EUROPA-
KOMMISSIONEN

Bruxelles, den 24.2.2025
COM(2025) 66 final

ANNEXES 1 to 3

BILAG

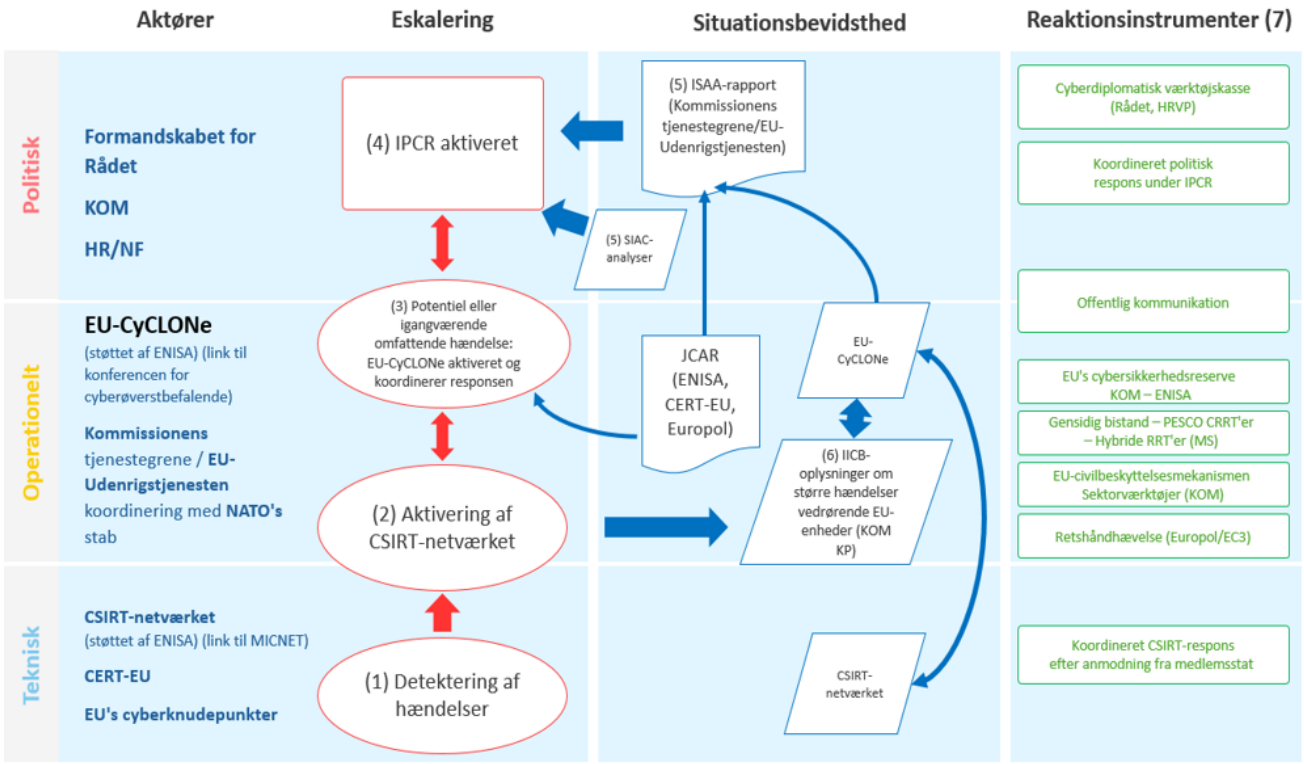
til

Forslag til RÅDETS HENSTILLING

om en EU-plan for cyberkrisestyring

BILAG I – Unionens plan for reaktion på en cybersikkerhedskrise

Nedenstående diagram illustrerer og sammenfatter Unionens cyberplan: Hvem der taler med hvem i en EU-cybersikkerhedskrise i overensstemmelse med de relevante EU-krisemekanismer i bilag II nedenfor. En sådan krise vil uundgåeligt få konsekvenser i den virkelige verden i en eller flere kritiske sektorer, hvilket kræver tæt koordinering mellem cybersamfundet og sektorspecifikke mekanismer og civilbeskyttelsesmekanismer. En cyberhændelse kan være en del af bredere hybride kampagner, og cyberindsatsen bør derfor koordineres med andre foranstaltninger i overensstemmelse med strategien for en beredskabsunion.



