EUROPA-
KOMMISSIONEN

Strasbourg, den 18.10.2022
COM(2022) 551 final

2022/0338 (NLE)

Forslag til

RÅDETS HENSTILLING

om en koordineret tilgang fra Unionens side til styrkelse af kritisk infrastrukturs modstandsdygtighed

(EØS-relevant tekst)

BEGRUNDELSE

1. BAGGRUND FOR FORSLAGET

• Forslagets begrundelse og formål

Sikkerhed er et vigtigt mål for Den Europæiske Union. Medlemsstaterne har det primære ansvar for at beskytte borgerne, men en fælles indsats på EU-plan udgør et vigtigt bidrag til sikkerheden i EU som helhed. Koordinering bidrager til at styrke modstandsdygtigheden, forbedre agtpågivenheden og styrke vores kollektive reaktion. I forbindelse med EU's sikkerhedsunion er der taget vigtige skridt til at opbygge kompetencer og kapacitet til at forebygge, opdage og hurtigt reagere på mange sikkerhedstrusler og til at knytte aktører i den offentlige og den private sektor sammen i en fælles indsats.

At ruste EU til at håndtere det stadigt skiftende trusselsbillede kræver konstant årvågenhed og tilpasning. Ruslands angrebskrig mod Ukraine har medført nye risici, ofte kombineret som en hybrid trussel. En af disse er risikoen for afbrydelser af leveringen af væsentlige tjenester fra enheder, der driver kritisk infrastruktur i Europa. Det er blevet endnu tydeligere med den øjensynlige sabotage mod Nord Stream-gasledningerne og andre nylige hændelser. Samfundet er stærkt afhængigt af både fysisk og digital infrastruktur, og afbrydelser af væsentlige tjenester, uanset om det sker ved konventionelle fysiske angreb eller cyberangreb eller en kombination af begge dele, kan have alvorlige konsekvenser for borgernes velfærd, vores økonomier og tilliden til vores demokratiske systemer.

Sikring af et velfungerende indre marked er et andet vigtigt mål for EU, bl.a. når det kommer til væsentlige tjenester, der leveres af enheder, der driver kritisk infrastruktur. EU har derfor allerede truffet en række foranstaltninger for at mindske sårbarheder og øge kritiske enheders modstandsdygtighed, både over for cyberrelaterede og ikkecyberrelaterede risici.

Der er et presserende behov for, at der bliver gjort en indsats for at øge EU's kapacitet til at modstå potentielle angreb på kritisk infrastruktur, hovedsagelig i selve EU, men, hvor det er relevant, også i dets umiddelbare nærområde.

Forslaget til Rådets henstilling har til formål at intensivere EU's støtte til at øge kritisk infrastrukturs modstandsdygtighed og sikre koordinering på EU-plan med hensyn til beredskab og indsats. Det har til formål at maksimere og fremskynde arbejdet med at beskytte disse aktiver, faciliteter og systemer, som er nødvendige for, at økonomien kan fungere, og at sikre leveringen af væsentlige tjenester på det indre marked, som borgerne er afhængige af, samt at afbøde virkningerne af ethvert angreb ved at sikre den hurtigst mulige genopretning. Al sådan infrastruktur bør beskyttes, men på nuværende tidspunkt er det energisektoren, sektoren for digital infrastruktur, transportsektoren og rumsektoren, der har første prioritet, eftersom de spiller en særlig generel rolle for samfundet og økonomien og de aktuelle risikovurderinger

EU har en særlig rolle at spille med hensyn til at sikre modstandsdygtigheden i forbindelse med infrastruktur, der krydser land- eller søgrænser og påvirker flere medlemsstaters interesser, eller som anvendes til at levere væsentlige tjenester på tværs af grænserne. Kritisk infrastruktur med relevans for flere medlemsstater kan imidlertid ligge i en enkelt medlemsstat eller endda uden for en medlemsstats område, f.eks. i tilfælde af undersøiske kabler eller rørledninger. Det er i alle medlemsstaters og hele EU's interesse klart at få kortlagt kritisk infrastruktur og de enheder, der driver den, samt truslerne mod dem og i fællesskab at forpligte sig til at beskytte dem.

Europa-Parlamentet og Rådet er allerede nået til politisk enighed om at uddybe den lovgivningsmæssige ramme for, at EU kan hjælpe med at styrke modstandsdygtigheden i de

enheder, der driver kritisk infrastruktur. I sommeren 2022 blev der indgået aftaler om direktivet om kritiske infrastrukturers modstandsdygtighed ("CER-direktivet")[1] og det reviderede direktiv om net- og informationssystemers sikkerhed ("NIS 2-direktivet")[2]. De vil udgøre en betydelig intensivering af kapaciteten i forhold til den eksisterende lovgivningsmæssige ramme, 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 ("ECI-direktivet")[3] og 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 ("NIS-direktivet")[4]. Den nye lovgivning forventes at træde i kraft i slutningen af 2022 eller begyndelsen af 2023, og medlemsstaterne bør i overensstemmelse med EU-retten prioritere gennemførelsen og anvendelsen heraf.

I lyset heraf og af det potentielle presserende behov for at imødegå trusler, der skyldes Ruslands angrebskrig mod Ukraine, bør de skridt, der er beskrevet i den nye lovgivning, når det er muligt og hensigtsmæssigt, fremskyndes med det samme. En intensivering af det gensidige samarbejde allerede nu vil også bidrage til at skabe momentum for en effektiv gennemførelse, når den nye lovgivning er trådt fuldt ud i kraft.

Resultatet vil være, at indsatsen allerede vil strække sig ud over de nuværende rammer, både hvad angår omfanget af indsatsen og bredden i de sektorer, der er omfattet. Det nye CER-direktiv indeholder en ny ramme for samarbejde samt forpligtelser for medlemsstaterne og kritiske enheder med henblik på at styrke den fysiske ikkecyberrelaterede modstandsdygtighed over for naturlige og menneskeskabte trusler mod disse enheder, som leverer væsentlige tjenester på det indre marked, og der specificeres heri elleve sektorer[5]. Med NIS 2-direktivet vil der blive indført cybersikkerhedsforpligtelser, der sikrer en bred sektormæssig dækning. Som et nyt krav vil medlemsstaterne, når det relevant, skulle medtage undersøiske kabler i deres cybersikkerhedsstrategier.

I henhold til denne lovgivning skal Kommissionen påtage sig en betydelig koordinerende rolle. I henhold til CER-direktivet har Kommissionen en støttende og formidlende opgave, der skal udføres med støtte fra og inddragelse af Gruppen for Kritiske Enheders Modstandsdygtighed (CERG), der blev oprettet ved nævnte direktiv, og Kommissionen bør supplere medlemsstaternes aktiviteter ved at udvikle bedste praksis, vejledningsmateriale og metoder. Med hensyn til cybersikkerhed har Rådet allerede i sine konklusioner om EU's cyberposition i sommeren 2022 opfordret Kommissionen, den højtstående repræsentant og NIS-samarbejdsgruppen til at arbejde med risikovurderinger og scenarier ud fra et cybersikkerhedsperspektiv. En sådan koordinering kan give inspiration til tilgangen til andre typer vigtig kritisk infrastruktur.

Den 5. oktober 2022 fremlagde kommissionsformand Ursula von der Leyen en fempunktsplan med en koordineret tilgang til den nødvendige indsats fremover. De vigtigste elementer heri er: styrkelse af katastrofeberedskabet, samarbejde med medlemsstaterne med henblik på at stressteste deres kritiske infrastruktur, idet der begyndes med energisektoren, og derefter følger andre højrisikosektorer, forøgelse af reaktionskapaciteten, navnlig gennem EU-civilbeskyttelsesmekanismen, udnyttelse af satellitkapaciteten til at opdage potentielle trusler og styrkelse af samarbejdet med NATO og vigtige partnere om kritisk infrastrukturs

---

1 COM(2020) 829 final.
2 COM(2020) 823 final.
3 EUT L 345 af 23.12.2008.
4 EUT L194 af 19.7.2016.
5 Energi, transport, digital infrastruktur, bankvæsen, finansmarkedsinfrastruktur, sundhed, drikkevand, spildevand, offentlige forvaltning, rummet og fødevarer.

modstandsdygtighed. I fempunktsplanen blev værdien af at foregribe den lovgivning, der allerede er politisk enighed om, fremhævet.

