Rådet for
Den Europæiske Union

Bruxelles, den 9. december 2022
(OR. en)

15623/22

Interinstitutionel sag:
2022/0338(NLE)

PROCIV 149	**ATO 102**
ENV 1248	**CSC 561**
JAI 1617	**ECOFIN 1279**
SAN 650	**CSCI 189**
COSI 315	**DATAPROTECT 346**
CHIMIE 100	**MI 912**
ENFOPOL 619	**CODEC 1916**
RECH 645	**COPS 581**
CT 220	**JAIEX 103**
DENLEG 93	**COPEN 430**
COTER 297	**IND 533**
RELEX 1657	**POLMIL 297**
ENER 654	**IPCR 116**
HYBRID 116	**DIGIT 231**
TRANS 768	**DISINFO 102**
CYBER 397	**CSDP/PSDC 848**
TELECOM 512	**MARE 71**
ESPACE 125	**POLMAR 78**

RESULTAT AF DRØFTELSERNE

fra:	Generalsekretariatet for Rådet
til:	delegationerne
Tidl. dok. nr.:	13713/22, 15454/22
Vedr.:	RÅDETS HENSTILLING om en koordineret EU-tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed

Vedlagt følger til delegationerne Rådets henstilling om en koordineret EU-tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed som vedtaget af Rådet på 3920. samling den 8. december 2022.

BILAG

RÅDETS HENSTILLING (EU) 2022/…

af ...

om en koordineret EU-tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed

(EØS-relevant tekst)

RÅDET FOR DEN EUROPÆISKE UNION,

som henviser til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 114 og artikel 292, første og andet punktum,

som henviser til forslag fra Europa-Kommissionen, og

som tager følgende i betragtning:

(1) Med henblik på at sikre det indre markeds funktion er det i alle medlemsstaters og hele Unionens interesse klart at identificere og beskytte relevant kritisk infrastruktur, der leverer væsentlige tjenester i dette marked, navnlig i nøglesektorer såsom energi, digital infrastruktur, transport og rummet, samt kritisk infrastruktur med væsentlig grænseoverskridende relevans[1], hvis afbrydelse kan påvirke andre medlemsstater betydeligt.

[1] Medlemsstaterne bør vurdere en sådan relevans i overensstemmelse med deres nationale praksis og kan gøre dette på grundlag af bl.a. en risikovurdering og begivenhedens indvirkning eller art.

(2) Denne henstilling, som er en ikkebindende retsakt, viser medlemsstaternes politiske vilje til at samarbejde indbyrdes og deres engagement i de anbefalede foranstaltninger som fremhævet i en fempunktsplan fra Europa-Kommissionens formand, samtidig med at medlemsstaternes kompetence respekteres fuldt ud. Denne henstilling berører ikke beskyttelsen af medlemsstaternes væsentlige interesser med hensyn til national sikkerhed, offentlig sikkerhed eller forsvar, og ingen medlemsstat bør forventes at dele oplysninger, der er til skade for disse interesser.

(3) Hovedansvaret for at garantere sikkerheden og leveringen af væsentlige tjenester fra kritisk infrastruktur ligger hos medlemsstaterne og deres operatører af kritisk infrastruktur, men en øget koordinering på EU-plan er hensigtsmæssig, navnlig i lyset af nye trusler, der kan påvirke flere medlemsstater samtidig, såsom Ruslands angrebskrig mod Ukraine og hybride kampagner mod medlemsstaterne, eller påvirke EU's økonomis, det indre markeds og samfundenes modstandsdygtighed og funktion som helhed. Der bør lægges særlig vægt på kritisk infrastruktur uden for medlemsstaternes område, såsom undersøisk kritisk infrastruktur eller offshore energiinfrastruktur.

(4) Det Europæiske Råd har i sine konklusioner fra den 20.-21. oktober 2022 på det kraftigste fordømt sabotagehandlingerne mod kritisk infrastruktur som dem mod Nord Stream-rørledningerne, hvilket viser, at Unionen er rede til at besvare enhver forsætlig afbrydelse af kritisk infrastruktur eller andre hybride aktioner med en fælles og beslutsom reaktion.

(5) I lyset af hvor hurtigt trusselsbilledet udvikler sig, bør der snarest muligt træffes foranstaltninger, der øger modstandsdygtigheden, i nøglesektorer som f.eks. energi, digital infrastruktur, transport og rummet og i andre relevante sektorer, som medlemsstaterne har udpeget. Sådanne foranstaltninger bør fokusere på at styrke kritisk infrastrukturs modstandsdygtighed under hensyntagen til relevante risici, navnlig kaskadevirkninger, forstyrrelse i forsyningskæden, afhængighed, virkninger af klimaændringer, upålidelige leverandører og partnere og hybride trusler og kampagner, herunder udenlandsk informationsmanipulation og indblanding. Med hensyn til national kritisk infrastruktur bør kritisk infrastruktur af væsentlig grænseoverskridende relevans prioriteres i lyset af de mulige konsekvenser. Medlemsstaterne opfordres til hurtigst muligt at træffe sådanne foranstaltninger, der øger modstandsdygtigheden, hvis det er relevant, og samtidig fastholde den tilgang, der er fastlagt i den retlige ramme, der er under udvikling.

(6) Beskyttelsen af europæisk kritisk infrastruktur i energi- og transportsektoren er i øjeblikket reguleret ved Rådets direktiv 2008/114/EF[2], og sikkerheden i net- og informationssystemer i hele Unionen med fokus på cyberrelaterede trusler sikres ved Europa-Parlamentets og Rådets direktiv (EU) 2016/1148[3]. Med henblik på at sikre et højere fælles niveau for modstandsdygtighed for og beskyttelse af kritisk infrastruktur, cybersikkerhed og det finansielle marked ændres og suppleres den eksisterende retlige ramme med vedtagelsen af nye regler for kritiske enheder ("CER-direktivet"), styrkede regler for et højt fælles cybersikkerhedsniveau i hele Unionen ("NIS 2-direktivet") og nye regler for digital operationel modstandsdygtighed i den finansielle sektor ("DORA").

