Europeiska unionens råd

Bryssel den 7 september 2023
(OR. en)

12485/23

Interinstitutionellt ärende:
2023/0318(NLE)

PROCIV 57	**ATO 48**
ENV 925	**CSC 408**
JAI 1084	**ECOFIN 839**
SAN 494	**CSCI 149**
COSI 140	**DATAPROTECT 216**
CHIMIE 85	**MI 698**
ENFOPOL 356	**CODEC 1500**
RECH 380	**COPS 418**
CT 133	**JAIEX 46**
DENLEG 38	**COPEN 292**
COTER 153	**IND 441**
RELEX 987	**POLMIL 221**
ENER 467	**IPCR 55**
HYBRID 53	**DIGIT 160**
TRANS 329	**DISINFO 62**
CYBER 203	**CSDP/PSDC 608**
TELECOM 251	**MARE 18**
ESPACE 45	**POLMAR 47**

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	6 september 2023
till:	Thérèse BLANCHET, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2023) 526 final
Ärende:	Förslag till RÅDETS REKOMMENDATION om en plan för samordnade insatser på unionsnivå vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse

För delegationerna bifogas dokument – COM(2023) 526 final.

Bilaga: COM(2023) 526 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 6.9.2023
COM(2023) 526 final

2023/0318 (NLE)

Förslag till

RÅDETS REKOMMENDATION

om en plan för samordnade insatser på unionsnivå vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse

(Text av betydelse för EES)

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

I dagens geopolitiska läge som kännetecknas av ökande instabilitet, främst på grund av Rysslands anfallskrig mot Ukraina och allt mer komplexa säkerhetshot, och av klimatförändringseffekter såsom allt fler ovanliga klimathändelser och ökande vattenbrist, måste unionen förbli vaksam och ständigt anpassa sig. Enskilda, företag och myndigheter i unionen är beroende av kritisk infrastruktur[1] på grund av de samhällsviktiga tjänster som de entiteter som driver infrastrukturen tillhandahåller. Tjänsterna är avgörande för upprätthållandet av viktiga samhällsfunktioner, ekonomisk verksamhet, folkhälsa, allmän säkerhet och miljön och måste tillhandahållas obehindrat på den inre marknaden. På grund av dessa samhällsviktiga tjänsters betydelse för den inre marknaden och det resulterande behovet av att göra kritisk infrastruktur mer motståndskraftig och att mer allmänt se till att kritiska entiteter som tillhandahåller dessa tjänster är motståndskraftiga, måste unionen vidta åtgärder för att stärka denna motståndskraft och mildra eventuella avbrott i tillhandahållandet av sådana samhällsviktiga tjänster. Sådana avbrott kan annars få allvarliga konsekvenser för unionsinvånarna, våra ekonomier och förtroendet för våra demokratiska system och kan påverka den inre marknadens funktion, särskilt mot bakgrund av det ökande ömsesidiga beroendet mellan sektorer och över gränserna.

Unionen har redan vidtagit ett antal åtgärder för att bättre skydda den kritiska infrastrukturen, framför allt gränsöverskridande infrastruktur, och öka kritiska entiteters motståndskraft, i syfte att undvika eller mildra effekterna av avbrott i de samhällsviktiga tjänster som de tillhandahåller på den inre marknaden.

Direktiv 2008/114/EG om identifiering av, och klassificering som, europeisk kritisk infrastruktur[2] (*ECI-direktivet*) var det första rättsliga instrument som fastställde ett EU-omfattande förfarande för identifiering av och klassificering som europeisk kritisk infrastruktur och en gemensam unionsstrategi för att bedöma behovet av att förbättra skyddet av sådan infrastruktur mot både avsiktliga och oavsiktliga hot orsakade av människan och naturkatastrofer. Direktivet är dock enbart inriktat på energi- och transportsektorerna samt skyddet av kritisk infrastruktur och innehåller inga mer omfattande åtgärder för att öka motståndskraften hos de entiteter som driver sådan infrastruktur.

Då transaktioner på den inre marknaden blev alltmer sammankopplade och gränsöverskridande uppstod ett behov av att täcka fler än två sektorer och göra mer än att vidta skyddsåtgärder för enskilda tillgångar. År 2022 antogs därför direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft[3] (*CER-direktivet*) tillsammans med direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen[4] (*NIS 2-*

---

[1] Med kritisk infrastruktur avses en tillgång, en anläggning, utrustning, ett nätverk eller ett system, eller en del av en tillgång, en anläggning, utrustning, ett nätverk eller ett system, som krävs för tillhandahållandet av en samhällsviktig tjänst (artikel 2.4 i direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft).

[2] 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).

[3] Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (EUT L 333, 27.12.2022, s. 164).

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

direktivet). Syftet var att säkerställa en övergripande nivå av fysisk och digital motståndskraft för kritiska entiteter. CER-direktivet trädde i kraft den 16 januari 2023 och syftar till att hjälpa medlemsstaterna att öka kritiska entiteters övergripande motståndskraft och samtidigt stärka samordningen på unionsnivå. Det kommer att ersätta ECI-direktivet från och med den 18 oktober 2024, då medlemsstaterna senast måste ha vidtagit de åtgärder som krävs för att följa CER-direktivet. CER-direktivet är tillämpligt på elva sektorer[5]. Fokus utvidgas från skyddet av kritisk infrastruktur till det mer omfattande konceptet motståndskraft hos kritiska entiteter som driver sådan kritisk infrastruktur, så att hela processen före, under och efter en incident täcks in. NIS 2-direktivet trädde också i kraft den 16 januari 2023 och moderniserar den befintliga rättsliga ramen så att den anpassas till den ökade digitaliseringen och det föränderliga cyberhotlandskapet. NIS 2-direktivet utvidgar också tillämpningsområdet för cybersäkerhetsreglerna till nya sektorer och entiteter och förbättrar motståndskraften och incidenthanteringskapaciteten för offentliga och privata entiteter, behöriga myndigheter och unionen som helhet.

