I

(Resolutioner, rekommendationer och yttranden)

REKOMMENDATIONER

RÅDET

RÅDETS REKOMMENDATION

av den 8 december 2022

om en unionsomfattande samordnad strategi för att stärka den kritiska infrastrukturens motståndskraft

(Text av betydelse för EES)

(2023/C 20/01)

EUROPEISKA UNIONENS RÅD HAR UTFÄRDAT DENNA REKOMMENDATION

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114 och artikel 292 första och andra meningarna,

med beaktande av Europeiska kommissionens förslag, och

av följande skäl:

(1) I syfte att säkra den inre marknadens funktion ligger det i alla medlemsstaters och hela unionens intresse att tydligt identifiera och skydda relevant kritisk infrastruktur som tillhandahåller samhällsviktiga tjänster inom den marknaden, särskilt i nyckelsektorer såsom energi, digital infrastruktur, transport och rymden samt kritisk infrastruktur med stor gränsöverskridande betydelse ([1]) där störningar skulle kunna få en betydande inverkan på andra medlemsstater.

(2) Denna rekommendation, som är en icke-bindande akt, visar medlemsstaternas politiska vilja att samarbeta och deras engagemang för de rekommenderade åtgärderna, vilket framhålls i en fempunktsplan som Europeiska kommissionens ordförande utfärdat, samtidigt som medlemsstaternas befogenheter respekteras fullt ut. Denna rekommendation påverkar inte skyddet av medlemsstaternas väsentliga intressen i fråga om nationell och allmän säkerhet eller försvar, och ingen medlemsstat bör förväntas lämna ut information som inverkar negativt på dessa intressen.

(3) Det primära ansvaret för att säkerställa den kritiska infrastrukturens säkerhet och tillhandahållande av samhällsviktiga tjänster vilar på medlemsstaterna och deras operatörer av kritisk infrastruktur, men det är lämpligt med ökad samordning på unionsnivå, särskilt mot bakgrund av föränderliga hot som kan påverka flera medlemsstater samtidigt, såsom Rysslands anfallskrig mot Ukraina och hybridkampanjer mot medlemsstater, eller påverka motståndskraften och funktionen hos unionens ekonomi, inre marknad och samhälle som helhet. Särskild uppmärksamhet bör ägnas kritisk infrastruktur utanför medlemsstaternas territorium, såsom kritisk undervattensinfrastruktur eller infrastruktur för havsbaserad energi.

([1]) Medlemsstaterna bör bedöma sådan betydelse i enlighet med sin nationella praxis och kan göra detta på grundval av bland annat en riskbedömning och händelsens konsekvenser och art.

(4) I sina slutsatser av den 20–21 oktober 2022 fördömde Europeiska rådet i starka ordalag sabotagen mot kritisk infrastruktur, till exempel mot Nord Stream-ledningarna, och förklarade att unionen kommer att bemöta varje avsiktlig störning av kritisk infrastruktur eller andra hybridåtgärder med enade och beslutsamma motåtgärder.

(5) Med tanke på hur snabbt hotbilden förändras bör åtgärder för stärkt motståndskraft vidtas som en prioritet inom nyckelsektorer såsom energi, digital infrastruktur, transport och rymden och inom andra relevanta sektorer som medlemsstaterna identifierar. Sådana åtgärder bör inriktas på att stärka motståndskraften hos kritisk infrastruktur med beaktande av relevanta risker, särskilt kaskadeffekter, störningar i leveranskedjorna, beroende, klimatförändringarnas effekter, opålitliga leverantörer och partner samt hybridhot och hybridkampanjer, inbegripet utländsk informationsmanipulering och inblandning. Med tanke på de möjliga konsekvenserna vad gäller nationell kritisk infrastruktur bör prioritet ges åt kritisk infrastruktur med stor gränsöverskridande betydelse. Medlemsstaterna uppmanas att tillhandahålla sådana åtgärder för stärkt motståndskraft, när så är lämpligt och så snart som möjligt, och samtidigt bibehålla den strategi som anges i den framväxande rättsliga ramen.

(6) Skyddet av europeisk kritisk infrastruktur inom energi- och transportsektorerna regleras för närvarande av rådets direktiv 2008/114/EG ([2]), och säkerheten i nätverks- och informationssystem i hela unionen med inriktning på cyberrelaterade hot säkerställs genom Europaparlamentets och rådets direktiv (EU) 2016/1148 ([3]). I syfte att säkerställa en högre gemensam nivå av motståndskraft och skydd avseende kritisk infrastruktur, cybersäkerhet och finansmarknaden ändras och kompletteras den befintliga rättsliga ramen genom antagandet av nya regler som är tillämpliga på kritiska entiteter (*CER-direktivet*), skärpta regler för en hög gemensam cybersäkerhetsnivå i hela unionen (*NIS 2-direktivet*) och nya regler om digital operativ motståndskraft för finanssektorn (*DORA-förordningen*).

(7) Medlemsstaterna bör, i enlighet med unionsrätten och nationell rätt, använda alla tillgängliga verktyg för att agera och bidra till att stärka den fysiska motståndskraften och cyberresiliensen. I detta avseende bör kritisk infrastruktur anses omfatta 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 CER-direktivet eller, i förekommande fall, entiteter som omfattas av NIS 2-direktivet. Begreppet ”motståndskraft” bör förstås som syftande på en kritisk infrastrukturs förmåga att förebygga, skydda mot, reagera på, stå emot, mildra, 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.

