EUROPEISKA
KOMMISSIONEN

Strasbourg den 18.10.2022
COM(2022) 551 final

2022/0338 (NLE)

Förslag till

RÅDETS REKOMMENDATION

om en samordnad strategi från unionens sida för att stärka den kritiska infrastrukturens motståndskraft

(Text av betydelse för EES)

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

Säkerhet är ett viktigt mål för Europeiska unionen. Det är visserligen medlemsstaterna som har huvudansvaret för att skydda medborgarna, men gemensamma åtgärder på unionsnivå bidrar i hög grad till säkerheten i EU som helhet. Samordning bidrar till att stärka motståndskraften, öka vaksamheten och stärka våra gemensamma insatser. Inom ramen för EU:s säkerhetsunion har viktiga åtgärder vidtagits för att bygga upp förmågor och kapacitet för att förebygga, upptäcka och vidta snara insatser vid många typer av säkerhetshot och för att koppla samman aktörer inom den offentliga och den privata sektorn i en gemensam insats.

För att EU ska kunna hantera en hotbild som ständigt förändras krävs konstant vaksamhet och anpassning. Rysslands anfallskrig mot Ukraina har lett till nya risker, som ofta kombineras till hybridhot. En av dessa är risken för störningar i tillhandahållandet av samhällsviktiga tjänster av entiteter som driver kritisk infrastruktur i Europa. Detta har blivit ännu tydligare genom det uppenbara sabotaget av Nord Stream-gasledningarna och andra nyligen inträffade händelser. Samhället är starkt beroende av både fysisk och digital infrastruktur, och avbrott i samhällsviktiga tjänster, oavsett om det sker genom konventionella fysiska angrepp eller cyberattacker, eller en kombination av dem, kan få allvarliga konsekvenser för medborgarnas välbefinnande, våra ekonomier och förtroendet för våra demokratiska system.

Att säkerställa en väl fungerande inre marknad är ett annat viktigt mål för EU, bland annat när det gäller samhällsviktiga tjänster som tillhandahålls av entiteter som driver kritisk infrastruktur. EU har därför redan vidtagit flera åtgärder för att minska sårbarheter och öka kritiska entiteters motståndskraft, både när det gäller cyberrisker och andra risker.

Det finns ett akut behov av åtgärder för att öka EU:s kapacitet att stå emot potentiella angrepp mot kritisk infrastruktur, främst inom EU, men där så är relevant även i unionens direkta grannskap.

Syftet med det här förslaget till en rådsrekommendation är att förstärka EU:s stöd för att förbättra motståndskraften hos kritisk infrastruktur och säkerställa samordning på EU-nivå när det gäller beredskap och insatser. Förslaget syftar till att maximera och påskynda arbetet med att skydda de tillgångar, anläggningar och system som är nödvändiga för att ekonomin ska fungera och tillhandahålla grundläggande tjänster på den inre marknaden som medborgarna är beroende av, samt att mildra effekterna av eventuella angrepp genom att säkerställa en så snar återhämtning som möjligt. Även om sådan infrastruktur bör skyddas, prioriteras för närvarande energi-, digitalinfrastruktur- och transportsektorerna, eftersom de spelar en utpräglad horisontell roll i samhället och ekonomin, samt aktuella riskbedömningar.

EU har en särskild roll att spela i fråga om att säkerställa motståndskraften hos den infrastruktur som korsar land- eller sjögränser och påverkar flera medlemsstaters intressen, eller som används för att tillhandahålla gränsöverskridande samhällsviktiga tjänster. Kritisk infrastruktur av betydelse för flera medlemsstater kan dock ligga i en enda medlemsstat eller till och med utanför en medlemsstats territorium, till exempel när det gäller undervattenskablar eller rörledningar. Det ligger i alla medlemsstaters och EU:s intresse att tydligt identifiera den kritiska infrastrukturen och de entiteter som driver den, liksom de risker som hotar den, och ett gemensamt åtagande att skydda den.

Europaparlamentet och rådet har redan nått en politisk överenskommelse om att fördjupa EU:s rättsliga ram för att bidra till att stärka motståndskraften hos entiteter som driver kritisk infrastruktur. Sommaren 2022 nåddes överenskommelser om direktivet om kritiska entiteters

motståndskraft (*CER-direktivet*)[1] och det ändrade nätverks- och informationssäkerhetsdirektivet (*NIS 2-direktivet*)[2]. Dessa två direktiv kommer att leda till en betydande intensifiering av kapaciteter jämfört med dagens rättsliga ramverk som består av direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (*ECI-direktivet*)[3] och Europarlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (*NIS-direktivet*)[4]. Den nya lagstiftningen förväntas träda i kraft i slutet av 2022 eller i början av 2023, och införlivandet och tillämpningen bör prioriteras av medlemsstaterna, i enlighet med unionsrätten.

Mot denna bakgrund, och med tanke på att det brådskar att möta hoten från Rysslands anfallskrig mot Ukraina, bör de steg som planeras i den nya lagstiftningen tidigareläggas från och med i dag. Att intensifiera det ömsesidiga samarbetet redan nu skulle också bidra till att skapa tyngd för ett effektivt genomförande när den nya lagstiftningen har trätt i kraft fullt ut.

Resultatet skulle bli att man redan nu går längre än de nuvarande ramarna, både när det gäller åtgärdernas djup och bredden på de sektorer som omfattas. Det nya CER-direktivet innehåller ett nytt ramverk för samarbete, samt skyldigheter för medlemsstaterna och de kritiska enheterna som syftar till att förstärka den fysiska icke-cyberresiliensen mot naturliga hot, och hot som människan skapat, hos entiteter som erbjuder samhällsviktiga tjänster på den inre marknaden. I direktivet specificeras elva sektorer[5]. Genom NIS 2-direktivet kommer en bred sektoriell täckning av skyldigheter på cybersäkerhetsområdet att införas. Detta kommer att omfatta ett nytt krav på att medlemsstaterna i förekommande fall ska låta undervattenskablar ingå i sina cybersäkerhetsstrategier.

Enligt direktivet ska kommissionen påta sig en viktig samordnande roll. Enligt CER-direktivet har kommissionen en stödjande och underlättande roll, som ska genomföras med stöd av och med deltagande av den grupp för kritiska entiteters motståndskraft som inrättades genom det direktivet, och den bör komplettera medlemsstaternas verksamhet genom att utveckla bästa praxis, vägledningsmaterial och metoder. När det gäller cybersäkerhet uppmanade rådet redan sommaren 2022 i sina slutsatser om EU:s arbete på cyberområdet kommissionen, den höga representanten och samarbetsgruppen för nät- och informationssäkerhet att arbeta med riskbedömning och scenarier ur ett it-säkerhetsperspektiv. Den typen av samordning kan inspirera till en strategi för annan viktig kritisk infrastruktur.

Den 5 oktober 2022 presenterade kommissionens ordförande Ursula von der Leyen en fempunktsplan med en samordnad strategi för det nödvändiga arbete som ligger framför oss. De viktigaste inslagen i planen är att förbättra beredskapen, samarbeta med medlemsstaterna i syfte att stresstesta deras kritiska infrastruktur, med början i energisektorn och därefter andra högrisksektorer, öka insatskapaciteten, särskilt genom unionens civilskyddsmekanism, utnyttja satellitkapaciteten för att upptäcka potentiella hot och stärka samarbetet med Nato och viktiga partner när det gäller motståndskraften hos kritisk infrastruktur. I fempunktsplanen underströks värdet av att föregripa den lagstiftning det redan nåtts politisk överenskommelse om.

---

1 COM(2020) 829 final.
2 COM(2020) 823 final.
3 EUT L 345, 23.12.2008.
4 EUT L 194, 19.7.2016.
5 Energi, transport, digital infrastruktur, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, offentlig förvaltning, rymden och livsmedelsproduktion

I förslaget till rådets rekommendation välkomnas denna strategi för att strukturera stödet till medlemsstaterna och samordna deras insatser för att öka riskmedvetenheten, riskberedskapen och hanteringen av de nuvarande hoten. I detta avseende sammankallas expertmöten för att diskutera motståndskraften hos entiteter som driver kritisk infrastruktur inför ikraftträdandet av CER-direktivet och gruppen för kritiska entiteters motståndskraft som inrättats genom det direktivet.

Ett förstärkt samarbete med viktiga partner och grannländer samt andra relevanta tredjeländer om motståndskraften hos entiteter som driver kritisk infrastruktur kommer att vara mycket viktigt, särskilt genom den strukturerade dialogen mellan EU och Nato om motståndskraft.

