EUROPEISKA UNIONEN

EUROPAPARLAMENTET **RÅDET**

Bryssel den 19 december 2024
(OR. en)

2023/0109(COD)
LEX 2422

PE-CONS 94/1/24
REV 1

CYBER 208
TELECOM 218
CADREFIN 109
FIN 595
BUDGET 47
IND 328
JAI 1084
MI 633
DATAPROTECT 247
RELEX 881
CODEC 1588

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING OM ÅTGÄRDER FÖR ATT STÄRKA SOLIDARITETEN OCH KAPACITETEN I UNIONEN ATT UPPTÄCKA, FÖRBEREDA SIG INFÖR OCH HANTERA CYBERHOT OCH CYBERSÄKERHETSINCIDENTER OCH OM ÄNDRING AV FÖRORDNING (EU) 2021/694 (CYBERSOLIDARITETSFÖRORDNINGEN)

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2024/…

av den 19 december 2024

om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter och om ändring av förordning (EU) 2021/694 (cybersolidaritetsförordningen)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artiklarna 173.3 och 322.1 a,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av revisionsrättens yttrande[1],

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[2],

med beaktande av Regionkommitténs yttrande[3],

i enlighet med det ordinarie lagstiftningsförfarandet[4], och

---

1 Yttrande av den 18 april 2023 (ännu inte offentliggjort i EUT).
2 EUT C 349, 29.9.2023, s. 167.
3 EUT C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.
4 Europaparlamentets ståndpunkt av den 24 april 2024. (ännu inte offentliggjord i EUT) och rådets beslut av den 2 december 2024.

av följande skäl:

(1) Användningen och beroendet av informations- och kommunikationsteknik har blivit grundläggande för alla sektorer av ekonomin och samhället mot bakgrund av att medlemsstaternas offentliga förvaltningar, företag och medborgare är mer sammanlänkade och ömsesidigt beroende än någonsin tidigare, över både sektors- och nationsgränser, samtidigt som detta har medfört eventuella sårbarheter.

(2) Cybersäkerhetsincidenternas omfattning, frekvens och konsekvenser, inbegripet attacker i distributionskedjor som syftar till cyberspionage, utpressning eller störningar, ökar på unionsnivå och global nivå. De utgör ett allvarligt hot mot nätverks- och informationssystemens funktion. Med tanke på det snabbt föränderliga hotlandskapet innebär hotet om eventuella storskaliga cybersäkerhetsincidenter som skulle orsaka betydande störningar eller skador på kritisk infrastruktur att det krävs ökad beredskap inom ramarna för unionens cybersäkerhetsarbete. Hotet sträcker sig bortom Rysslands anfallskrig mot Ukraina och kommer sannolikt att fortgå, med tanke på det stora antalet aktörer som är inblandade i dagens geopolitiska spänningar. Sådana incidenter kan hindra tillhandahållandet av offentliga tjänster, eftersom cyberattacker ofta riktas mot lokala, regionala eller nationella offentliga tjänster och infrastruktur, varvid lokala myndigheter är särskilt sårbara, bland annat på grund av sina begränsade resurser. De kan också hindra utövandet av ekonomisk verksamhet, även i högkritiska sektorer eller andra kritiska sektorer, leda till betydande ekonomiska förluster, undergräva användarnas förtroende, orsaka stora skador på unionens ekonomi och demokratiska system och till och med få hälsomässiga eller livshotande konsekvenser. Dessutom är cybersäkerhetsincidenter oförutsägbara, eftersom de ofta uppstår och utvecklas mycket snabbt, inte är begränsade till något specifikt geografiskt område och inträffar samtidigt i flera länder eller sprids omedelbart över landsgränserna. Det är viktigt med nära och samordnat samarbete mellan den offentliga sektorn, den privata sektorn, den akademiska världen och medierna.

(3) Det är nödvändigt att stärka konkurrensställningen för industri och tjänster i unionen i hela den digitala ekonomin och stödja deras digitala omställning genom att stärka cybersäkerhetsnivån på den digitala inre marknaden enligt rekommendationerna i tre olika förslag från konferensen om Europas framtid. Det är nödvändigt att öka resiliensen hos medborgare, företag – inbegripet mikroföretag samt små och medelstora företag samt uppstartsföretag – och entiteter som driver kritisk infrastruktur mot de ökande cyberhoten, som kan få förödande samhälleliga och ekonomiska konsekvenser. Därför behövs investeringar i infrastruktur och tjänster samt kapacitetsuppbyggnad för att utveckla cybersäkerhetskompetens som kommer att stödja snabbare upptäckt och hantering av cyberhot och cybersäkerhetsincidenter. Medlemsstaterna behöver också hjälp med att bättre förbereda sig inför**,** hantera och påbörja återhämtningen från betydande cybersäkerhetsincidenter och storskaliga cybersäkerhetsincidenter. Med utgångspunkt i befintliga strukturer och i nära samarbete med dem bör unionen också öka sin kapacitet på dessa områden, särskilt när det gäller insamling och analys av data om cyberhot och cybersäkerhetsincidenter.

(4) Unionen har redan vidtagit ett antal åtgärder för att minska sårbarheterna för och öka resiliensen mot risker hos kritiska infrastrukturer och entiteter, framför allt Europaparlamentets och rådets förordning (EU) 2019/881[5], Europaparlamentets och rådets direktiv 2013/40/EU[6] och (EU) 2022/2555[7] och kommissionens rekommendation (EU) 2017/1584[8]. I rådets rekommendation av den 8 december 2022 om en unionsomfattande samordnad strategi för att stärka den kritiska infrastrukturens motståndskraft uppmanas medlemsstaterna dessutom att vidta åtgärder och att samarbeta med varandra, kommissionen och andra relevanta offentliga myndigheter samt de berörda entiteterna för att öka motståndskraften hos kritisk infrastruktur som används för att tillhandahålla samhällsviktiga tjänster på den inre marknaden.