(8) Nationella experter bör sammankallas i syfte att samordna arbetet för att uppnå en högre gemensam nivå på motståndskraften hos och skyddet av kritisk infrastruktur, vilket ska ske med hjälp av de nya reglerna för kritiska entiteter. Detta samordnade arbete skulle möjliggöra samarbete mellan medlemsstater och informationsutbyte om verksamheter såsom utarbetande av metoder för att identifiera samhällsviktiga tjänster som tillhandahålls av kritisk infrastruktur. Kommissionen har redan börjat sammankalla dessa experter och underlätta deras arbete, och avser att fortsätta göra detta. När CER-direktivet har trätt i kraft, och en grupp för kritiska entiteters motståndskraft har inrättats inom ramen för det direktivet, bör denna grupp fortsätta med sådant föregripande arbete i enlighet med sina arbetsuppgifter.

(9) Med tanke på den förändrade hotbilden bör möjligheterna att stresstesta kritisk infrastruktur på nationell nivå vidareutvecklas eftersom sådana tester skulle kunna vara användbara för att stärka motståndskraften hos kritisk infrastruktur. När det gäller energisektorns särskilda betydelse, och de unionsomfattande konsekvenser som eventuella störningar inom denna skulle få, skulle denna sektor kunna dra störst nytta av att stresstester genomförs på grundval av gemensamt överenskomna principer. Sådana stresstester faller under medlemsstaternas behörighet, och medlemsstaterna bör uppmuntra och stödja operatörer av kritisk infrastruktur så att de genomför sådana stresstester, om de bedöms vara till nytta och överensstämma med deras nationella rättsliga ramar.

([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) 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).

(10) För att säkerställa ett samordnat och ändamålsenligt svar på nuvarande och förväntade hot uppmanas kommissionen att ge ytterligare stöd till medlemsstaterna, särskilt genom att tillhandahålla relevant information i form av genomgångar, icke-bindande handböcker och vägledningar. Europeiska utrikestjänsten bör, särskilt genom EU:s underrättelse- och lägescentral och dess enhet för hybridhot, med stöd av Europeiska unionens militära stabs (EUMS) underrättelsedirektorat inom ramen för den gemensamma kapaciteten för underrättelseanalys (SIAC), tillhandahålla hotbildsbedömningar. Kommissionen uppmanas också att i samarbete med medlemsstaterna verka för att unionsfinansierade forsknings- och innovationsprojekt utnyttjas.

(11) Genom det allt större ömsesidiga beroendet mellan fysisk och digital infrastruktur kan skadlig cyberverksamhet som riktar sig mot kritiska områden leda till störningar eller skador på fysisk infrastruktur, och sabotage av fysisk infrastruktur kan göra digitala tjänster otillgängliga. Medlemsstaterna uppmanas att påskynda det förberedande arbetet för att införliva och tillämpa den nya rättsliga ramen för kritiska entiteter och den stärkta rättsliga ramen för cybersäkerhet på grundval av erfarenheterna från den samarbetsgrupp som inrättats genom direktiv (EU) 2016/1148 (*samarbetsgruppen för nät- och informationssäkerhet*), så snart som möjligt och med beaktande av införlivandefristerna och av att sådant förberedande arbete bör fortskrida parallellt och samstämmigt.

(12) Utöver att stärka beredskapen är det också viktigt att förbättra förmågan att reagera snabbt och ändamålsenligt vid en störning av samhällsviktiga tjänster som tillhandahålls av kritisk infrastruktur. Därför innehåller denna rekommendation åtgärder på både unionsnivå och nationell nivå, inbegripet genom att betona den stödjande roll och det mervärde som kan erhållas genom införande av förstärkt samarbete och informationsutbyte inom ramen för unionens civilskyddsmekanism, som inrättades genom Europaparlamentets och rådets beslut nr 1313/2013/EU ([4]), och användning av relevanta tillgångar i unionens rymdprogram, som inrättades genom Europaparlamentets och rådets förordning (EU) 2021/696 ([5]).

(13) Kommissionen, unionens höga representant för utrikes frågor och säkerhetspolitik (*den höga representanten*) och samarbetsgruppen för nät- och informationssäkerhet ska i samarbete med relevanta civila och militära organ och byråer och etablerade nätverk, däribland Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), göra en riskbedömning och utarbeta riskscenarier. Som en uppföljning av den gemensamma uppmaningen från ministermötet i Nevers genomförs dessutom en sådan riskbedömning för närvarande av samarbetsgruppen för nät- och informationssäkerhet med stöd av kommissionen och Europeiska unionens cybersäkerhetsbyrå (Enisa) och i samarbete med Organet för europeiska regleringsmyndigheter för elektronisk kommunikation (Berec). Dessa två arbetsuppgifter kommer att vara samstämmiga och samordnas med arbetet med att utarbeta scenarier inom ramen för unionens civilskyddsmekanism, inbegripet cybersäkerhetshändelser och deras konkreta konsekvenser, som för närvarande håller på att utarbetas av kommissionen och medlemsstaterna. Av skäl som hänför sig till effektivitet, ändamålsenlighet och samstämmighet, och för en korrekt tillämpning av denna rekommendation, ska resultaten av detta arbete återspeglas på nationell nivå.