I forslaget til Rådets henstilling hilses denne tilgang velkommen med henblik på at strukturere støtten til medlemsstaterne og koordinere deres indsats for at øge risikobevidstheden, beredskabet og reaktionen i forhold til de aktuelle trusler. Med henblik herpå sammenkaldes eksperter for at drøfte modstandsdygtigheden i enheder, der driver kritisk infrastruktur, allerede forud for ikrafttrædelsen af CER-direktivet og oprettelsen af CERG ved dette direktiv.

Det vil være afgørende at styrke samarbejdet med centrale partnere og nabolande samt andre relevante tredjelande om modstandsdygtigheden i de enheder, der driver kritisk infrastruktur, navnlig gennem den strukturerede dialog mellem EU og NATO om modstandsdygtighed.

I denne henstilling er der fokus på at styrke Unionens kapacitet til at foregribe, forhindre og reagere på de nye trusler, der skyldes Ruslands angrebskrig mod Ukraine. I de foreslåede henstillinger fokuseres der derfor på at håndtere sikkerhedsrelaterede risici og trusler mod kritisk infrastruktur. Det bør dog bemærkes, at nylige hændelser også har understreget det presserende behov for at være mere opmærksom på klimaændringernes indvirkning på kritisk infrastruktur og kritiske tjenester, f.eks. hvad angår sæsonmæssigt alarmerende lave og uforudsigelige vandforsyninger til atomkraftværkers køling, vandkraft og sejlads ad indre vandveje eller risikoen for materielle skader på transportinfrastrukturen, som kan forårsage alvorlige forstyrrelser af væsentlige tjenester. Der vil fortsat blive taget hånd om disse problemer gennem relevant lovgivning og koordinering.

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

Dette forslag til Rådets henstilling er fuldt ud i overensstemmelse med den nuværende og fremtidige retlige ramme for modstandsdygtigheden i de enheder, der driver kritisk infrastruktur i EU, ECI-direktivet og CER-direktivet, da det bl.a. tager sigte på at lette samarbejdet mellem medlemsstaterne på dette område og støtte konkrete foranstaltninger til at øge modstandsdygtigheden over for de nuværende overhængende trusler mod enheder, der driver kritisk infrastruktur i EU.

Det supplerer og foregriber også CER-direktivet ved, at medlemsstaterne allerede nu opfordres til at prioritere en rettidig gennemførelse af direktivet ved at samarbejde via de ekspertmøder, der afholdes som led i den fempunktsplan, som Kommissionen har bebudet, og ved at sigte mod at koordinere vejen henimod en fælles tilgang til gennemførelse af stresstest af kritisk infrastruktur i EU.

Forslaget er også i overensstemmelse med NIS-direktivet og det kommende NIS 2-direktiv, som vil ophæve NIS-direktivet, idet der opfordres til at starte implementeringen og gennemførelsen tidligt. Det afspejler også den fælles opfordring i Nevers i marts 2022 og Rådets konklusioner om EU's cyberposition fra maj 2022 for så vidt angår medlemsstaternes anmodning til Kommissionen om at udarbejde risikovurderinger og risikoscenarier.

Forslaget er endvidere i overensstemmelse med EU's civilbeskyttelsespolitik, hvor medlemsstaterne og tredjelande i tilfælde af en omfattende forstyrrelse af driften af kritisk infrastruktur/kritiske enheder kan anmode om bistand via Katastrofeberedskabskoordinationscentret (ERCC) og EU-civilbeskyttelsesmekanismen. I tilfælde af aktivering af EU-civilbeskyttelsesmekanismen er ERCC i stand til at koordinere og medfinansiere indsættelsen af det væsentlige udstyr, de væsentlige materialer og den væsentlige ekspertise, der er til rådighed i medlemsstaterne (delvis i forbindelse med Den Europæiske Civilbeskyttelsespulje) og inden for rammerne af rescEU i det berørte land. Den

bistand, der kan stilles til rådighed efter anmodning, omfatter f.eks. brændstof, generatorer, elinfrastruktur, indkvarteringskapacitet, vandrensningskapacitet og medicinsk nødberedskab.

Forslaget er også i overensstemmelse med gældende EU-ret vedrørende energiforsyningssikkerhed.

Kerneenergisektoren er ikke specifikt medtaget i forslaget til Rådets henstilling, undtagen f.eks. tilknyttet infrastruktur (såsom transmissionsledninger til kernekraftværker), som kan påvirke forsyningssikkerheden. De specifikke nukleare elementer er omfattet af relevant nuklear lovgivning i henhold til Euratomtraktaten og/eller national lovgivning[6]. På grundlag af erfaringerne fra Fukushimaulykken blev den europæiske lovgivning om nuklear sikkerhed styrket, og som følge heraf skal de nationale myndigheder derfor regelmæssigt foretage periodiske sikkerhedsvurderinger af hver enkelt installation for at sikre, at de fortsat overholder de højeste sikkerhedskrav, og indkredse yderligere sikkerhedsmæssige forbedringer samt foretage seks årlige tematiske peerevalueringer på EU-plan.

I EU-strategien for maritim sikkerhed[7] og den tilknyttede handlingsplan[8] fremhæves den skiftende karakter af truslerne på det maritime område, og der opfordres til fornyet engagement i beskyttelsen af kritisk maritim infrastruktur, herunder undervandsinfrastruktur, og navnlig søtransport-, energi- og kommunikationsinfrastruktur, bl.a. ved at øge den maritime situationsbevidsthed gennem forbedret interoperabilitet og strømlinet informationsudveksling.

Forslaget er også i overensstemmelse med anden relevant sektorspecifik lovgivning. Gennemførelsen af denne henstilling bør derfor være i overensstemmelse med de specifikke foranstaltninger, der regulerer eller i fremtiden kan regulere visse aspekter af modstandsdygtigheden i enheder, der er aktive i de berørte sektorer såsom transportsektoren. Dette omfatter andre relevante initiativer såsom beredskabsplanen for transport[9] eller beredskabsplanen for fødevareforsyning og fødevaresikkerhed i krisetider[10] og den tilknyttede europæiske beredskabs- og reaktionsmekanisme for fødevaresikkerhed. Mere generelt bør henstillingen naturligvis gennemføres under fuld overholdelse af alle gældende regler i EU-retten, herunder dem, der er fastsat i ECI-direktivet og NIS-direktivet.

Forslaget er også i overensstemmelse med det strategiske kompas for sikkerhed og forsvar, hvori behovet for at styrke partnerlandenes modstandsdygtighed og kapacitet til at imødegå hybride trusler og cyberangreb såvel som behovet for at styrke partnerlandenes modstandsdygtighed og samarbejdet med NATO blev fremhævet. Det er desuden i overensstemmelse med rammen for en koordineret EU-reaktion på hybride trusler og kampagner, der påvirker EU, medlemsstaterne og partnere[11].

---

6 Betragtning 9 i Rådets direktiv 2008/114/EF (ECI-direktivet).
7 11205/14.
8 10494/18.
9 COM(2022) 211.
10 COM(2021) 689.
11 Rådet for Den Europæiske Union, 10016/22, 21. juni 2022.

2. RETSGRUNDLAG, NÆRHEDSPRINCIPPET OG PROPORTIONALITETSPRINCIPPET

- **Retsgrundlag**

Forslaget har hjemmel i artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF), som vedrører tilnærmelse af lovgivningerne med henblik på forbedring af det indre marked, sammenholdt med artikel 292 i TEUF. Dette begrundes med det forhold, at forslaget til Rådets henstilling hovedsagelig tager sigte på at foregribe de foranstaltninger, der er fastsat i det nye CER-direktiv og NIS 2-direktiv, som begge også har hjemmel i artikel 114 i TEUF. I overensstemmelse med den logik, der begrunder anvendelsen af nævnte artikel som retsgrundlag for disse direktiver, er der behov for en EU-indsats for at sikre et velfungerende indre marked, navnlig i betragtning af de pågældende tjenesters grænseoverskridende karakter og omfang og de potentielle konsekvenser i tilfælde af forstyrrelser samt de nuværende og nye nationale foranstaltninger, der tager sigte på at øge modstandsdygtigheden i enheder, der driver kritisk infrastruktur, der anvendes til at levere væsentlige tjenester på det indre marked.