CER-direktivet innehåller bestämmelser om incidentanmälan från den kritiska entiteten till den nationella behöriga myndigheten, anmälan från den nationella behöriga myndigheten till andra (potentiellt) berörda medlemsstater och anmälan till kommissionen om incidenten påverkar sex eller flera medlemsstater. I CER-direktivet fastställs vissa skyldigheter att anmäla incidenter som har eller kan ha en betydande påverkan på kritiska entiteter och kontinuiteten i tillhandahållandet av samhällsviktiga tjänster till eller i en eller flera andra medlemsstater[6].

Som sabotaget mot Nord Stream-gasledningarna i september 2022 visade har säkerhetssituationen för kritisk infrastruktur förändrats avsevärt, och ytterligare brådskande åtgärder behövs på unionsnivå för att stärka den kritiska infrastrukturens motståndskraft i fråga om såväl beredskap som samordnade insatser.

I detta sammanhang antog rådet på kommissionens förslag den 8 december 2022 en rekommendation om en unionsomfattande samordnad strategi för att stärka den kritiska infrastrukturens motståndskraft[7] (*rekommendationen om den kritiska infrastrukturens motståndskraft*). Den rekommendationen betonar bland annat behovet av att på unionsnivå säkerställa ett samordnat och ändamålsenligt svar på nuvarande och framtida risker för tillhandahållandet av samhällsviktiga tjänster. Mer specifikt uppmanade rådet kommissionen att utarbeta ”en plan för samordnade insatser vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse”. I rekommendationen nämns att planen bör vara samstämmig med EU-protokollet för att motverka hybridhot[8], ta hänsyn till kommissionens rekommendation 2017/1584 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser[9] (*cyberplanen*) samt respektera arrangemangen för integrerad politisk krishantering[10] (IPCR).

---

5 Energi, transport, bankverksamhet, finansmarknadsinfrastruktur, digital infrastruktur, offentlig förvaltning, rymden, hälso- och sjukvård, dricksvatten, avloppsvatten samt produktion, bearbetning och distribution av livsmedel.

6 I enlighet med artikel 15.1 och 15.3 i CER-direktivet.

7 Rådets rekommendation av den 8 december 2022 om en unionsomfattande samordnad strategi för att stärka den kritiska infrastrukturens motståndskraft, 2023/C 20/01 (EUT C 20, 20.1.2023, s. 1).

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

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

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

Mot denna bakgrund innehåller detta förslag till ytterligare en rådsrekommendation en sådan plan. Förslaget syftar till att komplettera den nuvarande rättsliga ramen genom att beskriva de samordnade insatserna på unionsnivå när det gäller störningar av kritisk infrastruktur med stor gränsöverskridande betydelse samtidigt som befintliga unionsarrangemang används. Rent konkret beskriver förslaget planens tillämpningsområde och mål samt de aktörer, processer och befintliga verktyg som skulle kunna användas för att på unionsnivå samordnat reagera på en allvarlig incident avseende kritisk infrastruktur med betydande gränsöverskridande effekter. Förslaget beskriver också formerna för samarbete mellan medlemsstaterna och unionens institutioner, organ och byråer i sådana situationer.

- **Förenlighet med befintliga bestämmelser inom området**

Detta förslag till rådets rekommendation ligger i linje med och kompletterar den nuvarande rättsliga ramen för skydd av kritisk infrastruktur och kritiska entiteters motståndskraft – ECI-direktivet respektive CER-direktivet och rekommendationen om den kritiska infrastrukturens motståndskraft – eftersom det syftar till att på ett kompletterande sätt säkerställa samordningen mellan medlemsstaterna och mellan dem och unionens institutioner, organ och byråer när det gäller att hantera incidenter som orsakar störningar av kritisk infrastruktur med stor gränsöverskridande betydelse och tillhandahållandet av samhällsviktiga tjänster. Förslaget gör bruk av befintliga strukturer och mekanismer på unionsnivå, bland annat de som inrättats genom CER-direktivet, dvs. samarbetet mellan behöriga myndigheter och gruppen för kritiska entiteters motståndskraft, vilket är en grupp som inrättats genom CER-direktivet för att stödja kommissionen och underlätta samarbetet mellan medlemsstaterna och informationsutbytet i frågor som rör CER-direktivet.

Detta förslag till rådets rekommendation är också i linje med och ett komplement till den unionsram för cybersäkerhet som fastställs i NIS 2-direktivet.

Förslaget syftar till att på området kritiska entiteters motståndskraft och skydd av kritisk infrastruktur lägga fram en plan för kritisk infrastruktur liknande cyberplanen.

I del I punkt 4 b i bilagan förklaras också kopplingarna till cyberplanen, som är avsedd att användas vid storskaliga cyberincidenter som leder till störningar som är så omfattande att den berörda medlemsstaten inte kan hantera dem på egen hand, eller som påverkar två eller flera medlemsstater eller EU-institutioner och har så vidsträckta och betydande tekniska eller politiska konsekvenser att det krävs snabb politisk samordning och reaktion på EU-nivå. I NIS 2-direktivet definieras incident som ”en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem” (*cyberincident*).

Behöriga myndigheter enligt CER-direktivet och NIS 2-direktivet är skyldiga att samarbeta och utbyta information om cyberincidenter och incidenter som påverkar kritiska entiteter, även när det gäller relevanta åtgärder som vidtagits. I situationer där en betydande incident avseende kritisk infrastruktur och en storskalig cyberincident påverkar samma entitet bör de berörda aktörerna samordna sina möjliga insatser.