(7) Medlemsstaterne bør i overensstemmelse med EU-retten og national ret anvende alle tilgængelige værktøjer til at komme videre og bidrage til at styrke den fysiske og cyberrelaterede modstandsdygtighed. I denne forbindelse bør kritisk infrastruktur forstås som omfattende relevant kritisk infrastruktur, som en medlemsstat har identificeret på nationalt plan, eller som er udpeget som en europæisk kritisk infrastruktur i henhold til direktiv 2008/114/EF, samt kritiske enheder, der skal identificeres i henhold til CER-direktivet, eller, hvis det er relevant, enheder, der er omfattet af NIS 2-direktivet. Begrebet modstandsdygtighed bør forstås som en kritisk infrastrukturs evne til at forebygge, beskytte sig mod, reagere på, modstå, afbøde, absorbere, tilpasse sig til eller komme sig over hændelser, som i væsentlig grad forstyrrer eller har potentiale til i væsentlig grad at forstyrre leveringen af væsentlige tjenester på det indre marked, dvs. tjenester, som er afgørende for opretholdelsen af vitale samfundsmæssige og økonomiske funktioner, den offentlige sikkerhed og sikring, befolkningens sundhed eller miljøet.

---

2 Rådets direktiv 2008/114/EF af 8. december 2008 om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre (EUT L 345 af 23.12.2008, s. 75).

3 Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

(8) Nationale eksperter bør sammenkaldes for at koordinere arbejdet med at opnå et højere fælles niveau af modstandsdygtighed for og beskyttelse af kritisk infrastruktur, der skal indføres med de nye regler for kritiske enheder. Dette koordinerede arbejde vil muliggøre samarbejde mellem medlemsstaterne og udveksling af oplysninger om aktiviteter såsom udarbejdelse af metoder til at identificere væsentlige tjenester, der leveres af kritisk infrastruktur. Kommissionen er allerede begyndt at sammenkalde disse eksperter og lette deres arbejde, og den har til hensigt at fortsætte dette arbejde. Når CER-direktivet er trådt i kraft, og Gruppen for Kritiske Enheders Modstandsdygtighed er oprettet i henhold til det pågældende direktiv, bør denne gruppe fortsætte dette foregribende arbejde i overensstemmelse med dens opgaver.

(9) I erkendelse af det ændrede trusselsbillede bør potentialet for at foretage stresstest af kritisk infrastruktur på nationalt niveau videreudvikles, da sådanne test kan være nyttige til at øge kritisk infrastrukturs modstandsdygtighed. Med hensyn til energisektorens særlige betydning og konsekvenser for hele Unionen som følge af en mulig forstyrrelse heraf kan denne sektor drage størst fordel af, at der foretages stresstest på grundlag af principper, der i fællesskab er opnået enighed om. Sådanne test henhører under medlemsstaternes kompetence, og medlemsstaterne bør tilskynde og støtte operatører af kritisk infrastruktur til at foretage sådanne test, når de vurderes at være gavnlige og i overensstemmelse med deres nationale retlige rammer.

(10) For at sikre en koordineret og effektiv reaktion på de nuværende og forventede trusler opfordres Kommissionen til at yde yderligere støtte til medlemsstaterne, navnlig ved at stille relevante oplysninger til rådighed i form af briefinger, ikkebindende manualer og retningslinjer. Tjenesten for EU's Optræden Udadtil (EU-Udenrigstjenesten), navnlig gennem EU's Efterretnings- og Situationscenter og dets analyseenhed for hybride trusler, bør med støtte fra Den Europæiske Unions Militærstabs (EUMS') efterretningsdirektorat inden for den fælles efterretningsanalysekapacitets SIAC-ramme tilvejebringe trusselsvurderinger. Kommissionen opfordres også til i samarbejde med medlemsstaterne at fremme deltagelsen i EU-finansierede forsknings- og innovationsprojekter.

(11) Med den stigende indbyrdes afhængighed mellem fysisk og digital infrastruktur er det muligt, at ondsindede cyberaktiviteter rettet mod kritiske områder kan føre til forstyrrelse eller beskadigelse af fysisk infrastruktur, eller at sabotage mod fysisk infrastruktur kan gøre digitale tjenester utilgængelige. Medlemsstaterne opfordres til at fremskynde det forberedende arbejde med henblik på gennemførelse og anvendelse af den nye retlige ramme for kritiske enheder og den styrkede retlige ramme for cybersikkerhed på grundlag af de erfaringer, der er gjort i samarbejdsgruppen oprettet ved direktiv (EU) 2016/1148 ("NIS-samarbejdsgruppen"), så hurtigt som muligt, idet der tages højde for gennemførelsesfristerne, og at sådant forberedelsesarbejde bør skride frem parallelt og i sammenhæng hermed.

(12) Ud over at styrke beredskabet er det også vigtigt at øge kapaciteten til at reagere hurtigt og effektivt på en forstyrrelse af væsentlige tjenester, der leveres af kritisk infrastruktur. Denne henstilling indeholder derfor foranstaltninger på både EU-plan og nationalt plan, herunder ved at fremhæve den støttende rolle og merværdi, der kan opnås ved at indføre et styrket samarbejde og udveksling af oplysninger i forbindelse med EU-civilbeskyttelsesmekanismen oprettet ved Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU[4] og ved at anvende relevante aktiver i Unionens rumprogram oprettet i henhold til Europa-Parlamentets og Rådets forordning (EU) 2021/696[5].