---

5 Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).

6 Europaparlamentets och rådets direktiv 2013/40/EU av den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF (EUT L 218, 14.8.2013, s. 8).

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 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80).

8 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).

(5) De ökande cybersäkerhetsriskerna och ett överlag sett komplext hotlandskap, med en tydlig risk för att incidenter snabbt sprider sig från en medlemsstat till andra och från ett tredjeland till unionen, kräver att solidariteten på unionsnivå stärks för att det ska bli lättare att upptäcka, förbereda oss inför, hantera och återhämta oss från cyberhot och cybersäkerhetsincidenter, särskilt genom att stärka de befintliga strukturernas kapacitet. I rådets slutsatser av den 23 maj 2022 om utvecklingen av Europeiska unionens arbete på cyberområdet uppmanades kommissionen vidare att lägga fram ett förslag om en ny fond för hantering av cybersäkerhetsincidenter.

(6) I det gemensamma meddelandet från kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik av den 10 november 2022 till Europaparlamentet och rådet om EU:s politik för cyberförsvar tillkännagavs ett EU-cybersolidaritetsinitiativ med målen att stärka EU:s gemensamma upptäckts-, situationsmedvetenhets- och insatsförmåga genom att främja utbyggnaden av en EU-infrastruktur för säkerhetscentrum (SOC), stödja en gradvis uppbyggnad av en cyberreserv på EU-nivå med tjänster från betrodda privata leverantörer samt stödja sårbarhetstestning av kritiska entiteter på grundval av EU:s riskbedömningar.

(7) Det är nödvändigt att förbättra upptäckten av och situationsmedvetenheten om cyberhot och cyberincidenter i hela unionen och att stärka solidariteten genom att öka medlemsstaternas och unionens beredskap och förmåga att förebygga och hantera betydande cybersäkerhetsincidenter och storskaliga cybersäkerhetsincidenter. Därför bör ett europeiskt nätverk av cybernav (*europeiskt system med cybersäkerhetsvarningar*) inrättas för att bygga upp en samordnad kapacitet för upptäckt och situationsmedvetenhet, och stärka unionens förmåga att upptäcka hot och utbyta information. En cybernödmekanism bör skapas för att på begäran från medlemsstaterna hjälpa dem att förbereda sig inför, hantera, mildra effekterna av och initiera återhämtning från betydande cybersäkerhetsincidenter och storskaliga cybersäkerhetsincidenter, och att stödja andra användare när det gäller att hantera betydande cybersäkerhetsincidenter och storskaliga cybersäkerhetsincidenter, och en europeisk mekanism för utvärdering av cybersäkerhetsincidenter bör inrättas för att granska och analysera specifika betydande cybersäkerhetsincidenter eller storskaliga cybersäkerhetsincidenter. De åtgärder som vidtas enligt denna förordning bör genomföras med vederbörlig respekt för medlemsstaternas behörighet och bör komplettera och inte överlappa den verksamhet som bedrivs av CSIRT-nätverket, Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) eller samarbetsgruppen för nät- och informationssäkerhet, alla inrättade genom direktiv (EU) 2022/2555. Dessa åtgärder påverkar inte tillämpningen av artiklarna 107 och 108 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget).

(8) För att uppnå dessa mål är det nödvändigt att ändra Europaparlamentets och rådets förordning (EU) 2021/694[9] på vissa områden. Denna förordning bör ändra förordning (EU) 2021/694 i synnerhet genom att lägga till nya operativa mål med anknytning till det europeiska systemet med cybersäkerhetsvarningar och cybernödmekanismen under specifikt mål nr 3 i programmet för ett digitalt Europa, som syftar till att garantera den digitala inre marknadens resiliens, integritet och tillförlitlighet, öka kapaciteten att bevaka cyberattacker och cyberhot och hantera dem samt stärka det gränsöverskridande samarbetet om och samordningen av cybersäkerhet. Det europeiska systemet med cybersäkerhetsvarningar skulle kunna fylla en viktig funktion för att stödja medlemsstaterna när det gäller att förutse och skydda sig mot cyberhot, och EU-cybersäkerhetsreserven skulle kunna fylla en viktig funktion för att stödja medlemsstaterna, unionens institutioner, organ och byråer samt tredjeländer som är associerade till programmet för digitalt Europa när det gäller att hantera och mildra effekterna av betydande cybersäkerhetsincidenter, storskaliga cybersäkerhetsincidenter och incidenter som är likvärdiga med en storskalig cybersäkerhetsincident. Dessa effekter skulle kunna inbegripa betydande materiell eller ideell skada och allvarliga hot mot den allmänna tryggheten och säkerheten. Mot bakgrund av den särskilda funktion som det europeiska systemet med cybersäkerhetsvarningar och EU-cybersäkerhetsreserven skulle kunna fylla, bör denna förordning ändra förordning (EU) 2021/694 i fråga om deltagandet av rättsliga enheter som är etablerade i unionen men kontrolleras från tredjeländer, där det råder en verklig risk för att nödvändiga och tillräckliga verktyg, infrastrukturer och tjänster, eller teknik, expertis och kapacitet, inte finns i unionen och fördelarna med att inkludera sådana enheter uppväger säkerhetsrisken. De särskilda villkor enligt vilka ekonomiskt stöd kan beviljas för åtgärder som genomför det europeiska systemet med cybersäkerhetsvarningar och EU-cybersäkerhetsreserven bör fastställas och de styrnings- och samordningsmekanismer som krävs för att uppnå de avsedda målen bör definieras. Förordning (EU) 2021/694 bör också ändras genom införande av beskrivningar av föreslagna åtgärder inom ramen för de nya operativa målen samt mätbara indikatorer för att övervaka genomförandet av dessa nya operativa mål.