Förslaget är förenligt med EU-protokollet för att motverka hybridhot, som är tillämpligt vid hybridincidenter. I del I punkt 4 a i bilagan förklaras kopplingarna till EU-protokollet, till exempel vilket instrument som är tillämpligt vid en betydande incident avseende kritisk infrastruktur vilken har en hybriddimension.

Förslaget är också samstämmigt med andra befintliga krishanteringsmekanismer på unionsnivå, som rådets IPCR-arrangemang, kommissionens interna krissamordningsprocess

Argus[11] och unionens civilskyddsmekanism[12], med stöd av dess centrum för samordning av katastrofberedskap (ERCC), samt Europeiska utrikestjänstens krishanteringsmekanism.

Förslaget är också förenligt med annan relevant sektorslagstiftning, i synnerhet de specifika åtgärder i denna som reglerar vissa aspekter av hur entiteter verksamma inom de berörda sektorerna hanterar störningar.

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

• Rättslig grund

Förslaget grundar sig på artikel 114 i fördraget om Europeiska unionens funktionssätt (*EUF-fördraget*), som omfattar tillnärmning av lagstiftning för att förbättra den inre marknaden, tillsammans med artikel 292 i EUF-fördraget, som fastställer relevanta regler för antagande av rekommendationer.

Valet av artikel 114 i EUF-fördraget som materiell rättslig grund motiveras av att den föreslagna rådsrekommendationen syftar till att säkerställa samordnade insatser vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse. Sådana störningar påverkar flera medlemsstater och riskerar att påverka den inre marknadens funktion på grund av det allt större ömsesidiga beroendet mellan infrastruktur och sektorer i en alltmer sammanlänkad unionsekonomi. Bättre hantering av störningar kommer i sin tur att förebygga störningar i den inre marknadens funktion, eftersom denna kritiska infrastruktur och de samhällsviktiga tjänster som tillhandahålls av denna infrastruktur är avgörande för upprätthållandet av viktiga samhällsfunktioner, ekonomisk verksamhet, folkhälsa, allmän säkerhet och miljön.

Förslaget kompletterar ECI-direktivet och CER-direktivet, som också grundar sig på artikel 114 i EUF-fördraget. Rekommendationen om den kritiska infrastrukturens motståndskraft grundar sig också, likt den rekommendation som nu föreslås, på artiklarna 114 och 292 i EUF-fördraget.

• Subsidiaritetsprincipen (för icke-exklusiv befogenhet)

Det är först och främst medlemsstaternas ansvar att hantera störningar av kritisk infrastruktur och av de tjänster som tillhandahålls av kritiska entiteter som driver den kritiska infrastrukturen, men unionen har en viktig roll vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse, eftersom sådana störningar kan påverka flera eller till och med alla ekonomiska sektorer på den inre marknaden, liksom även unionens säkerhet och internationella förbindelser. I syfte att säkerställa den inre marknadens funktion är samordning på unionsnivå vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse inte bara lämplig utan också nödvändig, eftersom sådana samordnade insatser på unionsnivå kommer att stödja medlemsstaternas hantering av störningarna genom gemensam situationsmedvetenhet, samordnad kommunikation till allmänheten och minskning av störningarnas effekter på den inre marknaden.

---

[11] Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén - Kommissionens bestämmelser gällande inrättandet av det allmänna förvarningssystemet ”ARGUS”, KOM(2005) 662 slutlig.

[12] Europaparlamentets och rådets förordning (EU) 2021/836 av den 20 maj 2021 om ändring av beslut nr 1313/2013/EU om en civilskyddsmekanism för unionen (EUT L 185, 26.5.2021, s. 1).

- **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 åtgärder som föreslås står i proportion till de eftersträvade målen, som är inriktade på att säkerställa samordnade insatser på unionsnivå vid störningar med stor gränsöverskridande betydelse av kritisk infrastruktur eller av de tjänster som tillhandahålls av de kritiska entiteter som driver den kritiska infrastrukturen. Dessa föreslagna samordnade insatser står i proportion till medlemsstaternas befogenheter och skyldigheter enligt nationell lagstiftning. Incidenter som stör kritisk infrastruktur eller kritiska entiteters tillhandahållande av samhällsviktiga tjänster faller ofta under gränsen för att betecknas som en betydande incident avseende kritisk infrastruktur och kan hanteras ändamålsenligt på nationell nivå. Användningen av den mekanism som föreskrivs i detta förslag är därför begränsad till större störningar som har en stor gränsöverskridande betydelse och påverkar flera medlemsstater.

- **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. I enlighet med artikel 288 i EUF-fördraget är rekommendationerna inte bindande. En rådsrekommendation är ett lämpligt instrument i detta fall eftersom den signalerar medlemsstaternas ansvar för de åtgärder som ingår och utgör en gedigen grund för samarbete på området samordnade insatser vid betydande störningar av kritisk infrastruktur. På detta sätt kompletterar den föreslagna rekommendationen den bindande rättsliga ramen (särskilt CER-direktivet) och även den tidigare antagna rekommendationen om den kritiska infrastrukturens motståndskraft, där sådana kompletterande åtgärder efterlyses, samtidigt som medlemsstaternas ansvar på det berörda området respekteras fullt ut.

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

- **Samråd med berörda parter**

Vid utarbetandet av detta förslag rådfrågades medlemsstaterna och unionens institutioner och byråer. Dessutom beaktades de synpunkter som medlemsstaternas experter framförde både vid ett seminarium den 24 april 2023 och skriftligen efteråt.

Överlag rådde enighet om att det i det rådande hotläget vore bra med mer samordning av insatserna på unionsnivå vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse, samtidigt som medlemsstaternas befogenhet på detta område och sekretessen för känslig information respekteras. Man var även överens om behovet av att undvika dubblering av instrument och utnyttja befintliga unionsmekanismer för samordning, informationsutbyte och insatser.

