyte av cybersäkerhetsinformation och samordning av incidenthantering i enlighet med artikel 13 i förordning (EU) 2023/2841. CERT-EU är medlem i CSIRT-nätverket och stöder kommissionen i EU-CyCLONe. CERT-EU verkar på teknisk nivå och ansvarar för att samordna hanteringen av större incidenter som påverkar unionsentiteterna.

17. EU-CyCLONe fungerar som en mellanhand mellan den tekniska och politiska nivån, särskilt under storskaliga cybersäkerhetsincidenter och cyberkriser. EU-CyCLONe stöder en samordnad hantering av storskaliga cybersäkerhetsincidenter och cyberkriser på operativ nivå och säkerställer ett regelbundet utbyte av relevant information mellan medlemsstaterna och unionens institutioner, organ och byråer i enlighet med artikel 16 i direktiv (EU) 2022/2555. Ordföranden för EU-CyCLONe får delta som observatör i den interinstitutionella cybersäkerhetsstyrelsen.

18. Enisa är den unionsbyrå som utför de uppgifter som tilldelas enligt förordning (EU) 2019/881[11] i syfte att uppnå en hög gemensam cybersäkerhetsnivå i hela unionen, bland annat genom att aktivt stödja medlemsstaterna och unionens institutioner, organ och byråer. Enisa fungerar bland annat som sekretariat för CSIRT-nätverket och EU-CyCLONe, tillhandahåller tjänster för situationsmedvetenhet och bistår medlemsstaterna genom att regelbundet anordna cybersäkerhetsövningar på unionsnivå. I enlighet med direktiv (EU) 2022/2555 och förordning (EU) 2024/2847[12] får Enisa information om betydande gränsöverskridande incidenter och aktivt utnyttjade sårbarheter och incidenter som påverkar digitala produkter.

19. Europeiska unionens råd (*rådet*) är den institution som fastställer politik och fungerar samordnande i enlighet med artikel 16 i fördraget om Europeiska unionen (*EU-fördraget*) och anförtros IPCR, som rör samordning och hantering på unionspolitisk nivå. Rådet verkar genom rådets olika konstellationer, Ständiga representanternas kommitté och relevanta förberedande rådsorgan, särskilt den övergripande arbetsgruppen för cyberfrågor, samt, i förekommande fall, IPCR-arrangemangen.

---

[11] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).

[12] Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) (EUT L, 2024/2847, 20.11.2024, s. 1).

20. Kommissionen är, i egenskap av den institution som främjar unionens allmänna intresse och tar lämpliga initiativ i detta syfte samt säkerställer tillämpningen av fördragen och av åtgärder som antagits av institutionerna i enlighet med artikel 17 i EU-fördraget, ansvarig för vissa allmänna beredskapsåtgärder på unionsnivå och vissa åtgärder avseende situationsmedvetenhet, inbegripet förvaltningen av ERCC och det gemensamma kommunikations- och informationssystem för olyckor (Cecis), i enlighet med beslutet om unionens civilskyddsmekanism. Den underlättar samstämmighet och samordning mellan relaterade krishanteringsåtgärder på unionsnivå när det gäller den operativa nivån. Den rådfrågas om beslut om att aktivera eller avaktivera IPCR. Kommissionens avdelningar utarbetar tillsammans med utrikestjänsten ISAA-rapporterna. Den är medlem i EU-CyCLONe i fall där en potentiell eller pågående storskalig cybersäkerhetsincident har eller sannolikt kommer att ha en betydande inverkan på tjänster och verksamhet som omfattas av direktiv (EU) 2022/2555, och observatör i övriga fall. Den är den interinstitutionella cybersäkerhetsstyrelsens kontaktpunkt för EU-CyCLONe. Den är observatör i CSIRT-nätverket.

21. Den höga representanten för utrikes frågor och säkerhetspolitik (*den höga representanten*), biträdd av utrikestjänsten, leder unionens gemensamma utrikes- och säkerhetspolitik (Gusp) och bidrar genom sina förslag till utvecklingen av denna politik, inbegripet den gemensamma säkerhets- och försvarspolitiken (GSFP). Detta inbegriper diplomatiska, underrättelserelaterade och militära strukturer och mekanismer, särskilt den gemensamma kapaciteten för underrättelseanalys (SIAC) som gemensam kontaktpunkt för medlemsstaternas underrättelser, EU:s militära stab (EUMS) som källa till militär expertis, EU:s verktygslåda för cyberdiplomati samt nätverket av EU-delegationer, vilka kan bidra till krishantering från en yttre dimension. Utrikestjänsten utarbetar också ISAA-rapporterna tillsammans med kommissionen.

22. I bilaga II beskrivs roller och befogenheter för relevanta aktörer på unionsnivå när det gäller hantering av cyberkriser, inbegripet huvudsakliga nätverk och aktörer.

V: Förberedelser inför storskaliga cybersäkerhetsincidenter och en cyberkris

Hotbild

23. Medlemsstaterna och relevanta unionsentiteter bör vidta nödvändiga åtgärder för att förbättra situationsmedvetenheten, med kännedom om att hotbilden och den incidentspecifika situationsmedvetenheten kräver olika arbetssätt. Medlemsstaterna och relevanta unionsentiteter bör samarbeta på grundval av verifierade, tillförlitliga uppgifter, inbegripet om trender när det gäller incidenter, taktik, metoder och förfaranden, och aktivt utnyttjade sårbarheter.

24. När medlemsstaterna delar information på EU-nivå bör de fullt ut utnyttja befintliga plattformar för tekniskt och operativt samarbete, t.ex. de som används av CSIRT-nätverket och EU-CyCLONe.

25. För att öka den gemensamma situationsmedvetenheten och underlätta bedömningen av inverkan på EU bör EU-CyCLONe och CSIRT-nätverket med stöd av Enisa använda en internt överenskommen rapporteringsmekanism för att ta fram en EU-översikt över teknisk och operativ verksamhet på grundval av den information som samlas in på nationell nivå.

26. EU-CyCLONe och CSIRT-nätverket bör

    a) samarbeta för att förbättra informationsutbytet mellan den tekniska och den operativa nivån och situationsmedvetenheten som helhet,

    b) fortsätta att bygga upp förtroende mellan sina medlemmar och mellan nätverken,

    c) fullt ut utnyttja de tillgängliga verktygen för informationsutbyte, med stöd av Enisa, överväga hur dessa verktyg kan förbättras och säkerställa interoperabilitet mellan nätverken.

27. EU-CyCLONe, CSIRT-nätverket och den interinstitutionella cybersäkerhetsstyrelsen bör samarbeta för att säkerställa ett effektivt utbyte av relevant information.

28. Enisa har, i egenskap av sekretariat för CSIRT-nätverket och EU-CyCLONe, en central roll när det gäller att stödja medlemsstaterna och unionens institutioner, organ och byråer för att skapa en gemensam situationsmedvetenhet för EU på teknisk och operativ nivå till stöd för förberedelserna inför storskaliga cybersäkerhetsincidenter och kriser.

29. I enlighet med direktiv (EU) 2022/2555 och förordning (EU) 2019/881 bör medlemsstaterna och relevanta unionsentiteter samordna med den privata sektorn, inbegripet grupper och tillverkare som arbetar med öppen källkod, för att förbättra informationsutbytet. I synnerhet Enisa bör utnyttja sitt partnerskapsprogram i detta avseende. Dessutom skulle medlemsstaterna och relevanta unionsentiteter också kunna bygga vidare på befintliga informations- och analyscentraler på EU-nivå och nationell nivå i syfte att öka cybersäkerhetskapaciteten och reagera på cybersäkerhetsincidenter, bland annat genom gemensamma möten mellan den privata sektorn och EU-CyCLONe eller CSIRT-nätverket.

30. För att förbättra informationsutbytet inom och mellan nätverken, och för att klargöra de ömsesidiga förväntningarna på ett sådant utbyte, bör EU-CyCLONe, med stöd av Enisa som sekretariat och efter samråd med CSIRT-nätverket och samarbetsgruppen för nät- och informationssäkerhet, inom 24 månader från och med denna rekommendations antagande enas om en gemensam anpassad taxonomi för incidenternas allvarlighetsgrad. Denna taxonomi bör möjliggöra jämförelser av incidenternas allvarlighetsgrad mellan medlemsstaterna genom beaktande av inverkan på tillhandahållandet av tjänster, antalet berörda entiteter och deras respektive relevans, inverkan på andra tjänster och annan infrastruktur samt den ekonomiska, anseendemässiga och politiska skada som åsamkas. Den bör bygga på relevanta befintliga skalor eller taxonomier, såsom *Reference Incident Classification Taxonomy*.

Teknisk nivå

31. CSIRT-nätverket är plattformen för tekniskt samarbete och informationsutbyte mellan alla medlemsstater och, genom CERT-EU, med unionens entiteter.

32. I enlighet med direktiv (EU) 2022/2555 har varje CSIRT-enhet till uppgift att övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå. CSIRT-enheterna bör, både inom CSIRT-nätverket och bilateralt, utbyta relevant information om incidenter, tillbud, cyberhot, risker och sårbarheter för att skapa en gemensam situationsmedvetenhet.