---

[9] Europaparlamentets och rådets förordning (EU) 2021/694 av den 29 april 2021 om inrättande av programmet för ett digitalt Europa och om upphävande av beslut (EU) 2015/2240 (EUT L 166, 11.5.2021, s. 1).

(9) För att stärka unionens hantering av cyberhot och cybersäkerhetsincidenter är det absolut nödvändigt att samarbeta med internationella organisationer samt med betrodda och likasinnade internationella partner. I detta sammanhang bör betrodda och likasinnade internationella partner förstås som de länder som delar de principer som inspirerade skapandet av unionen, nämligen om demokrati, rättsstaten, de mänskliga rättigheternas och grundläggande friheternas universalitet och odelbarhet, respekt för människors värdighet, jämlikhet och solidaritet, och som respekterar principerna i FN:s stadga och folkrätten, och inte undergräver unionens eller dess medlemsstaters väsentliga säkerhetsintressen. Ett sådant samarbete skulle också kunna gynna de åtgärder som vidtas enligt denna förordning, särskilt det europeiska systemet med cybersäkerhetsvarningar och EU-cybersäkerhetsreserven. Förordning (EU) 2021/694 bör föreskriva, med förbehåll för vissa villkor för tillgänglighet och säkerhet, att anbudsförfaranden med avseende på det europeiska systemet med cybersäkerhetsvarningar och EU-cybersäkerhetsreserven ska vara öppna för rättsliga enheter som kontrolleras från tredjeländer, med förbehåll för säkerhetskrav. När en bedömning görs av säkerhetsrisken med att öppna upp upphandlingsförfarandet på detta sätt är det viktigt att beakta de principer och värden som unionen delar med likasinnade internationella partner, när dessa principer och värden rör unionens väsentliga säkerhetsintressen. När sådana säkerhetskrav övervägs enligt förordning (EU) 2021/694 kan dessutom flera faktorer beaktas, såsom en entitets företagsstruktur och beslutsprocess, säkerheten för uppgifter och säkerhetsskyddsklassificerade eller känsliga uppgifter, och att åtgärdens resultat inte kontrolleras eller begränsas av icke stödberättigade tredjeländer.

(10) Finansieringen av åtgärder enligt denna förordning bör föreskrivas i förordning (EU) 2021/694, som bör förbli den berörda grundakten för åtgärderna inom ramen för specifikt mål nr 3 i programmet för ett digitalt Europa. Särskilda villkor för deltagandet i respektive åtgärd ska föreskrivas i de berörda arbetsprogrammen, i enlighet med förordning (EU) 2021/694.

(11) Övergripande finansiella regler som antas av Europaparlamentet och rådet på grundval av artikel 322 i EUF-fördraget är tillämpliga på denna förordning. De reglerna fastställs i Europaparlamentets och rådets förordning (EU, Euratom) 2024/2509[10] och anger särskilt förfarandet för upprättande och genomförande av unionens budget och föreskriver kontroller av de finansiella aktörernas ansvar. Bland de regler som antagits på grundval av artikel 322 i EUF-fördraget märks även en generell villkorlighetsordning för skydd av unionsbudgeten som fastställs i Europaparlamentets och rådets förordning (EU, Euratom) 2020/2092[11].

---

[10] Europaparlamentets och rådets förordning (EU, Euratom) 2024/2509 av den 23 september 2024 om finansiella regler för unionens allmänna budget (EUT L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

[11] Europaparlamentets och rådets förordning (EU, Euratom) 2020/2092 av den 16 december 2020 om en generell villkorlighetsordning för skydd av unionsbudgeten (EUT L 433 I, 22.12.2020, s. 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).

(12) Förebyggande åtgärder och beredskapsåtgärder är avgörande för att öka unionens resiliens när det gäller att hantera betydande cybersäkerhetsincidenter, storskaliga cybersäkerhetsincidenter och incidenter som är likvärdiga med en storskalig cybersäkerhetsincident, men förekomsten, tidpunkten och omfattningen av sådana incidenter är till sin natur oförutsägbar. De ekonomiska resurser som krävs för att säkerställa adekvat hantering kan variera kraftigt från år till år och bör kunna göras tillgängliga omedelbart. En sammanjämkning av budgetprincipen om förutsebarhet och behovet av att reagera snabbt på nya behov kräver därför en anpassning av det finansiella genomförandet av arbetsprogrammen. Det är därför lämpligt att tillåta överföring av outnyttjade anslag, men endast till det följande året och endast till EU-cybersäkerhetsreserven och åtgärderna till stöd för ömsesidigt bistånd, utöver den överföring av anslag som godkänts enligt artikel 12.4 i förordning (EU, Euratom) 2024/2509.