Vissa medlemsstater ställde sig positiva till det bredare tillämpningsområdet för planen för kritisk infrastruktur, medan andra ansåg att CER-direktivets gräns på sex eller fler medlemsstater för identifiering av kritiska entiteter av särskild europeisk betydelse var tillräcklig och att det inte var nödvändigt att ta med en andra typ av incident i tillämpningsområdet. Några medlemsstater påpekade vikten av att i tillämpliga fall involvera operatörer av kritisk infrastruktur som tillhandahåller samhällsviktiga tjänster på grund av deras sakkunskap och vikten av att beakta cyberdimensionen.

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

Förslaget till rådets rekommendation består av en huvuddel och en bilaga.

Huvuddelen består av följande elva punkter:

I punkt 1 anges behovet av ökat samarbete när det gäller hanteringen av betydande incidenter avseende kritisk infrastruktur i enlighet med den plan för kritisk infrastruktur som ingår i detta förslag till rekommendation, inbegripet de relevanta delarna av dess bilaga.

I punkt 2 fastställs tillämpningsområdet för planen för kritisk infrastruktur, som avser två typer av störningar som skulle utlösa tillämpningen av planen för kritisk infrastruktur: incidenten har antingen en betydande störande effekt på tillhandahållandet av samhällsviktiga tjänster till eller i sex eller fler medlemsstater eller en betydande störande effekt i två eller flera medlemsstater och berörda aktörer som nämns i punkten är överens om att det behövs samordning på unionsnivå på grund av incidentens betydande inverkan.

Punkt 3 handlar om identifiering av de berörda aktörer som ska delta i planen för kritisk infrastruktur och de nivåer på vilka planen för kritisk infrastruktur kommer att fungera (operativ, strategisk/politisk). Detta förklaras närmare i bilagan till rekommendationen.

I punkt 4 rekommenderas att planen för kritisk infrastruktur tillämpas tillsammans med andra relevanta instrument, vilket beskrivs i bilagan.

I punkt 5 rekommenderas medlemsstaterna att på nationell nivå ändamålsenligt hantera betydande störningar av kritisk infrastruktur.

I punkt 6 rekommenderas att berörda aktörer inrättar eller utser kontaktpunkter som bör stödja användningen av planen för kritisk infrastruktur. Om möjligt bör dessa kontaktpunkter vara desamma som de gemensamma kontaktpunkterna enligt CER-direktivet.

Punkt 7 avser informationsflödet i händelse av en betydande incident avseende kritisk infrastruktur.

I punkt 8 vidareutvecklas hur informationsutbytet bör gå till.

I punkt 9 rekommenderas att man genom övningar testar hur planen för kritisk infrastruktur fungerar.

I punkt 10 rekommenderas att lärdomar diskuteras i gruppen för kritiska entiteters motståndskraft, som bör utarbeta en rapport med rekommendationer. Rapporten bör antas av kommissionen.

I punkt 11 rekommenderas medlemsstaterna att diskutera rapporten i rådet.

I bilagan beskrivs mål, principer, huvudaktörer, samspelet med befintliga krishanteringsmekanismer och hur planen för kritisk infrastruktur ska fungera med dess två samarbetsformer, dvs. informationsutbytet och insatserna.

2023/0318 (NLE)

Förslag till

RÅDETS REKOMMENDATION

om en plan för samordnade insatser på unionsnivå vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse

(Text av betydelse för EES)

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA REKOMMENDATION

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

med beaktande av Europeiska kommissionens förslag, och

av följande skäl:

(1) För att den inre marknaden och samhället som helhet ska fungera väl måste vi kunna förlita oss på motståndskraftig kritisk infrastruktur och motståndskraftiga kritiska entiteter som tillhandahåller tjänster som är avgörande för upprätthållandet av centrala samhällsfunktioner, ekonomisk verksamhet, folkhälsa, allmän säkerhet och miljön.

(2) I dagens föränderliga risklandskap och mot bakgrund av det allt större ömsesidiga beroendet mellan infrastruktur och sektorer och, mer allmänt, kopplingarna mellan sektorer och över gränser, finns det ett behov av att på ett övergripande och samordnat sätt ta itu med och förbättra skyddet av kritisk infrastruktur och motståndskraften hos kritiska entiteter som driver sådan infrastruktur.

(3) En incident som stör kritisk infrastruktur och därigenom omöjliggör eller allvarligt hämmar tillhandahållandet av samhällsviktiga tjänster kan få betydande gränsöverskridande effekter och inverka negativt på den inre marknaden. För att säkerställa ett riktat, proportionellt och ändamålsenligt tillvägagångssätt bör åtgärder vidtas för att i synnerhet hantera betydande incidenter avseende kritisk infrastruktur, enligt definitionen i denna rekommendation, som till exempel omfattar situationer där den störning som orsakas av incidenten varar länge eller kan få betydande kaskadeffekter inom samma eller andra sektorer eller medlemsstater.

(4) Samordnade insatser vid betydande incidenter avseende kritisk infrastruktur är avgörande för att undvika större störningar på den inre marknaden och för att säkerställa att tillhandahållandet av dessa samhällsviktiga tjänster återställs så snart som möjligt, eftersom sådana incidenter kan få allvarliga konsekvenser för ekonomin och invånarna i unionen. Snabb och ändamålsenlig hantering på unionsnivå av sådana incidenter kräver ändamålsenligt samarbete med kort varsel mellan alla berörda aktörer och samordnade åtgärder som stöds av unionen. En sådan hantering förutsätter därför att det finns på förhand fastställda och i möjligaste mån beprövade samarbetsförfaranden och samarbetsmekanismer, med angivna roller och ansvarsområden för de viktigaste aktörerna på nationell nivå och unionsnivå.