(13) Kommissionen, Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik ("den højtstående repræsentant") og NIS-samarbejdsgruppen skal i samarbejde med relevante civile og militære organer og agenturer og etablerede netværk, herunder Det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser (EU-CyCLONe), foretage en risikovurdering og opstille risikoscenarier. Efter den fælles opfordring fra ministermødet i Nevers foretager NIS-samarbejdsgruppen desuden i øjeblikket en risikovurdering med støtte fra Kommissionen og Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) og i samarbejde med Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC). Disse to arbejdsforløb vil være i overensstemmelse med og blive koordineret med det scenarieopbyggende arbejdsforløb inden for rammerne af EU-civilbeskyttelsesmekanismen, herunder cybersikkerhedshændelser og deres reelle konsekvenser, som Kommissionen og medlemsstaterne i øjeblikket er ved at udvikle. Af hensyn til effektiviteten, virkningen og sammenhængen og for at sikre en korrekt anvendelse af denne henstilling bør resultaterne af disse arbejdsforløb afspejles på nationalt plan.

---

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

5 Europa-Parlamentets og Rådets forordning (EU) 2021/696 af 28. april 2021 om oprettelse af Unionens rumprogram og Den Europæiske Unions Agentur for Rumprogrammet og om ophævelse af forordning (EU) nr. 912/2010, (EU) nr. 1285/2013 og (EU) nr. 377/2014 og afgørelse nr. 541/2014/EU (EUT L 170 af 12.5.2021, s. 69).

(14) For straks at styrke beredskabet og kapaciteten til at reagere på en omfattende cybersikkerhedshændelse har Kommissionen fastlagt et kortsigtet program til støtte for medlemsstaterne ved at afsætte yderligere midler til ENISA. De foreslåede tjenester omfatter bl.a. beredskabsforanstaltninger såsom penetrationstest af enheder med henblik på at kortlægge sårbarheder. Programmet kan også forbedre mulighederne for at bistå medlemsstaterne i tilfælde af en omfattende cybersikkerhedshændelse, der påvirker kritiske enheder. Dette er et første skridt i overensstemmelse med Rådets konklusioner af 23. maj 2022 om udviklingen af Den Europæiske Unions cyberposition ("Rådets konklusioner om EU's cyberposition"), hvori Kommissionen anmodes om at fremsætte et forslag til en cyberberedskabsfond. Medlemsstaterne bør fuldt ud udnytte disse muligheder i overensstemmelse med de gældende krav og opfordres til at fortsætte arbejdet inden for Unionens cyberkrisestyring, navnlig ved regelmæssigt at overvåge og gøre status over de fremskridt, der er gjort med gennemførelsen af køreplanen for cyberkrisestyring, der for nylig er udarbejdet i Rådet. Denne køreplan er et levende dokument og bør revideres og ajourføres, når det er nødvendigt.

(15) Globale undersøiske kommunikationskabler er af afgørende betydning for konnektiviteten på globalt plan og inden for EU. Som følge af sådanne kablers betydelige længde og deres placering på havbunden er det ekstremt udfordrende at sikre visuel overvågning af de fleste kabelafsnit. Den delte kompetence og andre kompetencespørgsmål i forbindelse med sådanne kabler udgør et særligt argument for et europæisk og internationalt samarbejde om beskyttelse og genopretning af infrastruktur. Det er derfor nødvendigt at supplere igangværende og planlagte risikovurderinger vedrørende digital og fysisk infrastruktur, der understøtter digitale tjenester, med specifikke risikovurderinger og muligheder for at træffe afbødende foranstaltninger i forbindelse med undersøiske kommunikationskabler. Medlemsstaterne opfordrer Kommissionen til at gennemføre undersøgelser med henblik herpå og dele sine resultater med medlemsstaterne.

(16) Energi- og transportsektoren kan også blive påvirket af trusler i forbindelse med digital infrastruktur, f.eks. i forbindelse med energiteknologier, der integrerer digitale komponenter. Sikkerheden i de tilknyttede forsyningskæder er vigtig for kontinuiteten i leveringen af væsentlige tjenester og for den strategiske kontrol med kritisk infrastruktur i energisektoren. Der bør i overensstemmelse med denne henstilling tages hensyn til disse omstændigheder, når der træffes foranstaltninger til at øge kritisk infrastrukturs modstandsdygtighed.

(17) Ruminfrastrukturs, rumrelaterede jordbaserede aktivers, herunder produktionsfaciliteters, og rumbaserede tjenesters voksende betydning for sikkerhedsrelaterede aktiviteter gør det vigtigt at sikre, at Unionens rum- og jordbaserede aktiver og tjenester inden for Unionen er modstandsdygtige og beskyttede. Af samme årsager er det også vigtigt inden for rammerne af denne henstilling at gøre mere struktureret brug af de rumbaserede data og tjenester, som rumsystemer og -programmer tilvejebringer til overvågning og sporing og til beskyttelse af kritisk infrastruktur i andre sektorer. I den kommende EU-rumstrategi for sikkerhed og forsvar vil der blive foreslået passende foranstaltninger i denne henseende, som der bør tages hensyn til ved gennemførelsen af denne henstilling.

(18) Der er også behov for samarbejde på internationalt plan for effektivt at håndtere risici for bl.a. kritisk infrastruktur i internationale farvande. Medlemsstaterne opfordres derfor til at samarbejde med Kommissionen og den højtstående repræsentant om at tage visse skridt til at opnå et sådant samarbejde, med tanke på at alle sådanne skridt dog kun skal tages i overensstemmelse med deres respektive opgaver og ansvarsområder i henhold til EU-retten, navnlig traktaternes bestemmelser om eksterne forbindelser.

(19) Kommissionen vil som fastsat i sin meddelelse af 15. februar 2022 om Kommissionens bidrag til europæisk forsvar til støtte for "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" vurdere de sektorspecifikke referencekrav til hybrid modstandsdygtighed i samarbejde med den højtstående repræsentant og medlemsstaterne ved at kortlægge mangler og behov samt tage skridt til at afhjælpe og dække disse senest i 2023. Dette initiativ bør danne grundlag for arbejdet i medfør af denne henstilling og bidrage til at styrke udvekslingen af oplysninger og koordineringen af tiltag med henblik på at styrke modstandsdygtigheden yderligere, herunder kritisk infrastrukturs modstandsdygtighed.