(13) För att mer effektivt förebygga, analysera, hantera och återhämta sig från cyberhot och cyberincidenter är det nödvändigt att utveckla mer omfattande kunskap om hoten mot kritiska tillgångar och kritisk infrastruktur på unionens territorium, inbegripet deras geografiska spridning, sammanlänkning och potentiella effekter i händelse av cyberattacker som påverkar denna infrastruktur. En proaktiv strategi för att identifiera, begränsa och förebygga cyberhot inbegriper en ökad kapacitet när det gäller den avancerade förmågan att upptäcka cyberhot. Det europeiska systemet med cybersäkerhetsvarningar bör bestå av flera interoperativa gränsöverskridande cybernav som vart och ett omfattar tre eller flera nationella cybernav. Denna infrastruktur bör tjäna nationella och europeiska cybersäkerhetsintressen och cybersäkerhetsbehov genom att utnyttja den senaste tekniken för avancerad insamling av relevanta data och relevant information, när så är lämpligt i anonymiserad form, samt dataanalys, förbättra den samordnade kapaciteten för upptäckt och hantering av cyberhot och tillhandahålla situationsmedvetenhet i realtid. Denna infrastruktur bör tjäna till att förbättra arbetet på cyberområdet genom att öka upptäckten, aggregeringen och analysen av data och information i syfte att förebygga cyberhot och cybersäkerhetsincidenter och därigenom komplettera och stödja unionens entiteter och nätverk med ansvar för cyberkrishantering i unionen, särskilt EU-CyCLONe.

(14) Det är frivilligt för medlemsstaterna att delta i det europeiska systemet med cybersäkerhetsvarningar. Varje medlemsstat bör utse en enda entitet som på nationell nivå har till uppgift att samordna åtgärder för att upptäcka cyberhot i den medlemsstaten. Dessa nationella cybernav bör fungera som referenspunkt och gränssnitt på nationell nivå för deltagande i det europeiska systemet med cybersäkerhetsvarningar och bör säkerställa att information om cyberhot från offentliga och privata entiteter utbyts och samlas in på nationell nivå på ett effektivt och enhetligt sätt. Nationella cybernav skulle kunna stärka samarbetet och informationsutbytet mellan offentliga och privata entiteter och skulle också kunna stödja utbytet av relevanta data och relevant information med relevanta sektorsspecifika och sektorsövergripande grupper, inbegripet relevanta informations- och analyscentraler (ISAC) inom industrin. Ett nära och samordnat samarbete mellan offentliga och privata entiteter är centralt för att stärka unionens cyberresiliens. Sådant samarbete är särskilt värdefullt i samband med utbyte av underrättelseinformation om cyberhot för att förbättra det aktiva cyberskyddet. Som en del av sådant samarbete och informationsutbyte skulle de nationella cybernaven kunna begära och ta emot specifik information. Dessa nationella cybernav är varken skyldiga eller bemyndigade genom denna förordning att se till att sådana begäranden verkställs. När så är lämpligt och i enlighet med unionsrätten och nationell rätt skulle den begärda eller mottagna informationen kunna omfatta telemetri-, sensor- eller loggningsdata från entiteter, såsom leverantörer av utlokaliserade säkerhetstjänster, som är verksamma inom högkritiska sektorer eller andra kritiska sektorer inom den medlemsstaten, i syfte att förbättra förmågan att snabbt upptäcka potentiella cyberhot och cybersäkerhetsincidenter i ett tidigare skede och därigenom förbättra situationsmedvetenheten. Om det nationella cybernavet inte är den behöriga myndighet som utsetts eller inrättats av den berörda medlemsstaten enligt artikel 8.1 i direktiv (EU) 2022/2555 är det av avgörande vikt att den samordnar med den behöriga myndigheten när det gäller begäranden om och mottagande av sådana data.

(15) Som en del av det europeiska systemet med cybersäkerhetsvarningar bör ett antal gränsöverskridande cybernav inrättas. Dessa gränsöverskridande cybernav bör sammanföra nationella cybernav från minst tre medlemsstater, för att säkerställa att fördelarna med gränsöverskridande hotupptäckt och informationsutbyte och hantering kan utnyttjas fullt ut. Det allmänna målet med gränsöverskridande cybernav bör vara att stärka kapaciteten att analysera, förebygga och upptäcka cyberhot och stödja produktionen av högkvalitativ underrättelseinformation om cyberhot, i synnerhet genom delning av relevant information, när så är lämpligt i anonymiserad form, i en betrodd och säker miljö, från olika offentliga eller privata källor samt genom delning och gemensam användning av förstklassiga verktyg och gemensam utveckling av kapacitet för upptäckt, analys och förebyggande i en betrodd och säker miljö. De gränsöverskridande cybernaven bör tillhandahålla ny ytterligare kapacitet som bygger på och kompletterar befintliga säkerhetscentrum, CSIRT-enheter och andra relevanta aktörer, däribland CSIRT-nätverket.