Fokuset för denna rekommendation ligger på att stärka unionens kapacitet att förutse, förebygga och reagera på de nya hot som uppstår till följd av Rysslands anfallskrig mot Ukraina. De föreslagna rekommendationerna är därför inriktade på att ta itu med säkerhetsrelaterade risker och hot mot kritisk infrastruktur. Man bör dock också notera att den senaste tidens händelser har betonat det akuta behovet av att fästa ökad vikt vid klimatförändringens följder för kritisk infrastruktur och tjänster, till exempel i fråga om oförutsägbar och säsongsberoende kylvattenförsörjning av kärnkraftverk, vattenkraft och inre sjöfart, eller risken för väsentliga skador på transportinfrastruktur, som kan leda till större avbrott i samhällsviktiga tjänster. Dessa orosväckande områden kommer fortsätta att hanteras genom relevant lagstiftning och samordning.

- **Förenlighet med befintliga bestämmelser inom området**

Detta förslag till en rådsrekommendation är helt i linje med den nuvarande och framtida rättsliga ramen för motståndskraften hos entiteter som driver kritisk infrastruktur, ECI-direktivet respektive CER-direktivet, eftersom det bland annat syftar till att underlätta samarbetet mellan medlemsstaterna på detta område och stödja konkreta åtgärder för att stärka motståndskraften mot de nuvarande överhängande hoten mot entiteter som driver kritisk infrastruktur i EU.

Det kompletterar och föregriper också CER-direktivet genom att redan nu uppmana medlemsstaterna att prioritera ett snart införlivande av direktivet, genom att samarbeta genom expertmöten som sammankallas som en del av den fempunktsplan som kommissionen aviserat och genom att sträva efter att samordna vägen till en gemensam strategi för genomförande av stresstester av kritisk infrastruktur i EU.

Förslaget är också i linje med NIS-direktivet och det kommande NIS2-direktivet, som kommer att upphäva NIS-direktivet, genom att det efterlyser en tidig start på genomförande- och införlivandearbetet. Det återspeglar också den gemensamma uppmaningen från ministermötet i Nevers i mars 2022 samt rådets slutsatser om utveckling av Europeiska unionens arbete på cyberområdet från maj 2022 när det gäller medlemsstaternas begäranden att kommissionen ska utveckla riskbedömningar och riskscenarier.

Förslaget är också i linje med EU:s politik för civilskydd där situationer med omfattande störningar av driften av kritisk infrastruktur eller hos entiteter gör att medlemsstater och tredjeländer kan begära hjälp via Centrumet för samordning av katastrofberedskap (*ERCC*) inom ramen för unionens civilskyddsmekanism. Om civilskyddsmekanismen aktiveras kan ERCC samordna och medfinansiera utplaceringen av nödvändig utrustning, materiel och expertis som finns tillgänglig i medlemsstaterna (delvis inom ramen för den europeiska civilskyddspoolen) och inom ramen för rescEU till det drabbade landet. Bistånd som kan göras tillgängligt på begäran omfattar t.ex. bränsle, generatorer, elinfrastruktur, inkvarteringskapacitet, vattenreningskapacitet och akut medicinsk kapacitet.

Förslaget är också i linje med EU:s regelverk om trygg energiförsörjning.

I förslaget till en rådsrekommendation ingår inte kärnenergisektorn, förutom exempelvis tillhörande infrastruktur (till exempel överföringsledningar till kärnkraftsanläggningar) som kan påverka tryggheten i energiförsörjningen. Särskilda kärnkraftsrelaterade delar täcks av relevant kärnkraftslagstiftning i Euratomfördraget och/eller nationell lagstiftning[6]. Mot bakgrund av lärdomarna från Fukushima-olyckan har den europeiska kärnsäkerhetslagstiftningen skärpts, och därför måste de nationella myndigheterna genomföra dels regelbundna säkerhetsgranskningar av varje anläggning för att säkerställa fortsatt efterlevnad av de högsta säkerhetskraven och identifiera ytterligare säkerhetsförbättringar, dels expertgranskningar på EU-nivå sex gånger per år.

I EU:s strategi för sjöfartsskydd[7] med tillhörande handlingsplan[8] belyses den föränderliga karaktären hos hoten på sjöfartsområdet och man efterlyser ett förnyat åtagande för att skydda kritisk sjöfartsinfrastruktur, inklusive undervattensmiljön, och framförallt sjöfartstransporter, energi- och kommunikationsinfrastruktur, till exempel genom att förbättra den maritima lägesbilden, vilket ska ske genom förstärkt interoperabilitet och effektivare informationsutbyte.

Förslaget är också i linje med annan relevant sektorslagstiftning. Genomförandet av denna rekommendation bör därför vara förenligt med särskilda åtgärder som reglerar eller i framtiden kan reglera vissa aspekter av motståndskraften hos entiteter som är verksamma inom berörda sektorer, som transportsektorn. Detta omfattar andra relevanta initiativ som beredskapsplanen för transportsektorn[9] eller beredskapsplanen för att trygga livsmedelstillgången och livsmedelsförsörjningen under kristider[10] och den tillhörande europeiska mekanismen för beredskap och insatser vid livsmedelsförsörjningskriser. Mer allmänt bör rekommendationen naturligtvis genomföras med full respekt för alla tillämpliga bestämmelser i EU-lagstiftningen, inbegripet de som fastställs i ECI-direktivet och NIS-direktivet.

Förslaget är också i linje med den strategiska kompassen för säkerhet och försvar, där man betonade behovet av att avsevärt stärka motståndskraften och förmågan att motverka hybridhot och cyberangrepp samt behovet av att stärka partnerländernas motståndskraft och samarbete med Nato. Det är också i linje med ramverket för en samordnad EU-reaktion på hybridhot och hybridkampanjer mot EU, medlemsstaterna och partner[11].

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

• Rättslig grund

Förslaget baseras på artikel 114 i fördraget om Europeiska unionens funktionssätt (*EUF-fördraget*) som rör tillnärmning av lagstiftning för att förbättra den inre marknaden, tillsammans med artikel 292 i samma fördrag. Detta motiveras av det faktum att den föreslagna rådsrekommendationen huvudsakligen syftar till att föregripa de åtgärder som fastställs i det nya CER-direktivet och det nya NIS2-direktivet, vilka båda även grundar sig på artikel 114 i EUF-fördraget. I linje med den logik som motiverade användningen av den

6 Skäl 9 i rådets direktiv 2008/114/EG (ECI-direktivet)
7 11205/14.
8 10494/18.
9 COM(2022) 211.
10 COM(2021) 689.
11 Europeiska unionens råd 10016/22, 21 juni 2022

artikeln som rättslig grund för de direktiven, krävs åtgärder från EU:s sida för att säkerställa en väl fungerande inre marknad, inte minst mot bakgrund av de berörda tjänsternas gränsöverskridande karaktär och omfattning samt potentiella konsekvenser i fråga om avbrott, samt de pågående och kommande nationella åtgärderna för att förbättra motståndskraften hos entiteter som driver kritisk infrastruktur och som har erfarenhet av att tillhandahålla samhällsviktiga tjänster på den inre marknaden.

- **Subsidiaritetsprincipen (för icke-exklusiv befogenhet)**

Att det fortsatta arbetet ska ske på europeisk nivå när det gäller motståndskraften hos entiteter som driver kritisk infrastruktur är motiverat med tanke på att förbindelserna mellan kritisk infrastruktur och de samhällsviktiga tjänster som tillhandahålls är inbördes beroende och gränsöverskridande, och med tanke på att det behövs en mer gemensam och samordnad europeisk strategi för att säkerställa att de berörda entiteterna är tillräckligt motståndskraftiga i den nuvarande geopolitiska situationen. Även om många av de gemensamma svårigheterna, till exempel det uppenbara sabotaget av Nord Stream-gasledningarna, i första hand hanteras genom nationella åtgärder eller av entiteter som driver kritisk infrastruktur, är det nödvändigt att det finns stöd från EU, inklusive relevanta organ där så är lämpligt, för att stärka motståndskraften, öka beredskapen och stärka EU:s gemensamma svar.

- **Proportionalitetsprincipen**

Detta förslag är förenligt med subsidiaritetsprincipen i artikel 5.4 i fördraget om Europeiska unionen (*EU-fördraget*).