(14) I syfte att omedelbart stärka beredskapen och kapaciteten att hantera en storskalig cybersäkerhetsincident har kommissionen inrättat ett kortsiktigt program för att stödja medlemsstaterna genom ytterligare anslag till Enisa. Till de tjänster som föreslås hör bland annat beredskapsåtgärder, såsom penetrationstester av entiteter för att upptäcka sårbarheter. Programmet kan även förbättra möjligheterna att bistå medlemsstaterna i händelse av en storskalig cybersäkerhetsincident som påverkar kritiska entiteter. Detta är ett första steg i linje med rådets slutsatser av den 23 maj 2022 om utvecklingen av Europeiska unionens arbete på cyberområdet (*rådets slutsatser om EU:s arbete 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 och uppmanas att fortsätta med arbetet med unionens hantering av cyberkriser, i synnerhet genom att regelbundet övervaka och utvärdera framstegen med genomförandet av den färdplan för hantering av cyberkriser som nyligen utarbetats av rådet. Den färdplanen är ett levande dokument och bör vid behov ses över och uppdateras.

([4]) 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).

([5]) Europaparlamentets och rådets förordning (EU) 2021/696 av den 28 april 2021 om inrättande av unionens rymdprogram och Europeiska unionens rymdprogrambyrå och om upphävande av förordningarna (EU) nr 912/2010, (EU) nr 1285/2013 och (EU) nr 377/2014 och beslut nr 541/2014/EU (EUT L 170, 12.5.2021, s. 69).

(15) Globala undervattenskablar för kommunikation är av grundläggande betydelse för konnektiviteten globalt och inom EU. Den betydande längden på sådana kablar och det faktum att de är anlagda på havsbottnen gör det utomordentligt svårt att övervaka merparten av kabelnätets delar under vattnet. Den gemensamma jurisdiktionen och andra jurisdiktionsfrågor gällande sådana kablar är ett särskilt 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 den digitala och fysiska infrastruktur som ligger till grund för digitala tjänster med särskilda riskbedömningar och alternativ när det gäller riskreducerande åtgärder inriktade på undervattenskablar. Medlemsstaterna uppmanar kommissionen att genomföra studier för ändamålet och informera medlemsstaterna om resultaten av dessa.

(16) Energi- och transportsektorerna kan också påverkas av hot mot digital infrastruktur, till exempel då energiteknik innehåller digitala komponenter. Säkerheten i därmed sammanhängande leveranskedjor är viktig för kontinuiteten i tillhandahållandet av samhällsviktiga tjänster och för den strategiska kontrollen av kritisk infrastruktur inom energisektorn. Dessa omständigheter bör beaktas när åtgärder i enlighet med denna rekommendation vidtas för att stärka motståndskraften hos kritisk infrastruktur.

(17) Den växande betydelse som rymdinfrastruktur, rymdrelaterade marktillgångar – inbegripet produktionsanläggningar – och rymdbaserade tjänster har för säkerhetsrelaterad verksamhet gör det mycket viktigt att säkerställa att unionens rymd och dess markbaserade tillgångar och tjänster är motståndskraftiga och skyddas inom EU. Av samma skäl är det också viktigt att, inom ramen för denna rekommendation, på ett mer strukturerat sätt dra nytta av de rymdbaserade data och tjänster som tillhandahålls av rymdsystem och rymdprogram för att övervaka, spåra 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 vid genomförandet av denna rekommendation.

(18) Samarbete på internationell nivå behövs också för att på ett ändamålsenligt sätt hantera risker för kritisk infrastruktur, bland annat i internationella vatten. Medlemsstaterna uppmanas därför att samarbeta med kommissionen och den höga representanten för att vidta vissa åtgärder i riktning mot ett sådant samarbete, med beaktande av att sådana åtgärder bara får vidtas i enlighet med deras respektive uppgifter och ansvarsområden enligt unionsrätten, i synnerhet bestämmelserna i fördragen om yttre förbindelser.

(19) Som fastställs i dess meddelande av den 15 februari 2022 *Kommissionens bidrag till det europeiska försvaret, 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* kommer kommissionen att bedöma utgångsvärdena 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 ligga till grund för arbetet inom ramen för denna rekommendation och bidra till att öka utbytet av information och samordningen av åtgärder som syftar till att stärka motståndskraften hos bland annat kritisk infrastruktur.

(20) I EU:s strategi för sjöfartsskydd från 2014 och dess reviderade handlingsplan efterlystes ökat skydd för kritisk sjöfartsinfrastruktur, inbegripet undervattensinfrastruktur, och i synnerhet sjötransport-, energi- och kommunikationsinfrastruktur, bland annat genom en förbättrad maritim lägesbild genom ökad driftskompatibilitet och effektivare informationsutbyte (obligatoriskt och frivilligt). Den strategin och den handlingsplanen håller för närvarande på att uppdateras och kommer att innehålla stärkta åtgärder som syftar till att skydda kritisk sjöfartsinfrastruktur. Dessa åtgärder bör komplettera denna rekommendation.