(20) I EU-strategien for maritim sikkerhed fra 2014 og den tilknyttede reviderede handlingsplan opfordres der til at øge beskyttelsen af kritisk maritim infrastruktur, herunder undervandsinfrastruktur, og navnlig søtransport-, energi- og kommunikationsinfrastruktur, blandt andet ved at øge den maritime situationsbevidsthed gennem forbedret interoperabilitet og strømlinet informationsudveksling (obligatorisk og frivillig). Nævnte strategi og handlingsplan er i øjeblikket ved at blive ajourført og vil omfatte skærpede foranstaltninger, som har til formål at beskytte kritisk maritim infrastruktur. Disse foranstaltninger bør supplere denne henstilling.

(21) En styrkelse af kritisk infrastrukturs modstandsdygtighed bidrager til en bredere indsats for at imødegå hybride trusler og kampagner mod Unionen og dens medlemsstater. Denne henstilling bygger på den fælles meddelelse til Europa-Parlamentet og Rådet med titlen "Fælles ramme for imødegåelse af hybride trusler – Den Europæiske Unions indsats". Foranstaltning 1 i den fælles ramme, nemlig undersøgelsen af hybride risici, spiller en central rolle med hensyn til at identificere sårbarheder, der potentielt kan påvirke nationale og paneuropæiske strukturer og netværk. Desuden vil gennemførelsen af Rådets konklusioner af 21. juni 2022 om en ramme for en koordineret EU-reaktion på hybride kampagner give mulighed for en stærkere koordineret indsats gennem anvendelse af EU's hybride værktøjskasse på alle berørte områder,

HAR VEDTAGET DENNE HENSTILLING:

KAPITEL I: MÅL, ANVENDELSESOMRÅDE OG PRIORITERING

1) I denne henstilling fastsættes en række målrettede foranstaltninger på EU-plan og nationalt plan for at støtte og øge kritisk infrastrukturs modstandsdygtighed på frivillig basis med fokus på kritisk infrastruktur af væsentlig grænseoverskridende relevans og i identificerede nøglesektorer såsom energi, digital infrastruktur, transport og rummet. Disse målrettede foranstaltninger består af øget beredskab, styrket reaktion og internationalt samarbejde.

2) Oplysninger, der deles for at nå denne henstillings mål, og som er fortrolige i henhold til EU-regler og nationale regler, samt regler om forretningshemmeligheder bør kun udveksles med Kommissionen og andre relevante myndigheder, hvis en sådan udveksling er nødvendig for den rette anvendelse af denne henstilling. Denne henstilling berører ikke beskyttelsen af medlemsstaternes væsentlige interesser med hensyn til national sikkerhed, offentlig sikkerhed eller forsvar, og ingen medlemsstat bør forventes at dele oplysninger, der strider mod disse interesser.

KAPITEL II: ØGET BEREDSKAB

Foranstaltninger på medlemsstatsplan

3) Medlemsstaterne bør overveje en tilgang, der omfatter alle farer, når de ajourfører deres risikovurderinger eller deres eksisterende tilsvarende analyser i overensstemmelse med udviklingen i arten af de aktuelle trusler mod deres kritiske infrastruktur, navnlig i identificerede nøglesektorer og så vidt muligt i alle sektorer, der er omfattet af den kommende nye retlige ramme for kritiske enheder.

4) Medlemsstaterne opfordres til at fremskynde det forberedende arbejde og vedtage foranstaltninger, der øger modstandsdygtigheden, hvor det er muligt, som fastsat i den kommende retlige ramme for kritiske enheder, med særligt fokus på samarbejde og relevant informationsudveksling mellem medlemsstaterne og med Kommissionen, på at identificere kritiske enheder med væsentlig grænseoverskridende relevans og på at øge støtten til identificerede kritiske enheder med henblik på at forbedre deres modstandsdygtighed.

5) Medlemsstaterne bør støtte eksperters uddannelse og øvelser samt udveksling af bedste praksis og erfaringer mellem eksperter. Medlemsstaterne bør tilskynde eksperter til at deltage i eksisterende uddannelsesplatforme, både nationale og internationale, for eksempel inden for rammerne af EU-civilbeskyttelsesmekanismen.

6) Medlemsstaterne bør opfordre og støtte operatører af kritisk infrastruktur, i hvert fald i energisektoren, til at foretage stresstest i overensstemmelse med principper, der i fællesskab er opnået enighed om på EU-plan, hvor det er gavnligt. Ved stresstest bør kritisk infrastrukturs modstandsdygtighed over for antagonistiske menneskeskabte trusler vurderes. Medlemsstaterne bør derfor sigte mod at identificere relevant kritisk infrastruktur, der skal testes, og rådføre sig med relevante operatører af kritisk infrastruktur så hurtigt som muligt og inden udgangen af første kvartal 2023. Desuden bør medlemsstaterne støtte operatørerne af kritisk infrastruktur, så de gennemfører disse test så hurtigt som muligt og tilstræber at afslutte dem inden udgangen af 2023 i overensstemmelse med national ret. Rådet agter at vurdere status for stresstest inden udgangen af april 2023.

7) På grund af den hastige udvikling i truslerne mod kritisk infrastruktur er det af afgørende betydning at opretholde et højt beskyttelsesniveau. Medlemsstaterne opfordres til at afsætte tilstrækkelige finansielle ressourcer til at styrke deres relevante nationale myndigheders kapacitet og til at støtte dem med henblik på at øge kritisk infrastrukturs modstandsdygtighed. Medlemsstaterne opfordres også til at afsætte tilstrækkelige finansielle ressourcer til de myndigheder, der er ansvarlige for håndteringen af omfattende cybersikkerhedshændelser, for at støtte dem og for at sikre, at deres enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), og kompetente myndigheder mobiliseres fuldt ud i henholdsvis netværket af CSIRT'er og EU-CyCLONe.