Varken innehållet i eller utformningen av denna föreslagna rådsrekommendation går utöver vad som är nödvändigt för att uppnå målen. De föreslagna åtgärderna står i proportion till de eftersträvade målen eftersom de respekterar medlemsstaternas befogenheter och skyldigheter enligt nationell lagstiftning.

Slutligen innehåller förslaget ett potentiellt differentierat tillvägagångssätt som återspeglar medlemsstaternas olika nationella förhållanden när det gäller beredskap och insatser vid fysiska hot mot kritisk infrastruktur.

- **Val av instrument**

För att uppnå ovannämnda mål föreskrivs i EUF-fördraget, särskilt i artikel 292, att rådet ska anta rekommendationer på grundval av ett förslag från kommissionen. En rådsrekommendation är ett lämpligt instrument i detta fall, även med beaktande av den nuvarande lagstiftningssituationen enligt förklaringen ovan. Även om den inte är av bindande karaktär, signalerar en rådsrekommendation medlemsstaternas åtagande i fråga om åtgärderna i rekommendationen och lägger en solid politisk grund för samarbete på dessa områden, samtidigt som medlemsstaternas befogenheter respekteras.

3. RESULTAT AV EFTERHANDSUTVÄRDERINGAR, SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

- **Samråd med berörda parter**

Vid utarbetandet av detta förslag beaktades de synpunkter som medlemsstaternas experter framförde vid mötet den 12 oktober 2022. Det rådde bred enighet om nyttan av mer samordning på unionsnivå när det gäller beredskap och insatser i den rådande hotsituationen och om att föregripa vissa delar av CER-direktivet innan det formellt antas. Medlemsstaterna uttryckte villighet att utbyta erfarenheter och bästa praxis om åtgärder och metoder för att öka motståndskraften hos entiteter som driver kritisk infrastruktur. Medlemsstaterna uttryckte

också sitt gillande i fråga om en samordnad strategi för stresstester av entiteter som driver kritisk infrastruktur på frivillig basis och på grundval av gemensamma principer. Medlemsstaterna angav att entiteter som driver kritisk infrastruktur inom områdena energi, digital infrastruktur och transport bör prioriteras när det gäller denna rekommendation, särskilt sådana som är relevanta för flera medlemsstater. Medlemsstaterna välkomnade också kommissionens avsikt att sammankalla ytterligare möten med medlemsstaternas experter under de närmaste veckorna.

- **Ingående redogörelse för de specifika bestämmelserna i förslaget**

I förslaget till rådets rekommendation anges följande:

– I kapitel I fastställs förslagets syfte, vad det omfattar och prioritering av rekommenderade åtgärder.

– Kapitel II är inriktat på åtgärder som bör vidtas för att förbättra beredskapen, både på unionsnivå och på medlemsstatsnivå.

– Kapitel III omfattar förstärkta insatser, både på EU-nivå och på medlemsstatsnivå.

– Kapitel IV avser internationellt samarbete och de åtgärder som bör vidtas för att öka motståndskraften hos entiteter som driver kritisk infrastruktur.

2022/0338 (NLE)

Förslag till

RÅDETS REKOMMENDATION

om en samordnad strategi från unionens sida för att stärka den kritiska infrastrukturens motståndskraft

(Text av betydelse för EES)

EUROPEISKA UNIONENS RÅD UTFÄRDAR DENNA REKOMMENDATION

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

med beaktande av Europeiska kommissionens förslag, och

av följande skäl:

(1) Unionen har en särskild roll att spela när det gäller infrastruktur som överskrider gränser och påverkar flera medlemsstaters intressen, eller som på annat sätt används av entiteter för att tillhandahålla samhällsviktiga tjänster över gränserna. I vissa fall tillhandahålls sådana tjänster eller finns kritisk infrastruktur av betydelse för flera medlemsstater i en enda medlemsstat eller utanför medlemsstaternas territorium, vilket till exempel gäller undervattenskablar och rörledningar. Det ligger i alla medlemsstaters och unionens intresse att tydligt identifiera sådan infrastruktur och sådana entiteter samt hoten mot dem, och att göra ett kollektivt åtagande om att skydda dem.

(2) För närvarande regleras skyddet av kritisk infrastruktur inom två sektorer genom rådets direktiv 2008/114/EG[12]. Genom det direktivet fastställs ett förfarande för identifiering och klassificering av europeisk kritisk infrastruktur, samt en gemensam metod för bedömning av behovet att stärka skyddet av sådan infrastruktur för att bidra till att skydda människor. Det omfattar energi- och transportsektorerna. För att förbättra motståndskraften hos kritiska entiteter, de samhällsviktiga tjänster som de tillhandahåller och den kritiska infrastruktur som de är beroende av håller ett nytt direktiv om kritiska entiteters motståndskraft[13] (*CER-direktivet*) på att antas av unionslagstiftaren, vilket kommer att ersätta direktiv 2008/114/EG och omfatta fler sektorer, däribland digital infrastruktur.

(3) Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen[14] inriktas på cyberrelaterade hot. Det direktivet kommer att ersättas av ett nytt direktiv

---

12 Rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (EUT L 345, 23.12.2008, s. 75).

13 COM(2020) 829.

14 Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (*NIS 2-direktivet*)[15], som också håller på att antas av unionslagstiftaren.

(4) Mot bakgrund av den snabbt föränderliga hotbilden, särskilt det uppenbara sabotaget av gasinfrastrukturen Nord Stream 1 och 2, står entiteter som driver kritisk infrastruktur inför särskilda utmaningar när det gäller deras motståndskraft mot fientliga handlingar och andra hot orsakade av människan, samtidigt som problemen som orsakas av naturliga faktorer och klimatförändringar ökar och kan utnyttjas för fientliga handlingar. Dessa entiteter måste därför, med stöd från medlemsstaterna, vidta lämpliga åtgärder för att stärka sin motståndskraft. Dessa åtgärder bör vidtas och detta stöd bör ges utöver de åtgärder som krävs enligt direktiv 2008/114/EG och direktiv (EU) 2016/1148, till och med innan de nya CER- och NIS 2-direktiven antas, träder i kraft och införlivas.

(5) I avvaktan på att dessa nya direktiv antas, träder i kraft och införlivas uppmanas unionen och medlemsstaterna, i enlighet med unionsrätten, att använda alla tillgängliga verktyg för att gå vidare och bidra till att stärka den fysiska motståndskraften och cyberresiliensen hos de berörda entiteterna och den kritiska infrastruktur som dessa driver för att tillhandahålla samhällsviktiga tjänster på den inre marknaden, dvs. tjänster som är avgörande för upprätthållandet av centrala samhällsfunktioner, ekonomisk verksamhet, människors hälsa och säkerhet samt miljön. I detta avseende bör begreppet ”motståndskraft” förstås som en hänvisning till en entitets förmåga att förebygga, skydda mot, reagera på, stå emot, mildra, absorbera, anpassa sig till och återhämta sig från händelser som skulle kunna leda till en betydande störning av, eller faktiskt stör, tillhandahållandet av de samhällsviktiga tjänsterna i fråga.

(6) För att säkerställa att strategin både är ändamålsenlig och i så stor utsträckning som möjligt överensstämmer med det nya CER-direktivet bör åtgärderna i denna rekommendation avse infrastruktur som av en medlemsstat betecknas som kritisk infrastruktur, vilket omfattar både nationell och europeisk kritisk infrastruktur, oavsett om den entitet som driver den kritiska infrastrukturen redan har utsetts till kritisk entitet enligt det nya direktivet eller inte. I denna rekommendation bör begreppet ”kritisk infrastruktur” förstås i enlighet med detta.

(7) Med tanke på de befintliga hoten bör åtgärder som stärker motståndskraften vidtas som en prioriterad fråga inom nyckelsektorerna energi, digital infrastruktur, transport och rymden, och de bör inriktas på att öka motståndskraften mot risker orsakade av människan hos entiteter som driver kritisk infrastruktur. Med tanke på de möjliga konsekvenserna om riskerna mot nationell kritisk infrastruktur skulle förverkligas bör prioritet ges åt infrastruktur av gränsöverskridande betydelse.

(8) De åtgärder som fastställs i denna rekommendation syftar därför huvudsakligen till att komplettera de nya CER- och NIS 2-direktiven, som grundar sig på artikel 114 i fördraget om Europeiska unionens funktionssätt (*EUF-fördraget*), genom att föregripa och komplettera de åtgärder som kommer att föreskrivas i dessa nya direktiv. Med tanke på dessa samhällsviktiga tjänsters och denna kritiska infrastrukturs gränsöverskridande karaktär och relevans och de nuvarande och framväxande skillnaderna i nationell lagstiftning som snedvrider den inre marknaden, är det därför lämpligt att även grunda denna rekommendation på artikel 114 i EUF-fördraget, tillsammans med artikel 292 i samma fördrag.