(21) En stärkt motståndskraft hos kritisk infrastruktur bidrar till bredare insatser för att motverka hybridhot och hybridkampanjer mot unionen och dess medlemsstater. Denna rekommendation bygger vidare på det gemensamma meddelandet till Europaparlamentet och rådet *Gemensam ram för att motverka hybridhot – Europeiska unionens insatser*. Åtgärd 1 i den gemensamma ramen, dvs. undersökning av risker i samband med hybridhot, spelar en viktig roll när det gäller att identifiera sårbarheter som kan påverka nationella och alleuropeiska strukturer och nätverk. Dessutom kommer genomförandet av rådets slutsatser av den 21 juni 2022 om en ram för en samordnad EU-reaktion på hybridkampanjer att möjliggöra en kraftfullare samordnad insats genom tillämpning av EU:s verktygslåda för hantering av hybridhot på alla berörda områden.

HÄRIGENOM REKOMMENDERAS FÖLJANDE.

KAPITEL I: SYFTE, TILLÄMPNINGSOMRÅDE OCH PRIORITERING

1. I denna rekommendation fastställs en rad riktade åtgärder på unionsnivå och nationell nivå för att stödja och stärka motståndskraften hos kritisk infrastruktur, på frivillig basis, med fokus på kritisk infrastruktur med stor gränsöverskridande betydelse och inom identifierade nyckelsektorer, såsom energi, digital infrastruktur, transport och rymden. Dessa riktade åtgärder består av ökad beredskap, ökade insatser och internationellt samarbete.

2. Information som utbyts i syfte att uppfylla målen för denna rekommendation och som är konfidentiell enligt unionsbestämmelser och nationella bestämmelser samt bestämmelser om affärshemligheter bör utbytas med kommissionen och andra relevanta myndigheter endast när sådant utbyte är nödvändigt för att tillämpa denna rekommendation. Denna rekommendation påverkar inte skyddet av medlemsstaternas väsentliga intressen i fråga om nationell och allmän säkerhet eller försvar, och ingen medlemsstat bör förväntas lämna ut information som går emot dessa intressen.

KAPITEL II: ÖKAD BEREDSKAP

Åtgärder på medlemsstatsnivå

3. Medlemsstaterna bör överväga en allriskstrategi när de uppdaterar sina riskbedömningar eller sina befintliga likvärdiga analyser, i linje med den föränderliga karaktären hos de nuvarande hoten mot deras kritiska infrastruktur, särskilt inom identifierade nyckelsektorer och, om möjligt, inom alla sektorer som omfattas av kommande nya rättsliga ramar som är tillämpliga på kritiska entiteter.

4. Medlemsstaterna uppmanas att påskynda det förberedande arbetet och anta åtgärder för stärkt motståndskraft, där så är möjligt, i enlighet med den kommande rättsliga ramen för kritiska entiteter, med särskilt fokus på samarbete och utbyte av relevant information mellan medlemsstaterna och med kommissionen, på identifiering av kritiska entiteter med stor gränsöverskridande betydelse och på ökat stöd till identifierade kritiska entiteter för att förbättra deras motståndskraft.

5. Medlemsstaterna bör ge stöd till utbildning av experter och övningar och utbyte av bästa praxis och lärdomar. Medlemsstaterna bör uppmuntra experter att delta i befintliga utbildningsplattformar, både nationella och internationella, till exempel inom ramen för unionens civilskyddsmekanism.

6. Medlemsstaterna bör uppmuntra och stödja operatörer av kritisk infrastruktur, åtminstone inom energisektorn, att genomföra stresstester i enlighet med gemensamt överenskomna principer på unionsnivå i fall där detta är fördelaktigt. Stresstesterna bör syfta till att bedöma den kritiska infrastrukturens motståndskraft mot antagonistiska hot orsakade av människan. Medlemsstaterna bör därför sträva efter att identifiera relevant kritisk infrastruktur för testning och samråda med relevanta operatörer av kritisk infrastruktur så snart som möjligt och senast i slutet av det första kvartalet 2023. Dessutom bör medlemsstaterna stödja operatörerna av kritisk infrastruktur så att de gör dessa tester så snart som möjligt och strävar efter att slutföra dem senast före utgången av 2023, i enlighet med nationell lagstiftning. Rådet har för avsikt att utvärdera läget i fråga om stresstester senast i slutet av april 2023.

7. Hoten mot kritisk infrastruktur förändras snabbt, och det är därför av avgörande betydelse att upprätthålla en hög skyddsnivå. Medlemsstaterna uppmuntras att anslå tillräckliga finansiella resurser för att stärka kapaciteten hos sina relevanta nationella myndigheter och att stödja dem i syfte att kunna stärka den kritiska infrastrukturens motståndskraft. Medlemsstaterna uppmuntras också att anslå tillräckliga finansiella resurser till de myndigheter som ansvarar för hanteringen av storskaliga cybersäkerhetsincidenter för att stödja dem och att säkerställa att deras enheter för hantering av it-säkerhetsincidenter (CSIRT) och behöriga myndigheter till fullo mobiliseras i CSIRT-nätverket respektive EU-CyCLONe.