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

Den indbyrdes afhængige grænseoverskridende karakter af kritisk infrastruktur og de væsentlige tjenester, den leverer, og af behovet for en mere fælles og koordineret europæisk tilgang berettiger en løsning på europæisk plan med hensyn til modstandsdygtigheden i de enheder, der driver kritisk infrastruktur, for derved at sikre, at de pågældende enheder er tilstrækkeligt modstandsdygtige i den nuværende geopolitiske kontekst. Mange af de fælles udfordringer såsom den øjensynlige sabotage af North Stream-gasrørledningerne håndteres først og fremmest gennem nationale foranstaltninger eller af enheder, der driver kritisk infrastruktur, men det er nødvendigt med støtte fra EU, herunder relevante agenturer, når det er relevant, for at øge modstandsdygtigheden, forbedre agtpågivenheden og styrke EU's kollektive reaktion.

- **Proportionalitetsprincippet**

Dette forslag er i overensstemmelse med proportionalitetsprincippet, jf. artikel 5, stk. 4, i traktaten om Den Europæiske Union (TEU).

Hverken indholdet i eller udformningen af dette forslag til Rådets henstilling går videre, end hvad der er nødvendigt for at nå dets mål. De foreslåede foranstaltninger står i et rimeligt forhold til de forfulgte mål, eftersom de respekterer medlemsstaternes prærogativer og forpligtelser i henhold til national ret.

I forslaget tages der desuden højde for en potentielt differentieret tilgang, som afspejler medlemsstaternes forskellige interne situationer, når det drejer sig om beredskab og reaktion på fysiske trusler mod kritisk infrastruktur.

- **Valg af retsakt**

Med henblik på at nå de tilstræbte mål indeholder TEUF bestemmelser, navnlig artikel 292, om, at Rådet kan vedtage henstillinger efter forslag fra Kommissionen. Rådets henstilling er et passende instrument i dette tilfælde, også i lyset af den nuværende lovgivningsmæssige kontekst som forklaret ovenfor. Rådets henstilling som retsakt, selv om den er af ikkebindende karakter, viser, at medlemsstaterne er fast besluttet på at gennemføre de foranstaltninger, den indeholder, og danner et stærkt politisk grundlag for samarbejde på disse områder, samtidig med at medlemsstaternes kompetencer respekteres.

3. RESULTATER AF EFTERFØLGENDE EVALUERINGER, HØRINGER AF INTERESSEREDE PARTER OG KONSEKVENSANALYSER

• Høringer af interesserede parter

Ved udarbejdelsen af dette forslag blev der taget hensyn til de synspunkter, som medlemsstaternes eksperter gav udtryk for på mødet den 12. oktober 2022. Der var bred enighed om nytten af mere koordinering på EU-plan for så vidt angår beredskab og reaktion i den nuværende trusselssituation og for at foregribe visse elementer i CER-direktivet inden dets formelle vedtagelse. Medlemsstaterne var åbne over for at dele erfaringer og bedste praksis om foranstaltninger og metoder til at øge modstandsdygtigheden i enheder, der driver kritisk infrastruktur. Medlemsstaterne var også åbne over for på frivillig basis og på grundlag af fælles principper at anvende en koordineret tilgang til stresstest af enheder, der driver kritisk infrastruktur. Medlemsstaterne anførte, at enheder, der driver kritisk infrastruktur inden for energisektoren, sektoren for digital infrastruktur og transportsektoren, navnlig dem, der er relevante for flere medlemsstater, bør prioriteres i forbindelse med denne henstilling. Medlemsstaterne udtrykte også tilfredshed med, at Kommissionen har til hensigt at indkalde til yderligere møder for medlemsstaternes eksperter i de kommende uger.

• Nærmere redegørelse for de enkelte bestemmelser i forslaget

Forslaget til Rådets henstilling indeholder følgende:

– I kapitel I fastsættes formålet med forslaget, hvad det omfatter, og prioriteringen af de anbefalede foranstaltninger.

– I kapitel II fokuseres der på de foranstaltninger, der bør træffes for at øge beredskabet, på både EU-plan og medlemsstatsplan.

– Kapitel III vedrører øget reaktion på både EU-plan og medlemsstatsplan.

– Kapitel IV omhandler internationalt samarbejde og de foranstaltninger, der bør træffes for at øge modstandsdygtigheden i enheder, der driver kritisk infrastruktur.

2022/0338 (NLE)

Forslag til

RÅDETS HENSTILLING

om en koordineret tilgang fra Unionens side til styrkelse af kritisk infrastrukturs modstandsdygtighed

(EØS-relevant tekst)

RÅDET FOR DEN EUROPÆISKE UNION HAR —

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

under henvisning til forslag fra Europa-Kommissionen, og

ud fra følgende betragtninger:

(1) Unionen har en særlig rolle at spille med hensyn til infrastruktur, der krydser grænser og påvirker flere medlemsstaters interesser, eller som på anden vis anvendes af enheder til at levere væsentlige tjenester på tværs af grænserne. Leveringen af sådanne tjenester og sådan kritisk infrastruktur af relevans for flere medlemsstater kan imidlertid ligge i en enkelt medlemsstat eller uden for medlemsstaternes område, f.eks. i tilfælde af undersøiske kabler eller rørledninger. Det er i alle medlemsstaters og hele Unionens interesse klart at få kortlagt denne infrastruktur og disse enheder samt truslerne mod dem og i fællesskab at forpligte sig til at beskytte dem.

(2) Beskyttelsen af kritisk infrastruktur i to sektorer reguleres på nuværende tidspunkt ved Rådets direktiv 2008/114/EF[12]. I det pågældende direktiv fastsættes der en procedure for indkredsning og udpegning af europæisk kritisk infrastruktur og en fælles fremgangsmåde til vurdering af behovet for at beskytte denne type infrastruktur med henblik på at bidrage til beskyttelsen af mennesker. Direktivet dækker energi- og transportsektoren. For at forbedre modstandsdygtigheden i kritiske enheder, de væsentlige tjenester, de leverer, og den kritiske infrastruktur, de er afhængige af, er EU-lovgiveren ved at vedtage et nyt direktiv om kritiske enheders modstandsdygtighed[13] ("CER-direktivet"), som skal erstatte direktiv 2008/114/EF, og som omfatter flere sektorer, herunder digital infrastruktur.

(3) Derudover fokuseres der i Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen[14], på cyberrelaterede trusler. Det pågældende direktiv vil blive erstattet af et nyt direktiv om foranstaltninger til sikring af et højt

---

12 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).

13 COM(2020) 829.

14 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).

fælles cybersikkerhedsniveau i hele Unionen[15] ("NIS 2-direktivet"), som også er ved at blive vedtaget af EU-lovgiveren.

(4) I lyset af, hvor hurtigt trusselsbilledet udvikler sig, navnlig i forbindelse med den øjensynlige sabotage af gasinfrastrukturen Nord Stream 1 og 2, står enheder, der driver kritisk infrastruktur, over for særlige udfordringer med hensyn til deres modstandsdygtighed over for fjendtlige handlinger og andre menneskeskabte trusler, samtidig med at udfordringerne som følge af naturlige faktorer og klimaændringerne fortsat vokser er stigende og kan risikere at blive udnyttet med fjendtlige handlinger. De er derfor med støtte fra medlemsstaterne nødt til at træffe passende foranstaltninger, der øger deres modstandsdygtighed. Disse foranstaltninger bør træffes, og denne støtte bør ydes ud over foranstaltningerne i direktiv 2008/114/EF og direktiv (EU) 2016/1148 og endda før vedtagelsen, ikrafttrædelsen og gennemførelsen af det nye CER-direktiv og NIS 2-direktiv.

(5) Indtil disse nye direktiver vedtages, træder i kraft og gennemføres, bør Unionen og medlemsstaterne opfordres til i overensstemmelse med EU-retten at anvende alle tilgængelige værktøjer til at komme videre og bidrage til at styrke de pågældende enheders fysiske og cyberrelaterede modstandsdygtighed og den kritiske infrastruktur, de driver med henblik på at levere væsentlige tjenester på det indre marked, dvs. tjenester, som er afgørende for opretholdelsen af vitale samfundsmæssige funktioner, økonomiske aktiviteter, folkesundheden og sikkerheden eller miljøet. I den henseende bør begrebet modstandsdygtighed forstås som en enheds evne til at forhindre, beskytte sig mod, reagere på, modstå, afbøde, absorbere, tilpasse sig til og komme sig over hændelser, som har potentiale til i væsentlig grad at forstyrre eller som forstyrrer leveringen af de pågældende væsentlige tjenester.