---

15 COM(2020) 823.

(9) Genomförandet av denna rekommendation bör inte anses påverka nuvarande och framtida krav i unionsrätten när det gäller vissa aspekter av de berörda enheternas motståndskraft, utan bör vara förenligt med dessa krav. Sådana krav fastställs i allmänna instrument som direktiv 2008/114/EG och direktiv (EU) 2016/1148 och de nya CER- och NIS 2-direktiven som ersätter dem, men också i vissa sektorsspecifika instrument, t.ex. på transportområdet, där kommissionen bland annat har tagit initiativ till en beredskapsplan för transporter.[16] I enlighet med principen om lojalt samarbete bör denna rekommendation genomföras med full ömsesidig respekt och fullt ömsesidigt bistånd.

(10) Den 5 oktober 2022 tillkännagav kommissionen en fempunktsplan med en samordnad strategi för att hantera de kommande utmaningarna, vilken inbegriper arbetet med att stärka beredskapen genom att bygga vidare på och föregripa antagandet och ikraftträdandet av det nya CER-direktivet och också omfattar samarbete med medlemsstaterna på grundval av gemensamma principer i syfte att stresstesta entiteter som driver kritisk infrastruktur, till att börja med inom energisektorn. I denna rekommendation, som kommer att bidra till den planen, välkomnas den föreslagna strategin och beskrivs hur den kan omsättas i handling.

(11) Mot bakgrund av den snabbt föränderliga hotbilden och den nuvarande riskmiljön som kännetecknas av risker orsakade av människan, särskilt när det gäller kritisk infrastruktur med gränsöverskridande betydelse, är det viktigt att ha en korrekt, aktuell och fullständig bild av de viktigaste riskerna för entiteter som driver kritisk infrastruktur. Medlemsstaterna bör därför vidta nödvändiga åtgärder för att bedöma dessa risker eller uppdatera sina riskbedömningar. Även om denna rekommendation är inriktad på säkerhetsrelaterade risker bör insatserna för att ta itu med klimatförändringar och miljörisker fortsätta, särskilt vad gäller naturfenomen som ytterligare kan förvärra risker orsakade av människan.

(12) Med beaktande av denna hotbild bör medlemsstaterna uppmanas att utöver de nämnda riskbedömningarna så snart som möjligt vidta lämpliga åtgärder för att göra kritisk infrastruktur mer motståndskraftig, vilket kommer att krävas enligt det nya CER-direktivet.

(13) Som en del av genomförandet av den fempunktsplan som kommissionen har aviserat är det nödvändigt att samordna arbetet genom att sammankalla nationella experter inför inrättandet av gruppen för kritiska entiteters motståndskraft enligt det nya CER-direktivet, för att möjliggöra samarbete mellan medlemsstaterna samt utbyte av information om motståndskraften hos entiteter som driver kritisk infrastruktur. Detta bör inbegripa samarbete och utbyte av information om åtgärder såsom identifiering av kritiska entiteter och kritisk infrastruktur, förberedelser för att utveckla och främja en gemensam uppsättning principer för att genomföra stresstester och dra gemensamma lärdomar av dem, samt identifiering av sårbarheter och möjlig kapacitet. Dessa processer bör också stärka motståndskraften mot klimat- och miljörisker hos entiteter som driver kritisk infrastruktur. Detta arbete skulle också göra det möjligt att gemensamt prioritera arbetet med stresstester, med tonvikt på energi-, digitalinfrastruktur-, transport- och rymdsektorerna. Kommissionen har redan börjat sammankalla dessa experter och underlätta deras arbete, och avser att fortsätta göra detta. När det nya CER-direktivet har trätt i kraft, och gruppen för kritiska entiteters

[16] COM(2022) 211.

motståndskraft har inrättats, bör denna grupp fortsätta med sådant föregripande arbete i enlighet med sina uppgifter enligt CER-direktivet.

(14) Stresstestet bör kompletteras med utarbetandet av en plan för incidenter och kriser som rör kritisk infrastruktur, där man beskriver och fastställer målen och formerna för samarbetet mellan medlemsstaterna och EU:s institutioner, organ och byråer för att hantera incidenter som rör kritisk infrastruktur, särskilt när dessa medför betydande störningar i tillhandahållandet av samhällsviktiga tjänster för den inre marknaden. I denna plan bör insatserna samordnas genom befintliga arrangemang för integrerad politisk krishantering; arbetet bör överensstämma med och komplettera strategin för storskaliga cyberincidenter och man bör även nå en överenskommelse om viktiga budskap till allmänheten, med tanke på att kriskommunikation spelar en viktig roll när det gäller att mildra de negativa effekterna av incidenter och kriser som rör kritisk infrastruktur.

(15) För att säkerställa ett samordnat och effektivt svar på nuvarande och förväntade hot kommer kommissionen att ge ytterligare stöd till medlemsstaterna i syfte att stärka motståndskraften i förhållande till dessa hot, särskilt genom att tillhandahålla relevant information genom genomgångar, handböcker och riktlinjer, främja utnyttjandet av unionsfinansierade forsknings- och innovationsprojekt, vidta nödvändiga föregripande åtgärder och optimera användningen av unionens övervakningsresurser. Europeiska utrikestjänsten bör, särskilt genom EU:s underrättelse- och lägescentral, tillhandahålla hotbildsbedömningar.

(16) Sektorsrelevanta unionsbyråer och andra relevanta organ bör också tillhandahålla stöd i frågor som rör motståndskraften, i den mån deras respektive mandat enligt relevanta instrument i unionsrätten tillåter det. I synnerhet skulle Europeiska unionens cybersäkerhetsbyrå (Enisa) kunna bistå i frågor som rör cybersäkerhet; Europeiska sjösäkerhetsbyrån (Emsa) skulle kunna bistå medlemsstaterna i frågor som rör sjöfartsskydd och sjösäkerhet genom sin sakkunskap och sin havsövervakningstjänst; Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) skulle kunna ge stöd i samband med insamling av information och med utredningar om gränsöverskridande brottsbekämpande åtgärder, medan Europeiska unionens rymdprogrambyrå (EUSPA) och EU:s satellitcentrum skulle kunna bistå genom insatser inom ramen för unionens rymdprogram.

(17) Det primära ansvaret för att säkerställa den kritiska infrastrukturens och de berörda entiteternas säkerhet ligger hos medlemsstaterna, men ökad samordning på unionsnivå är lämplig, särskilt mot bakgrund av hot som samtidigt kan påverka flera medlemsstater, såsom Rysslands anfallskrig mot Ukraina, eller påverka motståndskraften och funktionen hos unionens ekonomi, inre marknad och samhällen.

(18) Denna rekommendation innebär inte att information ska tillhandahållas vars röjande strider mot medlemsstaternas väsentliga intressen i fråga om nationell och allmän säkerhet eller försvar.

(19) Genom det ökande ömsesidiga beroendet mellan fysisk och digital infrastruktur kan skadlig cyberverksamhet som riktar sig mot kritiska områden leda till störningar eller skador på fysisk infrastruktur, medan sabotage av fysisk infrastruktur kan göra digitala tjänster otillgängliga. Med tanke på det ökade hotet från sofistikerade hybridattacker bör medlemsstaterna också ta med sådana överväganden i genomförandet av denna rekommendation. Med tanke på kopplingarna mellan cybersäkerhet och operatörernas fysiska säkerhet är det viktigt att arbetet med att förbereda införlivandet och

tillämpningen av det nya NIS 2-direktivet inleds så snart som möjligt och att detta arbete fortskrider parallellt inom ramen för det nya CER-direktivet.

(20) Förutom att stärka beredskapen är det också viktigt att förbättra förmågan att reagera snabbt och effektivt om risker materialiseras som påverkar tillhandahållandet av samhällsviktiga tjänster som tillhandahålls av entiteter som driver kritisk infrastruktur. Denna rekommendation bör därför ange vilka åtgärder som bör vidtas på både medlemsstats- och unionsnivå, däribland utökat samarbete och informationsutbyte inom ramen för unionens civilskyddsmekanism samt användning av relevanta resurser i unionens rymdprogram.