33. För att stärka det operativa samarbetet på unionsnivå bör CSIRT-nätverket överväga att bjuda in unionens organ och byråer som arbetar med frågor som rör cybersäkerhetspolitiken, såsom Europol, att delta i dess arbete.

34. I enlighet med förordning 2023/2841 bör CERT-EU samla in, hantera, analysera och dela information med unionens institutioner, organ och byråer om cyberhot, sårbarheter och incidenter som rör icke-säkerhetsskyddsklassificerad IKT-infrastruktur och vid behov utfärda specifika förslag till den interinstitutionella cybersäkerhetsstyrelsen om riktlinjer och rekommendationer till unionens institutioner, organ och byråer. CERT-EU bör samarbeta och utbyta information med medlemsstaternas motparter, bland annat genom CSIRT-nätverket.

Operativ nivå

35. I enlighet med direktiv (EU) 2022/2555 bör EU-CyCLONe fungera som en plattform för samarbete mellan medlemsstaternas cyberkrishanteringsmyndigheter och genom kommissionen med relevanta unionsentiteter i syfte att öka beredskapen för hantering av storskaliga cybersäkerhetsincidenter och cyberkriser och utveckla en gemensam situationsmedvetenhet om storskaliga cybersäkerhetsincidenter och cyberkriser.

36. I enlighet med direktiv (EU) 2022/2555 och förordning (EU) 2024/2847 får Enisa information om betydande gränsöverskridande incidenter och aktivt utnyttjade sårbarheter och incidenter som påverkar digitala produkter. Enisa bör i sin roll som sekretariat ge CSIRT-nätverket och EU-CyCLONe råd i syfte att stödja nätverken när det gäller att avgöra om ytterligare åtgärder bör vidtas och för att bidra till den gemensamma situationsmedvetenheten.

Politisk nivå

37. Medlemsstaterna och relevanta unionsentiteter bör övervaka internationell utveckling som påverkar cybersäkerheten (inbegripet cyberhot, hybridhot och utländsk informationsmanipulering och inblandning, inbegripet desinformation, i förekommande fall). Initiativ såsom de tekniska lägesrapporterna om cybersäkerheten i EU, SIAC:s analyser och andra relevanta produkter som ger specialiserade insikter bör beaktas.

38. Den höga representanten bör fortsätta att informera och involvera medlemsstaterna i unionens diplomatiska insatser med koppling till cyberhot, särskilt sådana som involverar statliga aktörer, dennes kontakter med tredjeländer och internationella organisationer, inbegripet Nato, och genomförandet av diplomatiska åtgärder, inbegripet restriktiva åtgärder.

39. Ordförandeskapet i Europeiska unionens råd får lansera en övervakningssida på IPCR-webbplattformen där medlemsstaterna och EU:s institutioner och organ kan utbyta information om en eventuell kris som håller på att utvecklas.

Gemensamma övningar

40. Kommissionen bör, i samordning med den höga representanten och med stöd av Enisa, efter samråd med EU-CyCLONe och CSIRT-nätverket, sammanställa ett effektivt löpande årligt program för cyberövningar för att man ska kunna förbereda sig inför cyberkriser och öka den organisatoriska effektiviteten. Det löpande programmet för cyberövningar bör ta hänsyn till övningar inom ramen för unionens civilskyddsmekanism och andra krishanteringsmekanismer på unionsnivå, inbegripet den övning som beskrivs i EU-planen för kritisk infrastruktur. Det första löpande programmet bör utarbetas inom tolv månader från cyberplanens antagande, och efterföljande program bör slutföras senast den 31 mars varje år. Det löpande programmet bör föreläggas rådet för kännedom.

41. Det löpande programmet bör också innehålla övningar som utarbetas med hjälp av EU:s scenarier för samordnad riskbedömning. Det bör innehålla övningar där alla berörda aktörer medverkar, särskilt den privata sektorn och Nato.

42. Enisa bör, i sin roll som sekretariat för CSIRT-nätverket och EU-CyCLONe, säkerställa en systematisk insamling av lärdomar från övningar samt identifiering av och förslag till sätt att genomföra de resulterande åtgärderna i syfte att garantera att de verkställs på ett ändamålsenligt sätt och inverkar positivt på EU:s gemensamma resiliens, inbegripet respektive standardiserade tillvägagångssätt.

43. Alla aktörer och nätverk bör förbättra samordningen i händelse av en storskalig cybersäkerhetsincident eller cyberkris på grundval av lärdomarna från övningarna. I synnerhet bör EU-CyCLONe och CSIRT-nätverket ta itu med de utmaningar som identifieras under övningarna för att förbättra samordningen, särskilt de som rör samarbetet mellan nätverken och, vid behov, snabbt anpassa de standardiserade tillvägagångssätten.

44. Samarbetsgruppen för nät- och informationssäkerhet bör uppmana CSIRT-nätverket, EU-CyCLONe och Enisa att redogöra för de lärdomar som dragits av övningarna samt för identifieringen av och förslagen till sätt att genomföra de resulterande åtgärderna.

45. Rådet får uppmana ordförandena för CSIRT-nätverket, EU-CyCLONe, samarbetsgruppen för nät- och informationssäkerhet och Enisa att redogöra för hur lärdomarna från övningarna har genomförts.

46. Enisa uppmanas att i samarbete med kommissionen och den höga representanten anordna en övning för att testa cyberplanen under nästa Cyber Europe-övning. Alla berörda aktörer bör delta i övningen, även den politiska nivån. Enisa uppmanas att samordna den politiska nivåns medverkan med ordförandeskapet i Europeiska unionens råd. Den privata sektorn och Nato kan också medverka vid övningen.

VI: Upptäckt av en incident som kan trappas upp till en storskalig cybersäkerhetsincident eller cyberkris

47. Alla aktörer bör, i enlighet med sina respektive mandat och på grundval av en allriskstrategi, bidra med information som indikerar en potentiell storskalig cybersäkerhetsincident eller cyberkris till relevanta nätverk.

48. I enlighet med förordning (EU) 2025/38[13] bör de gränsöverskridande cybernaven, om de erhåller information om en potentiell eller pågående storskalig cybersäkerhetsincident, för att skapa en gemensam situationsmedvetenhet säkerställa att relevant information tillhandahålls medlemsstaternas myndigheter och kommissionen genom EU-CyCLONe och CSIRT-nätverket utan onödigt dröjsmål.

[13] Europaparlamentets och rådets förordning (EU) 2025/38 av den 19 december 2024 om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter och om ändring av förordning (EU) 2021/694 (cybersolidaritetsförordningen) (EUT L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

49. När en betydande incident observeras, i synnerhet om den har omedelbar inverkan, kan den anmälas till eller upptäckas av en CSIRT-enhet samt av medlemsstaternas cyberkrishanteringsmyndigheter eller andra sektorsmyndigheter. Medlemsstaterna uppmanas att utbyta information om sådana incidenter inom nätverken, som bör överväga att vidta lämpliga åtgärder. CSIRT-nätverket respektive EU-CyCLONe kan aktiveras oberoende av varandra beroende på incidentens karaktär och vilka insatser som krävs. Båda nätverken uppmanas dock att fortsätta samarbeta med varandra på grundval av överenskomna förfaranden. Ett beslut om aktivering fattas uteslutande och självständigt av respektive nätverk.

50. CSIRT-nätverket bör ge EU-CyCLONe råd om huruvida en observerad cybersäkerhetsincident kan betraktas som en potentiell eller pågående storskalig cybersäkerhetsincident.

51. Såsom anges i direktiv (EU) 2022/2555 bör CSIRT-nätverket och EU-CyCLONe utan dröjsmål komma överens om förfaranden som ska tillämpas i händelse av en potentiell eller pågående storskalig cybersäkerhetsincident, för att säkerställa teknisk och operativ samordning samt aktuell och relevant information till den politiska nivån.

VII: Hantering av en storskalig cybersäkerhetsincident eller cyberkris på unionsnivå

Hantering av en storskalig cybersäkerhetsincident eller cyberkris för vilken IPCR inte har aktiverats fullt ut

52. För en effektiv hantering av storskaliga cybersäkerhetsincidenter eller cyberkriser på EU-nivå krävs ett effektivt tekniskt, operativt och politiskt samarbete inom ramen för en myndighetsövergripande strategi, inbegripet brottsbekämpning där så är möjligt.

53. På varje nivå bör de berörda aktörerna bedriva specifik verksamhet för att skapa en gemensam situationsmedvetenhet och samordnade insatser. Sådana åtgärder ska säkerställa en ordnad och effektiv spridning av information.

54. Insatserna bör vara lämpliga i förhållande till den storskaliga cybersäkerhetsincidentens eller cyberkrisens inverkan. I enlighet med direktiv (EU) 2022/2555 bör medlemsstaternas myndigheter för hantering av cyberkriser säkerställa nationell samstämmighet och samordning mellan de sektorsspecifika insatserna mot cyberkrisen.