(5) Huvudansvaret för att säkerställa hantering av betydande incidenter avseende kritisk infrastruktur ligger hos medlemsstaterna och de entiteter som driver kritisk infrastruktur och tillhandahåller samhällsviktiga tjänster, men det är lämpligt med ökad samordning på unionsnivå vid störningar med stor gränsöverskridande betydelse. Snabba och ändamålsenliga insatser kräver inte bara att medlemsstaterna sätter in nationella mekanismer, utan även att samordnade åtgärder vidtas med unionsstöd, vilket inbegriper relevant samarbete på ett ändamålsenligt sätt med kort varsel.

(6) Skyddet av europeisk kritisk infrastruktur regleras för närvarande genom rådets direktiv 2008/114/EG[1], som endast omfattar två sektorer, dvs. transport och energi. I det direktivet fastställs ett förfarande för identifiering av och klassificering som europeisk kritisk infrastruktur och en gemensam metod för bedömning av behovet att stärka skyddet av sådan infrastruktur. Det är hörnstenen i det europeiska programmet för skydd av kritisk infrastruktur[2], som antogs av kommissionen 2006 som en europeisk allriskram för skydd av kritisk infrastruktur.

(7) För att åstadkomma mer än skyddet av kritisk infrastruktur och på bredare front säkerställa motståndskraften hos kritiska entiteter vilka driver sådan infrastruktur som tillhandahåller samhällsviktiga tjänster på den inre marknaden kommer Europaparlamentets och rådets direktiv (EU) 2022/2557[3] att ersätta direktiv 2008/114/EG från och med den 18 oktober 2024. Direktiv (EU) 2022/2557 omfattar elva sektorer och föreskriver skyldigheter för medlemsstater och kritiska entiteter att vidta åtgärder för att stärka motståndskraften, samarbete mellan medlemsstaterna och med kommissionen samt stöd från kommissionen till nationella myndigheter och kritiska entiteter och stöd från medlemsstaterna till de kritiska entiteterna.

(8) Efter sabotaget av Nord Stream-gasledningarna finns det ett behov av fler åtgärder på unionsnivå för att öka den kritiska infrastrukturens motståndskraft. Därför antog rådet, på förslag av kommissionen, en rekommendation om en unionsomfattande samordnad strategi för att stärka den kritiska infrastrukturens motståndskraft[4] (*rekommendation 2023/C 20/01*), som syftar till att förbättra beredskapen, insatserna och det internationella samarbetet på detta område. I rekommendationen betonades särskilt behovet av att på unionsnivå säkerställa ett samordnat och ändamålsenligt svar på risker för tillhandahållandet av samhällsviktiga tjänster.

(9) Det är därför nödvändigt att komplettera den befintliga rättsliga ramen med ytterligare en rådsrekommendation om fastställande av en plan för samordnade insatser vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse (*planen för kritisk infrastruktur*), samtidigt som befintliga unionsarrangemang används.

(10) Denna rekommendation bör anpassas till rekommendation 2023/C 20/01 för att säkerställa konsekvens och undvika dubblering. Denna rekommendation bör därför inte i sig omfatta övriga inslag i krishanteringens livscykel, dvs. förebyggande, beredskap och återhämtning.

---

[1] 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).

[2] Meddelande från kommissionen om ett europeiskt program för skydd av kritisk infrastruktur, KOM(2006) 786 slutlig av den 12 december 2006.

[3] Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (EUT L 333, 27.12.2022, s. 164).

[4] Rådets rekommendation av den 8 december 2022 om en unionsomfattande samordnad strategi för att stärka den kritiska infrastrukturens motståndskraft, 2023/C 20/01 (EUT C 20, 20.1.2023, s. 1).

(11) Denna rekommendation bör komplettera direktiv (EU) 2022/2557, särskilt när det gäller samordnade insatser, och bör genomföras samtidigt som överensstämmelse säkerställs med det direktivet och andra tillämpliga regler i unionsrätten. Denna rekommendation bör därför också bygga på och i möjligaste mån använda begreppen, verktygen och processerna i det direktivet, såsom gruppen för kritiska entiteters motståndskraft, som agerar inom ramen för sina uppgifter enligt det direktivet, och kontaktpunkter. Dessutom bör begreppet ”kritisk infrastruktur” som används i denna rekommendation förstås på samma sätt som i skäl 7 i rekommendation 2023/C 20/01, dvs. omfattande relevant kritisk infrastruktur som identifierats av en medlemsstat på nationell nivå eller som klassificerats som europeisk kritisk infrastruktur enligt direktiv 2008/114/EG samt kritiska entiteter som ska identifieras enligt direktiv (EU) 2022/2557. För att säkerställa överensstämmelse med direktiv (EU) 2022/2557 bör de begrepp som används i denna rekommendation därför tolkas som att de har samma innebörd som i det direktivet. Exempelvis bör begreppet ”motståndskraft”, som definieras i artikel 2.2 i det direktivet, också förstås som syftande på en kritisk infrastrukturs förmåga att förebygga, skydda mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till eller återhämta sig från händelser som innebär en betydande störning av, eller som skulle kunna leda till en betydande störning av, tillhandahållandet av samhällsviktiga tjänster på den inre marknaden, dvs. tjänster som är avgörande för upprätthållandet av centrala samhällsfunktioner och ekonomiska funktioner, den allmänna säkerheten och tryggheten, befolkningens hälsa och miljön.