(1) CSIRT'er og/eller grænseoverskridende cyberknudepunkter opdager en omfattende cybersikkerhedshændelse.
(2) CSIRT-netværket eskalerer i overensstemmelse med interne procedurer.
(3) EU-CyCLONe koordinerer den operationelle indsats i tilfælde af en omfattende hændelse.
(4) Formandskabet for Rådet afgør i samråd med medlemsstaterne, Kommissionen og den højtstående repræsentant, om EU's kriseordninger (IPCR) skal aktiveres eller deaktiveres.
(5) Hvis IPCR aktiveres, danner ISAA-rapporter udarbejdet af Kommissionens tjenestegrene og EU-Udenrigstjenesten grundlag for drøftelserne. EU-CyCLONe og JCAR bør levere input til ISAA. Rådet modtager også SIAC-analyser til orientering.
(6) CERT-EU er ansvarlig for den operationelle reaktion på kriser, der påvirker EU-enheder. Relevante oplysninger kan gives til EU-CyCLONe af IICB via Kommissionen som kontaktpunkt.
(7) Rådet, EU-CyCLONe og CSIRT-netværket har overblik over svarene på henholdsvis politisk, operationelt og teknisk niveau.

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

(1) Relevante aktører på EU-plan i hele cyberkrisestyringens livscyklus

Niveau/trin	Beredskab	Detektion	Reaktion	Genoprettelse
Politisk	• Rådet • Kommissionen • EU-Udenrigstjenesten		• Rådet • Kommissionen • EU-Udenrigstjenesten	
Operationelt	• EU-CyCLONe • ENISA • Kommissionen • Europol		• EU-CyCLONe • Kommissionen • ENISA • CERT-EU (for hændelser, der påvirker EU-enheder) • Europol	• ENISA
Teknisk	• CSIRT-netværket • Grænseoverskridende cyberknudepunkter • CERT-EU	• CSIRT-netværket • Grænseoverskridende cyberknudepunkter • CERT-EU	• CSIRT-netværket • CERT-EU	• CSIRT-netværket • CERT-EU

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

Aktør	Niveau	Rolle og kompetence	Henvisning
CERT-EU	Teknisk/operationelt	Koordinerer indsatsen og håndteringen af større hændelser, der påvirker EU-enheder. Medlem af CSIRT-netværket. Støtter Kommissionen i EU-CyCLONe. Fungerer som knudepunkt for udveksling af cybersikkerhedsoplysninger og	Europa-Parlamentets og Rådets forordning (EU, Euratom) 2023/2841

Aktør	Niveau	Rolle og kompetence	Henvisning
		koordinering af reaktionen på hændelser og letter udvekslingen af oplysninger om hændelser, cybertrusler, sårbarheder og nærvedhændelser mellem EU-enheder og -modparter. Anmoder om indsættelse af EU's cybersikkerhedsreserve på vegne af EU-enheder. Samarbejder med NATO's Center for Cybersikkerhed på baggrund af deres tekniske aftale.	
Formandskabet for Rådet for Den Europæiske Union	Politisk	Beslutter (undtagen når solidaritetsbestemmelsen aktiveres i henhold til artikel 222 i TEUF), om IPCR skal aktiveres eller deaktiveres efter opfordring fra en medlemsstat, i samråd med de berørte medlemsstater, alt efter hvad der er relevant, samt Kommissionen og HR, og hvornår der skal ske en eskalering eller nedtrapning fra den ene aktiveringsfunktion til den anden.	Artikel 16 i traktaten om Den Europæiske Union, Rådets gennemførelsesafgørelse (EU) 2018/1993
Grænseoverskridende cyberknudepunkter	Teknisk	De består af tre eller flere nationale cyberknudepunkter og sikrer udveksling af relevante oplysninger vedrørende cybertrusler, nærvedhændelser, kompromitteringsindikatorer og cyberalarmer inden for det grænseoverskridende knudepunkt. Samarbejder tæt med CSIRT-netværket om at udveksle oplysninger. Giver oplysninger om en potentiel eller igangværende omfattende cybersikkerhedshændelse til	Forordning (EU) 2025/38