55. I händelse av en storskalig cybersäkerhetsincident eller en cyberkris bör alla aktörer och nätverk hantera denna i nära samordning enligt följande:

a) På teknisk nivå:

i. De berörda medlemsstaterna och deras CSIRT-enheter bör samarbeta med de berörda entiteterna för att hantera incidenter och ge stöd i tillämpliga fall.

ii. CSIRT-enheterna bör samarbeta genom CSIRT-nätverket för att utbyta relevant teknisk information om incidenten. CSIRT-enheterna samverkar i arbetet med att analysera tillgängliga tekniska artefakter och annan teknisk information som rör incidenten för att fastställa orsaken och möjliga tekniska begränsningsåtgärder.

iii. När en CSIRT-enhet eller en medlemsstats cyberkrishanteringsmyndighet får kännedom om en betydande incident uppmanas de att meddela detta inom CSIRT-nätverket eller EU-CyCLONe.

iv. CSIRT-nätverket bör, med stöd av Enisa, utarbeta en sammanställning av nationella rapporter från CSIRT-enheterna som bör läggas fram för EU-CyCLONe.

v. När en cybersäkerhetsincident har potential att trappas upp till en storskalig cybersäkerhetsincident eller en cyberkris bör CSIRT-nätverket dela lämplig information med EU-CyCLONe. EU-CyCLONe bör använda denna information för att informera rådet.

vi. CSIRT-nätverket bör stå i nära kontakt med Europol för att säkerställa utbyte av relevant teknisk information. CSIRT-nätverket och Europol bör inrätta kontaktpunkter för att förbättra informationsutbytet när detta är relevant i händelse av en storskalig cybersäkerhetsincident.

b) På operativ nivå:

i. Medlemsstaterna bör begränsa incidentens inverkan på nationell nivå med hjälp av lämpliga åtgärder.

ii. CSIRT-nätverket bör förse EU-CyCLONe med tekniska bedömningar, som kan användas av EU-CyCLONe, av pågående incidenter.

iii. EU-CyCLONe bör bedöma konsekvenserna och effekterna av relevanta storskaliga cybersäkerhetsincidenter och cyberkriser och föreslå möjliga begränsningsåtgärder, stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och cyberkriser samt ge stöd till beslutsfattande på politisk nivå.

iv. Om en storskalig cybersäkerhetsincident med sektorsövergripande inverkan skulle kräva aktivering av svarsåtgärder på unionsnivå, särskilt relevanta övergripande och sektorsspecifika krishanteringsmekanismer på unionsnivå enligt bilaga II

a) får lämpliga aktörer, beroende på typen av sektorsspecifika krishanteringsmekanismer på unionsnivå, begära att denna mekanism aktiveras,

b) ska de berörda entiteterna vid aktivering av en sådan sektorsspecifik mekanism stödja sektorsentiteterna när det gäller att begränsa incidentens effekter,

c) bör kommissionen underlätta flödet av nödvändig information mellan kontaktpunkterna för de relevanta övergripande och sektorsspecifika krismekanismer på unionsnivå som förtecknas i bilaga II och EU-CyCLONe, och göra en integrerad sektorsövergripande analys och föreslå alternativ för en lämplig integrerad insatsplan,

d) bör kommissionen, i förekommande fall genom EU-CyCLONe, i samarbete med den höga representanten, säkerställa samstämmighet och samordning av de operativa åtgärderna på EU-nivå på cyberområdet med relaterade svarsåtgärder på unionsnivå, särskilt när det gäller begäranden om bistånd genom civilskyddsmekanismen,

e) bör information om incidenten, dess inverkan och vidtagna åtgärder – om en övervakningssida för IPCR har lanserats – också utbytas mellan medlemsstaterna och unionsentiteterna via IPCR-webbplattformen.

v. Medlemsstaterna får begära tjänster från EU-cybersäkerhetsreserven i enlighet med artikel 15 i förordning (EU) 2025/38. Utan att det påverkar eventuella framtida genomförandeakter enligt den förordningen bör tjänster från EU-cybersäkerhetsreserven sättas in inom 24 timmar från begäran.

c) På politisk nivå:

i. Rådet får begära genomgångar från centrala berörda parter, särskilt kommissionen, den höga representanten och EU-CyCLONe i syfte att kunna vidta lämpliga politiska och strategiska svarsåtgärder.

ii. Rådet kan, med stöd av kommissionen och den höga representanten, besluta om lämpliga åtgärder för att hantera den storskaliga cybersäkerhetsincidenten, inbegripet eventuell diplomatisk respons i enlighet med kapitel IX.

iii. Medlemsstaterna kan aktivera ytterligare mekanismer eller instrument för hantering av cyberkriser beroende på incidentens karaktär och inverkan.

iv. När IPCR aktiveras i läget för informationsutbyte utlöses ISAA-stödkapaciteten, vilket intensifierar informationsutbytet via IPCR-webbplattformen och säkerställer en gemensam lägesöversikt. Lägesrapporterna från EU-CyCLONe och CSIRT-nätverket bör även fortsatt vara de främsta instrumenten för framläggande av gemensam situationsmedvetenhet på operativ respektive teknisk nivå. Dessa rapporter kan ligga till grund för ISAA-rapporterna.

v. Vid en incident som kräver aktivering av svarsåtgärder på unionsnivå, särskilt relevanta övergripande och sektorsspecifika krishanteringsmekanismer på unionsnivå som förtecknas i bilaga II, bör rådet, i samarbete med kommissionen och den höga representanten, säkerställa samstämmighet och samordning mellan insatserna mot cyberkrisen och relaterade insatser på unionsnivå.

vi. När relevanta mekanismer, särskilt cybersäkerhetsreservens tjänster, begärs bör kommissionens avdelningar och, när så är lämpligt, utrikestjänsten samt relevanta rådsorgan, särskilt den övergripande arbetsgruppen för cyberfrågor och övergripande arbetsgruppen för förstärkning av motståndskraft och motverkande av hybridhot, beroende på vad som är lämpligt samordna utformningen och genomförandet av åtgärder samt den lämpliga beslutsprocessen med ytterligare åtgärder, i linje med verktygslådan för hybridhot[14] vid skadlig cyberverksamhet som ingår i en bredare hybridkampanj.

Hantering av en storskalig cybersäkerhetsincident eller cyberkris för vilken IPCR har aktiverats i läget för full aktivering

56. De åtgärder som förtecknas i avsnittet ”Hantering av en storskalig cybersäkerhetsincident eller cyberkris för vilken IPCR inte har aktiverats fullt ut” ovan bör genomföras.

57. När IPCR aktiveras i läget för full aktivering säkerställer ISAA-rapporterna en gemensam situationsmedvetenhet på politisk nivå. Lägesrapporterna från EU-CyCLONe och CSIRT-nätverket bör även fortsatt vara de främsta instrumenten för framläggande av gemensam situationsmedvetenhet på operativ respektive teknisk nivå. Dessa rapporter kan ligga till grund för ISAA-rapporterna.

58. I händelse av en storskalig cybersäkerhetsincident eller cyberkris som leder till att IPCR aktiveras i läget för full aktivering bör alla aktörer hantera denna i nära samordning inom ramen för en myndighetsövergripande strategi enligt följande:

a) Samordningen av insatserna på unionspolitisk nivå bör skötas av rådet med hjälp av IPCR-arrangemangen.

[14] Verktygslådan för hybridhot är en ram för en samordnad hantering av hybridkampanjer som påverkar EU och dess medlemsstater. Den omfattar till exempel förebyggande åtgärder, samarbetsåtgärder, stabilitetsåtgärder, restriktiva åtgärder och återhämtningsåtgärder, och stöder solidaritet och ömsesidigt bistånd.

b) EU-CyCLONe bör i samarbete med CSIRT-nätverket ge tydlig information till den politiska nivån om incidentens inverkan, möjliga konsekvenser och åtgärder för att hantera och avhjälpa den, bland annat genom att bidra till ISAA-rapporterna.

c) Utöver ISAA-kapaciteten kan ordförandeskapet i Europeiska unionens råd sammankalla IPCR-rundabordsmöten för att möjliggöra politisk och strategisk samordning av EU:s reaktion, med åtgärder inom ramen för cyberplanen och arbetet i relevanta sektoriella mekanismer som bidrar till IPCR-arbetet. Vid rundabordsmötena kan man dessutom identifiera vissa specifika brister i insatserna och uppmana specifika EU-aktörer att ta itu med dem och rapportera tillbaka vid framtida rundabordsmöten för att stödja den politiska och strategiska samordningen i IPCR.

d) Ordförandeskapet i Europeiska unionens råd bör överväga att bjuda in EU-CyCLONe till relevanta möten, inbegripet rundabordsmöten inom ramen för IPCR-arrangemangen och andra relevanta rådsmöten.

e) Medlemsstaternas krishanteringsmyndigheter bör säkerställa samstämmighet och samordning mellan de sektorsspecifika insatser mot cyberkrisen som stöds av cyberkrishanteringsmyndigheter.

f) Eventuell diplomatisk respons bör övervägas och genomföras i enlighet med kapitel IX.

VIII: Insatser för kommunikation till allmänheten

59. Kommunikation till allmänheten i en enskild medlemsstat om en pågående storskalig cybersäkerhetsincident eller cyberkris, inbegripet kommunikation i samband med kampanjer för att öka medvetenheten, faller visserligen under nationell behörighet, men medlemsstaterna, kommissionen och den höga representanten bör sträva efter att i största möjliga utsträckning samordna sin kommunikation till allmänheten. Vid behov kan det informella IPCR-nätverket av krisinformatörer involveras.