8. Medlemsstaterna uppmanas att, i enlighet med tillämpliga krav, utnyttja potentiella finansieringsmöjligheter på unionsnivå och nationell nivå för att stärka motståndskraften hos kritisk infrastruktur i unionen för sig själva, och även att uppmuntra operatörerna av kritisk infrastruktur att utnyttja sådana finansieringsmöjligheter, inbegripet till exempel transeuropeiska nät, mot alla typer av betydande hot, särskilt inom ramen för de program som finansieras av Fonden för inre säkerhet, som inrättades genom Europaparlamentets och rådets förordning (EU) 2021/1149 ([6]), Europeiska regionala utvecklingsfonden, som inrättades genom Europaparlamentets och rådets förordning (EU) nr 1301/2013 ([7]), unionens civilskyddsmekanism och kommissionens REPowerEU-plan. Medlemsstaterna uppmuntras också att på bästa sätt utnyttja resultaten av relevanta projekt inom ramen för forskningsprogrammen, såsom Horisont Europa, som inrättades genom Europaparlamentets och rådets förordning (EU) 2021/695 ([8]).

9. När det gäller kommunikations- och nätinfrastrukturen i unionen uppmanas samarbetsgruppen för nät- och informationssäkerhet att, i enlighet med artikel 11 i direktiv (EU) 2016/1148, påskynda sitt pågående arbete på grundval av den gemensamma uppmaningen från ministermötet i Nevers med en riktad riskbedömning, och gruppen bör lägga fram de första rekommendationerna så snart som möjligt. Den riskbedömningen bör tillföra information till det pågående sektorsövergripande arbetet med den cyberriskbedömning och de cyberriskscenarier som efterfrågades i rådets slutsatser om EU:s arbete på cyberområdet. 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.

10. Samarbetsgruppen för nät- och informationssäkerhet uppmanas också att, med stöd av kommissionen och Enisa, fortsätta sitt arbete med säkerheten i den digitala infrastrukturen, inbegripet avseende undervattensinfrastruktur, nämligen undervattenskablar. Den uppmanas också att påbörja sitt arbete med rymdsektorn, inbegripet genom att vid behov utarbeta policyer och metoder för hantering av cybersäkerhetsrisker som grundar sig på en allriskstrategi och en riskbaserad strategi för operatörer i 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 program för stöd på kort sikt som kommissionen genomför tillsammans med Enisa, till exempel penetrationstester för att identifiera sårbarheter, och de uppmuntras i detta sammanhang att prioritera entiteter som driver kritisk infrastruktur inom sektorerna för energi, digital infrastruktur och transport.

12. Medlemsstaterna bör fullt ut utnyttja Europeiska kompetenscentrumet för cybersäkerhet (ECCC). Medlemsstaterna bör uppmuntra sina nationella samordningscentrum att proaktivt samarbeta med medlemmar i cybersäkerhetsgrupper för att bygga upp kapacitet på unionsnivå och nationell nivå för att bättre kunna stödja leverantörer av samhällsviktiga tjänster.

13. Det är viktigt att medlemsstaterna genomför de åtgärder som rekommenderas i EU:s verktygslåda för 5G-cybersäkerhet och i synnerhet att medlemsstaterna inför restriktioner för högriskleverantörer, med tanke på att förlorad tid kan öka nätens sårbarhet i unionen, och även stärker det fysiska och icke-fysiska skyddet av kritiska och känsliga delar av 5G-näten, bland annat genom strikta åtkomstkontroller. Dessutom bör medlemsstaterna i samarbete med kommissionen bedöma behovet av kompletterande åtgärder för att säkerställa en enhetlig nivå av säkerhet och motståndskraft i 5G-näten.

14. Medlemsstaterna bör tillsammans med kommissionen och Enisa fokusera på att genomföra rådets slutsatser av den 17 oktober 2022 om säkerheten i IKT-leveranskedjan.

([6]) Europaparlamentets och rådets förordning (EU) 2021/1149 av den 7 juli 2021 om inrättande av Fonden för inre säkerhet (EUT L 251, 15.7.2021, s. 94).

([7]) Europaparlamentets och rådets förordning (EU) nr 1301/2013 av den 17 december 2013 om Europeiska regionala utvecklingsfonden och om särskilda bestämmelser för målet Investering för tillväxt och sysselsättning samt om upphävande av förordning (EG) nr 1080/2006 (EUT L 347, 20.12.2013, s. 289).

([8]) Europaparlamentets och rådets förordning (EU) 2021/695 av den 28 april 2021 om inrättande av Horisont Europa – ramprogrammet för forskning och innovation, om fastställande av dess regler för deltagande och spridning och om upphävande av förordningarna (EU) nr 1290/2013 och (EU) nr 1291/2013 (EUT L 170, 12.5.2021, s. 1).

15. Medlemsstaterna bör beakta den kommande nätföreskriften avseende cybersäkerhetsaspekter av gränsöverskridande elflöden[...], på grundval av erfarenheterna från genomförandet av direktiv (EU) 2016/1148 och relevant vägledning från samarbetsgruppen för nät- och informationssäkerhet, särskilt dess referensdokument om säkerhetsåtgärder för operatörer av samhällsviktiga tjänster.

16. Medlemsstaterna bör utveckla användningen av Copernicus, Galileo och European Geostationary Navigation Overlay Service (Egnos) för övervakning för att förmedla relevant information till 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 krisprognoser och krishantering.