(16) En medlemsstat som väljs ut av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning (Europeiska kompetenscentrumet för cybersäkerhet), inrättat genom Europaparlamentets och rådets förordning (EU) 2021/887[12], efter en inbjudan att anmäla intresse för att inrätta, eller förbättra kapaciteten hos, ett nationellt cybernav bör gemensamt med Europeiska kompetenscentrumet för cybersäkerhet köpa in relevanta verktyg, infrastruktur eller tjänster. En sådan medlemsstat bör vara berättigad till ett bidrag för att driva verktygen, infrastrukturen eller tjänsterna. Ett värdkonsortium bestående av minst tre medlemsstater som valts ut av europeiska kompetenscentrumet för cybersäkerhet efter en inbjudan att anmäla intresse för att inrätta eller förbättra kapaciteten hos ett gränsöverskridande cybernav, bör köpa in relevanta verktyg, infrastruktur eller tjänster gemensamt med Europeiska kompetenscentrumet för cybersäkerhet. Detta värdkonsortium bör vara berättigat till bidrag för att driva verktygen, infrastrukturen eller tjänsterna. Upphandlingsförfarandet för inköp av relevanta verktyg, infrastruktur eller tjänster bör genomföras tillsammans med Europeiska kompetenscentrumet för cybersäkerhet och relevanta upphandlande myndigheter från de medlemsstater som valts ut efter en sådan inbjudan att anmäla intresse. Sådan upphandling bör vara förenlig med artikel 168.2 i förordning (EU, Euratom) 2024/2509 och de finansiella bestämmelserna för Europeiska kompetenscentrumet för cybersäkerhet. Privata entiteter bör därför inte vara berättigade att delta i inbjudningar att anmäla intresse för att köpa in verktyg, infrastruktur eller tjänster gemensamt med Europeiska kompetenscentrumet för cybersäkerhet, eller att få bidrag för att driva dessa verktyg, infrastrukturer och tjänster. Medlemsstaterna bör dock ha möjlighet att involvera privata entiteter när det gäller att inrätta, förbättra och driva sina nationella cybernav och gränsöverskridande cybernav på andra sätt som de anser vara lämpliga, i enlighet med unionsrätten och nationell rätt. Privata entiteter skulle också kunna vara berättigade till unionsfinansiering enligt förordning (EU) 2021/887 i syfte att tillhandahålla stöd för nationella cybernav.

---

[12] Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum (EUT L 202, 8.6.2021, s. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

(17) För att förbättra upptäckten av cyberhot och situationsmedvetenheten i unionen bör en medlemsstat som efter en inbjudan att anmäla intresse har valts ut för att inrätta eller förbättra kapaciteten hos ett nationellt cybernav åta sig att ansöka om att delta i ett gränsöverskridande cybernav. Om en medlemsstat inte deltar i ett gränsöverskridande cybernav inom två år från den dag då verktygen, infrastrukturen eller tjänsterna förvärvas eller då den får bidragsfinansiering, beroende på vilket som inträffar först, bör den inte vara berättigad att delta i unionens ytterligare stödåtgärder inom ramen för det europeiska systemet med cybersäkerhetsvarningar för att förbättra sitt nationella cybernavs kapacitet. I sådana fall skulle entiteter från medlemsstaterna fortfarande kunna delta i ansökningsomgångar med anknytning till andra ämnen inom ramen för programmet för ett digitalt Europa eller andra av unionens finansieringsprogram, inbegripet ansökningsomgångar avseende kapacitet för upptäckt av cyberhot och informationsutbyte, förutsatt att dessa entiteter uppfyller de kriterier för stödberättigande som fastställs i de programmen.

(18) CSIRT-enheterna utbyter information inom CSIRT-nätverket, i enlighet med direktiv (EU) 2022/2555. Det europeiska systemet med cybersäkerhetsvarningar bör utgöra en ny kapacitet som kompletterar CSIRT-nätverket genom att bidra till att bygga upp en situationsmedvetenhet i unionen som gör det möjligt att stärka CSIRT-nätverkets kapacitet. Gränsöverskridande cybernav bör samordna och samarbeta nära med CSIRT-nätverket. De bör agera genom att samla data och utbyta relevantinformation, när så är lämpligt i anonymiserad form, om cyberhot från offentliga och privata entiteter, öka värdet av sådana data och sådan information genom expertanalyser och gemensamt förvärvade infrastrukturer och förstklassiga verktyg, och bidra till unionens tekniska suveränitet, dess öppna strategiska oberoende, konkurrenskraft och resiliens samt till utvecklingen av unionens kapacitet.

(19) De gränsöverskridande cybernaven bör fungera som centrala punkter som möjliggör en bred sammanslagning av relevanta data och underrättelseinformation om cyberhot samt göra det möjligt att sprida hotinformation till en mängd olika typer av intressenter, såsom incidenthanteringsorganisationer (CERT), CSIRT-enheter, informations- och analyscentraler (ISAC) och operatörer av kritisk infrastruktur. Värdkonsortiets medlemmar bör i konsortieavtalet ange vilken relevant information som ska delas mellan deltagarna i det berörda gränsöverskridande cybernavet. Exempel på information som kan utbytas mellan deltagarna i ett gränsöverskridande cybernav är data från nätverk och sensorer, hotunderrättelseflöden, angreppsindikatorer och kontextualiserad information om incidenter, cyberhot, tillbud, sårbarheter, tekniker och förfaranden, kontradiktorisk taktik, specifik information om hotaktörer, cybersäkerhetsvarningar och rekommendationer om konfigurationen av cybersäkerhetsverktyg för att upptäcka cyberattacker. Dessutom bör gränsöverskridande cybernav också ingå samarbetsavtal med varandra. I sådan samarbetsavtal bör särskilt principer för informationsutbyte och interoperabilitet anges. Villkoren om interoperabilitet i dessa, särskilt format och protokoll för informationsutbyte, bör vägledas av och därför utgå från de riktlinjer för interoperabilitet som utfärdats av Europeiska unionens cybersäkerhetsbyrå (Enisa) som inrättats genom förordning (EU) 2019/881. Dessa riktlinjer bör utfärdas snabbt för att säkerställa att de i ett tidigt skede kan beaktas av gränsöverskridande cybernav. De bör ta hänsyn till internationella standarder och bästa praxis samt funktionen hos befintliga gränsöverskridande cybernav.