(21) Till följd av rådets uppmaning i slutsatserna om EU:s arbete på cyberområdet[17] genomför kommissionen, unionens höga representant för utrikes frågor och säkerhetspolitik (*den höga representanten*) och den samarbetsgrupp som inrättats genom direktiv (EU) 2016/1148 (*samarbetsgruppen för nät- och informationssäkerhet*), i samordning med relevanta civila och militära organ och byråer samt etablerade nätverk, inbegripet EU CyCLONe, en riskbedömning och utarbetar riskscenarier ur ett cybersäkerhetsperspektiv i en situation med hot eller möjlig attack mot medlemsstater eller partnerländer. Detta arbete är inriktat på kritiska sektorer såsom energi, digital infrastruktur, transport och rymden.

(22) I den gemensamma uppmaningen från ministermötet i Nevers[18] och i rådets slutsatser om EU:s arbete på cyberområdet efterlystes också åtgärder för att stärka motståndskraften hos kommunikationsinfrastruktur och kommunikationsnät i unionen genom att utfärda rekommendationer till medlemsstaterna och kommissionen på grundval av en riskbedömning. En sådan riskbedömning genomförs för närvarande av samarbetsgruppen för nät- och informationssäkerhet med stöd av kommissionen och Enisa och i samarbete med Organet för europeiska regleringsmyndigheter för elektronisk kommunikation (Berec). I riskbedömningen och gapanalysen granskas riskerna för cyberattacker för olika delsektorer av kommunikationsinfrastrukturen, inbegripet fast och mobil infrastruktur, satelliter, undervattenskablar, internetdirigering etc., och de utgör därför underlag för arbetet inom ramen för denna rekommendation. Den riskbedömningen ger information som används i det pågående arbetet med den cyberriskbedömning och de cyberriskscenarier på tvärsektoriell nivå som rådet efterfrågade i sina slutsatser av den 23 maj 2022.

(23) Dessa två övningar kommer att vara samstämmiga och samordnas med den övning som gäller scenarier för civilskydd i samband med en rad olika naturkatastrofer och katastrofer orsakade av människan, inbegripet cybersäkerhetshändelser och deras konkreta konsekvenser, som kommissionen och medlemsstaterna för närvarande arbetar med inom ramen för Europaparlamentets och rådets beslut 1313/2013/EU[19]. Denna rekommendation bör av skäl som hänför sig till effektivitet, ändamålsenlighet och samstämmighet tillämpas på ett sätt som beaktar resultaten av dessa övningar.

(24) I EU:s verktygslåda för 5G-cybersäkerhet[20] fastställs relevanta åtgärder och riskminskningsplaner för att stärka 5G-nätens säkerhet. Med tanke på att många

---

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

20 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

samhällsviktiga tjänster är beroende av 5G-nät och att de digitala ekosystemen är sammanlänkade med varandra är det mycket viktigt att alla medlemsstater snarast genomför de åtgärder som rekommenderas i verktygslådan och i synnerhet tillämpar relevanta begränsningar för högriskleverantörer när det gäller nyckeltillgångar som definierats som kritiska och känsliga i EU:s samordnade riskbedömning.

(25) I syfte att omedelbart stärka beredskapen och förmågan att hantera en större cyberincident har kommissionen inrättat ett kortsiktigt program för att stödja medlemsstaterna genom att ge Enisa ytterligare anslag. Tjänster som omfattas är bland annat beredskapsåtgärder, såsom penetrationstester av kritiska entiteter för att upptäcka sårbarheter. Programmet kommer även att förbättra möjligheterna att bistå medlemsstaterna i händelse av en större incident som påverkar kritiska entiteter. Detta är ett första steg i linje med rådets slutsatser om arbetet på cyberområdet, i vilka kommissionen uppmanades att lägga fram ett förslag om en fond för hantering av cybersäkerhetsincidenter. Medlemsstaterna bör dra full nytta av dessa möjligheter i enlighet med gällande krav.

(26) Det globala sjökabelnätet för datatrafik och elektronisk kommunikation är av grundläggande betydelse för konnektiviteten globalt och inom EU. På grund av kablarnas betydande längd och det faktum att de är anlagda på havsbotten är merparten av kabelnätets delar utomordentligt svåra att visuellt övervaka under vatten. Den gemensamma jurisdiktionen och andra jurisdiktionsfrågor gällande detta kabelnät är ett särskilt starkt argument för europeiskt och internationellt samarbete när det gäller skydd och återställande av infrastruktur. Det är därför nödvändigt att komplettera pågående och planerade riskbedömningar av de digitala och fysiska infrastrukturer som ligger till grund för digitala tjänster med särskilda riskbedömningar och handlingsalternativ när det gäller riskreducerande åtgärder inriktade på undervattenskablar. Kommissionen kommer därför att genomföra studier angående detta och informera medlemsstaterna om resultaten av dessa.

(27) De prioriterade sektorer som anges i denna rekommendation vad gäller energi och transport kan också påverkas av risker som rör den digitala infrastrukturen. En sådan påverkan kan till exempel uppstå när det gäller energiteknik som integrerar digitala komponenter. Säkerheten i därmed sammanhängande leveranskedjor är viktig för kontinuiteten i tillhandahållandet av samhällsviktiga tjänster och för den strategiska kontrollen av kritisk infrastruktur som drivs av entiteter inom energisektorn. Dessa omständigheter bör beaktas när åtgärder vidtas i enlighet med denna rekommendation för att stärka motståndskraften hos entiteter som driver kritisk infrastruktur.

(28) Den växande betydelse som rymdinfrastruktur och rymdbaserade tjänster har i säkerhetsrelaterad verksamhet gör att det är mycket viktigt att säkerställa att unionens rymdtillgångar och rymdtjänster är motståndskraftiga och skyddas inom EU, men också, inom ramen för denna rekommendation, att på ett mer strukturerat sätt dra nytta av de rymdbaserade data och tjänster som tillhandahålls av rymdsystem och rymdprogram för att övervaka och skydda kritisk infrastruktur inom andra sektorer. EU:s kommande rymdstrategi för säkerhet och försvar kommer i detta sammanhang att innehålla förslag till lämpliga åtgärder, vilka bör beaktas i genomförandet av denna rekommendation.

(29) Det behövs även samarbete på internationell nivå för att på ett effektivt sätt hantera risker för motståndskraften hos entiteter som driver kritisk infrastruktur i antingen unionen, relevanta tredjeländer eller i internationella vatten. Medlemsstaterna bör därför uppmanas att samarbeta med kommissionen och den höga representanten för att

vidta vissa åtgärder i detta syfte, under förutsättning att alla sådana åtgärder bara vidtas i enlighet med parternas respektive uppgifter och ansvarsområden enligt unionsrätten, i synnerhet bestämmelserna i EU-fördragen om yttre förbindelser.

(30) Som fastställs i meddelandet Kommissionens bidrag till det europeiska försvaret[21], till stöd för En strategisk kompass för säkerhet och försvar – För ett EU som skyddar sina medborgare, värden och intressen och bidrar till internationell fred och säkerhet[22] kommer kommissionen att bedöma EU:s utgångsvärden för sektorsspecifik hybridresiliens i samarbete med den höga representanten och medlemsstaterna genom att senast 2023 identifiera brister och behov samt vad som behöver göras för att åtgärda dem. Detta initiativ bör beaktas i arbetet inom ramen för denna rekommendation för att öka utbytet av information och samordningen av åtgärder som syftar till att stärka motståndskraften hos bland annat kritisk infrastruktur.

(31) I EU:s strategi för sjöfartsskydd och dess handlingsplan från 2014 efterlystes ökat skydd för kritisk maritim infrastruktur, inbegripet undervattensinfrastruktur, och i synnerhet sjötransport-, energi- och kommunikationsinfrastruktur, bland annat genom en förbättrad maritim lägesbild genom ökad driftskompatibilitet och effektivt informationsutbyte (obligatoriskt och frivilligt). Strategin och handlingsplanen håller för närvarande på att uppdateras och kommer att inkludera stärkta åtgärder för att skydda kritisk maritim infrastruktur. Dessa åtgärder bör beaktas i, och komplettera, denna rekommendation.

(32) Medlemsstaterna bör beakta hela den potential som ligger i unionens säkerhetsforskningsprogram och i synnerhet utnyttja dess särskilda insatsområde gällande kritisk infrastruktur, särskilt genom de program som finansieras genom Fonden för inre säkerhet, samt även andra potentiella finansieringsmöjligheter på unionsnivå, såsom Europeiska regionala utvecklingsfonden i den mån särskilda åtgärder uppfyller fondens krav för stödberättigande. REPowerEU kan också erbjuda möjligheter till finansiering i fråga om motståndskraft. Varje sådant utnyttjande av de möjligheter som finns att få finansiering från unionen måste uppfylla tillämpliga rättsliga krav.