Åtgärder på unionsnivå

17. Dialogen och samarbetet mellan medlemsstaternas utsedda experter och med kommissionen bör stärkas i syfte att stärka den fysiska motståndskraften hos kritisk infrastruktur, särskilt genom att

    a) bidra till förberedelserna för och utvecklingen och främjandet av gemensamma frivilliga verktyg för att stödja medlemsstaterna i arbetet med att stärka sådan motståndskraft, inbegripet metoder och riskscenarier,

    b) stödja medlemsstater vid genomförandet av den nya rättsliga ramen för kritiska entiteter, inbegripet genom att uppmuntra kommissionen att anta den delegerade akten i god tid,

    c) stödja genomförandet av de stresstester som avses i punkt 6, på grundval av gemensamma principer, med början i sådana tester som fokuserar på antagonistiska hot orsakade av människan inom energisektorn och därefter inom andra nyckelsektorer, samt ge stöd till och rådgivning om genomförandet av sådana stresstester, på begäran av en medlemsstat,

    d) utnyttja en säker plattform, så snart en sådan inrättats av kommissionen, för att samla in, utvärdera och, på frivillig basis, utbyta bästa praxis, lärdomar av nationella erfarenheter och annan information om sådan motståndskraft.

    Dessa utsedda experter bör i sitt arbete ägna särskild uppmärksamhet åt sektorsövergripande beroenden och kritisk infrastruktur med stor gränsöverskridande betydelse, och arbetet bör följas upp av rådet och kommissionen när så är lämpligt.

18. Medlemsstaterna uppmuntras att utnyttja det stöd som kommissionen erbjuder, till exempel genom utarbetande av handböcker och vägledningar, såsom utarbetandet av en handbok om skydd av kritisk infrastruktur och offentliga platser mot obemannade luftfartygssystem och verktyg för riskbedömningar. Utrikestjänsten uppmanas att, särskilt genom EU:s underrättelse- och lägescentral och dess enhet för hybridhot, med stöd av EUMS underrättelsedirektorat inom ramen för SIAC, hålla genomgångar om hoten mot kritisk infrastruktur i unionen i syfte att förbättra lägesbilden.

19. Medlemsstaterna bör stödja kommissionens åtgärder för att utnyttja resultaten från projekt om motståndskraften hos kritisk infrastruktur, vilka finansieras genom unionens forsknings- och innovationsprogram. Rådet noterar kommissionens avsikt att, inom ramen för den budget som anslagits till Horisont Europa inom den fleråriga budgetramen för 2021–2027, öka anslagen till sådan motståndskraft, utan att detta inverkar negativt på finansieringen av andra civila säkerhetsrelaterade forsknings- och innovationsprojekt inom ramen för Horisont Europa.

20. På grundval av de arbetsuppgifter som föreskrivs i rådets slutsatser om EU:s arbete på cyberområdet uppmanas kommissionen, den höga representanten och samarbetsgruppen för nät- och informationssäkerhet att, i enlighet med sina respektive uppgifter och ansvarsområden enligt unionsrätten, intensifiera arbetet med relevanta nätverk och civila och militära organ och byråer för att genomföra riskbedömningar och utarbeta scenarier för cybersäkerhetsrisker, med särskild hänsyn till vikten av energi, digital infrastruktur, transport- och rymdinfrastruktur och det ömsesidiga beroendet mellan sektorer och medlemsstater. Detta arbete bör ta hänsyn till de relaterade riskerna för den infrastruktur som dessa sektorer är beroende av. Riskbedömningarna och riskscenarierna kan, om det är fördelaktigt, 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.

21. Kommissionen uppmanas att påskynda sin verksamhet i enlighet med sina respektive arbetsuppgifter inom hanteringen av cyberkriser, för att stödja medlemsstaternas beredskap och insatser vid storskaliga cybersäkerhetsincidenter, och i synnerhet

    a) genomföra, som ett komplement till relevanta riskbedömningar rörande nät- och informationssäkerhet, en heltäckande studie ([9]) av den undervattensinfrastruktur, nämligen undervattenskablar, som kopplar samman medlemsstaterna såväl som Europa globalt, vars resultat bör förmedlas till medlemsstaterna,

    b) stödja medlemsstaternas och unionens institutioners, organs och byråers beredskap för och insatser vid storskaliga cybersäkerhetsincidenter eller större incidenter, i enlighet med den stärkta rättsliga ramen för cybersäkerhet och andra relevanta tillämpliga regler ([10]),

    c) påskynda arbetet med huvudkonceptet för fonden för hantering av cybersäkerhetsincidenter med en ordentlig diskussion med medlemsstaterna.

22. Kommissionen uppmuntras att intensifiera arbetet med framåtblickande föregripande åtgärder, bland annat samarbetet 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 (ERCC) och dess insatser vid störningar av kritisk infrastruktur, öka investeringarna i förebyggande strategier och befolkningens beredskap och öka stödet avseende kapacitetsuppbyggnad inom ramen för unionens kunskapsnätverk för civilskydd.

23. Kommissionen bör främja användningen av unionens övervakningsresurser (Copernicus, Galileo och Egnos) för att stödja medlemsstaterna i övervakningen av kritisk infrastruktur, och i relevanta fall deras omedelbara närhet, och för att stödja andra övervakningsalternativ som föreskrivs i unionens rymdprogram, såsom ramarna för rymdlägesbild och EU:s rymdövervakning och spårning.