(6) For at sikre en tilgang, der både er effektiv og så meget i overensstemmelse med det nye CER-direktiv som muligt, bør foranstaltningerne i denne henstilling vedrøre den infrastruktur, som medlemsstaterne har udpeget som kritisk infrastruktur, og som omfatter både national kritisk infrastruktur og europæisk kritisk infrastruktur, uanset om den enhed, der driver den kritiske infrastruktur, allerede er udpeget som en kritisk enhed i henhold til dette nye direktiv. Med henblik på denne henstilling bør begrebet "kritisk infrastruktur" forstås i overensstemmelse hermed.

(7) I lyset af de eksisterende trusler bør det i vigtige sektorer som energisektoren, sektoren for digital infrastruktur, transportsektoren og rumsektoren prioriteres, at der træffes foranstaltninger, der øger modstandsdygtigheden, og sådanne foranstaltninger bør fokusere på at øge modstandsdygtigheden i enheder, der driver kritisk infrastruktur, over for menneskeskabte risici. Med hensyn til national kritisk infrastruktur bør infrastruktur, der er af grænseoverskridende relevans, prioriteres i lyset af de mulige konsekvenser, hvis risiciene bliver til virkelighed.

(8) Foranstaltningerne i denne henstilling tager derfor hovedsagelig sigte på at supplere det nye CER-direktiv og NIS 2-direktiv, som har hjemmel i artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF), ved at foregribe og supplere de foranstaltninger, der følger af disse nye direktiver. Med henblik herpå og i lyset af den grænseoverskridende karakter og relevans af de pågældende væsentlige tjenester og den pågældende kritiske infrastruktur og af de nuværende og nye forskelle i de nationale lovgivninger, som forvrider det indre marked, er det hensigtsmæssigt også at

[15] COM(2020) 823.

lade denne henstilling have hjemmel i artikel 114 i TEUF sammenholdt med artikel 292 i TEUF.

(9) Gennemførelsen af denne henstilling bør derfor ikke forstås således, at den påvirker nuværende og fremtidige krav i EU-retten vedrørende visse aspekter af de berørte enheders modstandsdygtighed, og den bør være i overensstemmelse med dem. Disse krav er fastsat i generelle retsakter såsom direktiv 2008/114/EF og direktiv (EU) 2016/1148 og det nye CER-direktiv og NIS 2-direktiv, som erstatter dem, men også i visse sektorspecifikke retsakter på f.eks. transportområdet, hvor bl.a. Kommissionen har taget et initiativ vedrørende beredskabsplanen for transport[16]. I overensstemmelse med princippet om loyalt samarbejde bør denne henstilling gennemføres med fuld gensidig respekt og bistand.

(10) Kommissionen bebudede den 5. oktober 2022 en fempunktsplan, hvori der fastsættes en koordineret tilgang til at håndtere de kommende udfordringer, som omfatter arbejdet vedrørende beredskab ved at bygge videre på og foregribe vedtagelsen og ikrafttrædelsen af det nye CER-direktiv, og som også omfatter samarbejdet med medlemsstaterne med henblik på at udføre stresstest af enheder, der driver kritisk infrastruktur, på grundlag af fælles principper, idet der begyndes med energisektoren. I denne henstilling, som vil bidrage til ovennævnte plan, hilses den foreslåede tilgang velkommen, og det beskrives, hvordan den kan omsættes til handling.

(11) På baggrund af et trusselsbillede i hastig udvikling og det nuværende risikomiljø, der er kendetegnet ved menneskeskabte risici, navnlig hvad angår kritisk infrastruktur af grænseoverskridende relevans, er det vigtigt at have et nøjagtigt, ajourført og fuldstændigt billede af de vigtigste risici, som enheder, der driver kritisk infrastruktur, står over for. Medlemsstaterne bør derfor træffe de nødvendige foranstaltninger for at foretage en vurdering af disse risici eller ajourføre deres vurdering af dem. I denne henstilling fokuseres der på sikkerhedsrelaterede risici, men derudover bør der fortsat gøres en indsats for at imødegå klimaændringer og miljørisici, navnlig når naturbetingede hændelser kan forværre de menneskeskabte risici yderligere.

(12) I betragtning af dette trusselsbillede bør medlemsstaterne opfordres til snarest muligt at træffe passende foranstaltninger til at styrke kritisk infrastrukturs modstandsdygtighed, også ud over de nævnte risikovurderinger, som senere vil blive krævet i henhold til det nye CER-direktiv.

(13) Som led i gennemførelsen af den fempunktsplan, som Kommissionen har bebudet, er det nødvendigt at koordinere arbejdet ved at sammenkalde nationale eksperter for at foregribe oprettelsen af Gruppen for Kritiske Enheders Modstandsdygtighed i medfør af det nye CER-direktiv og at muliggøre samarbejde mellem medlemsstaterne og udveksling af oplysninger om modstandsdygtigheden i enheder, der driver kritisk infrastruktur. Dette bør omfatte samarbejde og udveksling af oplysninger vedrørende aktiviteter såsom kortlægning af kritiske enheder og kritisk infrastruktur, forberedelse af udviklingen og fremme af et fælles sæt principper for gennemførelse af stresstest og indhøstning af fælles erfaringer fra stresstest samt indkredsning af sårbarheder og mulige kapaciteter. Disse processer bør også gavne modstandsdygtigheden i de enheder, der driver kritisk infrastruktur, over for klima- og miljørisici. Dette arbejde vil desuden give mulighed for fælles prioritering af arbejdet med stresstest med vægt på energisektoren, sektoren for digital infrastruktur, transportsektoren og rumsektoren. Kommissionen er allerede begyndt at sammenkalde disse eksperter og lette deres

[16] COM(2022) 211.

arbejde, og den har til hensigt at fortsætte dette arbejde. Når det nye CER-direktiv er trådt i kraft, og Gruppen for Kritiske Enheders Modstandsdygtighed er oprettet, bør denne gruppe fortsætte dette foregribende arbejde i overensstemmelse med dens opgaver i henhold til CER-direktivet.

(14) Stresstesten bør suppleres med udarbejdelsen af en plan for hændelser vedrørende kritisk infrastruktur og kriser, hvori der redegøres for og fastsættes mål og metoder for samarbejdet mellem medlemsstaterne og EU's institutioner, organer, kontorer og agenturer med hensyn til at reagere på hændelser mod kritisk infrastruktur, navnlig hvis disse medfører betydelige forstyrrelser af leveringen af væsentlige tjenester på det indre marked. I denne plan bør der gøres brug af de eksisterende integrerede ordninger for politisk kriserespons med henblik på koordineringen af reaktionen, sikres sammenhæng og komplementaritet med planen for væsentlige cyberhændelser og desuden gives mulighed for at nå til enighed om centrale offentlige kommunikationsbudskaber, da kommunikation i krisesituationer spiller en vigtig rolle med hensyn til at afbøde de negative virkninger af hændelser og kriser, der vedrører kritisk infrastruktur.

(15) For at sikre en koordineret og effektiv reaktion på de nuværende og forventede trusler vil Kommissionen yde yderligere støtte til medlemsstaterne med henblik på at øge modstandsdygtigheden i lyset af disse trusler, navnlig ved at stille relevante oplysninger til rådighed i form af briefinger, manualer og retningslinjer, fremme deltagelsen i EU-finansierede forsknings- og innovationsprojekter, træffe de nødvendige foregribende foranstaltninger og optimere anvendelsen af Unionens overvågningsaktiver. EU-Udenrigstjenesten bør tilvejebringe trusselsvurderinger, navnlig gennem EU's Efterretnings- og Situationscenter.