60. I syfte att förbereda för storskaliga cybersäkerhetsincidenter och cyberkriser uppmanas medlemsstaterna och, vid behov, kommissionen och CERT-EU att utbyta information om sina kommunikationsinsatser inom EU-CyCLONe och CSIRT-nätverket, inbegripet bästa praxis, såsom rådgivning eller kampanjer för att öka medvetenheten. Enisa bör tillhandahålla verktyg som stöder ett sådant utbyte och säkerställa att de är lättillgängliga.

61. Vid en storskalig cybersäkerhetsincident eller cyberkris uppmanas medlemsstaterna att inom EU-CyCLONe utbyta information om sina insatser för kommunikation till allmänheten för att skapa en gemensam medvetenhet och samordna åtgärderna. EU-CyCLONe kan på eget initiativ eller på begäran av rådet dela med sig av en översikt över sådana strategier till rådet.

IX: Diplomatisk respons och samarbete med strategiska partner

62. Den höga representanten bör i nära samarbete med kommissionen och andra relevanta unionsentiteter

    a) stödja beslutsfattandet i rådet, bland annat genom analyser, rapporter och förslag, om användningen av möjliga åtgärder som en del av EU:s verktygslåda för cyberdiplomati. Detta kommer att göra det möjligt att använda hela spektrumet av tillgängliga unionsverktyg för att förebygga, avskräcka från och reagera på skadlig cyberverksamhet, stärka säkerhetsstatusen och främja internationell fred, säkerhet och stabilitet i cyberrymden,

b) underlätta flödet av nödvändig information med strategiska partner ifall en relevant incident identifieras, inbegripet med Nato när så är lämpligt,

c) öka samordningen med strategiska partner, inbegripet Nato när så är lämpligt, när det gäller insatser mot långvarig fientlig cyberverksamhet från aktörer som utgör ihållande hot, särskilt när EU:s verktygslåda för cyberdiplomati används, i enlighet med dess genomföranderiktlinjer.

63. Medlemsstaterna, den höga representanten, kommissionen och andra relevanta unionsentiteter bör samarbeta med strategiska partner och internationella organisationer för att främja god praxis och staters ansvarsfulla agerande i cyberrymden samt säkerställa snabba och samordnade insatser vid potentiella eller storskaliga cybersäkerhetsincidenter.

64. Samarbetet mellan Europeiska unionen och Nato bör ske i enlighet med de överenskomna vägledande principerna om delaktighet, ömsesidighet och insyn, samt med full respekt för unionens autonoma beslutsfattande.

65. Kommissionen och den höga representanten bör, med beaktande av befintliga avtal såsom det tekniska avtalet mellan CERT-EU och Nato från 2016, inrätta kontaktpunkter för samordning med Nato i händelse av en cyberkris för att utbyta nödvändig information om situationen och om användningen av krishanteringsmekanismer, i syfte att förbättra samarbetet kring och öka effektiviteten i insatserna. I detta syfte bör unionen undersöka olika sätt att förbättra informationsutbytet med Nato på ett inkluderande, ömsesidigt och icke-diskriminerande sätt, särskilt genom att säkerställa verktyg för säker kommunikation samtidigt som hänsyn tas till olika medlemsstaters standarder för informationsutbyte.

66. Som en del av det rullande program för unionens cyberövningar som avses i kapitel V ovan bör kommissionens avdelningar och utrikestjänsten överväga att anordna en övning på personalnivå med Nato för att testa samarbetet mellan civila och militära enheter i händelse av en storskalig cybersäkerhetsincident eller cyberkris där medlemsstater eller Natoallierade ska försöka hantera en cyberattack som påverkar deras säkerhet Övningen bör genomföras på ett inkluderande och icke-diskriminerande sätt samt med full respekt för de överenskomna principerna för parametrarna för samarbetet mellan EU och Nato. Övningen bör genomföras inom ramen för övningen EU Integrated Resolve (parallell och samordnad övning (PACE)). Alla nödvändiga åtgärder bör vidtas för att säkerställa att alla aktörer som avses i cyberplanen deltar.

67. Gemensamma cyberövningar på unionsnivå med länderna på västra Balkan, Republiken Moldavien, Ukraina samt andra strategiska partner och likasinnade tredjeländer bör också övervägas, i samråd med rådet, kommissionen och den höga representanten.

X. Samordning av hanteringen av cyberkriser med militära aktörer på EU-nivå

68. Medlemsstaterna bör fortsätta att stärka samarbetet mellan civila och militära cyberaktörer på nationell nivå.

69. EU-CyCLONe och CSIRT-nätverket bör identifiera hur man på olika sätt och med olika förfaranden kan samarbeta med EU:s berörda militära aktörer, såsom konferensen för EU:s cyberbefälhavare och nätverket för militära incidenthanteringsorganisationer (Micnet), för att dra nytta av ett gemensamt militärt och civilt perspektiv, särskilt genom gemensamma möten. EU-CyCLONe och CSIRT-nätverket bör informera rådet om de framsteg som görs när det gäller detta samarbete.

70. Den berörda medlemsstaten uppmanas att informera EU-CyCLONe och utrikestjänsten om relevant nationell eller multinationell militär insatsförmåga används i samband med en storskalig cybersäkerhetsincident eller cyberkris och om tillhandahållandet av denna information är ömsesidigt överenskommet mellan användaren och den part som tillhandahåller insatskapaciteten.

71. Som en del av det rullande program för unionens cyberövningar som avses i kapitel V ovan bör kommissionen och den höga representanten överväga att anordna en gemensam övning för att testa samarbetet mellan både civila och militära cyberaktörer i händelse av en storskalig cybersäkerhetsincident som påverkar medlemsstaterna.

XI: Återhämtning och lärdomar från en cyberkris

72. Medlemsstaterna, berörda unionsentiteter och nätverk bör samarbeta under återhämtningsfasen efter en cyberkris för att säkerställa ett snabbt återställande av centrala funktioner. När så är lämpligt bör även brottsbekämpande myndigheter involveras i detta samarbete. Under denna fas är samarbete med den privata sektorn avgörande, särskilt för att underlätta dataåterställning och återställande av system. I en effektiv samordning mellan berörda parter bör minimering av störningar och säkerställande av driftskontinuitet prioriteras.

73. Medlemsstaterna och berörda unionsentiteter och unionsnätverk bör samarbeta under återhämtningsfasen, med utgångspunkt i lärdomar från tidigare cyberkriser eller hanterade cybersäkerhetsincidenter samt incidentrapporter, särskilt inom ramen för den europeiska mekanism för granskning av cybersäkerhetsincidenter som inrättats genom förordning (EU) 2025/38.

74. EU-CyCLONe bör förse CSIRT-nätverket, samarbetsgruppen för nät- och informationssäkerhet och rådet med en fullständig förteckning över lärdomar från tidigare cyberkriser eller hanterade cybersäkerhetsincidenter och bästa praxis. Enisa bör säkerställa att dessa lärdomar återspeglas korrekt i framtida beredskapsverksamhet och beaktas vid planeringen av framtida övningar.

XII: Säker kommunikation

75. På grundval av kartläggningen av befintliga säkra kommunikationsverktyg[15] bör kommissionen senast i slutet av 2026 föreslå en interoperabel uppsättning säkra kommunikationslösningar. Rådet, kommissionen, den höga representanten, EU-CyCLONe och CSIRT-nätverket bör komma överens om denna uppsättning senast i slutet av 2027. Dessa lösningar bör gynnas av de åtgärder på området säker kommunikation som EU-institutionerna skulle kunna vidta inom ramen för unionens strategi för krisberedskap, och bör omfatta alla nödvändiga kommunikationssätt (röstsamtal, data, videokonferenser, meddelanden, samarbete och dokumentdelning samt samråd). Lösningarna bör uppfylla gemensamt fastställda krav för skydd av känsliga icke-säkerhetsskyddsklassificerade uppgifter. Lösningar som bygger på öppna protokoll med genomförande med öppen källkod som lämpar sig för kommunikation i realtid och som förvaltas av en entitet baserad i EU bör användas.

76. I syfte att vid behov kunna utbyta uppgifter på säkerhetskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED bör EU-CyCLONe och CSIRT-nätverket kunna använda säkra kommunikationskanaler som säkerställs för EU:s institutioner, organ och byråer för utbyte av säkerhetsskyddsklassificerade uppgifter dem emellan och med medlemsstaterna.

---

15 WK 862/2023.

77. Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning, som inrättades genom förordning (EU) 2021/887[16], bör, utan att det påverkar den framtida fleråriga budgetramen, överväga finansiering genom programmet för ett digitalt Europa för att hjälpa medlemsstaterna att använda säkra kommunikationsverktyg. Dubblering av investeringar i interoperabla säkra system bör undvikas.

78. I synnerhet bör EU-entiteter och medlemsstater utveckla beredskapsplaner för allvarliga kriser där normala kommunikationskanaler som är beroende av internet eller telekommunikationsnät är drabbade av störningar eller inte är tillgängliga.