(20) De gränsöverskridande cybernaven och CSIRT-nätverket bör ha ett nära samarbete för att säkerställa synergier och komplementaritet i verksamheten. I detta syfte bör de komma överens om förfaranden för samarbete och utbyte av relevant information. Detta skulle kunna inbegripa att relevant information om cyberhot och betydande cybersäkerhetsincidenter utbyts, och att erfarenheter av förstklassiga verktyg, i synnerhet artificiell intelligens och dataanalysteknik, som används inom de gränsöverskridande cybernaven, delas med CSIRT-nätverket.

(21) Gemensam situationsmedvetenhet mellan berörda myndigheter är en nödvändig förutsättning för unionsomfattande beredskap och samordning när det gäller betydande cybersäkerhetsincidenter och storskaliga cybersäkerhetsincidenter. Genom direktiv (EU) 2022/2555 inrättades EU-CyCLONe för att stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och cyberkriser på operativ nivå och säkerställa ett regelbundet utbyte av relevant information mellan medlemsstaterna och unionens institutioner, organ och byråer. Genom direktiv (EU) 2022/2555 inrättades även CSIRT-nätverket för att främja snabbt och effektivt operativt samarbete mellan alla medlemsstater. För att säkerställa situationsmedvetenhet och stärka solidariteten i situationer där gränsöverskridande cybernav får information om en potentiell eller pågående storskalig cybersäkerhetsincident bör de därför tillhandahålla relevant information till CSIRT-nätverket och, som en tidig varning, informera EU-CyCLONe. Beroende på situationen skulle den information som ska utbytas i synnerhet kunna inbegripa tekniska uppgifter, uppgifter om angriparens eller den potentiella angriparens karaktär och motiv samt icke-teknisk information på högre nivå om en potentiell eller pågående storskalig cybersäkerhetsincident. I detta sammanhang bör vederbörlig hänsyn tas till principen om behovsenlig behörighet och den delade informationens potentiellt känsliga art. I direktiv (EU) 2022/2555 erinras också om kommissionens ansvar inom ramen för unionens civilskyddsmekanism, som inrättades genom Europaparlamentets och rådets beslut 1313/2013/EU[13], och dess ansvar för att tillhandahålla de analytiska rapporterna för EU-arrangemangen för integrerad politisk krishantering (IPCR-arrangemangen) enligt rådets genomförandebeslut (EU) 2018/1993[14].

---

13 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, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).

14 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, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

När gränsöverskridande cybernav utbyter relevant information och tidiga varningar om en potentiell eller pågående storskalig cybersäkerhetsincident med EU-CyCLONe och CSIRT-nätverket är det absolut nödvändigt att utbyta denna information via dessa nätverk med medlemsstaternas myndigheter samt med kommissionen. I detta avseende föreskrivs i direktiv (EU) 2022/2555 att syftet med EU-CyCLONe är att stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och cyberkriser på operativ nivå och säkerställa ett regelbundet utbyte av relevant information mellan medlemsstaterna och unionens institutioner, organ och byråer. I EU-CyCLONes uppgifter ingår bland annat att utveckla en gemensam situationsmedvetenhet om sådana incidenter och kriser. Det är av yttersta vikt att EU-CyCLONe, i linje med detta syfte och sina uppgifter, säkerställer att sådan information tillhandahålls omedelbart till med de berörda medlemsstaternas företrädare och till kommissionen. Det är därför mycket viktigt att EU-CyCLONes arbetsordning innehåller lämpliga bestämmelser i detta avseende.

(22) Entiteter som deltar i det europeiska systemet med cybersäkerhetsvarningar bör säkerställa en hög grad av interoperabilitet sinsemellan, även, i enlighet med vad som är lämpligt, när det gäller dataformat, taxonomi och verktyg för datahantering och dataanalys. De bör även säkerställa säkra kommunikationskanaler, en miniminivå av säkerhet i applikationslagret, en informationspanel för situationsmedvetenhet och indikatorer. Vid antagandet av en gemensam taxonomi och utarbetandet av en mall för situationsrapporter för att beskriva orsakerna till de upptäckta cyberhoten och riskerna bör det arbete som sker i samband med genomförandet av direktiv (EU) 2022/2555 beaktas.

(23) För att möjliggöra utbyte av relevanta data och relevant information om cyberhot från olika källor i stor skala i en tillförlitlig och säker miljö bör entiteter som deltar i det europeiska systemet med cybersäkerhetsvarningar utrustas med förstklassiga verktyg, utrustning och infrastrukturer som har hög säkerhet samt kvalificerad personal. Detta bör göra det möjligt att förbättra den kollektiva upptäcktskapaciteten och ge varningar i rätt tid till myndigheter och berörda entiteter, särskilt genom att använda den senaste AI-tekniken (artificiell intelligens) och dataanalystekniken.

(24) Genom att samla in, analysera, dela och utbyta relevanta data och relevant information bör det europeiska systemet med cybersäkerhetsvarningar förbättra unionens tekniska suveränitet och öppna strategiska oberoende på cybersäkerhetsområdet samt dess konkurrenskraft och resiliens. Sammanslagningen av högkvalitativa kurerade data kan också bidra till utvecklingen av avancerad AI-teknik och dataanalysteknik. Mänsklig tillsyn och således en kvalificerad arbetskraft är fortfarande avgörande för en effektiv sammanslagning av högkvalitativa data.

(25) Även om det europeiska systemet med cybersäkerhetsvarningar är ett civilt projekt skulle cyberförsvarsgemenskapen gynnas av starkare civil kapacitet för upptäckt och situationsmedvetenhet vilken utvecklats för att skydda kritisk infrastruktur.