(12) Dessutom bör begreppet ”betydande störande effekt” förstås mot bakgrund av kriterierna i artikel 7.1 i direktiv (EU) 2022/2557, som avser följande: i) Antalet användare som är beroende av den samhällsviktiga tjänst som den berörda entiteten tillhandahåller. ii) Den grad till vilken andra sektorer och undersektorer som anges i bilagan till direktivet är beroende av den samhällsviktiga tjänsten i fråga. iii) Vilken effekt incidenter skulle kunna ha på ekonomisk och samhällelig verksamhet, miljön, den allmänna säkerheten och tryggheten eller befolkningens hälsa, uttryckt i grad och varaktighet. iv) Entitetens marknadsandel på marknaden för den eller de berörda samhällsviktiga tjänsterna. v) Det geografiska område som skulle kunna påverkas av en incident, inbegripet eventuella gränsöverskridande konsekvenser, med beaktande av den sårbarhet som är förknippad med graden av isolering för vissa typer av geografiska områden, såsom öregioner, avlägsna områden eller bergsområden. vi) Entitetens betydelse för upprätthållandet av en tillräcklig nivå på den samhällsviktiga tjänsten, med beaktande av tillgången till alternativa sätt att tillhandahålla den samhällsviktiga tjänsten på.

(13) För att uppnå effektivitet och ändamålsenlighet bör planen för kritisk infrastruktur vara helt samstämmig och driftskompatibel med unionens reviderade operativa protokoll för att motverka hybridhot[5] och ta hänsyn till den befintliga planen för samordnade insatser vid storskaliga gränsöverskridande cyberincidenter och cyberkriser i kommissionens rekommendation (EU) 2017/1584[6] (*cyberplanen*) och det mandat för Europeiska kontaktnätverket för cyberkriser (*EU-CyCLONe*) som fastställs

[5] Gemensamt arbetsdokument från kommissionens avdelningar, *EU Protocol for countering hybrid threats* (ej översatt till svenska), SWD(2023) 116 final.

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

i Europaparlamentets och rådets direktiv (EU) 2022/2555[7] samt undvika överlappning av strukturer och verksamheter. Den bör också fullt ut respektera rådets arrangemang för integrerad politisk krishantering[8] (IPCR) för samordningen av insatserna.

(14) Denna rekommendation bygger på samt är mer allmänt förenlig med och kompletterar unionens etablerade krishanteringsmekanismer, särskilt rådets IPCR-arrangemang, kommissionens interna krissamordningsprocess Argus[9] och unionens civilskyddsmekanism[10], som stöds av centrumet för samordning av katastrofberedskap (ERCC)[11], Europeiska utrikestjänstens krishanteringsmekanism samt krisinstrumentet för den inre marknaden[12], vilka alla kan spela en roll när det gäller att hantera mer omfattande störningar i den kritiska infrastrukturens funktion.

(15) Ovannämnda verktyg eller mekanismer på unionsnivå kan användas för att hantera en betydande incident avseende kritisk infrastruktur i enlighet med tillämpliga regler och förfaranden, som denna rekommendation bör komplettera men inte påverka. Exempelvis är rådets IPCR-arrangemang fortfarande det främsta verktyget för medlemsstaternas samordning av insatser på politisk unionsnivå. Intern samordning inom kommissionen sker inom ramen för Argus sektorsövergripande krissamordningsprocess. Om krisen är av ett sådant slag att den yttre politiken eller den gemensamma säkerhets- och försvarspolitiken (GSFP) berörs kan den Europeiska utrikestjänstens krishanteringsmekanism användas. I enlighet med beslut nr 1313/2013/EU om en civilskyddsmekanism för unionen organiseras operativa insatser inom ramen för civilskyddsmekanismen vid faktiska eller nära förestående naturkatastrofer och katastrofer orsakade av människan inom och utanför unionen (även sådana som påverkar kritisk infrastruktur) av ERCC, kommissionens samlade operativa krishanteringscentrum med beredskap dygnet runt. I sådana situationer kan ERCC ge tidig varning, underrättelse och analys och stöder informationsutbyte och, om en medlemsstat aktiverar civilskyddsmekanismen, utplacering av operativt stöd och experter i drabbade områden. Dessutom kan ERCC underlätta sektoriell och sektorsövergripande samordning både på EU-nivå och mellan EU och relevanta nationella myndigheter, bland annat sådana som ansvarar för civilskydd och den kritiska infrastrukturens motståndskraft.

(16) De processer som fastställs i denna rekommendation bör i tillämpliga fall övervägas i samband med att dessa andra verktyg eller mekanismer används, men rekommendationen bör också beskriva åtgärder som skulle kunna vidtas på unionsnivå i fråga om gemensam situationsmedvetenhet, samordnad kommunikation till

---

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

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

[9] Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén - Kommissionens bestämmelser gällande inrättandet av det allmänna förvarningssystemet ”ARGUS”, KOM(2005) 662 slutlig.

[10] 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).

[11] Genom beslut nr 1313/2013/EU om en civilskyddsmekanism skapas en allriskram med arrangemang för förebyggande, beredskap och insatser på unionsnivå för att hantera alla typer av naturkatastrofer och katastrofer orsakade av människan eller överhängande fara för sådana katastrofer inom och utanför EU.

[12] Europaparlamentets och rådets förordning .../.. om inrättande av ett krisinstrument för den inre marknaden och om upphävande av rådets förordning (EG) nr 2679/98, COM(2022) 459 final.

allmänheten och effektiva insatser i situationer där dessa unionsmekanismer för krissamordning inte används.