79. Mekanismer för kommunikation och informationsutbyte mellan brottsbekämpande myndigheter och cybersäkerhetsnätverk, särskilt på teknisk nivå, bör inrättas för effektiv hantering av cyberkriser. Dessa mekanismer bör respektera varje parts roll och undvika att störa pågående insatser samt garantera redundans i kommunikationen. Det EU-system för kritisk kommunikation som för närvarande håller på att utvecklas kan gynna de gemensamma insatserna med berörda cybergemenskaper.

XIII: Slutbestämmelser

80. EU-CyCLONe bör, i samarbete med CSIRT-nätverket och andra huvudaktörer inom EU:s ekosystem för hantering av cyberkriser, samt med stöd av Enisa, inom ett år efter offentliggörandet av rekommendationen, utarbeta detaljerade processflödesdiagram som beskriver informationsflödena mellan berörda aktörer, beslutsprocesser och rapporter som skapats under hanteringen av en storskalig cybersäkerhetsincident eller cyberkris, i enlighet med beskrivningen i denna rekommendation. Flödesdiagrammen bör omfatta olika samarbetsformer och samarbetslager. Flödesdiagrammen bör uppdateras efter behov.

[16] Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum (EUT L 202, 8.6.2021, s. 31).

81. För att stödja en effektiv tillämpning av den reviderade cyberplanen, och med utgångspunkt i erfarenheterna från de gemensamma cyberövningar som genomförts inom ramen för cyberplanen, kan rådet vid behov ta fram en uppsättning genomföranderiktlinjer. I dessa riktlinjer kan man ta upp de praktiska utmaningar som konstaterats under övningarnas gång och åtgärda identifierade brister och felande länkar i samordningen, kommunikationen och den operativa samverkan.

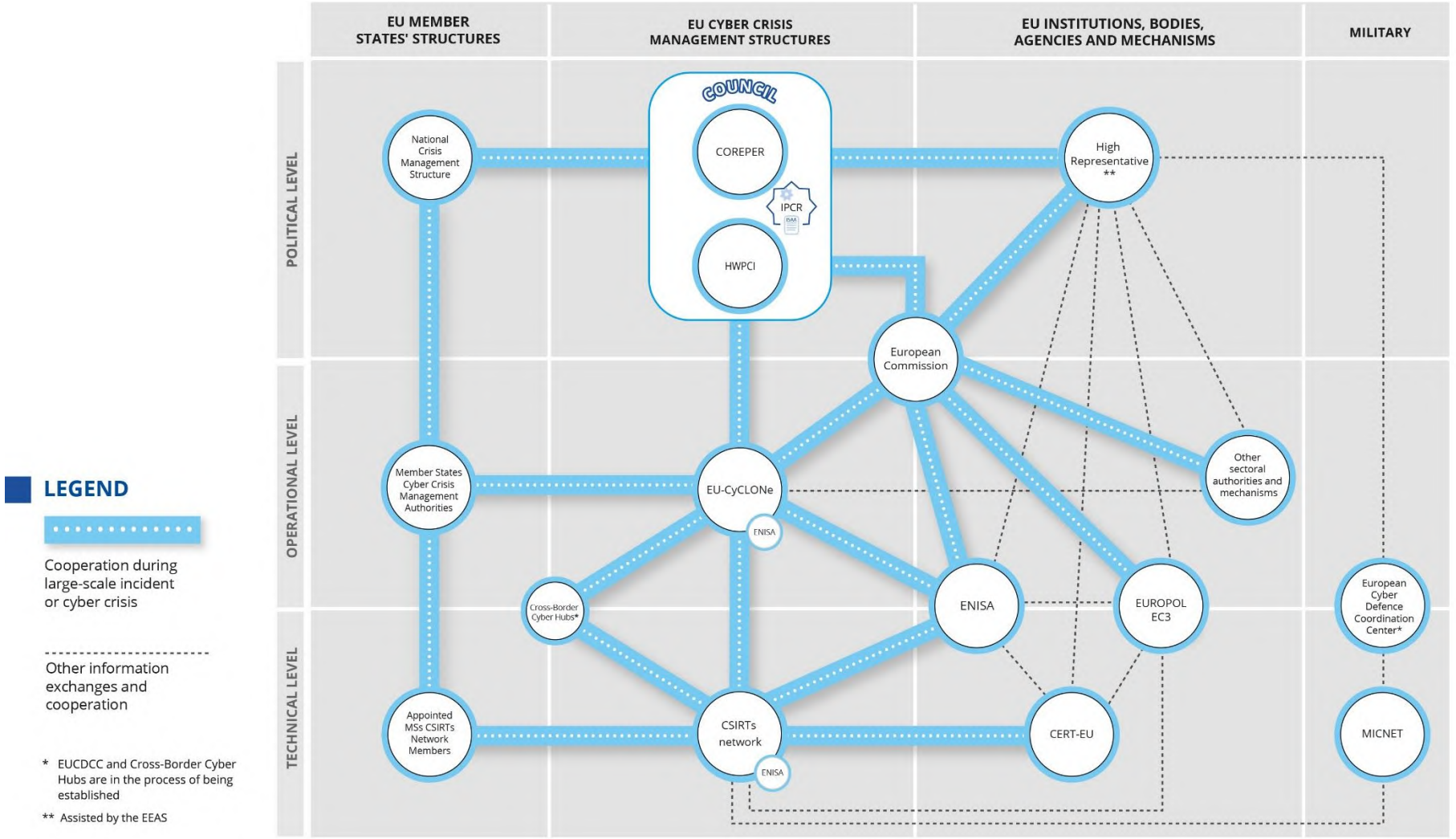
82. Kommissionen bör, i samarbete med medlemsstaterna, se över denna rekommendation åtminstone vart fjärde år efter det att den har offentliggjorts. Efter varje översyn bör kommissionen offentliggöra en rapport och lägga fram den för rådet. Kommissionen och medlemsstaterna bör särskilt beakta effekterna av den föränderliga hotbilden, resultaten av gemensamma övningar och lagstiftningsändringar – i synnerhet eventuella ändringar till följd av översynen av förordning (EU) 2019/881.

Utfärdad i Bryssel den

På rådets vägnar

Ordförande

BILAGA I – Unionsplanen för hantering av en cybersäkerhetskris



BILAGA II – BERÖRDA AKTÖRER PÅ UNIONSNIVÅ (ENTITETER OCH NÄTVERK) OCH KRISHANTERINGSMEKANISMER

(1) Huvudaktörernas deltagande under hela livscykeln för hantering av cyberkriser (storskaliga cybersäkerhetsincidenter och cyberkriser)

	Beredskap	Upptäckt	Insatser för att hantera en storskalig cybersäkerhetsincident eller cyberkris			Kommunikation till allmänheten	Återhämtning och lärdomar
			på teknisk nivå	på operativ nivå	på politisk nivå		
Medlemsstaterna	X	X	X	X	X	X	X
Kommissionen	X			X	X	X	
Den höga representanten, biträdd av utrikestjänsten	X			X	X	X	
Rådet	X				X	X	X
Enisa	X		X	X			
CERT-EU	X	X	X	X		X	X
CSIRT-nätverket	X	X	X				X
EU-CyCLONe	X			X	X		X

(2) Roller och befogenheter för berörda aktörer och mekanismer på unionsnivå (i alfabetisk ordning enligt det engelska namnet) i samband med hantering av cyberkriser

Aktör	Nivå	Roll och befogenhet	Referens
CERT-EU	Teknisk/operativ	Samordnar krisinsatserna på teknisk nivå och hanteringen av större incidenter som påverkar unionens entiteter. För en förteckning över den tillgängliga tekniska expertis som skulle behövas för incidenthantering i händelse av större incidenter och bistår interinstitutionella cybersäkerhetsstyrelsen med att samordna unionsentiteternas cyberkrishanteringsplaner för större incidenter. Medlem i CSIRT-nätverket. Stöder kommissionen i EU-CyCLONe vad gäller den samordnade hanteringen av storskaliga cybersäkerhetsincidenter och cyberkriser. Fungerar som nav för utbyte av information om cybersäkerhet och incidenthantering och underlättar utbytet av information om incidenter, cyberhot, sårbarheter och	Förordning (EU, Euratom) 2023/2841 Förordning (EU) 2025/38

Aktör	Nivå	Roll och befogenhet	Referens
		tillbud mellan unionens entiteter och motparter. Begär att EU-cybersäkerhetsreserven ska sättas in på unionsentiteternas vägnar. Samarbetar med Natos cybersäkerhetscentrum på grundval av deras tekniska avtal.	
Europeiska unionens råd	Politisk	Fattar politiska beslut och fungerar samordnande. Anförtros IPCR, som rör samordning och hantering på politisk unionsnivå.	Artikel 16 i fördraget om Europeiska unionen
Ordförandeskapet i Europeiska unionens råd	Politisk	Beslutar (utom när solidaritetsklausulen åberopas enligt artikel 222 i fördraget om Europeiska unionens funktionssätt) om IPCR ska aktiveras, vid behov i samråd med berörda medlemsstater samt kommissionen och den höga representanten.	Artikel 16 i fördraget om Europeiska unionen Rådets genomförandebeslut (EU) 2018/1993
Gränsöverskridande cybernav	Teknisk	Gränsöverskridande cybernav är en flerlandsplattform, inrättad genom ett skriftligt konsortieavtal, som inom en samordnad nätverksstruktur för	Förordning (EU) 2025/38

Aktör	Nivå	Roll och befogenhet	Referens
		samman nationella cybernav från minst tre medlemsstater, och som är utformad för att förbättra övervakning, upptäckt och analys av cyberhot för att förhindra incidenter och stödja produktionen av underrättelseinformation om cyberhot, i synnerhet genom utbyte av relevanta data och relevant information, när så är lämpligt i anonymiserad form, samt genom utbyte av förstklassiga verktyg och gemensam utveckling av kapacitet för cyberrelaterad upptäckt, analys, förebyggande och skydd i en betrodd miljö. Har ett nära samarbete med CSIRT-nätverket för att utbyta information. Tillhandahåller information om en potentiell eller pågående storskalig cybersäkerhetsincident till medlemsstaternas myndigheter och kommissionen genom EU-CyCLONe och CSIRT-nätverket.	