8) Medlemsstaterne opfordres til i overensstemmelse med de gældende krav at gøre brug af potentielle finansieringsmuligheder på EU-plan og nationalt plan for at øge kritisk infrastrukturs modstandsdygtighed i Unionen for dem selv og til også at tilskynde operatører af kritisk infrastruktur til at gøre brug af sådanne finansieringsmuligheder, herunder f.eks. transeuropæiske net, over for alle former for væsentlige trusler, navnlig inden for rammerne af de programmer, der finansieres af Fonden for Intern Sikkerhed, som er oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2021/1149[6], Den Europæiske Fond for Regionaludvikling, som er oprettet ved Europa-Parlamentets og Rådets forordning (EU) nr. 1301/2013[7], EU-civilbeskyttelsesmekanismen og Kommissionens REPowerEU-plan. Medlemsstaterne opfordres også til at gøre bedst mulig brug af resultaterne af relevante projekter inden for rammerne af forskningsprogrammer som Horisont Europa, der er oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2021/695[8].

---

6 Europa-Parlamentets og Rådets forordning (EU) 2021/1149 af 7. juli 2021 om oprettelse af Fonden for Intern Sikkerhed (EUT L 251 af 15.7.2021, s. 94).

7 Europa-Parlamentets og Rådets forordning (EU) nr. 1301/2013 af 17. december 2013 om Den Europæiske Fond for Regionaludvikling og om særlige bestemmelser vedrørende målet om investeringer i vækst og beskæftigelse og om ophævelse af forordning (EF) nr. 1080/2006 (EUT L 347 af 20.12.2013, s. 289).

8 Europa-Parlamentets og Rådets forordning (EU) 2021/695 af 28. april 2021 om oprettelse af Horisont Europa – rammeprogrammet for forskning og innovation – og om reglerne for deltagelse og formidling og om ophævelse af forordning (EU) nr. 1290/2013 og (EU) nr. 1291/2013 (EUT L 170 af 12.5.2021, s. 1).

9) Med hensyn til kommunikations- og netinfrastrukturen i Unionen opfordres NIS-samarbejdsgruppen til i overensstemmelse med artikel 11 i direktiv (EU) 2016/1148 at fremskynde sit igangværende arbejde på grundlag af den fælles opfordring fra ministermødet i Nevers med en målrettet risikovurdering og bør fremsætte de første anbefalinger snarest muligt. Denne risikovurdering bør give oplysninger til den igangværende tværsektorielle cyberrisikoevaluering og udarbejdelsen af scenarier, som der blev anmodet om i Rådets konklusioner om EU's cyberposition. I forbindelse med dette arbejde bør der desuden sikres sammenhæng og komplementaritet med det arbejde, der udføres af NIS-samarbejdsgruppen for sikkerhed i forsyningskæden inden for informations- og kommunikationsteknologi samt af andre relevante grupper.

10) NIS-samarbejdsgruppen opfordres også til med støtte fra Kommissionen og ENISA at fortsætte sit arbejde med sikkerheden i den digitale infrastruktur, herunder i forbindelse med undersøisk infrastruktur, navnlig undersøiske kommunikationskabler. Den opfordres desuden til at påbegynde sit arbejde med rumsektoren, herunder ved om nødvendigt at udarbejde politiske retningslinjer og metoder til styring af cybersikkerhedsrisici på grundlag af en tilgang, der omfatter alle farer, og en risikobaseret tilgang for operatører i rumsektoren med henblik på at øge modstandsdygtigheden i jordbaseret infrastruktur, som understøtter leveringen af rumbaserede tjenester.

11) Medlemsstaterne bør gøre fuld brug af de cybersikkerhedsberedskabstjenester, der tilbydes via Kommissionens kortsigtede støtteprogram, der gennemføres med ENISA, f.eks. penetrationstest for at kortlægge sårbarheder, og de opfordres i denne forbindelse til at prioritere enheder, der driver kritisk infrastruktur i sektorerne energi, digital infrastruktur og transport.

12) Medlemsstaterne bør gøre fuld brug af Det Europæiske Kompetencecenter for Cybersikkerhed (ECCC). Medlemsstaterne bør tilskynde deres nationale koordinationscentre til proaktivt at samarbejde med medlemmerne af cybersikkerhedsmiljøet for at opbygge kapacitet på EU-plan og nationalt plan med henblik på bedre at støtte operatører af væsentlige tjenester.

13) Det er vigtigt, at medlemsstaterne gennemfører de foranstaltninger, der anbefales i EU-værktøjskassen til cybersikkerhed i 5G-net, og navnlig at medlemsstaterne indfører restriktioner for højrisikoleverandører, da forsinkelser kan øge nettenes sårbarhed i Unionen, og også styrker den fysiske og ikkefysiske beskyttelse af kritiske og følsomme dele af 5G-net, herunder gennem streng adgangskontrol. Derudover bør medlemsstaterne i samarbejde med Kommissionen vurdere behovet for supplerende foranstaltninger for at sikre et ensartet niveau for 5G-nets sikkerhed og modstandsdygtighed.

14) Medlemsstaterne bør sammen med Kommissionen og ENISA fokusere på at gennemføre Rådets konklusioner af 17. oktober 2022 om sikkerhed i IKT-forsyningskæden.

15) Medlemsstaterne bør tage hensyn til de kommende netregler for cybersikkerhedsmæssige aspekter af grænseoverskridende elektricitetsstrømme[...] på grundlag af de indhøstede erfaringer med gennemførelsen af direktiv (EU) 2016/1148 og relevant vejledning udarbejdet af NIS-samarbejdsgruppen, navnlig dens referencedokument om sikkerhedsforanstaltninger for operatører af væsentlige tjenester.

16) Medlemsstaterne bør udvikle brugen af Copernicus, Galileo og den europæiske geostationære navigations-overlay-tjeneste (EGNOS) til overvågning for at sikre udvekslingen af relevante oplysninger med de eksperter, der sammenkaldes i overensstemmelse med punkt 15. De muligheder, som Unionens statslige satellitkommunikation (GOVSATCOM) inden for rammerne af dens rumprogram giver for at overvåge kritisk infrastruktur og understøtte forudsigelsen af kriser og kriseberedskabet, bør udnyttes.