HÄRIGENOM REKOMMENDERAS FÖLJANDE.

KAPITEL I: SYFTE, TILLÄMPNINGSOMRÅDE OCH PRIORITERING

(1) Genom denna rekommendation uppmanas medlemsstaterna att vidta skyndsamma och ändamålsenliga åtgärder, samt att samarbeta lojalt, effektivt, solidariskt och samordnat med varandra, kommissionen och andra relevanta offentliga myndigheter samt med berörda entiteter, för att stärka motståndskraften hos den kritiska infrastruktur som används för att tillhandahålla samhällsviktiga tjänster på den inre marknaden.

(2) De åtgärder som anges i denna rekommendation gäller infrastruktur som en medlemsstat klassificerat som kritisk infrastruktur, inbegripet som europeisk kritisk infrastruktur.

(3) I genomförandet av denna rekommendation ska åtgärder prioriteras som är inriktade på att stärka motståndskraften hos entiteter med verksamhet inom sektorerna energi,

[21] https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52022DC0060&from=EN

[22] Europeiska unionens råd, 7371/22, 21 mars 2022.

digital infrastruktur, transport och rymden, samt motståndskraften hos den kritiska infrastruktur som dessa entiteter driver som är av gränsöverskridande relevans, vad gäller risker orsakade av människan.

KAPITEL II: ÖKAD BEREDSKAP

Åtgärder på medlemsstatsnivå

(4) Medlemsstaterna uppmanas att genomföra eller uppdatera riskbedömningar av motståndskraften hos entiteter som driver infrastruktur som klassificerats som europeisk kritisk infrastruktur inom transport- och energisektorerna enligt direktiv 2008/114/EG och, om lämpligt och i enlighet med det direktivet, samarbeta med varandra i samband med sådana riskbedömningar och i samband med åtgärder för att stärka motståndskraften som dessa riskbedömningar leder till.

(5) Dessutom, och för att uppnå en hög nivå av motståndskraft hos entiteter som driver kritisk infrastruktur, bör medlemsstaterna påskynda det förberedande arbetet för att så snart som möjligt införliva och tillämpa det nya CER-direktivet genom att

(a) påskynda antagandet eller uppdateringen av nationella strategier för att öka motståndskraften hos entiteter som driver kritisk infrastruktur, i syfte att bemöta det aktuella hotet, varvid relevanta delar av dessa strategier bör meddelas kommissionen,

(b) utföra eller uppdatera riskbedömningar i linje med de aktuella hotens föränderliga karaktär, när det gäller motståndskraften hos entiteter som driver kritisk infrastruktur inom relevanta sektorer utöver energi, digital infrastruktur, transport och rymden och, om möjligt, inom de sektorer som omfattas av det nya CER-direktivet, nämligen bankverksamhet, finansmarknadsinfrastruktur, digital infrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, offentlig förvaltning, rymden samt produktion, bearbetning och distribution av livsmedel, med beaktande av de relevanta hotens potentiella hybridkaraktär, inbegripet kaskadeffekter och klimatförändringarnas effekter,

(c) informera kommissionen om de typer av risker som identifierats per sektor och delsektor och om resultaten av riskbedömningarna, vilket kan göras med hjälp av en gemensam rapporteringsmall som tagits fram av kommissionen i samarbete med medlemsstaterna,

(d) påskynda processen för identifiering och klassificering av kritiska entiteter, med prioritering av kritiska entiteter som

(a) använder kritisk infrastruktur som är fysiskt sammankopplad mellan två eller fler medlemsstater,

(b) ingår i företagsstrukturer som är sammankopplade eller sammanlänkade med kritiska entiteter i andra medlemsstater,

(c) har identifierats som sådana i en medlemsstat och tillhandahåller samhällsviktiga tjänster i eller till sex medlemsstater eller fler och därför är av särskild europeisk betydelse, och informera kommissionen om detta,

(d) samarbetar med varandra, särskilt när det gäller kritiska entiteter och samhällsviktiga tjänster och kritisk infrastruktur av gränsöverskridande betydelse, särskilt genom att samråda med varandra vid tillämpning av punkt 5 d och genom att informera varandra i händelse av en incident med betydande eller potentiellt betydande gränsöverskridande störningar, samtidigt som kommissionen vid behov hålls underrättad,

(e) öka stödet till utsedda kritiska entiteter för att förbättra deras motståndskraft, vilket kan inbegripa tillhandahållande av material och metoder för vägledning, anordnande av övningar för att testa deras motståndskraft och tillhandahållande av rådgivning och utbildning av deras personal, samt möjliggörande av bakgrundskontroller av personer med känsliga funktioner, i enlighet med unionslagstiftning och nationell lagstiftning och som en del av de kritiska entiteternas hantering av personalsäkerhet,

(f) påskynda utseendet eller inrättandet av en gemensam kontaktpunkt inom den behöriga myndigheten som ska utöva en sambandsfunktion, i syfte att säkerställa gränsöverskridande samarbete när det gäller motståndskraften hos entiteter som driver kritisk infrastruktur med de gemensamma kontaktpunkterna i andra medlemsstater.

(6) Medlemsstaterna uppmuntras att genomföra stresstester av entiteter som driver kritisk infrastruktur. Medlemsstaterna uppmanas särskilt att höja sin och de berörda entiteternas beredskap inom energisektorn och genomföra stresstester inom denna sektor, så långt som möjligt enligt principer som överenskommits på unionsnivå, samtidigt som ändamålsenlig kommunikation med de berörda entiteterna säkerställs. Stresstester inom andra prioriterade sektorer, nämligen digital infrastruktur, transport och rymden, kan vid behov övervägas senare, med vederbörlig hänsyn till inspektioner i luft- och sjöfartsdelsektorerna i enlighet med unionsrätten och med beaktande av relevanta bestämmelser i sektorslagstiftningen.

(7) Medlemsstaterna uppmanas att, när så är lämpligt och i enlighet med unionsrätten, samarbeta med relevanta tredjeländer när det gäller motståndskraften hos entiteter som driver kritisk infrastruktur av gränsöverskridande betydelse.

(8) Medlemsstaterna uppmanas att, i enlighet med tillämpliga krav, utnyttja potentiella finansieringsmöjligheter på unionsnivå och nationell nivå för att öka motståndskraften hos entiteter som driver kritisk infrastruktur i unionen, inbegripet till exempel längs transeuropeiska nät, mot alla typer av betydande hot, särskilt inom ramen för de program som finansieras av Fonden för inre säkerhet och Europeiska regionala utvecklingsfonden, förutsatt att respektive kriterier för stödberättigande uppfylls, och Fonden för ett sammanlänkat Europa, inbegripet bestämmelser om klimatsäkring. Finansiering från unionens civilskyddsmekanism kan också användas för detta ändamål, i enlighet med tillämpliga krav, särskilt för projekt som rör riskbedömningar, investeringsplaner eller investeringsstudier, kapacitetsuppbyggnad eller förbättring av kunskapsbasen. REPowerEU kan också erbjuda möjligheter till finansiering i fråga om motståndskraft.

(9) När det gäller kommunikations- och nätinfrastrukturen i unionen bör samarbetsgruppen för nät- och informationssäkerhet, i enlighet med artikel 11 i direktiv (EU) 2016/1148 och därefter artikel 14 i NIS 2-direktivet, påskynda sitt pågående arbete med en riktad riskbedömning och lägga fram de första rekommendationerna i början av 2023. Detta arbete bör utföras genom att man säkerställer samstämmighet och komplementaritet med det arbete som utförs av samarbetsgruppen för nät- och informationssäkerhet när det gäller säkerhet i leveranskedjan för informations- och kommunikationsteknik samt av andra relevanta grupper, såsom den grupp för kritiska entiteters motståndskraft som ska inrättas

enligt det nya CER-direktivet och det tillsynsforum som ska inrättas enligt den nya akten om digital operativ motståndskraft[23].