24. 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 kritisk infrastruktur, i synnerhet enligt följande:

    a) Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) när det gäller informationsinsamling, brottsanalys och utredningsstöd i samband med gränsöverskridande brottsbekämpande åtgärder och, när så är relevant och lämpligt, förmedling av resultaten till medlemsstaterna.

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

    c) Europeiska unionens rymdprogrambyrå (EUSPA) och Europeiska unionens satellitcentrum (Satcen) kan eventuellt bistå genom insatser inom ramen för unionens rymdprogram.

    d) ECCC skulle när det gäller verksamhet som rör cybersäkerhet, även i samarbete med Enisa, kunna stödja innovation och industripolitik inom cybersäkerhet.

([9]) Denna studie bör inbegripa en kartläggning av dess kapacitet och redundans, sårbarheter, hot och risker för tjänsternas tillgänglighet, effekterna av driftsavbrott för (transatlantiska) undervattenskablar för medlemsstaterna och unionen som helhet samt riskreducering, samtidigt som hänsyn tas till informationens känslighet och behovet av att skydda den.

([10]) Särskild uppmärksamhet bör också ägnas all verksamhet som förbereder ändamålsenliga samordnade motåtgärder på unionsnivå i händelse av en större gränsöverskridande cyberincident eller relaterade hot som skulle kunna få en systemisk effekt på unionens finanssektor, i enlighet med den nya rättsliga ramen för digital operativ motståndskraft.

KAPITEL III: ÖKADE INSATSER

Åtgärder på medlemsstatsnivå

25. Medlemsstaterna uppmanas att göra följande:

    a) Fortsätta att samordna sina insatser där detta är relevant och upprätthålla en samlad bild av de sektorsövergripande insatserna vid akuta störningar av samhällsviktiga tjänster som tillhandahålls av kritisk infrastruktur. Detta skulle kunna göras inom ramen för en framtida plan för samordnade insatser vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse, befintliga arrangemang för integrerad politisk krishantering (IPCR) för samordning av den politiska reaktionen när det gäller kritisk infrastruktur med gränsöverskridande betydelse, planen för samordnade insatser vid storskaliga cyberincidenter och cyberkriser enligt kommissionens rekommendation (EU) 2017/1584 ([11]), EU-CyCLONe, ramen för en samordnad EU-reaktion på hybridkampanjer och EU:s verktygslåda för hantering av hybridhot vid hybridhot och hybridkampanjer samt systemet för snabbt informationsutbyte vid desinformation.

    b) Öka informationsutbytet på operativ nivå med ERCC inom ramen för unionens civilskyddsmekanism för att förbättra systemet för tidig varning och samordna insatserna inom ramen för civilskyddsmekanismen i händelse av störningar av kritisk infrastruktur med stor gränsöverskridande betydelse, och på så sätt säkerställa snabbare och av unionen underlättade insatser när det behövs.

    c) Stärka sin beredskap att, där så är relevant, via befintliga eller ännu inte utvecklade verktyg reagera på sådana betydande störningar som avses i led a.

    d) Samarbeta för att vidareutveckla relevant insatskapacitet i den europeiska civilskyddspoolen (ECPP) och rescEU.

    e) Uppmuntra operatörer av kritisk infrastruktur och relevanta nationella myndigheter att öka sin kapacitet att snabbt återställa basprestanda för de samhällsviktiga tjänster som tillhandahålls av dessa operatörer av kritisk infrastruktur.

    f) Uppmuntra operatörer av kritisk infrastruktur att när de återuppbygger sin kritiska infrastruktur göra den så motståndskraftig som möjligt, med beaktande av åtgärdernas proportionalitet när det gäller riskbedömningar och kostnader, mot alla de betydande risker som den kan utsättas för, även i ogynnsamma klimatscenarier.

26. Medlemsstaterna uppmanas att påskynda det förberedande arbetet, där så är möjligt, enligt mandatet i den stärkta rättsliga ramen för cybersäkerhet, genom att sikta på att stärka de nationella CSIRT-enheternas resurser mot bakgrund av CSIRT-enheternas nya uppgifter och det ökade antalet entiteter från nya sektorer, att se över och uppdatera sina cybersäkerhetsstrategier i god tid och att snarast möjligt anta nationella incident- och krishanteringsplaner för cybersäkerhet, om sådana inte redan finns.

27. Medlemsstaterna uppmanas att på nationell nivå överväga de mest relevanta sätten att säkerställa att berörda parter är medvetna om behovet av att öka motståndskraften hos kritisk infrastruktur genom samarbete med pålitliga leverantörer och partner. Det är viktigt att investera i ytterligare kapacitet, särskilt i de sektorer där den nuvarande infrastrukturen närmar sig slutet på sin livstid, t.ex. infrastruktur för undervattenskablar, för att kunna säkerställa ett kontinuerligt tillhandahållande av samhällsviktiga tjänster i händelse av störningar och för att minska oönskade beroenden.

28. Medlemsstaterna uppmuntras att uppmärksamma proaktiv strategisk kommunikation på nationell nivå i samband med motverkande av hybridhot och hybridkampanjer och med tanke på den potential som motståndare kan försöka utnyttja med utländsk informationsmanipulering och inblandning genom att forma narrativen om incidenter som är riktade mot kritisk infrastruktur.