Aktør	Niveau	Rolle og kompetence	Henvisning
		medlemsstaternes myndigheder og Kommissionen gennem EU-CyCLONe og CSIRT-netværket.	
CSIRT-netværket	Teknisk	Udveksler relevant information om hændelser, nærvedhændelser, cybertrusler, risici og sårbarheder. Efter anmodning fra et medlem, der potentielt er berørt af en hændelse, udveksler og drøfter netværket oplysninger om den pågældende hændelse og tilknyttede cybertrusler. Netværket kan også gennemføre en koordineret reaktion på en hændelse, der er blevet identificeret inden for et anmodende medlems jurisdiktion. Modtager oplysninger fra medlemsstaterne vedrørende deres anmodninger til EU's cybersikkerhedsreserve.	Artikel 15 i direktiv (EU) 2022/2555
Konferencen af cyberøverstbefalende		Et forum for cyberøverstbefalende på nationalt plan i medlemsstaterne, hvor de kan samarbejde og udveksle vigtige oplysninger om igangværende cyberspaceoperationer og strategier til afbødning af omfattende cyberhændelser. Den organiseres af det roterende formandskab for Rådet for Den Europæiske Union med støtte fra Det Europæiske Forsvarsagentur (EDA), Tjenesten for EU's Optræden Udadtil (EU-Udenrigstjenesten) og EU's Militærstab (EUMS).	Fælles meddelelse om cyberforsvar

Aktør	Niveau	Rolle og kompetence	Henvisning
Kommissionen	Operationelt/politisk	Sikring af et velfungerende indre marked Udarbejdelse af analyserapporter (ISAA) til IPCR-mekanismen. Generelle beredskabsforanstaltninger, herunder forvaltning af Katastrofeberedskabskoordinationscentret og det fælles varslings- og informationssystem. Observatør i EU-CyCLONe og medlem i tilfælde af potentielle eller igangværende omfattende hændelser. Observatør i CSIRT-netværket. Overordnet ansvar for gennemførelsen af EU's cybersikkerhedsreserve. Kontaktpunkt for Det Interinstitutionelle Råd for Cybersikkerhed med henblik på udveksling af relevante oplysninger i relation til større hændelser med EU-CyCLONe. Strategisk tilsyn med Galileosikkerhedsovervågning scentret. (GSMC) Høres af formandskabet for Rådet om beslutninger om at aktivere eller deaktivere IPCR. Kommissionens tjenestegrene udarbejder sammen med EU-Udenrigstjenesten ISAA-rapporten.	Artikel 17 i traktaten om Den Europæiske Union Gennemførelsesafgørelse (EU) 2018/1993 Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU Direktiv (EU) 2022/2555 Forordning (EU) 2025/38, forordning (EU, Euratom) 2023/2841
Den Europæiske Unions Agentur for Cybersikkerhed (ENISA)	Teknisk/operationelt	Varetager sekretariatsfunktionen for CSIRT-netværket og EU-CyCLONe. Hjælper med at udvikle en fælles reaktion på omfattende grænseoverskridende	NIS 2-direktivet (EU) 2022/2555 Forordning (EU) 2019/881 Forordning (EU) 2025/38

Aktør	Niveau	Rolle og kompetence	Henvisning
		hændelser eller kriser ved at: samle og analysere rapporter fra nationale kilder sikre informationsstrømmen mellem teknisk, operationelt og politisk niveau lette håndteringen af hændelser støtte EU-enheder med hensyn til offentlig kommunikation afprøve kapaciteten til at reagere på hændelser. Driver og administrerer EU's cybersikkerhedsreserve, helt eller delvist, som fastsat i forordningen om cybersolidaritet. Gennemgår og vurderer trusler, kendte sårbarheder og afbødende foranstaltninger i forbindelse med en specifik væsentlig eller omfattende cyberhændelse. Udarbejder en rapport om gennemgang af hændelser.	Forordning (EU) 2024/2847
Det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe)	Operationelt	Støtter den koordinerede håndtering af store cybersikkerhedshændelser og -kriser på operationelt plan. Sikrer en regelmæssig udveksling af relevante oplysninger mellem medlemsstaterne og EU's institutioner, organer, kontorer og agenturer. Koordinerer håndteringen af omfattende cybersikkerhedshændelser og kriser og støtter beslutningstagningen på politisk plan i forbindelse med sådanne hændelser og kriser. Vurderer konsekvenserne og indvirkningen af relevante	Direktiv (EU) 2022/2555 Forordning (EU) 2025/38