(16) Sektorspecifikke EU-agenturer og andre relevante organer bør også yde støtte i forbindelse med anliggender vedrørende modstandsdygtighed, for så vidt som deres respektive mandater som fastsat i de relevante EU-retsakter giver mulighed for det. Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) kan bistå i spørgsmål om cybersikkerhed, Det Europæiske Agentur for Søfartssikkerhed (EMSA) kan bistå med ekspertise og yde støtte til medlemsstaterne via dets maritime overvågningstjeneste i forbindelse med anliggender vedrørende maritim sikkerhed, Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol) kan yde støtte i forbindelse med indsamling af oplysninger og efterforskning i forbindelse med grænseoverskridende retshåndhævelsesforanstaltninger, mens Den Europæiske Unions Agentur for Rumprogrammet (EUSPA) og EU-Satellitcentret kan bistå gennem operationer inden for Unionens rumprogram,

(17) Hovedansvaret for at garantere sikkerheden for kritisk infrastruktur og de pågældende enheder ligger hos medlemsstaterne, men en øget koordinering på EU-plan er hensigtsmæssig, navnlig i lyset af trusler, der kan påvirke flere medlemsstater ad gangen, såsom Ruslands angrebskrig mod Ukraine, eller påvirke EU's økonomis, det indre markeds og samfundenes modstandsdygtighed og funktion.

(18) Denne henstilling indebærer ikke meddelelse af oplysninger, hvis videregivelse strider mod medlemsstaternes væsentlige nationale sikkerhedsinteresser, offentlige sikkerhed eller forsvar.

(19) Med den stigende indbyrdes afhængighed mellem fysisk og digital infrastruktur kan ondsindede cyberaktiviteter rettet mod kritiske områder føre til forstyrrelse eller beskadigelse af fysisk infrastruktur, mens sabotage mod fysisk infrastruktur kan gøre digitale tjenester utilgængelige. I lyset af den øgede trussel fra sofistikerede hybride

angreb bør medlemsstaterne også medtage sådanne overvejelser i deres arbejde med gennemførelsen af denne henstilling. I lyset af de indbyrdes forbindelser mellem cybersikkerhed og operatørernes fysiske sikkerhed er det vigtigt, at arbejdet med at forberede gennemførelsen og anvendelsen af det nye NIS 2-direktiv indledes snarest muligt, og at dette arbejde i henhold til det nye CER-direktiv skrider frem parallelt hermed.

(20) Ud over at styrke beredskabet er det også vigtigt at øge kapaciteten til at reagere hurtigt og effektivt, hvis risici, der påvirker leveringen af væsentlige tjenester fra enheder, der driver kritisk infrastruktur, bliver til virkelighed. Denne henstilling bør derfor indeholde de foranstaltninger, der bør træffes på både medlemsstatsplan og EU-plan, herunder styrket samarbejde og udveksling af oplysninger i forbindelse med EU-Civilbeskyttelsesmekanismen og anvendelse af relevante aktiver i Unionens rumprogram.

(21) Efter opfordring fra Rådet i dets konklusioner om EU's cyberposition[17], er Kommissionen, Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik ("den højtstående repræsentant") og den samarbejdsgruppe, der blev nedsat ved direktiv (EU) 2016/1148 ("NIS-samarbejdsgruppen") i samarbejde med relevante civile og militære organer og agenturer og etablerede netværk, herunder EU CyCLONe, ved at foretage en risikoevaluering og udarbejde risikoscenarier ud fra et cybersikkerhedsmæssigt perspektiv i en situation med trusler eller et muligt angreb mod medlemsstaterne eller partnerlande. I dette arbejdsforløb fokuseres der på kritiske sektorer, herunder energisektoren, sektoren for digital infrastruktur, transportsektoren og rumsektoren.

(22) I den fælles opfordring fra ministermødet i Nevers[18] og Rådets konklusioner om EU's cyberposition opfordres der også til at styrke kommunikationsinfrastrukturens og -nettenes modstandsdygtighed, idet der fremsætte henstillinger til medlemsstaterne og Kommissionen på grundlag af en risikovurdering. Denne risikovurdering foretages i øjeblikket af NIS-samarbejdsgruppen med støtte fra Kommissionen og ENISA og i samarbejde med Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC). I forbindelse med risikovurderingen og mangelanalysen ses der på risikoen for cyberangreb i forskellige undersektorer af kommunikationsinfrastrukturer, herunder faste og mobile infrastrukturer, satellitter, undersøiske kabler, internetrouting osv. for derved at skabe grundlaget for arbejdet i henhold til denne henstilling. Resultaterne af risikovurderingen vil indgå i den igangværende tværsektorielle cyberrisikoevaluering og udarbejdelse af scenarier, som Rådet har anmodet om i dets konklusioner af 23. maj 2022.

(23) Disse to arbejdsforløb vil være i overensstemmelse med og blive koordineret med arbejdet med udarbejdelse af scenarier med fokus på civilbeskyttelse i forbindelse med en bred vifte af naturkatastrofer og menneskeskabte katastrofer, herunder cybersikkerhedshændelser og deres reelle konsekvenser, som Kommissionen og medlemsstaterne i øjeblikket gennemfører inden for rammerne af Europa-Parlamentets og Rådets afgørelse 1313/2013/EU[19]. Af hensyn til effektiviteten, virkningen og

---

17 Cyber posture: Council approves conclusions - Consilium (europa.eu).

18 https://www.regeringen.se/494477/contentassets/e5f13bec9b1140038eed9a3d0646f8cf/joint-call-to-reinforce-the-eus-cybersecurity-capabilities.pdf.

19 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).

sammenhængen bør denne henstilling gennemføres under hensyntagen til resultaterne af disse arbejdsforløb.

(24) EU-værktøjskassen til cybersikkerhed i 5G-net[20] indeholder relevante foranstaltninger og afbødningsplaner for at forbedre 5G-nets sikkerhed. I lyset af mange væsentlige tjenesters afhængighed af 5G-net og de digitale økosystemers indbyrdes forbundne karakter er det vigtigt, at alle medlemsstaterne hurtigt fuldfører gennemførelsen af de foranstaltninger, der anbefales i værktøjskassen, og navnlig anvender de relevante restriktioner for højrisikoleverandører i forbindelse med de centrale aktiver, der defineres som kritiske og følsomme i EU's koordinerede risikovurdering.

(25) For straks at styrke beredskabet og kapaciteten til at reagere på større cyberhændelser har Kommissionen fastlagt et kortsigtet program til støtte for medlemsstaterne ved at afsætte yderligere midler til ENISA. Blandt de omfattede tjenester vil være beredskabsforanstaltninger såsom penetrationstest af kritiske enheder med henblik på at kortlægge sårbarheder. Det vil også forbedre mulighederne for at bistå medlemsstaterne i tilfælde af en større hændelse, der påvirker kritiske enheder. Dette er et første skridt i overensstemmelse med Rådets konklusioner om cyberpositionen, hvori Kommissionen anmodes om at fremsætte et forslag til en cyberberedskabsfond. Medlemsstaterne bør fuldt ud udnytte disse muligheder i overensstemmelse med de gældende krav.

(26) Det globale undersøiske kabelnet for data og elektronisk kommunikation er af afgørende betydning for konnektiviteten på globalt plan og inden for EU. Som følge af disse 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 disse kabler kræver i særlig grad 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 særlige risikovurderinger og muligheder for at træffe afbødende foranstaltninger i forbindelse med undersøiske kabler. Kommissionen vil derfor gennemføre undersøgelser med henblik herpå og dele sine resultater med medlemsstaterne.

(27) Energi- og transportsektoren, der i denne henstilling er udpeget som prioriterede sektorer, kan også blive påvirket af risici i forbindelse med digital infrastruktur. Det kan f.eks. være tilfældet 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, der drives af enheder i energisektoren. Der bør i overensstemmelse med denne henstilling tages hensyn til disse omstændigheder, når der træffes foranstaltninger til at øge modstandsdygtigheden i enheder, der driver kritisk infrastruktur.

(28) Ruminfrastrukturs og rumbaserede tjenesters voksende betydning for sikkerhedsrelaterede aktiviteter gør det vigtigt at sikre, at Unionens rumaktiver og -tjenester inden for EU er modstandsdygtige og beskyttede, men også inden for rammerne af denne henstilling for derved at sikre en mere struktureret brug af de rumbaserede data og tjenester, som rumsystemer og -programmer til overvågning og beskyttelse af kritisk infrastruktur i andre sektorer leverer. I den kommende EU-

[20] 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf.

rumstrategi for sikkerhed og forsvar vil der blive foreslået passende foranstaltninger i den henseende, som der bør tages hensyn til ved gennemførelsen af denne henstilling.