(10) Samarbetsgruppen för nät- och informationssäkerhet, som ska utföra sina uppgifter i enlighet med artikel 11 i direktiv (EU) 2016/1148 och därefter artikel 14 i NIS 2-direktivet, uppmanas att, med stöd av kommissionen och Enisa, prioritera sitt arbete med säkerheten i den digitala infrastrukturen och rymdsektorerna, bland annat genom att utarbeta policyer och metoder och åtgärder för hantering av cybersäkerhetsrisker baserade på en allriskstrategi för undervattenskablar, i avvaktan på ikraftträdandet av NIS 2-direktivet, samt med utarbetandet av en vägledning för riskhanteringsåtgärder för cybersäkerhet för operatörer inom rymdsektorn i syfte att öka motståndskraften hos markbaserad infrastruktur som stöder tillhandahållandet av rymdbaserade tjänster.

(11) Medlemsstaterna bör fullt ut utnyttja de tjänster för cybersäkerhetsberedskap som erbjuds i det stödprogram på kort sikt som kommissionen genomför tillsammans med Enisa, särskilt penetrationstester för att identifiera sårbarheter, och de uppmuntras i detta sammanhang att prioritera entiteter som driver kritisk infrastruktur inom energi-, digitalinfrastruktur- och transportsektorerna.

(12) Medlemsstaterna bör skyndsamt genomföra de åtgärder som rekommenderas i EU:s verktygslåda för 5G-säkerhet[24]. Medlemsstater som ännu inte har infört restriktioner för högriskleverantörer bör göra detta utan ytterligare dröjsmål, med tanke på att förlorad tid kan öka nätens sårbarhet i unionen. De bör också stärka det fysiska och icke-fysiska skyddet av kritiska och känsliga delar av 5G-nät, bland annat genom strikta åtkomstkontroller. Dessutom bör medlemsstaterna i samarbete med kommissionen bedöma behovet av kompletterande åtgärder, inbegripet rättsligt bindande krav på unionsnivå, för att säkerställa en enhetlig nivå av säkerhet och motståndskraft i 5G-näten.

(13) Medlemsstaterna bör snarast möjligt genomföra den kommande nätföreskriften avseende cybersäkerhetsaspekter av gränsöverskridande elflöden, på grundval av erfarenheterna från genomförandet av NIS-direktivet och relevant vägledning från samarbetsgruppen för nät- och informationssäkerhet, särskilt dess referensdokument om säkerhetsåtgärder för operatörer av samhällsviktiga tjänster.

(14) Medlemsstaterna bör utveckla användningen av Galileo och/eller Copernicus för övervakning och dela relevant information med de experter som sammankallas i enlighet med punkt 15. Den kapacitet som erbjuds av unionens statliga satellitkommunikation (Govsatcom) inom unionens rymdprogram bör utnyttjas på ett bra sätt för övervakning av kritisk infrastruktur och stöd till krishantering.

Åtgärder på unionsnivå

(15) Kommissionen har för avsikt att stärka samarbetet mellan medlemsstaternas experter i syfte att bidra till att stärka den fysiska motståndskraften utanför cyberområdet för entiteter som driver kritisk infrastruktur, särskilt genom att

(a) förbereda utvecklingen och främjandet av gemensamma verktyg för att stödja medlemsstaterna i arbetet med att stärka sådan motståndskraft, inbegripet metoder och riskscenarier,

---

23 COM(2020) 595 final.

24 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

(b) stödja utvecklingen av gemensamma principer för medlemsstaternas genomförande av de stresstester som avses i punkt 6, med början i sådana tester som fokuserar på risker orsakade av människan inom energisektorn och därefter inom andra nyckelsektorer, såsom digital infrastruktur, transport och rymden, och åsyftar andra betydande risker och faror och, i relevanta fall, ge stöd till och rådgivning om genomförandet av sådana stresstester,

(c) tillhandahålla en säker plattform för att samla in, utvärdera och utbyta bästa praxis, lärdomar från nationella erfarenheter och annan information om sådan motståndskraft, bland annat om genomförande av dessa stresstester och överföring av resultaten av dessa till protokoll och beredskapsplaner.

Dessa experters arbete bör ägna särskild uppmärksamhet åt sektorsövergripande beroenden och entiteter som driver kritisk infrastruktur av gränsöverskridande betydelse, och bör fortsättas av gruppen för kritiska entiteters motståndskraft när den väl har inrättats.

(16) Medlemsstaterna bör delta fullt ut i det förstärkta samarbete som avses i punkt 15, bland annat genom att utse kontaktpunkter med relevant sakkunskap och genom att utbyta erfarenheter om metoder som används för stresstester och de protokoll och beredskapsplaner som utarbetas på grundval av dessa. Vid sådant utbyte bör informationens konfidentialitet och de kritiska entiteternas säkerhetsintressen och kommersiella intressen skyddas, samtidigt som medlemsstaternas säkerhet iakttas. Detta innebär inte tillhandahållande av information vars röjande strider mot medlemsstaternas väsentliga intressen avseende nationell säkerhet, allmän säkerhet eller försvar.

(17) Kommissionen kommer att stödja medlemsstaterna genom att tillhandahålla handböcker och vägledningar, såsom att utarbeta en handbok om skydd av kritisk infrastruktur och offentliga platser mot obemannade luftfartygssystem och verktyg för riskbedömningar. Utrikestjänsten uppmanas, särskilt genom EU:s underrättelse- och lägescentral och dess gemensamma enhet för hybridhot, att hålla genomgångar om hoten mot kritisk infrastruktur i EU i syfte att förbättra lägesuppfattningen.

(18) Kommissionen kommer att stödja utnyttjandet av resultat från projekt om motståndskraften hos entiteter som driver kritisk infrastruktur, vilka finansieras genom unionens forsknings- och innovationsprogram. Kommissionen avser, inom ramen för den budget som anslagits till Horisont Europa inom den fleråriga budgetramen för 2021–2027, att öka anslagen till sådan motståndskraft. Detta bör göra det möjligt att ta itu med nuvarande och framtida utmaningar på detta område, såsom klimatsäkring av kritisk infrastruktur, utan att detta inverkar negativt på finansieringen av annan civil säkerhetsrelaterad forskning och innovation inom ramen för Horisont Europa. Kommissionen kommer också att öka sina insatser för att sprida resultaten av relevanta unionsfinansierade forskningsprojekt.

(19) Samarbetsgruppen för nät- och informationssäkerhet uppmanas att i samarbete med kommissionen och den höga representanten, och i enlighet med sina respektive uppgifter och ansvarsområden enligt unionsrätten, intensifiera arbetet med relevanta nätverk och civila och militära organ för att genomföra riskbedömningar och utarbeta riskscenarier för cybersäkerhet, med ett inledande fokus på energi-, kommunikations-, transport- och rymdinfrastruktur och det ömsesidiga beroendet mellan sektorer och medlemsstater. Detta arbete bör ta hänsyn till de relaterade riskerna för den fysiska infrastruktur som dessa sektorer är beroende av. Riskbedömningarna och riskscenarierna bör genomföras regelbundet och bör komplettera, bygga vidare på

och undvika överlappning med befintliga eller planerade riskbedömningar inom dessa sektorer och ligga till grund för diskussioner om hur man kan stärka den övergripande motståndskraften hos entiteter som driver kritisk infrastruktur och hantera sårbarheter.

(20) Kommissionen kommer att påskynda sin verksamhet för att stödja medlemsstaternas beredskap och insatser vid storskaliga cybersäkerhetsincidenter, särskilt följande:

(a) Genomförande, som komplement till relevanta riskbedömningar rörande nät- och informationssäkerhet, av en heltäckande studie av den infrastruktur för sjökabel som förbinder medlemsstaterna och som förbinder Europa globalt, inbegripet en kartläggning av den, dess kapacitet och redundans, dess sårbarheter, risker för tjänsternas tillgänglighet och riskreducering. Resultaten bör delas med medlemsstaterna.

(b) Stöd till medlemsstaternas och EU:s institutioners, organs och byråers beredskap för insatser vid storskaliga cybersäkerhetsincidenter.

(21) Kommissionen kommer att intensifiera arbetet med framåtblickande föregripande åtgärder, bland annat inom ramen för unionens civilskyddsmekanism och i samarbete med medlemsstaterna enligt artiklarna 6 och 10 i beslut nr 1313/2013/EU, och i form av beredskapsplanering för att stödja den operativa beredskapen hos Centrumet för samordning av katastrofberedskap.

Kommissionen kommer i synnerhet att vidta följande åtgärder:

(a) Ytterligare arbete i Centrumet för samordning av katastrofberedskap när det gäller föregripande åtgärder och sektorsövergripande planering av förebyggande, beredskap och insatser för att förutse och förbereda sig för störningar i tillhandahållandet av samhällsviktiga tjänster från entiteter som driver kritisk infrastruktur.