Aktør	Niveau	Rolle og kompetence	Henvisning
		omfattende cybersikkerhedshændelser og kriser og foreslår mulige afbødende foranstaltninger. Udvikler sammen med ENISA den skabelon, der skal lette indgivelsen af anmodninger om støtte fra EU's cybersikkerhedsreserve. Modtager oplysninger fra medlemsstaterne vedrørende deres anmodninger til EU's cybersikkerhedsreserve. Modtager oplysninger om en potentiel eller igangværende omfattende cybersikkerhedshændelse fra de grænseoverskridende cyberknudepunkter eller CSIRT-netværket.	
Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik støttet af Tjenesten for EU's Optræden Udadtil	Politisk	Fører an i og koordinerer Unionens indsats for at imødegå eksterne sikkerhedstrusler på områderne hybride trusler og cybertrusler. Ansvarlig for Unionens cyberdiplomati og cyberforsvarsinstrumenter med henblik på at afskrække fra og reagere på eksterne trusler ved hjælp af Unionens hybride og cyberdiplomatiske værktøjskasser. Samarbejder med eksterne partnere, også gennem FSFP-engagement. Tilvejebringer Unionens og medlemsstaternes situationsbevidsthed og kapacitet til at reagere på hybride trusler og cybertrusler, f.eks. gennem praktiske øvelser, uddannelse og netværk. Håndterer sikkerheds- og	Rådets afgørelse 2010/427/EU

Aktør	Niveau	Rolle og kompetence	Henvisning
		forsvarsmæssige konsekvenser af Unionens rumaktiver, navnlig inden for rammerne af Unionens fælles sikkerheds- og forsvarspolitik (FSFP). Høres af formandskabet for Rådet om beslutninger om at aktivere eller deaktivere IPCR. EU-Udenrigstjenesten udarbejder sammen med Kommissionens tjenestegrene ISAA-rapporten.	
Europol	Operationelt	Yder operationel og teknisk støtte til medlemsstaternes kompetente myndigheder med henblik på forebyggelse af og afskrækkelse fra cyberkriminalitet.	Forordning (EU) 2016/794, herunder alle ændringer
Det Interinstitutionelle Råd for Cybersikkerhed		Godkender den interinstitutionelle cyberkrisestyringsplan for EU-enheder. Vedtager på grundlag af et CERT-EU-forslag retningslinjer eller henstillinger om samarbejde om reaktion på væsentlige hændelser vedrørende EU-enheder. .	Europa-Parlamentets og Rådets forordning (EU, Euratom) 2023/2841
Det operationelle netværk for militære IT-beredskabsenheder (MICNET)	Teknisk	Fremmer en mere solid og koordineret reaktion på cybertrusler, der påvirker forsvarssystemerne i Unionen, bl.a. de systemer, der anvendes til militære FSFP-missioner og -operationer. Oprettet og støttet af Det Europæiske Forsvarsagentur.	Fælles meddelelse om cyberforsvar 2022
Den fælles efterretningsanalysekapacitet (SIAC)		Består af 1) EU's Efterretnings- og Situationscenter (EU INTCEN), der håndterer civile efterretninger og efterretninger	Artikel 38 og 42-46 i traktaten om Den Europæiske Union, Rådets

Aktør	Niveau	Rolle og kompetence	Henvisning
		fra åbne kilder og leverer strategiske efterretninger om udenrigspolitik, terrorisme og hybride trusler, og 2) Efterretningsdirektoratet under EU's Militærstab (EUMS INT), der håndterer militære efterretninger til FSFP-missioner og støtter Unionens forsvars- og krisestyringsoperationer. Under den højtstående repræsentants myndighed.	fælles aktion 2001/555/FUSP Rådets afgørelse 2010/461/FUSP

(3) Relevante krisemekanismer på EU-plan

Mekanisme	Horisontal/sektor/cyberspecifik	Beskrivelse	Henvisning
ARGUS	Horisontal	Giver Kommissionen mulighed for at udveksle relevante oplysninger om nye multisektorale kriser eller forudseelige eller overhængende trusler, der kræver handling på EU-plan.	Meddelelse fra Kommissionen COM(2005) 662
EU-Udenrigstjenestens kriseresponscenter (CRC)	Horisontal	Det fælles kontaktpunkt for alle kriserelaterede spørgsmål i EU-Udenrigstjenesten og den permanente kriseberedskabskapacitet døgnet rundt til nødsituationer, der truer sikkerheden for personalet i EU-delegationerne og/eller som reaktion på kriser, der påvirker EU-borgere i udlandet. Det samler sikkerhedseksperter, konsulære eksperter og eksperter i situationsbevidsthed, samtidig med at der trækkes på engagerede fagfolk på stedet i EU-delegationerne.	Et strategisk kompas for sikkerhed og forsvar – For en Europæisk Union, der beskytter sine borgere, værdier og interesser og bidrager til international fred og sikkerhed (21.3.2022).
Plan for kritisk infrastruktur	Horisontal	Koordinerer en reaktion på EU-plan på forstyrrelser af kritisk infrastruktur af væsentlig	Rådets henstilling C/2024/4371