Aktör	Nivå	Roll och befogenhet	Referens
CSIRT-nätverket	Teknisk	Bidrar till att skapa förtroende och tillit och främjar ett snabbt operativt samarbete mellan medlemsstaterna. Är det främsta nätverket för utbyte av relevant information om incidenter, tillbud, cyberhot, risker och sårbarheter. På begäran av en medlem som kan påverkas av en incident utbyter och diskuterar nätverket information om den incidenten och relaterade cyberhot. Nätverket kan också underlätta samordnade insatser för att hantera en incident som har identifierats inom en begärande medlems jurisdiktion. Bistår medlemsstaterna med hanteringen av gränsöverskridande incidenter och undersöker ytterligare samarbetsformer, inbegripet ömsesidigt bistånd. Får information från medlemsstaterna om deras	Direktiv (EU) 2022/2555 Förordning (EU) 2025/38

Aktör	Nivå	Roll och befogenhet	Referens
		begäranden till EU-cybersäkerhetsreserven.	
Konferensen för EU:s cyberbefälhavare		Ett forum där cyberbefälhavare på nationell nivå i medlemsstaterna kan samarbeta och utbyta viktig information om pågående insatser i cyberrymden och strategier för att begränsa storskaliga cyberincidenter. Konferensen anordnas av det roterande ordförandeskapet i Europeiska unionens råd med stöd av Europeiska försvarsbyrån (EDA), Europeiska utrikestjänsten och EU:s militära stab (EUMS).	Det gemensamma meddelandet om EU:s politik för cyberförsvar (2022)
Kommissionen	Operativ/politisk	Europeiska unionens verkställande organ. Säkerställer en smidigt fungerande inre marknad. Underlättar samstämmighet och samordning mellan relaterade krishanteringsåtgärder på unionsnivå. Vissa allmänna beredskapsåtgärder på unionsnivå inom ramen för beslutet om en civilskyddsmekanism för	Artikel 17 i fördraget om Europeiska unionen Genomförandebeslut (EU) 2018/1993 Beslut nr 1313/2013/EU Direktiv (EU) 2022/2555

Aktör	Nivå	Roll och befogenhet	Referens
		unionen, inbegripet förvaltning av centrumet för samordning av katastrofberedskap och det gemensamma kommunikations- och informationssystemet för olyckor. Observatör i EU-CyCLONe och medlem vid potentiella eller pågående storskaliga incidenter som har eller sannolikt kommer att ha en betydande inverkan på tjänster och verksamhet som omfattas av direktiv (EU) 2022/2555. Observatör i CSIRT-nätverket. Övergripande ansvar för genomförandet av EU-cybersäkerhetsreserven. Kontaktpunkt i den interinstitutionella cybersäkerhetsstyrelsen för utbyte av relevant information om större incidenter med EU-CyCLONe. Rådfrågas av rådets ordförandeskap om beslut om att aktivera eller avaktivera IPCR (utom när solidaritetsklausulen åberopas	Förordning (EU) 2025/38 Förordning (EU, Euratom) 2023/2841

Aktör	Nivå	Roll och befogenhet	Referens
		enligt artikel 222 i EUF-fördraget). Kommissionens avdelningar utarbetar tillsammans med utrikestjänsten ISAA-rapporterna.	
Europeiska unionens cybersäkerhetsbyrå (Enisa)	Teknisk/operativ	Utför uppgifter i syfte att uppnå en hög cybersäkerhetsnivå i hela unionen, bland annat genom att aktivt stödja medlemsstaterna och unionens institutioner. Utgör sekretariatet för CSIRT-nätverket och EU-CyCLONe. Utarbetar regelbundet en teknisk lägesrapport om cybersäkerheten i EU med information om incidenter och cyberhot (tillsammans med EC3 och CERT-EU och i nära samarbete med medlemsstaterna). Bidrar till utvecklingen av gemensamma insatser vid storskaliga gränsöverskridande incidenter eller kriser, främst genom att – sammanställa och analysera rapporter från nationella källor,	Direktiv (EU) 2022/2555 Förordning (EU) 2019/881 Förordning (EU) 2025/38 Förordning (EU) 2024/2847

Aktör	Nivå	Roll och befogenhet	Referens
		– sörja för informationsflödet mellan teknisk, operativ och politisk nivå, – på begäran underlätta incidenthanteringen, – stödja unionsentiteterna när det gäller kommunikation till allmänheten, – på begäran stödja medlemsstaterna när det gäller kommunikation till allmänheten, – testa incidenthanteringskapaciteten och regelbundet anordna cybersäkerhetsövningar. Agerar som upphandlande myndighet om den har anförtrotts att helt eller delvis driva och administrera EU:s cybersäkerhetsreserv. Anordnar vartannat år en storskalig och omfattande cybersäkerhetsövning på unionsnivå med tekniska, operativa eller strategiska inslag. Utarbetar en incidentgranskningsrapport i samarbete med den berörda medlemsstaten och andra berörda aktörer för att bedöma orsakerna till, inverkan av och	

Aktör	Nivå	Roll och befogenhet	Referens
		begränsningsåtgärderna vid en incident (på begäran av kommissionen eller EU-CyCLONe och med den berörda medlemsstatens godkännande). Informerar EU-CyCLONe om den information som tillhandahållits enligt rapporteringsskyldigheterna i cyberresiliensförordningen är relevant för en samordnad hantering av storskaliga cybersäkerhetsincidenter och cyberkriser på operativ nivå.	
Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe)	Operativ	Stöder en samordnad hantering av storskaliga cybersäkerhetsincidenter och cyberkriser på operativ nivå. Säkerställer ett regelbundet utbyte av relevant information mellan medlemsstaterna och unionens institutioner, organ och byråer. Samordnar hanteringen av storskaliga cybersäkerhetsincidenter och kriser och ger stöd till beslutsfattande på politisk nivå i samband med sådana incidenter och kriser.	Direktiv (EU) 2022/2555 Förordning (EU) 2025/38

Aktör	Nivå	Roll och befogenhet	Referens
		Bedömer konsekvenserna och effekterna av relevanta storskaliga cybersäkerhetsincidenter och cyberkriser och föreslår möjliga begränsningsåtgärder. Diskuterar, på begäran av en berörd medlemsstat, nationella planer för hantering av storskaliga nationella cybersäkerhetsincidenter och kriser. Utarbetar tillsammans med Enisa och kommissionen mallen för att underlätta inlämning av begäranden om stöd från EU-cybersäkerhetsreserven. Får information från medlemsstaterna om deras begäranden till EU-cybersäkerhetsreserven. Får information om en potentiell eller pågående storskalig cybersäkerhetsincident från de gränsöverskridande cybernaven eller CSIRT-nätverket.	

Aktör	Nivå	Roll och befogenhet	Referens
Unionens höga representant för utrikes frågor och säkerhetspolitik, biträdd av Europeiska utrikestjänsten	Politisk	Leder och samordnar unionens insatser för att hantera externa hybridhot och cyberhot mot säkerheten. Ansvarar för unionens instrument för cyberdiplomati och cyberförsvar för att avskräcka från och reagera på externa hot, bland annat genom att använda unionens verktygslådor för hybridhot respektive cyberdiplomati. Samarbetar med externa partner, bland annat genom GSFP-engagemang. Tillhandahåller beredskap för unionens och medlemsstaternas situationsmedvetenhet om och kapacitet att reagera på hybrid- och cyberhot, till exempel genom praktiska övningar, träning och nätverk. Hanterar säkerhets- och försvarsmässiga konsekvenser av unionens rymdtillgångar, särskilt inom ramen för unionens gemensamma säkerhets- och försvarspolitik (GSFP). Stöder konferensen för EU:s cyberbefälhavare.	Rådets beslut 2010/427/EU