(b) Ökning av investeringarna i förebyggande strategier och befolkningsberedskap i händelse av sådana störningar, med särskilt fokus på kemiska, biologiska och radiologiska vapen och kärnsprängämnen eller andra framväxande hot orsakade av människan.

(c) Förstärkning av utbytet av relevant kunskap och bästa praxis samt bättre utformning och genomförande av kapacitetsutveckling, såsom utbildningskurser och övningar med de entiteter som driver kritisk infrastruktur via befintliga strukturer och befintlig expertis, såsom unionens kunskapsnätverk för civilskydd.

(22) Kommissionen kommer att främja användningen av EU:s övervakningsresurser (Copernicus och Galileo) för att stödja medlemsstaterna i övervakningen av kritisk infrastruktur, och i relevanta fall dess omedelbara närhet, och för att stödja andra övervakningsalternativ som föreskrivs i unionens rymdprogram.

(23) När så är relevant och i enlighet med deras respektive mandat uppmanas unionens byråer och andra relevanta organ att ge stöd i frågor som rör motståndskraften hos entiteter som driver kritisk infrastruktur, i synnerhet exempelvis följande organ:

(a) Europol, när det gäller informationsinsamling, brottsanalys och utredningsstöd i samband med gränsöverskridande brottsbekämpande åtgärder.

(b) Emsa, när det gäller sjöfartssektorns skydd och säkerhet i unionen, inbegripet sjöövervakningstjänster i frågor som rör sjöfartsskydd och sjösäkerhet.

(c) EUSPA, när det gäller verksamhet inom unionens rymdprogram.

(d) Enisa, när det gäller verksamhet som rör cybersäkerhet.

KAPITEL III: ÖKADE INSATSER

Åtgärder på medlemsstatsnivå

(24) Medlemsstaterna bör

(a) samordna sina insatser och upprätthålla en samlad bild av de sektorsövergripande insatserna vid betydande störningar i tillhandahållandet av samhällsviktiga tjänster från entiteter som driver kritisk infrastruktur inom ramen för rådets krismekanism (IPCR), när det gäller kritisk infrastruktur av gränsöverskridande betydelse, planen för storskaliga cyberincidenter och cyberkriser eller inom ramen för slutsatserna om en ram för en samordnad EU-reaktion på hybridkampanjer om sådana förs,

(b) öka informationsutbytet inom unionens civilskyddsmekanism för att förbättra systemet för tidig varning och samordna sina insatser inom ramen för den mekanismen i händelse av sådana betydande störningar, och på så sätt säkerställa snabbare av unionen underlättade insatser när det behövs,

(c) stärka sin beredskap att via unionens civilskyddsmekanism reagera på sådana betydande störningar, särskilt om de sannolikt kommer att få betydande gränsöverskridande eller till och med Europaomfattande, samt sektorsövergripande, konsekvenser,

(d) samarbeta med kommissionen för att vidareutveckla relevant insatskapacitet i den europeiska civilskyddspoolen (ECPP) och rescEU,

(e) uppmana entiteter som driver kritisk infrastruktur och relevanta nationella myndigheter att öka dessa entiteters kapacitet att snabbt återställa grundläggande prestanda för de samhällsviktiga tjänster som tillhandahålls,

(f) säkerställa, när det är nödvändigt att återuppbygga kritisk infrastruktur, att sådan återuppbyggd infrastruktur är motståndskraftig mot alla de betydande risker som den kan utsättas för, även i ogynnsamma klimatscenarier.

(25) Medlemsstaterna uppmanas att påskynda det förberedande arbetet för att införliva och tillämpa NIS 2-direktivet genom att omedelbart börja förstärka de nationella CSIRT-enheternas kapacitet, mot bakgrund av CSIRT-enheternas nya uppgifter och det ökade antalet entiteter från nya sektorer, snabbt uppdatera sina cybersäkerhetsstrategier och snarast möjligt anta nationella incident- och krishanteringsplaner för cybersäkerhet.

Åtgärder på unionsnivå

(26) Insatser vid betydande störningar i tillhandahållandet av samhällsviktiga tjänster från entiteter som driver kritisk infrastruktur bör samordnas mellan medlemsstaternas experter, när det gäller dessa entiteters motståndskraft och reaktionerna på sådana störningar som kan bidra till arbetet i rådets krismekanism (IPCR).

(27) Kommissionen kommer att ha ett nära samarbete med medlemsstaterna för att ytterligare utveckla insatskapacitet vid nödsituationer, inbegripet experter och rescEU-beredskapslager inom ramen för unionens civilskyddsmekanism, i syfte att stärka den operativa beredskapen för att hantera de omedelbara och indirekta effekterna av betydande störningar i tillhandahållandet av samhällsviktiga tjänster av entiteter som driver kritisk infrastruktur.

(28) Med beaktande av det föränderliga risklandskapet och i samarbete med medlemsstaterna kommer kommissionen inom ramen för unionens civilskyddsmekanism att

(a) kontinuerligt analysera och testa den befintliga insatskapacitetens lämplighet och operativa beredskap,

(b) regelbundet se över det potentiella behovet av att utveckla ny insatskapacitet på EU-nivå genom rescEU,

(c) ytterligare intensifiera det sektorsövergripande samarbetet för att säkerställa lämpliga insatser på EU-nivå och anordna regelbundna övningar för att testa detta samarbete,

(d) vidareutveckla ERCC som sektorsövergripande kriscentrum på EU-nivå för samordning av stödet till drabbade medlemsstater.

(29) Kommissionen kommer i samarbete med den höga representanten och i nära samråd med medlemsstaterna och med stöd av relevanta unionsorgan att utarbeta en plan för incidenter och kriser som rör kritisk infrastruktur, där man beskriver och fastställer målen och formerna för samarbetet mellan medlemsstaterna och EU:s institutioner, organ och byråer för att hantera incidenter som drabbar kritisk infrastruktur, särskilt när dessa medför betydande störningar i tillhandahållandet av samhällsviktiga tjänster för den inre marknaden. I denna plan bör man utnyttja de befintliga arrangemangen för integrerad politisk krishantering (IPCR) för att samordna insatserna.

(30) Kommissionen kommer att samarbeta med berörda parter och experter om möjliga åtgärder för återställande efter incidenter när det gäller infrastrukturen för undervattenskablar, som ska presenteras i samband med den studie som avses i punkt 20 a, samt för att ytterligare utveckla beredskapsplanering, riskscenarier och arbetet med unionens motståndskraft mot katastrofer inom ramen för unionens civilskyddsmekanism.

KAPITEL IV: INTERNATIONELLT SAMARBETE

(31) Kommissionen och den höga representanten kommer, när så är lämpligt och i enlighet med sina respektive uppgifter och ansvarsområden enligt unionsrätten, att stödja partnerländerna för att stärka motståndskraften hos entiteter som driver kritisk infrastruktur på deras territorium.

(32) Kommissionen och den höga representanten kommer, i linje med sina respektive uppgifter och ansvarsområden enligt unionsrätten, att stärka samordningen med Nato i fråga om motståndskraften hos kritisk infrastruktur genom den strukturerade dialogen mellan EU och Nato om motståndskraft och kommer att inrätta en arbetsgrupp för detta ändamål.

(33) Medlemsstaterna uppmanas att i samarbete med kommissionen och den höga representanten bidra till att påskynda utvecklingen och genomförandet av EU:s verktygslåda för hantering av hybridhot och de riktlinjer för genomförande som avses i rådets slutsatser om en ram för en samordnad EU-reaktion på hybridkampanjer[25] och därefter att tillämpa dem, i syfte att ge full verkan åt ramen

[25] Rådets slutsatser om en ram för en samordnad EU-reaktion på hybridkampanjer - Consilium (europa.eu)

för en samordnad EU-reaktion på hybridkampanjer, särskilt när de överväger och utarbetar övergripande och samordnade EU-reaktioner på hybridkampanjer och hybridhot, inbegripet de som riktar sig mot entiteter som driver kritisk infrastruktur.

(34) Kommissionen kommer att överväga deltagandet av företrädare för tredjeländer när så är relevant och lämpligt inom ramen för samarbetet och informationsutbytet mellan medlemsstaternas experter på området motståndskraft hos entiteter som driver kritisk infrastruktur.

[…]

Utfärdad i Strasbourg den

På rådets vägnar
Ordförande