Foranstaltninger på EU-plan

17) Dialogen og samarbejdet mellem medlemsstaternes udpegede eksperter og med Kommissionen bør styrkes med henblik på at øge kritisk infrastrukturs fysiske modstandsdygtighed, navnlig ved:

a) at bidrage til udarbejdelse, udvikling og fremme af fælles frivillige værktøjer til at bistå medlemsstaterne med at øge denne modstandsdygtighed, herunder metoder og risikoscenarier

b) at støtte medlemsstaterne i gennemførelsen af den nye retlige ramme for kritiske enheder, herunder ved at tilskynde Kommissionen til at vedtage den delegerede retsakt i god tid

c) at støtte foretagelse af de stresstest, der er omhandlet i punkt 6, på grundlag af fælles principper begyndende med de test, der fokuserer på antagonistiske menneskeskabte trusler i energisektoren og efterfølgende i andre nøglesektorer, samt at støtte og rådgive om foretagelse af sådanne stresstest efter anmodning fra en medlemsstat

d) at gøre brug af enhver sikker platform – når den er oprettet af Kommissionen – til på frivillig basis at indsamle, gøre status over og udveksle bedste praksis, oplysninger om nationale erfaringer og andre oplysninger vedrørende en sådan modstandsdygtighed.

Disse udpegede eksperters arbejde bør især fokusere på tværsektoriel afhængighed og kritisk infrastruktur af væsentlig grænseoverskridende relevans og bør følges op i Rådet og Kommissionen, hvis det er relevant.

18) Medlemsstaterne opfordres til at gøre brug af enhver støtte, der tilbydes af Kommissionen, f.eks. gennem udarbejdelse af manualer og retningslinjer såsom en håndbog om beskyttelse af kritisk infrastruktur og det offentlige rum mod ubemandede luftfartøjssystemer samt redskaber til at foretage risikovurderinger. EU-Udenrigstjenesten opfordres til navnlig gennem EU's Efterretnings- og Situationscenter og dets analyseenhed for hybride trusler – med støtte fra EUMS' efterretningsdirektorat inden for SIAC-rammen – at holde briefinger om truslerne mod kritisk infrastruktur i Unionen for at forbedre situationsbevidstheden.

19) Medlemsstaterne bør støtte de tiltag, der iværksættes af Kommissionen med henblik på at udbrede resultaterne af projekter om kritisk infrastrukturs modstandsdygtighed, som finansieres inden for rammerne af Unionens forsknings- og innovationsprogrammer. Rådet noterer sig, at Kommissionen har til hensigt inden for rammerne af det budget, der er afsat til Horisont Europa i den flerårige finansielle ramme for 2021-2027, at øge finansieringen af en sådan modstandsdygtighed, uden at det går ud over finansieringen af andre civile sikkerhedsrelaterede forsknings- og innovationsprojekter inden for rammerne af Horisont Europa.

20) På baggrund af de opgaver, der er beskrevet i Rådets konklusioner om EU's cyberposition, opfordres Kommissionen, den højtstående repræsentant og NIS-samarbejdsgruppen til i overensstemmelse med deres respektive opgaver og ansvarsområder i henhold til EU-retten at intensivere arbejdet med relevante net og civile og militære organer og agenturer om at gennemføre risikoevalueringer og opstille cybersikkerhedsrisikoscenarier under hensyntagen til navnlig betydningen af energi, digital infrastruktur, transport og ruminfrastruktur og den indbyrdes afhængighed på tværs af sektorer og medlemsstater. I forbindelse med dette arbejde bør der tages hensyn til de dermed forbundne risici for infrastruktur, som nævnte sektorer er afhængige af. Hvor det er gavnligt, kan risikoevalueringerne og scenarierne gennemføres regelmæssigt og bør supplere, bygge på og undgå overlapning med eksisterende eller planlagte risikovurderinger i nævnte sektorer og danne grundlag for drøftelser om, hvordan man kan styrke den overordnede modstandsdygtighed i enheder, der driver kritisk infrastruktur, og håndtere sårbarheder.

21) Kommissionen opfordres til i overensstemmelse med sine respektive opgaver inden for cyberkrisestyring at fremskynde sine aktiviteter vedrørende støtte til medlemsstaternes beredskab og reaktion over for de omfattende cybersikkerhedshændelser, navnlig:

a) som supplement til relevante risikovurderinger i forbindelse med net- og informationssikkerhed gennemføre en omfattende undersøgelse[9], der gør status over den undersøiske infrastruktur, nemlig undersøiske kommunikationskabler, der forbinder medlemsstaterne og Europa med resten af verden, og hvis resultater bør deles med medlemsstaterne

b) støtte medlemsstaternes og EU-institutionernes, -organernes og -agenturernes beredskab og reaktion over for omfattende cybersikkerhedshændelser eller større hændelser i overensstemmelse med den styrkede retlige ramme for cybersikkerhed og andre relevante gældende regler[10]

c) fremskynde hovedkonceptet for cyberberedskabsfonden med passende drøftelser med medlemsstaterne.

22) Kommissionen opfordres til at intensivere arbejdet med fremadrettede foregribende foranstaltninger, herunder samarbejdet med medlemsstaterne i henhold til artikel 6 og 10 i afgørelse 1313/2013/EU, og i form af beredskabsplanlægning til støtte for Katastrofeberedskabskoordinationscentrets (ERCC's) operationelle beredskab og reaktion over for forstyrrelser i kritisk infrastruktur, øge investeringerne i forebyggende tilgange og befolkningens beredskab og øge støtten til kapacitetsopbygning inden for rammerne af EU-Vidensnetværket om Civilbeskyttelse.

---

9 Denne undersøgelse bør omfatte kortlægning af dets kapacitet og redundans, sårbarheder, trusler og risici for tilgængeligheden af tjenester, virkningen af nedetid i (transatlantiske) undersøiske kabler for medlemsstaterne og Unionen som helhed og risikobegrænsning og samtidig tage hensyn til disse oplysningers følsomhed og behovet for at beskytte dem.