(17) För att bättre samordna insatserna vid betydande incidenter avseende kritisk infrastruktur bör samarbetet mellan medlemsstaterna och unionens institutioner och berörda organ och byråer förbättras genom befintliga arrangemang, i enlighet med planen för kritisk infrastruktur. Planen för kritisk infrastruktur bör därför vara tillämplig när den gräns på sex eller fler medlemsstater som föreskrivs i direktiv (EU) 2022/2557 för identifiering av kritiska entiteter av särskild europeisk betydelse är uppnådd, men också när incidenter som påverkar ett mindre antal medlemsstater inträffar eftersom sådana incidenter kan få vidsträckta konsekvenser på grund av kaskadeffekter över gränserna, varför unionssamordning av insatserna skulle vara till nytta.

(18) Även om en samarbetsram på unionsnivå för samordnade insatser vid betydande incidenter avseende kritisk infrastruktur anses nödvändig bör den inte avleda kritiska entiteters och behöriga myndigheters resurser från incidenthantering, vilket är något som bör prioriteras.

(19) De relevanta aktörer som deltar i genomförandet av planen för kritisk infrastruktur bör tydligt fastställas, så att det finns en tydlig och heltäckande översikt över de institutioner, organ, kontor, byråer och myndigheter som skulle kunna göra insatser vid en betydande incident avseende kritisk infrastruktur.

(20) Det är främst medlemsstaternas behöriga myndigheter som ansvarar för hanteringen av incidenter avseende kritisk infrastruktur, även betydande incidenter. Denna rekommendation bör inte påverka medlemsstaternas ansvar för nationell säkerhet och försvar eller deras befogenhet att skydda andra väsentliga statliga funktioner, i enlighet med unionsrätten, särskilt när det gäller allmän säkerhet, territoriell integritet och upprätthållande av lag och ordning. Denna rekommendation bör heller inte påverka nationella processer, såsom kommunikation och samverkan mellan operatörer av kritisk infrastruktur och behöriga nationella myndigheter. Denna rekommendation bör tillämpas utan att det påverkar relevanta bilaterala eller multilaterala överenskommelser som ingåtts mellan medlemsstaterna.

(21) För ett ändamålsenligt och snabbt samarbete inom ramen för planen för kritisk infrastruktur är det viktigt att berörda aktörer utser eller inrättar kontaktpunkter. För att säkerställa samstämmighet bör medlemsstaterna överväga möjligheten att som kontaktpunkter utsedda eller inrättade inom denna ram ha de gemensamma kontaktpunkter som ska utses eller inrättas inom ramen för direktiv (EU) 2022/2557.

(22) Av effektivitetsskäl bör testning och övning av planen för kritisk infrastruktur, samt rapportering och diskussioner om erfarenheterna av den, vara ett viktigt inslag i upprätthållandet av en hög beredskapsnivå i händelse av betydande incidenter avseende kritisk infrastruktur och av säkerställandet av förmågan att tillhandahålla snabba och väl samordnade insatser, med deltagande av berörda aktörer.

(23) Med tanke på hur rådets krissamordningsmekanism IPCR är uppbyggd, och mer allmänt med hänsyn till den potentiella aktiveringen av de krissamordningsmekanismer som redan finns på unionsnivå, bör planen för kritisk infrastruktur omfatta två samarbetsformer för att hantera en betydande incident avseende kritisk infrastruktur. Den första formen bör bestå av informationsutbyte mellan alla berörda aktörer, samordning av kommunikation till allmänheten och, om de används, samordning via redan befintliga mekanismer såsom IPCR-arrangemangen

i rådet eller Argus-samordning inom kommissionen, med stöd av ERCC som operativ kontaktpunkt dygnet runt, och utrikestjänstens krishanteringsmekanism. Den andra bör omfatta ytterligare insatser på grund av incidentens omfattning. Detta samarbete bör inbegripa engagemang på operativ och strategisk/politisk nivå, motsvarande nivåerna i rekommendation 2017/1584 och EU-protokollet för att motverka hybridhot, i syfte att samordna åtgärder och hantera den betydande incidenten avseende kritisk infrastruktur på ett effektivt och ändamålsenligt sätt. På grundval av principerna om proportionalitet, subsidiaritet, informationssekretess och komplementaritet och för att säkerställa effektivt samarbete bör planen för kritisk infrastruktur beskriva hur de relevanta aktörerna delar situationsmedvetenhet och hur samordnad kommunikation till allmänheten och effektiva insatser ombesörjs.

(24) Informationsutbytet enligt denna rekommendation bör skötas utan att äventyra den nationella säkerheten eller säkerhetsintressen och kommersiella intressen för entiteter som driver kritisk infrastruktur. Därför bör känslig information inhämtas, utbytas och hanteras med försiktighet, i enlighet med tillämpliga regler och med särskild hänsyn till de överföringskanaler och den lagringskapacitet som används.

HÄRIGENOM REKOMMENDERAS FÖLJANDE.

(1) Medlemsstaterna, rådet, kommissionen och, i tillämpliga fall, Europeiska utrikestjänsten och relevanta unionsorgan och unionsbyråer bör samarbeta med varandra inom ramen för den plan för kritisk infrastruktur som ingår i denna rekommendation, för att uppnå de mål som anges i del I punkt 1 i bilagan och, med beaktande av principerna i del I punkt 2 i bilagan, göra samordnade insatser vid betydande incidenter avseende kritisk infrastruktur.

(2) Medlemsstaterna, rådet, kommissionen och, i tillämpliga fall, utrikestjänsten och relevanta unionsorgan och unionsbyråer bör tillämpa planen för kritisk infrastruktur utan dröjsmål närhelst det inträffar en betydande incident avseende kritisk infrastruktur, dvs. en incident som inbegriper kritisk infrastruktur och som har någon av följande effekter:

   (a) En betydande störande effekt på tillhandahållandet av samhällsviktiga tjänster till eller i sex eller fler medlemsstater, inbegripet när den påverkar en kritisk entitet av särskild europeisk betydelse i den mening som avses i artikel 17 i direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft[13].