Mekanisme	Horisontal/sektor/cyberspecifik	Beskrivelse	Henvisning
		grænseoverskridende relevans.	
Varslingssystemet for cybersikkerhed	Cyberspecifik	Sikrer avanceret EU-kapacitet til at forbedre detektions-, analyse- og databehandlingskapaciteten i forbindelse med cybertrusler og forebyggelse af hændelser i Unionen.	Forordning (EU) 2025/38 (forordningen om cybersolidaritet), EUT L, 15.1.2025.
Cyberdiplomatisk værktøjskasse (ramme for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter)	Cyberspecifik	Unionens fælles diplomatiske reaktion på ondsindede cyberaktiviteter, der bidrager til forebyggelse af konflikter, afbødning af cybersikkerhedstrusler og øget stabilitet i internationale forbindelser.	Rådets konklusioner af 19. juni 2017 Reviderede gennemførelsesretningslinjer 10289/23, 8.6.2023
Den europæiske cyberreserve	Cyberspecifik	Mobiliserer cybersikkerhedseksperter og -ressourcer under kriser for at støtte indsatsen i medlemsstaterne, Unionens institutioner, organer eller agenturer	Forordning (EU) 2025/38
Netregler om sektorspecifikke regler for cybersikkerhedsaspekter af grænseoverskridende elektricitetsstrømme	Sektor	Fastlægger en tilbagevendende proces for cybersikkerhedsrisikovurderinger i elsektoren, indeholder bestemmelser, der er specifikke for krisestyring, og forbindelser til CSIRT-netværket og EU-CyCLONe.	Kommissionens delegerede forordning (EU) 2024/1366
EU-Koordinationscentret for Cyberforsvar	Horisontal	Dets oprindelige mål er primært at øge Unionens og dens medlemsstaters fælles situationsbevidsthed om ondsindede aktiviteter i cyberspace, navnlig i forbindelse med militære FSFP-missioner og -operationer.	Fælles meddelelse om cyberforsvar 2022
Hybridværktøjskasse	Horisontal	Indeholder et sæt bestemmelser, der skal sikre et overblik over, hvad der er tilgængeligt på EU-plan som reaktion på alle former for hybride trusler, deres koordinerede	Rådets konklusioner om en ramme for en koordineret EU-reaktion på hybride kampagner, 22. juni

Mekanisme	Horisontal/sektor/cyberspecifik	Beskrivelse	Henvisning
		anvendelse og sammenhæng i foranstaltningerne på tværs af områder. Den hybride værktøjskasse bidrager til at sikre, at beslutningstagningen baseres på en omfattende situationsbevidsthed og de indhøstede erfaringer.	2022
Hybride hurtige reaktionshold (EU-hybridberedskabshold)	Horisontal	Som led i den hybride EU-værktøjskasse trækker EU-hybridberedskabshold på relevant sektorspecifik national og EU's civile og militære ekspertise for at yde skræddersyet og målrettet kortsigtet bistand til medlemsstaterne, missioner og operationer under den fælles sikkerheds- og forsvarspolitik og partnerlande i forbindelse med imødegåelse af hybride trusler og kampagner.	Vejledende ramme for den praktiske oprettelse af EU-hybridberedskabshold (21.5.2024)
IPCR	Horisontal	Støtter en hurtig og koordineret beslutningstagning på EU's politiske niveau i forbindelse med større og komplekse kriser, herunder terrorhandlinger. Beslutningen om at aktivere og deaktivere træffes af formandskabet for Rådet, som (medmindre solidaritetsbestemmelsen er blevet påberåbt) hører de berørte medlemsstater, Kommissionen og HR. GSR, Kommissionens tjenestegrene og EU-Udenrigstjenesten kan også i samråd med formandskabet aftale at aktivere IPCR i informationsudvekslingsfunktion. Drøftelserne er baseret på ISAA-rapporten, der er udarbejdet af Kommissionens tjenestegrene og EU-Udenrigstjenesten. Rapporten baseres på relevante oplysninger og analyser fra medlemsstaterne (eksempelvis fra relevante nationale	Rådets gennemførelsesafgørelse (EU) 2018/1993