10 Der bør også lægges særlig vægt på alle aktiviteter, der forbereder en effektiv koordineret reaktion på EU-plan i tilfælde af en grænseoverskridende større cyberhændelse eller relateret trussel, der kan have en systemisk indvirkning på Unionens finansielle sektor, som fastsat i den nye retlige ramme for digital operationel modstandsdygtighed.

23) Kommissionen bør fremme anvendelsen af Unionens overvågningsaktiver (Copernicus, Galileo og EGNOS) for at støtte medlemsstaterne med at overvåge kritisk infrastruktur og omgivelserne i deres umiddelbare nærhed, når det er relevant, og støtte andre muligheder for overvågning i Unionens rumprogram såsom rammerne for kendskab til situationen i rummet og EU's overvågning og sporing i rummet.

24) EU-agenturerne og andre relevante organer opfordres til, når det er relevant og i overensstemmelse med deres respektive mandater, at yde støtte i spørgsmål vedrørende kritisk infrastrukturs modstandsdygtighed, navnlig:

a) Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol) vedrørende informationsindsamling, kriminalitetsanalyse og efterforskningsstøtte i forbindelse med grænseoverskridende retshåndhævelsesforanstaltninger og, hvor det er relevant og hensigtsmæssigt, deling af resultaterne med medlemsstaterne

b) Det Europæiske Agentur for Søfartssikkerhed (EMSA) vedrørende maritim sikkerhed i Unionen, herunder maritime overvågningstjenester i forbindelse med spørgsmål vedrørende maritim sikring og sikkerhed

c) Den Europæiske Unions Agentur for Rumprogrammet (EUSPA) og EU-Satellitcentret (Satcen) kan bistå gennem operationer inden for Unionens rumprogram

d) ECCC for så vidt angår aktiviteter vedrørende cybersikkerhed, også i samarbejde med ENISA, kan støtte innovation og industripolitik inden for cybersikkerhed.

KAPITEL III STYRKET REAKTION

Foranstaltninger på medlemsstatsplan

25) Medlemsstaterne opfordres til:

a) at fortsætte koordineringen af deres reaktion, hvor det er relevant, og bevare overblikket over den tværsektorielle reaktion på akutte forstyrrelser af væsentlige tjenester, der leveres af kritisk infrastruktur. Dette kan ske inden for rammerne af en fremtidig plan for en koordineret reaktion på betydelige forstyrrelser i kritisk infrastruktur af væsentlig grænseoverskridende relevans, eksisterende integrerede ordninger for politisk kriserespons (IPCR) til koordinering af den politiske reaktion i forbindelse med kritisk infrastruktur af grænseoverskridende relevans, planen vedrørende omfattende cybersikkerhedshændelser og -kriser i henhold til Kommissionens henstilling (EU) 2017/1584[11], EU-CyCLONe, inden for rammen for en koordineret EU-reaktion på hybride kampagner og EU-værktøjskassen i tilfælde af hybride trusler og kampagner og inden for det hurtige varslingssystem i tilfælde af desinformation

b) at øge informationsudvekslingen på operationelt plan med ERCC inden for rammerne af EU-civilbeskyttelsesmekanismen for i højere grad at sikre tidlig varsling og koordinere deres reaktion inden for rammerne af EU-civilbeskyttelsesmekanismen i tilfælde af forstyrrelser i kritisk infrastruktur af væsentlig grænseoverskridende relevans for derved at sikre en hurtigere EU-støttet reaktion, når det er nødvendigt

c) at øge deres parathed til, hvor det er relevant, at reagere ved hjælp af eksisterende værktøjer eller værktøjer, der skal udvikles, på sådanne betydelige forstyrrelser, der er nævnt i litra a)

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

d) at indgå i dialog om videreudvikling af relevant reaktionskapacitet i Den Europæiske Civilbeskyttelsespulje (ECCP) og rescEU

e) at opfordre operatører af kritisk infrastruktur og de relevante nationale myndigheder til at øge deres kapacitet til hurtigt at genetablere en basal levering af de væsentlige tjenester, der leveres af disse operatører af kritisk infrastruktur

f) at opfordre operatører af kritisk infrastruktur til, når de genopbygger deres kritiske infrastruktur – under hensyntagen til foranstaltningernes proportionalitet med hensyn til risikovurderinger og omkostninger – at opbygge den til at blive så modstandsdygtig som muligt over for alle former for væsentlige risici, som kan være forbundet med den, herunder negative klimascenarier.

26) Medlemsstaterne opfordres til om muligt at fremskynde det forberedende arbejde som fastsat i den styrkede retlige ramme for cybersikkerhed ved at tilstræbe at styrke kapaciteten i de nationale enheder, der håndterer CSIRT'er, med henblik på de nye opgaver, som disse CSIRT'er og det udvidede antal enheder fra nye sektorer har, ved rettidigt at revidere og ajourføre deres cybersikkerhedsstrategier og hurtigst muligt vedtage nationale planer vedrørende cybersikkerhedshændelser og kriseberedskab, hvis de ikke allerede har gjort det.

27) Medlemsstaterne opfordres til på nationalt plan at overveje de mest relevante midler til at sikre, at relevante interessenter er opmærksomme på behovet for at fremme kritisk infrastrukturs modstandsdygtighed gennem samarbejde med pålidelige leverandører og partnere. Det er vigtigt at investere i yderligere kapacitet, navnlig i de sektorer, hvor den nuværende infrastrukturs levetid er ved at udløbe (f.eks. infrastruktur til undersøiske kommunikationskabler), for at kunne sikre kontinuitet i leveringen af væsentlige tjenester i tilfælde af forstyrrelser og mindske uønskede afhængighedsforhold.

28) Medlemsstaterne opfordres til at være opmærksomme på proaktiv strategisk kommunikation på nationalt plan i forbindelse med imødegåelse af hybride trusler og kampagner og i betragtning af muligheden for, at modstandere kan søge at udøve udenlandsk informationsmanipulation og indblanding ved at udforme narrativer om hændelser rettet mod kritisk infrastruktur.