(29) Der er også behov for samarbejde på internationalt plan for effektivt at imødegå risici for modstandsdygtigheden i de enheder, der driver kritisk infrastruktur, enten i Unionen eller i relevante tredjelande eller i internationale farvande. Medlemsstaterne bør derfor opfordres til at samarbejde med Kommissionen og den højtstående repræsentant om at tage skridt til at nå dette mål, idet det er underforstået, at alle sådanne skridt dog kun skal træffes i overensstemmelse med deres respektive opgaver og ansvarsområder i henhold til EU-retten, navnlig EU-traktaternes bestemmelser om eksterne forbindelser.

(30) Som fastsat i meddelelsen om Kommissionens bidrag til europæisk forsvar[21] 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"[22] vil Kommissionen 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.

(31) I EU-strategien for maritim sikkerhed fra 2014 og den tilknyttede handlingsplan opfordres der til at øge beskyttelsen af kritisk maritim infrastruktur, herunder undervandsinfrastruktur, og navnlig søtransport-, energi- og kommunikationsinfrastruktur, bl.a. ved at øge den maritime situationsbevidsthed gennem forbedret interoperabilitet og strømlinet informationsudveksling (obligatorisk og frivillig). Strategien og handlingsplanen er i øjeblikket ved at blive ajourført og vil omfatte skærpede foranstaltninger til beskyttelse af kritisk maritim infrastruktur. Disse foranstaltninger bør danne grundlag for og supplere denne henstilling.

(32) Medlemsstaterne bør tage hensyn til det fulde potentiale i Unionens sikkerhedsforskningsprogram, især ved at udnytte, at kritisk infrastruktur heri i særlig grad prioriteres, navnlig inden for rammerne af de programmer, der finansieres inden for rammerne af Fonden for Intern Sikkerhed og andre potentielle finansieringsmuligheder på EU-plan, navnlig Den Europæiske Fond for Regionaludvikling, i det omfang de specifikke foranstaltninger opfylder støtteberettigelseskravene. REPowerEU giver også mulighed for finansiering til styrkelse af modstandsdygtighed. Enhver udnyttelse af mulighederne for EU-finansiering skal ske i overensstemmelse med de gældende retlige krav —

VEDTAGET DENNE HENSTILLING:

KAPITEL I: MÅL, ANVENDELSESOMRÅDE OG PRIORITERING

1) I denne henstilling opfordres medlemsstaterne til at træffe hastende og effektive foranstaltninger og til at samarbejde loyalt, effektivt, solidarisk og på koordineret vis med hinanden, Kommissionen og andre relevante offentlige myndigheder samt de berørte enheder for at øge modstandsdygtigheden i den kritiske infrastruktur, der anvendes til at levere væsentlige tjenester på det indre marked.

---

21 com_2022_60_1_en_act_contribution_european_defence.pdf (europa.eu).

22 Rådet for Den Europæiske Union, 7371/22, 21. marts 2022.

2) Foranstaltningerne i denne henstilling vedrører den infrastruktur, som en medlemsstat har udpeget som kritisk infrastruktur, herunder europæisk kritisk infrastruktur.

3) Ved gennemførelsen af denne henstilling bør det prioriteres at øge modstandsdygtigheden over for menneskeskabte risici i de enheder, der er aktive i energisektoren, sektoren for digital infrastruktur, transportsektoren og rumsektoren og i den kritiske infrastruktur, som disse enheder driver, og som er af grænseoverskridende relevans.

KAPITEL II: ØGET BEREDSKAB

Foranstaltninger på medlemsstatsplan

4) Medlemsstaterne opfordres til at foretage eller ajourføre risikovurderinger vedrørende modstandsdygtigheden i de enheder, der driver europæisk kritisk infrastruktur inden for transport- og energisektoren i henhold til direktiv 2008/114/EF og i overensstemmelse med nævnte direktiv at fortsætte det indbyrdes samarbejde om sådanne risikovurderinger og de deraf følgende foranstaltninger, der øger modstandsdygtigheden, når det er relevant.

5) For at opnå en høj grad af modstandsdygtighed i enheder, der driver kritisk infrastruktur, bør medlemsstaterne desuden fremskynde det forberedende arbejde med henblik på at gennemføre og anvende det nye CER-direktiv ved at:

a) fremskynde vedtagelsen eller ajourføringen af nationale strategier til styrkelse af modstandsdygtigheden i enheder, der driver kritisk infrastruktur, med henblik på at imødegå den aktuelle trussel. De relevante dele af denne strategi bør meddeles Kommissionen

b) foretage eller ajourføre risikovurderinger i overensstemmelse med udviklingen i arten af de aktuelle trusler for så vidt angår modstandsdygtigheden i enheder, der driver kritisk infrastruktur i relevante sektorer ud over energisektoren, sektoren for digital infrastruktur, transportsektoren og rumsektoren, og, når det er muligt, i de sektorer, der er omfattet af det nye CER-direktiv, nemlig bankvæsen, finansmarkedsinfrastruktur, digital infrastruktur, sundhed, drikkevand, spildevand, offentlige forvaltning, rummet og fødevareproduktion, -forarbejdning og -distribution, idet der tages hensyn til den potentielle hybride karakter af relevante trusler, herunder kaskadevirkninger og virkningerne af klimaændringer

c) informere Kommissionen om de typer risici, der er indkredset i hver sektor og delsektor, og resultaterne af risikovurderingerne, hvilket kan ske ved hjælp af en fælles rapporteringsmodel, som Kommissionen udvikler i samarbejde med medlemsstaterne

d) fremskynde processen med at indkredse og udpege kritiske enheder, med prioritering af de kritiske enheder, som:

e) anvender kritisk infrastruktur, som er fysisk forbundet mellem to eller flere medlemsstater

f) er en del af selskabsstrukturer, der er forbundet med eller knyttet til kritiske enheder i andre medlemsstater

g) er blevet udpeget som sådan i en medlemsstat og leverer væsentlige tjenester i eller til seks eller flere medlemsstater, og derfor er af særlig europæisk betydning, og underrette Kommissionen herom

h) samarbejde med hinanden, navnlig når det drejer sig om kritiske enheder og væsentlige tjenester og kritisk infrastruktur af grænseoverskridende relevans, navnlig ved at indlede konsultationer med hinanden med henblik på punkt 5, litra d), og ved at underrette hinanden i tilfælde af en hændelse med betydelig eller potentielt betydelig grænseoverskridende forstyrrende virkninger, samtidig med at Kommissionen om nødvendigt holdes underrettet

i) øge støtten til udpegede kritiske enheder med henblik på at forbedre deres modstandsdygtighed, hvilket kan omfatte tilvejebringelse af vejledningsmaterialer og metoder, tilrettelæggelse af øvelser for at teste deres modstandsdygtighed samt rådgivning og uddannelse af deres personale og mulighed for at foretage baggrundstjek af personer med følsomme roller i overensstemmelse med EU-lovgivningen og national lovgivning som led i de kritiske enheders sikkerhedsforanstaltninger i forbindelse med personaleforvaltningen

j) fremskynde udpegelsen eller oprettelsen af et centralt kontaktpunkt inden for den kompetente myndighed til at varetage en forbindelsesfunktion til andre medlemsstaters kontaktpunkter med henblik på at sikre grænseoverskridende samarbejde vedrørende modstandsdygtigheden i enheder, der driver kritisk infrastruktur.

6) Medlemsstaterne opfordres til at gennemføre stresstest af enheder, der driver kritisk infrastruktur. Medlemsstaterne opfordres navnlig til at fremme deres og de berørte enheders beredskab i energisektoren og gennemføre stresstest i denne sektor ved, når det er muligt, at følge de principper, der i fællesskab er opnået enighed om på EU-plan, samtidig med at der sikres en effektiv kommunikation med de berørte enheder. Det kan om nødvendigt overvejes efterfølgende at gennemføre stresstest i andre prioriterede sektorer, nemlig sektoren for digital infrastruktur, transportsektoren og rumsektoren, under behørig hensyntagen til tilsynet i delsektorerne luftfart og søfart i henhold til EU-retten og under hensyntagen til de relevante bestemmelser i sektorspecifik lovgivning.

7) Medlemsstaterne opfordres til, når det er relevant, og i overensstemmelse med EU-retten at samarbejde med relevante tredjelande for så vidt angår modstandsdygtigheden i enheder, der driver kritisk infrastruktur af grænseoverskridende relevans.