Åtgärder på unionsnivå

29. Kommissionen uppmanas ha ett nära samarbete med medlemsstaterna för att ytterligare utveckla relevanta organ och instrument och relevant insatskapacitet i syfte att stärka den operativa beredskapen för att hantera de omedelbara och indirekta effekterna av betydande störningar i relevanta samhällsviktiga tjänster som tillhandahålls av kritisk infrastruktur, särskilt med experter och resurser som finns tillgängliga genom ECPP och rescEU inom ramen för unionens civilskyddsmekanism eller framtida snabbinsatsteam för hybridhot.

([11]) 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).

30. Med beaktande av den föränderliga hotbilden och i samarbete med medlemsstaterna uppmanas kommissionen att, inom ramen för unionens civilskyddsmekanism,

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

b) regelbundet övervaka och identifiera potentiellt betydande brister avseende insatskapaciteten i ECPP och rescEU-kapaciteten,

c) ytterligare intensifiera det sektorsövergripande samarbetet för att säkerställa lämpliga insatser på unionsnivå och anordna regelbundna utbildningar eller övningar för att testa sådant samarbete tillsammans med en eller flera medlemsstater,

d) vidareutveckla ERCC som sektorsövergripande kriscentrum på unionsnivå för samordning av stödet till drabbade medlemsstater.

31. Rådet är fast beslutet att inleda arbetet med att godkänna en plan för samordnade insatser vid störningar av kritisk infrastruktur med stor gränsöverskridande betydelse, där man beskriver och fastställer målen och formerna för samarbetet mellan medlemsstaterna och unionens institutioner, organ och byråer för att hantera incidenter som drabbar sådan kritisk infrastruktur. Rådets ser fram emot kommissionens utkast till en sådan plan, på grundval av stöd och bidrag från relevanta unionsbyråer. Planen ska vara helt samstämmig och driftskompatibel med unionens reviderade operativa protokoll för att motverka hybridhot (*EU Playbook*), ta hänsyn till den befintliga planen för samordnade insatser vid storskaliga gränsöverskridande cyberincidenter ([12]) och cyberkriser och mandatet för EU-CyCLONe i enlighet med NIS 2-direktivet samt undvika överlappning av strukturer och verksamheter. I denna plan bör man fullt ut respektera de befintliga IPCR-arrangemangen för att samordna insatserna.

32. Kommissionen uppmanas att samråda med relevanta berörda parter och experter om lämpliga åtgärder avseende potentiellt betydande incidenter när det gäller undervattensinfrastruktur, som ska presenteras i samband med den studie som avses i punkt 20 a, samt för att ytterligare utveckla beredskapsplanering, riskscenarier och målen avseende unionens motståndskraft mot katastrofer som fastställs i beslut nr 1313/2013/EU.

KAPITEL IV: INTERNATIONELLT SAMARBETE

Åtgärder på medlemsstatsnivå

33. Medlemsstaterna bör, när så är lämpligt och i enlighet med unionsrätten, samarbeta med relevanta tredjeländer när det gäller motståndskraften hos kritisk infrastruktur med stor gränsöverskridande betydelse.

34. Medlemsstaterna uppmuntras att samarbeta med kommissionen och den höga representanten för att på ett ändamålsenligt sätt hantera risker för kritisk infrastruktur i internationella vatten.

35. 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 av den 21 juni 2022 om en ram för en samordnad EU-reaktion på hybridkampanjer och därefter tillämpa dem, i syfte att ge full verkan åt ramen för en samordnad EU-reaktion på hybridkampanjer, särskilt när de överväger och utarbetar övergripande och samordnade unionsreaktioner på hybridkampanjer och hybridhot, inbegripet dem som riktar sig mot operatörer av kritisk infrastruktur.

([12]) Kommissionens rekommendation (EU) 2017/1584 av den 13 september 2017 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser.

Åtgärder på unionsnivå

36. Kommissionen och den höga representanten uppmanas att, när så är lämpligt och i enlighet med sina respektive uppgifter och ansvarsområden enligt unionsrätten, stödja relevanta tredjeländer att stärka motståndskraften hos kritisk infrastruktur på deras territorium, särskilt kritisk infrastruktur som är fysiskt sammankopplad med deras och en medlemsstats territorium.

37. 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 av gemensamt intresse genom den strukturerade dialogen mellan EU och Nato om motståndskraft, med fullständig respekt för unionens och medlemsstaternas behörighet enligt fördragen och de centrala principer som styr samarbetet mellan EU och Nato och som Europeiska rådet har enats om, i synnerhet ömsesidighet, delaktighet och beslutsautonomi. I detta sammanhang kommer detta samarbete att fortsätta inom ramen för den strukturerade dialogen mellan EU och Nato om motståndskraft, som ingår i den befintliga mekanismen på tjänstemannanivå för genomförandet av de gemensamma förklaringarna, samtidigt som full insyn och alla medlemsstaters deltagande säkerställs.

38. Kommissionen uppmanas att överväga att låta företrädare för relevanta tredjeländer medverka, när så är nödvändigt och lämpligt, inom ramen för samarbetet och informationsutbytet mellan medlemsstaterna om motståndskraften hos kritisk infrastruktur som är fysiskt sammankopplad med en medlemsstats och ett tredjelands territorium.

Utfärdad i Bryssel den 8 december 2022.

På rådets vägnar
V. RAKUŠAN
Ordförande