Aktör	Nivå	Roll och befogenhet	Referens
		Stöder nätverket för militära it-incidenthanteringsorganisationer (Micnet). Rådfrågas av rådets ordförandeskap om beslut om att aktivera eller avaktivera IPCR (utom när solidaritetsklausulen åberopas enligt artikel 222 i EUF-fördraget). Utrikestjänsten utarbetar tillsammans med kommissionens avdelningar ISAA-rapporterna.	
EU:s samordningscentrum för cyberförsvar	Övergripande	Dess ursprungliga mål är i första hand att stärka unionens och dess medlemsstaters gemensamma situationsmedvetenhet om skadlig verksamhet i cyberrymden, särskilt när det gäller militära GSFP-uppdrag och GSFP-insatser.	Det gemensamma meddelandet om EU:s politik för cyberförsvar (2022)
Europol	Operativ	Tillhandahåller operativt och tekniskt stöd till medlemsstaternas behöriga myndigheter för förebyggande och avvärjande av it-brottslighet. Bistår på medlemsstaternas begäran deras behöriga myndigheter med att reagera på cyberattacker av misstänkt brottsligt ursprung.	Förordning (EU) 2016/794 med alla ändringar

Aktör	Nivå	Roll och befogenhet	Referens
Interinstitutionella cybersäkerhetsstyrelsen		Upprättar en cyberkrishanteringsplan i syfte att på operativ nivå stödja en samordnad hantering av större incidenter som berör unionens entiteter och bidra till ett regelbundet utbyte av relevant information. Samordnar antagandet av enskilda unionsentiteters cyberkrishanteringsplaner. Antar, på förslag av CERT-EU, riktlinjer eller rekommendationer om incidenthanteringssamarbete vid betydande incidenter som rör unionens entiteter.	Förordning (EU, Euratom) 2023/2841
Nätverket för militära it-incidenthanteringsorganisationer (Micnet)	Teknisk	Främjar mer robusta och samordnade responsåtgärder vid cyberhot som påverkar unionens försvarssystem, inbegripet sådana som används för militära GSFP-uppdrag och GSFP-insatser. Stöds av Europeiska försvarsbyrån.	Det gemensamma meddelandet om cyberförsvar från 2022

Aktör	Nivå	Roll och befogenhet	Referens
Den gemensamma kapaciteten för underrättelseanalys (SIAC)		Består av 1) EU:s underrättelse- och lägescentral (EU Intcen) och 2) direktoratet för underrättelseverksamhet vid EU:s militära stab (EUMS Int). Tillhandahåller strategiska underrättelser om utrikespolitik, terrorism samt cyber- och hybridhot. Hanterar militära underrättelser för GSFP-uppdrag och stöder unionens försvars- och krishanteringsinsatser. Under ledning av den höga representanten.	Artiklarna 38 och 42–46 i fördraget om Europeiska unionen

(3) Relevanta mekanismer och plattformar för krishantering på unionsnivå

Mekanism	Övergripande/sektorsspecifik/cyberspecifik	Beskrivning	Referens
Argus	Övergripande	Kommissionens samordningsprocess och allmänna förvarningssystem för enhetliga insatser i händelse av en större gränsöverskridande kris som kräver åtgärder på EU-nivå. Sammanför alla berörda avdelningar och kanslier för att besluta om och samordna åtgärder. Gör det möjligt för kommissionen att utbyta relevant information om framväxande sektorsövergripande kriser eller förutsebara eller överhängande hot som kräver åtgärder på unionsnivå.	Kommissionens meddelande (2005)662
Europeiska utrikestjänstens krishanteringscentrum (CRC)	Övergripande	Den gemensamma kontaktpunkten för alla krisrelaterade frågor inom utrikestjänsten och den dygnet runt-aktiva permanenta krishanteringskapaciteten för krissituationer som hotar säkerheten för personalen vid EU:s delegationer och/eller som reaktion på kriser som drabbar unionsmedborgare utomlands. Den sammanför experter på säkerhet, konsulärt arbete och situationsmedvetenhet, samtidigt som man förlitar sig på engagerad	En strategisk kompass för säkerhet och försvar – För ett EU som skyddar sina medborgare, värden och intressen och bidrar till internationell fred och säkerhet (21 mars 2022)

Mekanism	Övergripande/sektorsspecifik/cyberspecifik	Beskrivning	Referens
		personal på plats vid unionens delegationer.	
Planen för kritisk infrastruktur	Övergripande	Samordnar insatser på unionsnivå vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse.	Rådets rekommendation C/2024/4371
Systemet med cybersäkerhetsvarningar	Cyberspecifik	Säkerställer avancerad unionskapacitet för att öka kapaciteten för upptäckt, analys och databehandling i samband med cyberhot och förebyggandet av incidenter i unionen.	Förordning (EU) 2025/38
Verktygslådan för cyberdiplomati (ramen för en gemensam diplomatisk respons från EU mot skadlig it-verksamhet)	Cyberspecifik	Möjliggör unionens gemensamma diplomatiska reaktion på skadlig cyberverksamhet, som bidrar till att förbygga konflikter, begränsa hot mot cybersäkerheten och öka stabiliteten i internationella relationer.	Rådets slutsatser av den 19 juni 2017 Reviderade riktlinjer för genomförandet, 10289/23, 8 juni 2023
EU-cybersäkerhetsreserv	Cyberspecifik	Mobiliserar cybersäkerhetsexperter och cybersäkerhetsresurser under kriser för att stödja medlemsstaternas och unionens institutioners, organs och byråers insatser.	Förordning (EU) 2025/38

Mekanism	Övergripande/sektorsspecifik/cyberspecifik	Beskrivning	Referens
Nätföreskrift om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden	Sektorsspecifik	Inrättar en återkommande process för cybersäkerhetsriskbedömningar inom elsektorn, på unions-, medlemsstats-, region- och entitetsnivå. Innehåller bestämmelser som är specifika för krishantering och samarbetet med CSIRT och EU-CyCLONe i de fall då en storskalig cybersäkerhetsincident påverkar andra sektorer som är beroende av en trygg elförsörjning.	Kommissionens delegerade förordning (EU) 2024/1366
Verktygslådan för hybridhot	Övergripande	Innehåller bestämmelser som säkerställer en översikt över vad som finns tillgängligt på EU-nivå som svar på alla typer av hybridhot och en samordning av användningen av dem, så att samstämmighet säkerställs mellan våra åtgärder på olika områden. Verktygslådan för hybridhot bidrar till att säkerställa att beslutsfattandet bygger på en övergripande situationsmedvetenhet och lärdomar.	Rådets slutsatser om en ram för en samordnad EU-reaktion på hybridkampanjer, 22 juni 2022 Genomföranderiktlinjer för ramen för en samordnad EU-reaktion på hybridkampanjer, 14 december 2022

Mekanism	Övergripande/sektorsspecifik/cyberspecifik	Beskrivning	Referens
Snabbinsatsteam för hybridhot	Övergripande	Som en del av EU:s verktygslåda för hybridhot utnyttjar EU:s snabbinsatsteam för hybridhot relevant sektorsspecifik civil och militär expertis på nationell nivå och EU-nivå för att tillhandahålla skräddarsytt och riktat kortsiktigt stöd till medlemsstaterna, uppdrag och insatser inom den gemensamma säkerhets- och försvarspolitiken samt partnerländer för att motverka hybridhot och hybridkampanjer.	Vägledande ram för det praktiska inrättandet av EU:s snabbinsatsteam för hybridhot, 21 maj 2024 Operativ vägledning för utplacering av snabbinsatsteam för hybridhot, godkänd av Coreper den 4 december 2024
IPCR	Övergripande	Stöder ett snabbt och samordnat beslutsfattande på unionspolitisk nivå för större och komplexa kriser. Det är rådets ordförandeskap som fattar beslut om att aktivera och avaktivera mekanismen, efter samråd (utom när solidaritetsklausulen har åberopats) med de berörda medlemsstaterna, kommissionen och den höga representanten. Rådets generalsekretariat, kommissionens avdelningar och utrikestjänsten kan också i samråd med ordförandeskapet komma överens om att aktivera IPCR i läget informationsutbyte.	Rådets genomförandebeslut (EU) 2018/1993

Mekanism	Övergripande/sektorsspecifik/cyberspecifik	Beskrivning	Referens
		Arbetet i IPCR bygger på de ISAA-rapporter som utarbetats av kommissionens avdelningar och utrikestjänsten. Dessa rapporter baseras på relevant information och relevanta analyser som tillhandahålls av medlemsstaterna (t.ex. från relevanta nationella kriscentrum) och av relevanta unionsbyråer och unionsorgan.	
Beredskapsprotokollet för EU:s brottsbekämpningsinsatser	Övergripande	Ett verktyg för att hjälpa unionens brottsbekämpande myndigheter att omedelbart reagera på större gränsöverskridande cyberattacker genom snabb bedömning, säkert och snabbt utbyte av kritisk information och effektiv samordning av de internationella aspekterna av deras utredningar.	Rådets slutsatser (26 juni 2018) om EU:s samordnade insatser vid storskaliga cyberincidenter och cyberkriser
Pescos snabbinsatsteam för cybersäkerhet (CRRT)	Cyberspecifik	Pescos snabbinsatsteam för cybersäkerhet är en gemensamt utvecklad civil-militär cyberförsvarskapacitet för EU:s medlemsstater för att snabbt reagera på cyberincidenter och cyberkriser	Artiklarna 42.6 och 46 och protokoll 10 till fördraget om Europeiska unionen

Mekanism	Övergripande/sektorsspecifik/cyberspecifik	Beskrivning	Referens
		samt genomföra förebyggande åtgärder, såsom sårbarhetsbedömningar och valövervakning. Uppdraget för Pescos snabbinsatsteam för cybersäkerhet är att på begäran tillhandahålla cyberstöd till EU:s medlemsstater, institutioner, organ och byråer, EU:s militära GSFP-uppdrag och GSFP-insatser samt partnerländerna.	