8) Medlemsstaterne opfordres til i overensstemmelse med gældende krav at gøre brug af potentielle finansieringsmuligheder på EU-plan og nationalt plan for at øge modstandsdygtigheden i enheder, der driver kritisk infrastruktur i Unionen, herunder f.eks. langs de transeuropæiske net, over for alle former for betydelige trusler, navnlig inden for rammerne af de programmer, der finansieres via Fonden for Intern Sikkerhed og Den Europæiske Fond for Regionaludvikling, forudsat at de opfylder de respektive støtteberettigelseskriterier, og Connecting Europe-faciliteten, herunder bestemmelserne om klimasikring. EU-civilbeskyttelsesmekanismens midler kan også anvendes til dette formål i overensstemmelse med de gældende krav, navnlig til projekter vedrørende risikovurderinger, investeringsplaner eller -undersøgelser, kapacitetsopbygning eller forbedring af videnbasen. REPowerEU giver også mulighed for finansiering til styrkelse af modstandsdygtighed.

9) Med hensyn til kommunikations- og netinfrastrukturen i Unionen bør NIS-samarbejdsgruppen i overensstemmelse med artikel 11 i direktiv (EU) 2016/1148 og senere artikel 14 i NIS 2-direktivet fremskynde sit igangværende arbejde med en målrettet risikovurdering og fremsætte de første anbefalinger i begyndelsen af 2023.

I forbindelse med dette arbejde bør der 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 såsom Gruppen for Kritiske Enheders Modstandsdygtighed, der skal oprettes i henhold til det nye CER-direktiv, og det tilsynsforum, der skal oprettes i henhold til den nye retsakt om digital operationel modstandsdygtighed (DORA)[23].

10) NIS-samarbejdsgruppen, som skal udføre sine opgaver i overensstemmelse med artikel 11 i direktiv (EU) 2016/1148 og senere artikel 14 i NIS 2-direktivet, opfordres til med støtte fra Kommissionen og ENISA at prioritere sit arbejde med sikkerheden i sektoren for digital infrastruktur og rumsektoren, bl.a. ved at udarbejde politiske retningslinjer og metoder og foranstaltninger til styring af cybersikkerhedsrisici på grundlag af en tilgang, der omfatter alle farer i forbindelse med undersøiske kommunikationskabler, for at foregribe ikrafttrædelsen af NIS 2-direktivet samt udarbejdelsen af retningslinjer for foranstaltninger til styring af cybersikkerhedsrisici 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, navnlig penetrationstest for at kortlægge sårbarheder, og de opfordres i den forbindelse til at prioritere enheder, der driver kritisk infrastruktur inden for energisektoren, sektoren for digital infrastruktur og transportsektoren.

12) Medlemsstaterne bør hurtigst muligt fuldføre gennemførelsen af de foranstaltninger, der anbefales i EU-værktøjskassen for 5G-cybersikkerhed[24]. De medlemsstater, som endnu ikke har indført restriktioner for højrisikoleverandører, bør gøre det uden yderligere forsinkelse, da forsinkelser kan øge nettenes sårbarhed i Unionen. De bør også styrke 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, herunder retligt bindende krav på EU-plan, for at sikre et ensartet niveau for 5G-nets sikkerhed og modstandsdygtighed.

13) Medlemsstaterne bør hurtigst muligt gennemføre de kommende netregler for cybersikkerhedsmæssige aspekter af grænseoverskridende elektricitetsstrømme på grundlag af de indhøstede erfaringer med gennemførelsen af NIS-direktivet og relevant vejledning udarbejdet af NIS-samarbejdsgruppen, navnlig dens referencedokument om sikkerhedsforanstaltninger for operatører af væsentlige tjenester.

14) Medlemsstaterne bør udvikle brugen af Galileo og/eller Copernicus til overvågning og sikre udvekslingen af relevante oplysninger mellem 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 kriseberedskabet, bør udnyttes.

Foranstaltninger på EU-plan

---

23 COM(2020) 595 final.

24 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf.

15) Kommissionen har til hensigt at styrke samarbejdet mellem medlemsstaternes eksperter med henblik at øge den fysiske ikkecyberrelaterede modstandsdygtighed i enheder, der driver kritisk infrastruktur, navnlig ved at:

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

b) støtte udviklingen af fælles principper for medlemsstaternes gennemførelse af de stresstest, der er omhandlet i punkt 6, idet der tages udgangspunkt i de test, der fokuserer på menneskeskabte risici i energisektoren og senere i andre nøglesektorer såsom sektoren for digital infrastruktur, transportsektoren og rumsektoren imødegå andre væsentlige risici og farer samt støtte og rådgive om gennemførelsen af sådanne stresstest, når det er relevant

c) tilvejebringe en sikker platform til at indsamle, gøre status over og udveksle bedste praksis, oplysninger om nationale erfaringer og andre oplysninger vedrørende en sådan modstandsdygtighed, herunder om gennemførelse af disse stresstest og omsættelse af resultaterne heraf til protokoller og beredskabsplaner.

Disse eksperters arbejde bør især fokusere på tværsektoriel afhængighed og enheder, der driver kritisk infrastruktur af grænseoverskridende relevans, og det bør fortsættes af Gruppen for Kritiske Enheders Modstandsdygtighed, når den er oprettet.

16) Medlemsstaterne bør deltage fuldt ud i det styrkede samarbejde, der er omhandlet i punkt 15, herunder ved at udpege kontaktpunkter med relevant ekspertise og ved at udveksle erfaringer om de metoder, der anvendes til de stresstest og protokoller og beredskabsplaner, der udviklet på grundlag heraf. Ved udvekslingen af de pågældende oplysninger bør fortroligheden af oplysninger og de kritiske enheders sikkerhed og kommercielle interesser sikres, samtidig med at medlemsstaternes sikkerhed respekteres. Dette indebærer ikke meddelelse af oplysninger, hvis videregivelse strider mod medlemsstaternes væsentlige nationale sikkerhedsinteresser, offentlige sikkerhed eller forsvar.

17) Kommissionen vil støtte medlemsstaterne ved at stille manualer og retningslinjer til rådighed 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 at holde briefinger om truslerne mod kritisk infrastruktur i EU for at forbedre situationsbevidstheden.

18) Kommissionen vil støtte udbredelsen af resultaterne af projekter om modstandsdygtighed i enheder, der driver kritisk infrastruktur, og som finansieres inden for rammerne af Unionens forsknings- og innovationsprogrammer. Kommissionen har til hensigt inden for rammerene af det budget, der er afsat til Horisont Europa under den flerårige finansielle ramme for 2021-2027, at øge finansieringen af sådan modstandsdygtighed. Dette bør gøre det muligt at håndtere nuværende og fremtidige udfordringer på dette område såsom klimasikring af kritisk infrastruktur, uden at det går ud over finansieringen af anden sikkerhedsrelateret forskning og innovation inden for rammerne af Horisont Europa. Kommissionen vil også øge sin indsats for at formidle resultaterne af relevante EU-finansierede forskningsprojekter.

19) NIS-samarbejdsgruppen opfordres til i samarbejde med Kommissionen og den højtstående repræsentant i overensstemmelse med deres respektive opgaver og

ansvarsområder i henhold til EU-retten at intensivere arbejdet med relevante net og civile og militære organer om at gennemføre risikoevalueringer og udarbejde risikoscenarier, indledningsvis med fokus på energi-, kommunikations-, 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 fysisk infrastruktur, som disse sektorer er afhængige af. Risikovurderingerne og scenarierne bør gennemføres regelmæssigt og bør supplere, bygge videre på og undgå overlapning med eksisterende eller planlagte risikovurderinger i disse sektorer og danne grundlag for drøftelser om, hvordan man kan styrke den overordnede modstandsdygtighed i enheder, der driver kritisk infrastruktur, og håndtere sårbarheder.

20) Kommissionen vil fremskynde sine aktiviteter vedrørende støtte til medlemsstaternes beredskab og reaktion på væsentlige cybersikkerhedshændelser og navnlig:

a) som supplement til relevante risikovurderinger i forbindelse med net- og informationssikkerhed gennemføre en omfattende undersøgelse for at gøre status over den undersøiske kabelinfrastruktur, der forbinder medlemsstaterne, og som forbinder Europa med resten af verden, herunder kortlægning, kapacitet og redundans, sårbarheder, risici for tilgængeligheden af tjenester og risikobegrænsning. Resultaterne heraf bør deles med medlemsstaterne

b) støtte medlemsstaternes og EU-institutionernes, -organernes og -agenturernes beredskab og reaktion på væsentlige cybersikkerhedshændelser.