Foranstaltninger på EU-plan

29) Kommissionen opfordres til at arbejde tæt sammen med medlemsstaterne om at videreudvikle relevante organer, instrumenter og reaktionskapacitet med henblik på at styrke det operationelle beredskab for at håndtere de umiddelbare og indirekte virkninger af betydelige forstyrrelser af relevante væsentlige tjenester, der leveres af kritisk infrastruktur, navnlig eksperter og ressourcer, der er til rådighed gennem ECPP og rescEU inden for rammerne af EU-civilbeskyttelsesmekanismen eller fremtidige hybridberedskabshold.

30) Under hensyntagen til udviklingen i trusselsbilledet og i samarbejde med medlemsstaterne opfordres Kommissionen i forbindelse med EU-civilbeskyttelsesmekanismen til:

a) løbende at analysere og teste den eksisterende reaktionskapacitets tilstrækkelighed og operationelle parathed

b) regelmæssigt at overvåge og identificere potentielt betydelige mangler i reaktionskapaciteten i ECPP's og rescEU's kapacitet

c) yderligere at intensivere det tværsektorielle samarbejde for at sikre en passende reaktion på EU-plan og tilrettelægge regelmæssige uddannelsestiltag og øvelser for at teste et sådant samarbejde i samarbejde med en eller flere medlemsstater

d) at videreudvikle ERCC som det tværsektorielle nødknudepunkt på EU-plan for koordineringen af støtten til de berørte medlemsstater.

31) Rådet er fast besluttet på at indlede arbejdet med henblik på godkendelse af en plan for en koordineret reaktion på forstyrrelser i kritisk infrastruktur af væsentlig grænseoverskridende relevans, der beskriver og fastsætter mål og metoder for samarbejdet mellem medlemsstaterne og EU-institutionerne, -organerne, -kontorerne og -agenturerne med hensyn til at reagere på hændelser mod sådan kritisk infrastruktur. Rådet ser frem til Kommissionens udkast til en sådan plan, der bygger på støtte og bidrag fra relevante EU-agenturer. Planen skal være fuldt ud sammenhængende og interoperabel med Unionens reviderede operationelle protokol for at imødegå hybride trusler ("EU-drejebogen") og tage hensyn til den eksisterende plan for en koordineret reaktion på omfattende grænseoverskridende cybersikkerhedshændelser[12] og -kriser og EU-CyCLONe's mandat som fastsat i NIS 2-direktivet og undgå overlapning af strukturer og aktiviteter. Planen bør fuldt ud respektere de eksisterende IPCR-ordninger til at koordinere reaktionen.

[12] Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser.

32) Kommissionen opfordres til at rådføre sig med relevante interessenter og eksperter om passende foranstaltninger i forbindelse med mulige væsentlige hændelser vedrørende undersøisk infrastruktur, som skal fremlægges i forbindelse med den statusundersøgelse, der er omhandlet i punkt 20, litra a), samt om yderligere at udarbejde beredskabsplaner og risikoscenarier og EU-mål for katastrofemodstandsdygtighed som fastsat i afgørelse nr. 1313/2013/EU.

KAPITEL IV INTERNATIONALT SAMARBEJDE

Foranstaltninger på medlemsstatsplan

33) Medlemsstaterne bør, når det er relevant og i overensstemmelse med EU-retten, samarbejde med relevante tredjelande for så vidt angår modstandsdygtigheden i kritisk infrastruktur af væsentlig grænseoverskridende relevans.

34) Medlemsstaterne opfordres til at samarbejde med Kommissionen og den højtstående repræsentant for effektivt at håndtere risici for kritisk infrastruktur i internationale farvande.

35) Medlemsstaterne opfordres til i samarbejde med Kommissionen og den højtstående repræsentant at bidrage til den fremskyndede udvikling og gennemførelse af EU's hybride værktøjskasse og gennemførelsen af de retningslinjer, der er omhandlet i Rådets konklusioner af 21, juni 2022 om en ramme for en koordineret EU-reaktion på hybride kampagner, og senere anvende dem for derved at sikre, at denne ramme for en koordineret EU-reaktion på hybride kampagner får fuld virkning, navnlig når der pågår overvejelser om og forberedelse af en omfattende og koordineret EU-reaktion på hybride kampagner og hybride trusler, bl.a. mod operatører af kritisk infrastruktur.

Foranstaltninger på EU-plan

36) Kommissionen og den højtstående repræsentant opfordres til, hvor det er relevant og i overensstemmelse med deres respektive opgaver og ansvarsområder i henhold til EU-retten, at støtte relevante tredjelande for at øge modstandsdygtigheden af kritisk infrastruktur på deres område og navnlig kritisk infrastruktur, som er fysisk sammenkoblet med deres område og en medlemsstats område.

37) Kommissionen og den højtstående repræsentant vil i overensstemmelse med deres respektive opgaver og ansvarsområder i henhold til EU-retten styrke koordineringen med NATO om modstandsdygtigheden af kritisk infrastruktur af fælles interesse gennem den strukturerede dialog mellem EU og NATO om modstandsdygtighed under fuld overholdelse af Unionens og medlemsstaternes kompetencer i henhold til traktaterne og de centrale principper for samarbejdet mellem EU og NATO som fastlagt af Det Europæiske Råd, navnlig gensidighed, inklusion og beslutningsautonomi. I denne sammenhæng vil dette samarbejde blive videreført inden for rammerne af den strukturerede dialog mellem EU og NATO om modstandsdygtighed, der indgår i den eksisterende mekanisme på medarbejderniveau til gennemførelse af de fælles erklæringer, samtidig med at der sikres fuld gennemsigtighed og inddragelse af alle medlemsstater.

38) Kommissionen opfordres til at overveje deltagelse af repræsentanter for relevante tredjelande, hvor det er nødvendigt og relevant, inden for rammerne af samarbejdet og informationsudvekslingen mellem medlemsstaterne om modstandsdygtigheden af kritisk infrastruktur, som er fysisk sammenkoblet med en medlemsstats og et tredjelands område.

Udfærdiget i …, den … .

På Rådets vegne

Formand