Strukturen för hantering av rymdhot (STRA)	Sektorsspecifik (rymdhot, även cyberrelaterade sådana)	Strukturen för hantering av rymdhot (STRA) rör det ansvar som ska utövas av rådet och den höga representanten för att avvärja ett hot som uppstår till följd av driftsättningen, driften eller användningen av de system som inrättats och de tjänster som tillhandahålls inom ramen för unionens rymdprogram.	Rådets beslut (Gusp) 2021/698
Ramverket för samordning av åtgärder mot systemiska cyberincidenter (EU-SCICF)	Sektorsspecifik	Ett ramverk som håller på att utvecklas för kommunikation och samordning och som hanterar och beaktar potentiella systemiska cyberhändelser inom finanssektorn. Det kommer att bygga vidare på en av de europeiska tillsynsmyndigheternas planerade roller enligt förordning (EU) 2022/2554, nämligen att gradvis möjliggöra effektiva samordnade insatser på unionsnivå i händelse av en större gränsöverskridande IKT-relaterad incident eller därmed sammanhängande hot som har en systemeffekt på unionens finansiella sektor som helhet.	Europeiska systemrisknämndens rekommendation av den 2 december 2021 om ett europeiskt ramverk för relevanta myndigheters samordning av åtgärder mot systemiska cyberincidenter (ESRB/2021/17)
Unionens civilskyddsmekanism	Övergripande	Säkerställer civilskyddssamarbete för att förbättra förebyggande, beredskap och insatser vid katastrofer.	Beslut nr 1313/2013/EU

CISE – gemensam miljö för informationsutbyte	Maritimspecifik, gäller sju sektorer.	CISE är ett nätverk som kopplar samman systemen för EU/EES-myndigheter med ansvar för övervakning till havs. CISE möjliggör utbyte av relevant information över gränserna och mellan olika sektorer på ett smidigt och automatiserat sätt.	En strategisk kompass för säkerhet och försvar – För ett EU som skyddar sina medborgare, värden och intressen och bidrar till internationell fred och säkerhet (21 mars 2022)

(4) Högkritiska sektorer och andra kritiska sektorer enligt direktiv (EU) 2022/2555 och sektorsspecifika krismekanismer på unionsnivå (i tillämpliga fall)		
Sektorer	**Delsektor**	**Tillämpliga sektorsspecifika krismekanismer**
Energi	Elektricitet	Gruppen för samordning på elområdet
	Fjärrvärme och fjärrkyla	Ej tillämpligt
	Olja	Samordningsgruppen för olja Europeiska unionens grupp av myndigheter för olje- och gasverksamhet till havs
	Gas	Gruppen för samordning av gasförsörjningen
	Vätgas	Ej tillämpligt
Transporter	Lufttransport	Den europeiska samordningscellen för luftfartskriser
	Järnvägstransport	Ej tillämpligt
	Sjöfart	Europeiska fiskerikontrollbyrån (EFCA) SafeSeaNet (SSN) Integrerade sjöfartstjänster (IMS) Långdistansidentifiering och -spårning av fartyg (LRIT) Emsas marina stödtjänster

	Vägtransport	Ej tillämpligt
	Övergripande	Nätverket av kontaktpunkter inom transportsektorn, som inrättats genom beredskapsplanen för transportsektorn, COM(2022) 211
Bankverksamhet		EU-SCICF
Finansmarknadsinfrastruktur		EU-SCICF Europeiska finansiella stabiliseringsmekanismen

Hälso- och sjukvårdssektorn		Systemet för tidig varning och reaktion Centrumet för hantering av hälsokrislägen (HEOF), systemet för snabb varning för vävnader och celler respektive blodkomponenter (RATC/RAB) Ramen för åtgärder vid hot mot folkhälsan Systemet för snabb varning vid kemiska incidenter (RASCHEM) Den europeiska övervakningsportalen för smittsamma sjukdomar Myndigheten för beredskap och insatser vid hälsokriser (Hera) Det medicinska underrättelsesystemet (Medisys) Verkställande styrgruppen för brister på medicintekniska produkter Snabb varning – farmakovigilans EU:s arbetsgrupp för hälsa Hälsosäkerhetskommittén
Dricksvatten		Ej tillämpligt

Avloppsvatten		Ej tillämpligt
Digital infrastruktur		Ej tillämpligt
Förvaltning av IKT-tjänster		Ej tillämpligt
Offentlig förvaltning		Ej tillämpligt
Rymden		Strukturen för hantering av rymdhot (STRA)
Post- och budtjänster		Ej tillämpligt
Avfallshantering		Ej tillämpligt
Tillverkning, produktion och distribution av kemikalier		Systemet för snabb varning vid kemiska incidenter (RASCHEM)

Produktion, bearbetning och distribution av livsmedel		Det europeiska systemet för övervakning av grödor Tjänsten för upptäckt av områden med avvikande jordbruksproduktion i världen (ASAP), Europeiska nätverket av informationssystem för växtskydd (Europhyt), EU:s team för akuta veterinärmedicinska frågor Systemet för snabb varning för livsmedel och foder (RASFF) Den europeiska mekanismen för beredskap och insatser vid livsmedelsförsörjningskriser Förordningen om krissituationer och resiliens på den inre marknaden
Tillverkning	Medicintekniska produkter	Ej tillämpligt
	Datorer, elektronikvaror och optik	Ej tillämpligt
	Maskiner och utrustning	Ej tillämpligt
	Tillverkning av motorfordon, släpfordon och påhängsvagnar	Ej tillämpligt

	Tillverkning av andra transportmedel	Ej tillämpligt
Digitala leverantörer		Ej tillämpligt
Forskning		Ej tillämpligt

BILAGA III – EU:s ram för hantering av cybersäkerhetskriser och relaterade instrument

Sedan 2017 har unionen utvecklat sin cybersäkerhetsram genom flera instrument som innehåller bestämmelser av relevans för hanteringen av cybersäkerhetskriser:

- Europaparlamentets och rådets förordning (EU) 2019/881[1],
- Europaparlamentets och rådets direktiv (EU) 2022/2555[2],
- Kommissionens genomförandeförordning 2024/2690[3], Europaparlamentets och rådets förordning (EU, Euratom) 2023/2841[4],
- Europaparlamentets och rådets förordning (EU) 2021/887[5],
- Europaparlamentets och rådets förordning (EU) 2024/2847[6], och
- Europaparlamentets och rådets förordning (EU) 2025/38 (*cybersolidaritetsakten*)[7].

Bland de sektorsspecifika cyberkrisåtgärderna kan nämnas kommissionens delegerade förordning (EU) 2024/1366[8] och det kommande ramverket för samordning av åtgärder mot systemiska cyberincidenter (EU-SCICF) inom ramen för Europaparlamentets och rådets förordning (EU) 2022/2554[9].

Direktiv 2013/40/EU[10] utgör referensen för definitionen av brottslig verksamhet i samband med cyberattacker, och unionens regler om gränsöverskridande tillgång till elektroniska bevis, särskilt Europaparlamentets och rådets förordning (EU) 2023/1543[11], när den väl har genomförts, kommer det att i betydande mån underlätta brottsbekämpande åtgärder på detta område.

I EU:s politik för cyberförsvar[12] beskrivs rollerna för ett operativt EU-nätverk för militära it-incidenthanteringsorganisationer (Micnet) och konferensen för EU:s cyberbefälhavare samt planer på att inrätta EU:s samordningscentrum för cyberförsvar (EUCDCC).

Andra, icke-cyberrelaterade mekanismer för situationsmedvetenhet och krishantering finns inom vissa av de kritiska sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555.

I rådets rekommendation om en plan för samordnade insatser på unionsnivå vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse[13] föreskrivs samarbete mellan berörda aktörer när en incident påverkar både fysiska aspekter och cybersäkerheten för kritisk infrastruktur.

[1] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[2] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] Kommissionens genomförandeförordning (EU) 2024/2690 av den 17 oktober 2024 om fastställande av regler för tillämpningen av direktiv (EU) 2022/2555 vad gäller tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet och närmare angivelse av i vilka fall en incident ska anses vara betydande med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster (EUT L, 2024/2690, 18.10.2024). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] Europaparlamentets och rådets förordning (EU, Euratom) 2023/2841 av den 13 december 2023 om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer (EUT L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

[5] Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum (EUT L 202, 8.6.2021, s. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[6] Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) (EUT L, 2024/2847, 20.11. 2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Europaparlamentets och rådets förordning (EU) 2025/38 av den 19 december 2024 om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter och om ändring av förordning (EU) 2021/694 (cybersolidaritetsförordningen) (EUT L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] Kommissionens delegerade förordning (EU) 2024/1366 av den 11 mars 2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2019/943 genom inrättandet av en nätföreskrift om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden (EUT L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] Europaparlamentets och rådets direktiv 2013/40/EU av den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF (EUT L 218, 14.8.2013, s. 8, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden samt Europaparlamentets och rådets direktiv (EU) 2023/1544 av den 12 juli 2023 om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden (EUT L 191, 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