21) Kommissionen vil i samarbejde med medlemsstaterne, jf. artikel 6 og 10 i afgørelse 1313/2013/EU, intensivere arbejdet med fremadrettede foregribende foranstaltninger, bl.a. inden for rammerne af EU-civilbeskyttelsesmekanismen, og i form af beredskabsplanlægning til støtte for Katastrofeberedskabskoordinationscentrets operationelle beredskab.

Kommissionen vil navnlig:

a) fremme arbejdet i Katastrofeberedskabskoordinationscentret om foregribelse og tværsektoriel forebyggelses-, beredskabs- og reaktionsplanlægning for at foregribe og forberede sig på forstyrrelser af leveringen af væsentlige tjenester fra enheder, der driver kritisk infrastruktur

b) øge investeringerne i forebyggende tilgange og befolkningens beredskab i tilfælde af sådanne forstyrrelser med særligt fokus på kemiske, biologiske, radiologiske og nukleare stoffer og sprængstoffer og andre nye menneskeskabte trusler

c) øge udvekslingen af relevant viden og bedste praksis og forbedre udformningen og gennemførelsen af kapacitetsudviklingsaktiviteter såsom uddannelseskurser og øvelser med de enheder, der driver kritisk infrastruktur, ved brug af eksisterende strukturer og ekspertise såsom EU-Vidensnetværket om Civilbeskyttelse.

22) Kommissionen vil fremme anvendelsen af EU's overvågningsaktiver (Copernicus og Galileo) 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.

23) 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 modstandsdygtigheden i enheder, der driver kritisk infrastruktur, navnlig f.eks.:

a) Europol vedrørende informationsindsamling, kriminalitetsanalyse og efterforskningsstøtte i forbindelse med grænseoverskridende retshåndhævelsesforanstaltninger

b) EMSA vedrørende maritim sikkerhed i Unionen, herunder maritime overvågningstjenester i forbindelse med spørgsmål vedrørende maritim sikkerhed

c) EUSPA for så vidt angår aktiviteter inden for Unionens rumprogram

d) ENISA for så vidt angår aktiviteter vedrørende cybersikkerhed.

KAPITEL III STYRKET REAKTION

Foranstaltninger på medlemsstatsplan

24) Medlemsstaterne bør:

a) koordinere deres reaktion og bevare overblikket over den tværsektorielle reaktion på betydelige forstyrrelser af leveringen af væsentlige tjenester fra enheder, der driver kritisk infrastruktur, inden for rammerne af Rådets krisemekanisme (IPCR), når det drejer sig om kritisk infrastruktur af grænseoverskridende relevans, planen vedrørende væsentlige cybersikkerhedshændelser og -kriser eller inden for rammerne af EU's koordinerede reaktion på hybride kampagner i tilfælde af en hybrid kampagne

b) øge informationsudvekslingen inden for rammerne af EU-civilbeskyttelsesmekanismen for i højere grad at sikre tidlig varsling og koordinere deres reaktion inden for rammerne af mekanismen i tilfælde af sådanne betydelige forstyrrelser for derved at sikre en hurtigere EU-støttet reaktion, når det er nødvendigt

c) øge deres parathed til at reagere via EU-civilbeskyttelsesmekanismen på sådanne betydelige forstyrrelser, navnlig når de sandsynligvis vil få betydelige grænseoverskridende eller endda fælleseuropæiske såvel som tværsektorielle konsekvenser

d) indgå i dialog med Kommissionen om yderligere udvikling af relevant reaktionskapacitet i Den Europæiske Civilbeskyttelsespulje (ECCP) og rescEU

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

f) sikre, at når det er nødvendigt at genopbygge kritisk infrastruktur, vil en sådan genopbygget infrastruktur være modstandsdygtig over for alle former for væsentlige risici, som kan være forbundet med den, herunder negative klimascenarier.

25) Medlemsstaterne opfordres til at fremskynde det forberedende arbejde med gennemførelsen og anvendelsen af NIS 2-direktivet ved straks at begynde at styrke kapaciteten i de nationale enheder, der håndterer IT-sikkerhedshændelser (CSIRT), med henblik på de nye opgaver, som disse enheder og det udvidede antal enheder fra nye sektorer har, ved hurtigt at ajourføre deres cybersikkerhedsstrategier og hurtigst muligt vedtage nationale planer vedrørende cybersikkerhedshændelser og kriseberedskab.

Foranstaltninger på EU-plan

26) Reaktionen på betydelige forstyrrelser af leveringen af væsentlige tjenester fra enheder, der driver kritisk infrastruktur, bør koordineres mellem medlemsstaternes

eksperter for så vidt angår disse enheders modstandsdygtighed og reaktionen på sådanne forstyrrelser, som kan bidrage til Rådets krisemekanismes (IPCR) funktion.

27) Kommissionen vil arbejde tæt sammen med medlemsstaterne om at videreudvikle katastrofeberedskabskapaciteter, der kan indsættes, herunder eksperter og rescEU-beredskabslagre inden for rammerne af EU-civilbeskyttelsesmekanismen, med henblik på at styrke det operationelle beredskab til at håndtere de umiddelbare og indirekte virkninger af betydelige forstyrrelser af leveringen af væsentlige tjenester fra enheder, der driver kritisk infrastruktur.

28) Under hensyntagen til udviklingen i risikobilledet og i samarbejde med medlemsstaterne vil Kommissionen i forbindelse med EU-civilbeskyttelsesmekanismen:

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

b) regelmæssigt gennemgå det potentielle behov for at udvikle ny reaktionskapacitet på EU-plan gennem rescEU

c) yderligere intensivere det tværsektorielle samarbejde for at sikre en passende reaktion på EU-plan og tilrettelægge regelmæssige øvelser for at teste dette samarbejde

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

29) Kommissionen vil i samarbejde med den højtstående repræsentant og i tæt samråd med medlemsstaterne og med støtte fra relevante EU-agenturer udarbejde en plan for hændelser og kriser vedrørende kritisk infrastruktur, hvori der redegøres for og fastsættes mål og metoder for samarbejdet mellem medlemsstaterne og EU's institutioner, organer, kontorer og agenturer med hensyn til at reagere på hændelser mod kritisk infrastruktur, navnlig hvis disse medfører betydelige forstyrrelser af leveringen af væsentlige tjenester på det indre marked. I planen bør der gøres brug af de eksisterende integrerede ordninger for politisk kriserespons (IPCR) til at koordinere reaktionen.

30) Kommissionen vil samarbejde med interessenter og eksperter om mulige genopretningsforanstaltninger efter hændelser vedrørende undersøisk kabelinfrastruktur, som skal fremlægges i forbindelse med den statusundersøgelse, der er omhandlet i punkt 20, litra a), samt om at udarbejde yderligere beredskabsplaner og risikoscenarier og arbejde med Unionens modstandsdygtighed over for katastrofer inden for rammerne af EU-civilbeskyttelsesmekanismen.

KAPITEL IV INTERNATIONALT SAMARBEJDE

31) Kommissionen og den højtstående repræsentant vil, når det er relevant og i overensstemmelse med deres respektive opgaver og ansvarsområder i henhold til EU-retten, støtte partnerlande for at øge modstandsdygtigheden i enheder, der driver kritisk infrastruktur på deres område.

32) Kommissionen og den højtstående repræsentant vil i overensstemmelse med deres respektive opgaver og ansvarsområder i henhold til EU-retten styrke koordineringen med NATO om kritisk infrastrukturs modstandsdygtighed gennem den strukturerede

dialog mellem EU og NATO om modstandsdygtighed og vil oprette en taskforce til dette formål.

33) 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 om en ramme for en koordineret reaktion på hybride kampagner[25], 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 EU-reaktion på hybride kampagner og hybride trusler, bl.a. mod enheder, der driver kritisk infrastruktur.

34) Kommissionen vil overveje at inddrage tredjelandes repræsentanter, når det er relevant og hensigtsmæssigt, i forbindelse med samarbejdet og informationsudvekslingen mellem medlemsstaternes eksperter på området modstandsdygtigheden i enheder, der driver kritisk infrastruktur.

[…]

Udfærdiget i Strasbourg, den […].

På Rådets vegne
Formand

[25] Council conclusions on a Framework for a coordinated EU response to hybrid campaigns - Consilium (europa.eu).