   (b) En betydande störande effekt på tillhandahållandet av samhällsviktiga tjänster i två eller flera medlemsstater, om den medlemsstat som innehar det roterande ordförandeskapet i rådet, i samförstånd med dessa andra medlemsstater och i samråd med kommissionen, anser att det krävs en snabb samordning av insatserna på unionsnivå på grund av incidentens vidsträckta och betydande tekniska eller politiska konsekvenser.

(3) De berörda aktörerna i planen för kritisk infrastruktur, som fastställts på operativ och strategisk/politisk nivå i enlighet med del I punkt 3 i bilagan, bör sträva efter att samverka och samarbeta för att komplettera varandras insatser. De bör säkerställa ett

[13] Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (EUT L 333, 27.12.2022, s. 164).

lämpligt och snabbt informationsutbyte, inbegripet samordning av kommunikation till allmänheten, och samordnade insatser i enlighet med del II i bilagan.

(4) Planen för kritisk infrastruktur bör tillämpas med beaktande av och i överensstämmelse med andra relevanta instrument, i enlighet med del I punkt 4 i bilagan. Om en incident påverkar både fysiska aspekter och cybersäkerheten för kritisk infrastruktur bör synergier med relevanta processer i cyberplanen säkerställas.

(5) Medlemsstaterna bör säkerställa att de på nationell nivå och i enlighet med unionsrätten effektivt hanterar störningar av kritisk infrastruktur vid betydande incidenter avseende kritisk infrastruktur.

(6) Medlemsstaterna, rådet, utrikestjänsten, Europeiska unionens byrå för samarbete inom brottsbekämpning (*Europol*) och andra berörda unionsbyråer bör, liksom kommissionen, utse eller inrätta en kontaktpunkt för frågor som rör planen för kritisk infrastruktur. Kontaktpunkterna bör stödja tillämpningen av planen för kritisk infrastruktur genom att tillhandahålla nödvändig information och underlätta samordningsåtgärder vid hantering av en betydande incident avseende kritisk infrastruktur. För medlemsstaterna bör dessa kontaktpunkter om möjligt vara desamma som de gemensamma kontaktpunkter som ska utses eller inrättas i enlighet med artikel 9.2 i direktiv (EU) 2022/2557. För kommissionens del säkerställer ERCC operativ kontakt och kapacitet dygnet runt och samordnar, övervakar och stöder i realtid insatserna på unionsnivå vid katastrofer, samtidigt som centrumet betjänar medlemsstaterna och kommissionen i egenskap av operativt krishanteringscentrum som främjar en sektorsövergripande syn på katastrofhantering.

(7) Den medlemsstat som innehar det roterande ordförandeskapet i rådet bör i samförstånd med de berörda medlemsstaterna informera alla berörda aktörer via de kontaktpunkter som avses i punkt 6 om den betydande incidenten avseende kritisk infrastruktur och tillämpningen av planen för kritisk infrastruktur. Utbyte av information om en betydande incident avseende kritisk infrastruktur bör ske via lämpliga kommunikationskanaler, inbegripet, när så är tillämpligt och lämpligt, plattformen för integrerad politisk krishantering[14] (IPCR) och ERCC via det gemensamma kommunikations- och informationssystemet för olyckor (Cecis), en webbaserad applikation för varningar och meddelanden som möjliggör informationsutbyte i realtid.

(8) Vid behov bör säkrade överföringskanaler användas för att inte äventyra nationell säkerhet eller de berörda entiteternas säkerhetsintressen och kommersiella intressen. Det informationsutbyte som beskrivs i del II punkt 1 i bilagan till denna rekommendation bör också ske utan att äventyra nationell säkerhet eller kritiska entiteters säkerhetsintressen och kommersiella intressen och i enlighet med unionsrätten, särskilt Europaparlamentets och rådets förordning (EU) .../...[15]. I synnerhet bör känslig information inhämtas, utbytas och hanteras med försiktighet. Tillgängliga ackrediterade verktyg samt lämpliga säkerhetsåtgärder bör användas för hantering och utbyte av säkerhetsskyddsklassificerade uppgifter.

(9) De berörda aktörerna bör regelbundet öva och testa planen för kritisk infrastruktur och sina samordnade insatser vid en betydande incident avseende kritisk infrastruktur på nationell och regional nivå och unionsnivå, t.ex. genom övningar. Sådana övningar

[14] Rådets genomförandebeslut (EU) 2018/1993 av den 11 december 2018 om EU-arrangemangen för integrerad politisk krishantering, ST/13422/2018/INIT (EUT L 320, 17.12.2018, s. 28).

[15] Förordning (EU) .../... om informationssäkerhet i unionens institutioner, organ och byråer, COM(2022) 119 final.

och tester kan, när så är lämpligt, omfatta entiteter i den privata sektorn. En övning på unionsnivå som omfattar fysiska och cyberrelaterade aspekter bör äga rum senast den [*dagen för antagandet av denna rekommendation + 12 månader*].

(10) Efter tillämpningen av planen för kritisk infrastruktur vid en betydande incident avseende kritisk infrastruktur bör den grupp för kritiska entiteters motståndskraft som avses i artikel 19 i direktiv (EU) 2022/2557 inom lämplig tid diskutera med de berörda aktörerna om lärdomar som kan tyda på brister och områden där förbättringar krävs, och därefter utarbeta en rapport med rekommendationer för att uppnå sådana förbättringar. Utarbetandet av den rapporten bör stödjas av de berörda aktörer som deltar i tillämpningen av planen för kritisk infrastruktur. Rapporten bör antas av kommissionen.

(11) Medlemsstaterna bör diskutera den rapport som avses i punkt 10 i rådets berörda förberedande organ eller i rådet.

Utfärdad i Bryssel den

På rådets vägnar
Ordförande