(26) Informationsutbytet mellan deltagarna i det europeiska systemet med cybersäkerhetsvarningar bör vara förenligt med befintliga rättsliga krav, särskilt unionens och medlemsstaternas dataskyddslagstiftning och unionens konkurrensregler som reglerar informationsutbyte. Mottagaren av informationen bör, i den mån behandlingen av personuppgifter är nödvändig, vidta tekniska och organisatoriska åtgärder som skyddar registrerades rättigheter och friheter, och förstöra uppgifterna så snart de inte längre är nödvändiga för det angivna ändamålet och informera den entitet som tillhandahöll uppgifterna om att uppgifterna har förstörts.

(27) Att bevara konfidentialitet och informationssäkerhet är av yttersta vikt för alla tre pelare i denna förordning, oavsett om det gäller att uppmuntra informationsutbyte inom ramen för det europeiska systemet med cybersäkerhetsvarningar, bevara de entiteters intressen som ansöker om stöd inom ramen för cybernödmekanismen eller säkerställa att rapporter inom ramen för den europeiska mekanismen för utvärdering av cybersäkerhetsincidenter ger värdefulla lärdomar utan att inverka negativt på de entiteter som påverkas av incidenterna. Medlemsstaternas och entiteternas deltagande i dessa mekanismer är beroende av att det finns ett förtroende mellan deras delar. Om informationen är konfidentiell enligt unionsregler eller nationella regler bör utbytet av den enligt denna förordning begränsas till det som är relevant och står i proportion till syftet med utbytet. Ett sådant utbyte bör också bevara konfidentialiteten i denna information, inbegripet skydd av alla berörda entiteters säkerhetsintressen och kommersiella intressen. Informationsutbyte enligt denna förordning skulle kunna ske med användning av avtal om konfidentialitet eller vägledning om informationsspridning, t.ex. Traffic Light Protocol (TLP). TLP ska betraktas som ett sätt att tillhandahålla information om eventuella begränsningar när det gäller ytterligare spridning av information. Det används i nästan alla CSIRT-enheter och i vissa informations- och analyscentraler. Utöver dessa allmänna krav bör värdkonsortieavtal, när det gäller det europeiska systemet med cybersäkerhetsvarningar, fastställa särskilda regler för de villkor som rör informationsutbytet inom det berörda gränsöverskridande cybernavet. Dessa avtal skulle framför allt kunna kräva att information endast utbyts i enlighet med unionsrätten och nationell rätt.

(28) När det gäller användningen av EU-cybersäkerhetsreserven krävs särskilda regler om konfidentialitet. Stöd kommer att begäras, bedömas och tillhandahållas i en krissituation och till entiteter som är verksamma inom känsliga sektorer. För att EU-cybersäkerhetsreserven ska fungera effektivt är det viktigt att användare och entiteter utan dröjsmål kan utbyta och ge tillgång till all information som behövs för att varje entitet ska kunna fylla sin funktion när det gäller att bedöma begäranden och sätta in stöd. I denna förordning bör det därför föreskrivas att all sådan information endast får användas eller utbytas när det är nödvändigt för driften av EU-cybersäkerhetsreserven, och att information som är konfidentiell eller säkerhetsskyddsklassificerad enligt unionsrätten och nationell rätt endast får användas och delas i enlighet med den rätten. Dessutom bör användarna, när så är lämpligt, kunna använda protokoll för informationsutbyte, såsom Traffic Light Protocol, för att ytterligare specificera begränsningar. Även om användarna ges utrymme för skönsmässig bedömning i detta avseende är det viktigt att de vid tillämpningen av sådana begränsningar tar hänsyn till eventuella konsekvenser, särskilt när det gäller en försenad bedömning eller leverans av de begärda tjänsterna. För att EU-cybersäkerhetsreserven ska vara effektiv är det viktigt att den upphandlande myndigheten klargör dessa konsekvenser för användaren innan den lämnar in en begäran. Dessa skyddsåtgärder är begränsade till begäran om och tillhandahållandet av EU-cybersäkerhetsreservens tjänster och påverkar inte informationsutbytet i andra sammanhang, t.ex. vid upphandlingen av EU-cybersäkerhetsreserven.

(29) Med tanke på de ökande riskerna och antalet incidenter som påverkar medlemsstaterna är det nödvändigt att inrätta ett krisstödsinstrument, nämligen cybernödmekanismen, för att förbättra unionens resiliens mot betydande cybersäkerhetsincidenter, storskaliga cybersäkerhetsincidenter och incidenter som är likvärdiga med en storskalig cybersäkerhetsincident och komplettera medlemsstaternas åtgärder genom ekonomiskt krisstöd för beredskap, incidenthantering och initial återställning av samhällsviktiga tjänster. Eftersom en fullständig återhämtning från en incident är en omfattande process där funktionen hos en berörd entitet ska återställas till det skick som den var i före incidenten, vilket kan bli en lång process som medför betydande kostnader, bör stödet från EU-cybersäkerhetsreserven begränsas till det inledande skedet av återhämtningsprocessen som innebär att systemens grundläggande funktioner återställs. Cybernödmekanismen bör göra det möjligt att snabbt och effektivt sätta in bistånd under fastställda omständigheter och på tydliga villkor samt möjliggöra en noggrann övervakning och utvärdering av hur resurserna har använts. Cybernödmekanismen främjar solidaritet mellan medlemsstaterna i enlighet med artikel 3.3 i fördraget om Europeiska unionen (EU-fördraget), även om det alltjämt är medlemsstaterna som har det primära ansvaret för förebyggande av, beredskap inför och hantering av incidenter och kriser.