Mekanisme	Horisontal/sektor/cyberspecifik	Beskrivelse	Henvisning
		krisecentre), navnlig gennem webplatformen, og fra EU-agenturer.	
EU's beredskabsprotokol om retshåndhævelse	Horisontal	Et redskab til at støtte Unionens retshåndhævende myndigheder i at reagere øjeblikkeligt på større grænseoverskridende cyberangreb gennem hurtig vurdering, sikker og rettidig udveksling af kritiske oplysninger og effektiv koordinering af de internationale aspekter af deres efterforskning.	Rådets konklusioner (26.6.2018) om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser
PESCO's EU-hybridberedskabshold (CRRT)	Cyberspecifik	Udsender specialiserede teams til at reagere hurtigt på væsentlige cyberhændelser samt udføre forebyggende foranstaltninger, såsom sårbarhedsvurderinger og valgovervågning. Medlemsstatsinitiativ, delvist finansieret af Connecting Europe-faciliteten.	Artikel 42, stk. 6, artikel 46 og protokol nr. 10 til traktaten om Den Europæiske Union
Struktur for reaktion på rumtrusler (Space Threat Response Architecture, STRA)	Sektor (Rumtrusler, herunder cyberrelaterede)	Strukturen for reaktion på rumtrusler (STRA) for så vidt angår det ansvar, der skal udøves af Rådet og den højtstående repræsentant for at afværge en trussel, der opstår som følge af indførelsen, driften eller anvendelsen af de systemer, der er oprettet, og de tjenester, der leveres under Unionens rumprogram	Rådets afgørelse (FUSP) 2021/698
Rammen for koordinering af systemiske cyberhændelser (EU-SCICF)	Sektor	En ramme under udvikling til kommunikation og koordinering, som håndterer og styrer potentielle systemiske cyberhændelser i den finansielle sektor. Den vil bygge på en af de europæiske tilsynsmyndigheders (ESA'ers) planlagte roller i henhold til forordning (EU) 2022/2554 med hensyn til gradvist at muliggøre en effektiv koordineret reaktion på EU-plan i tilfælde af en større	Det Europæiske Udvalg for Systemiske Risicis henstilling af 2. december 2021 om en paneuropæisk ramme for relevante myndigheders koordinering i tilfælde af systemiske cyberhændelser (ESRB/2021/17)

Mekanisme	Horisontal/sektor/cyberspecifik	Beskrivelse	Henvisning
		grænseoverskridende hændelse vedrørende informations- og kommunikationsteknologi (IKT) eller en dermed forbundet trussel, der har en systemisk indvirkning på Unionens finansielle sektor som helhed.	
EU-civilbeskyttelsesmekanismen	Horisontal	Sikrer samarbejde om civilbeskyttelse for at forbedre katastrofeforebyggelsen, -beredskabet og -indsatsen.	Beslutning 1313/2013
CISE – Den fælles ramme for informationsudveksling	Specifikt maritimt område, der dækker syv sektorer	CISE er et netværk, der forbinder systemer hos EU/EØS-myndigheder med ansvar for havovervågning. CISE muliggør udveksling af relevante oplysninger på tværs af grænser og forskellige sektorer på en problemfri og automatiseret måde.	Et strategisk kompas for sikkerhed og forsvar – For en Europæisk Union, der beskytter sine borgere, værdier og interesser og bidrager til international fred og sikkerhed (21.3.2022)

(4) Sektorer af særligt kritisk betydning og andre kritiske sektorer i henhold til direktiv (EU) 2022/2555 og sektorspecifikke krisemekanismer på EU-plan (hvor det er relevant)

Sektor	Delsektor	Gældende sektorspecifikke krisemekanismer
Energi	Elektricitet	Elektricitetskoordinationsgruppen
	Fjernvarme og fjernkøling	Ikke relevant
	Olie	Oliekoordinationsgruppen Den Europæiske Unions Myndighedsgruppe for Offshore Olie- og Gasaktiviteter (EUOAG)
	Gas	Gaskoordinationsgruppen
	Brint	Ikke relevant

Transport	Luft	Krisekoordineringscellen for europæisk luftfart (EACCC)
	Jernbane	Ikke relevant
	Vand	EU-Fiskerikontrolagenturet (EFCA) SafeSeaNet (SSN) Integrerede maritime tjenester (IMS) Det Europæiske Datacenter for Identifikation og Sporing af Skibe på Lang Afstand (LRIT) EMSA's søfartsstøttetjenester
	Vejtransport	Ikke relevant
	Horisontal	Netværket af kontaktpunkter inden for transport, der er oprettet ved beredskabsplanen for transport (COM(2022) 211)
Bankvirksomhed		EU-SCICF
Finansielle markedsinfrastrukturer		EU-SCICF Den europæiske finansielle stabiliseringsmekanisme

Sundhed		Systemet for tidlig varsling og reaktion (EWRS) Centret for forebyggelse af og kontrol med sygdomme (HEOF) Hurtigt varslingssystem for vævs-, celle- og blodkomponenter (RATC/RAB) Ramme for folkesundhedsmæssige krisesituationer Systemet for hurtig varsling om kemiske hændelser (RASCHEM) Den europæiske overvågningsportal for smitsomme sygdomme Kriseberedskab og -indsats på Sundhedsområdet (HERA) Medicinsk sundhedsefterretningssystem (MedIsys) Højtstående Styringsgruppe vedrørende Medicinsk Udstyr (MDSSG) Hurtig varsling om lægemiddelovervågning EU-sundhedstaskforce (EUHTF)
Drikkevand		Ikke relevant
Spildevand		Ikke relevant
Digital infrastruktur		Ikke relevant
Forvaltning af IKT-tjenester		Ikke relevant
Offentlig administration		Ikke relevant
Rummet		Struktur for reaktion på rumtrusler (Space Threat Response Architecture, STRA)
Post- og kurertjenester		Ikke relevant
Affaldshåndtering		Ikke relevant

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

BILAG 3 – VEJLEDENDE PRINCIPPER

Principperne i cybersikkerhedsplanen fra 2017 er fortsat relevante.

Proportionalitetsprincippet: De fleste cybersikkerhedshændelser, der påvirker medlemsstaterne, ligger under, hvad der kan betragtes som en national krise eller en EU-krise. I tilfælde af cyberhændelser samarbejder medlemsstaterne inden for CSIRT-netværket og EU-CyCLONe i overensstemmelse med deres respektive procedurer.

Nærhedsprincippet: Medlemsstaterne har det primære ansvar for at reagere i tilfælde af væsentlige cybersikkerhedshændelser eller -kriser, der påvirker dem. Kommissionen, Tjenesten for EU's Optræden Udadtil, ENISA, CERT-EU, Europol og alle andre relevante EU-enheder spiller vigtige roller gennem hele krisens livscyklus. Disse roller er fastlagt i IPCR-ordningerne, men stammer også fra EU-retten og afspejler, hvordan cybersikkerhedshændelser og -kriser påvirker en eller flere dele af den økonomiske aktivitet i det indre marked, Unionens sikkerhed og internationale forbindelser samt institutionerne selv.

Komplementaritet: Denne henstilling tager fuldt ud hensyn til eksisterende krisestyringsmekanismer på EU-plan, nemlig IPCR-ordningerne, ARGUS og EU-Udenrigstjenestens krisereaktionsmekanisme. Den tager hensyn til CSIRT-netværkets og EU-CyCLONes ændrede roller i henhold til regler, der er vedtaget siden 2017 for at maksimere synergier og minimere dobbeltarbejde, og vedtagelsen af EU's beredskabsprotokol vedrørende retshåndhævelse.

Fortrolig behandling af oplysninger: Al informationsudveksling inden for rammerne af denne henstilling skal overholde de gældende regler om sikkerhed og beskyttelse af personoplysninger samt Traffic Light Protocol-systemet for klassifikation af følsomme oplysninger. For udveksling af klassificerede oplysninger bør der uanset det anvendte klassifikationssystem anvendes tilgængelige akkrediterede værktøjer. For så vidt angår behandling af personoplysninger skal navnlig de gældende EU-regler overholdes, herunder især Europa-Parlamentets og Rådets forordning (EU) 2016/679[1], Europa-Parlamentets og Rådets direktiv 2002/58/EF[2] samt Europa-Parlamentets og Rådets forordning (EU) 2018/1725[3].

---

1 Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

2 Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

3 Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).