(30) Cybernödmekanismen bör ge medlemsstaterna stöd som kompletterar deras egna åtgärder och resurser och andra befintliga stödalternativ vid insatser mot och initial återhämtning från betydande cybersäkerhetsincidenter och storskaliga cybersäkerhetsincidenter, såsom de tjänster som tillhandahålls av Enisa i enlighet med dess mandat, de samordnade insatserna och biståndet från CSIRT-nätverket, stödet till begränsningsåtgärder från EU-CyCLONe samt ömsesidigt bistånd mellan medlemsstaterna, bland annat inom ramen för artikel 42.7 i EU-fördraget och de snabbinsatsteam för cybersäkerhet inom ramen för permanent strukturerat samarbete (Pesco) som inrättats på grundval av rådets beslut (Gusp) 2017/2315[15]. Den bör vara ett svar på behovet av att säkerställa att särskilda medel finns tillgängliga för att stödja beredskap inför, insatser vid och återhämtning från sådana incidenter i hela unionen och i tredjeländer som är associerade till programmet för ett digitalt Europa.

[15] Rådets beslut (Gusp) 2017/2315 av den 11 december 2017 om upprättande av permanent strukturerat samarbete och om fastställande av förteckningen över deltagande medlemsstater (EUT L 331, 14.12.2017, s. 57, ELI: http://data.europa.eu/eli/dec/2017/2315/2023-05-23).

(31) Denna förordning påverkar inte förfaranden och ramar för samordning av krishantering på unionsnivå, särskilt direktiv (EU) 2022/2555, unionens civilskyddsmekanism inrättad genom Europaparlamentets och rådets beslut nr 1313/2013/EU[16], IPCR-arrangemang och kommissionens rekommendation (EU) 2017/1584[17]. Stöd inom ramen för cybernödmekanismen kan komplettera det bistånd som ges inom ramen för den gemensamma utrikes- och säkerhetspolitiken och den gemensamma säkerhets- och försvarspolitiken, däribland genom snabbinsatsteam för cybersäkerhet, med hänsyn till cybernödmekanismens civila karaktär. Stöd inom ramen för cybernödmekanismen kan komplettera åtgärder som genomförs inom ramen för artikel 42.7 i EU-fördraget, inbegripet bistånd från en medlemsstat till en annan medlemsstat, eller utgöra en del av unionens och medlemsstaternas gemensamma insatser eller i situationer som avses i artikel 222 i EUF-fördraget. Genomförandet av denna förordning bör också samordnas med genomförandet av de åtgärder som föreskrivs i verktygslådan för cyberdiplomati, när så är lämpligt.

---

16 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).

17 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).

(32) Bistånd som ges enligt denna förordning bör stödja och komplettera de åtgärder som vidtas av medlemsstaterna på nationell nivå. Därför bör nära samarbete och samråd mellan kommissionen, Enisa, medlemsstaterna och, i förekommande fall, Europeiska kompetenscentrumet för cybersäkerhet säkerställas. När medlemsstaterna begär stöd inom ramen för cybernödmekanismen bör de tillhandahålla relevant information som motiverar behovet av stöd.

(33) Enligt direktiv (EU) 2022/2555 är medlemsstaterna skyldiga att utse eller inrätta en eller flera myndigheter för hantering av cyberkriser och säkerställa att de har tillräckliga resurser för att kunna utföra sina uppgifter på ett ändamålsenligt och effektivt sätt. I direktivet åläggs medlemsstaterna också att identifiera vilka kapaciteter, tillgångar och förfaranden som kan användas i händelse av en kris och att anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser, där mål och villkor för hanteringen av storskaliga cybersäkerhetsincidenter och kriser fastställs. Medlemsstaterna är också skyldiga att inrätta en eller flera CSIRT-enheter som ansvarar för incidenthantering i enlighet med ett tydligt fastställt förfarande och som omfattar minst de sektorer, delsektorer och typer av entiteter som direktivet är tillämpligt på, samt att säkerställa att CSIRT-enheterna har tillräckliga resurser för att på ett ändamålsenligt sätt kunna utföra sina uppgifter. Denna förordning påverkar inte kommissionens roll när det gäller att säkerställa att medlemsstaterna fullgör sina skyldigheter enligt direktiv (EU) 2022/2555. Cybernödmekanismen bör ge bistånd till beredskapshöjande åtgärder och incidenthanteringsåtgärder för att minska konsekvenserna av betydande cybersäkerhetsincidenter och storskaliga cybersäkerhetsincidenter, stödja initial återhämtning eller återställa väsentliga funktioner i de tjänster som tillhandahålls av de entiteter som är verksamma inom högkritiska sektorer eller entiteter verksamma i andra kritiska sektorer.

(34) För att främja en konsekvent strategi och stärka säkerheten i hela unionen och på dess inre marknad bör stöd som en del av beredskapsåtgärderna ges till samordnad testning och bedömning av cybersäkerheten hos entiteter som är verksamma i högkritiska sektorer som identifierats i enlighet med direktiv (EU) 2022/2555, bland annat genom övning och fortbildning. I detta syfte bör kommissionen, efter samråd med Enisa, samarbetsgruppen för nät- och informationssäkerhet och EU-CyCLONe, regelbundet identifiera relevanta sektorer eller delsektorer som bör vara berättigade till ekonomiskt stöd för samordnad beredskapstestning på unionsnivå. Sektorerna eller delsektorerna bör väljas från de högkritiska sektorer som förtecknas i bilaga I till direktiv (EU) 2022/2555. De samordnade beredskapstesterna bör baseras på gemensamma riskscenarier och metoder.

Vid valet av sektorer och utarbetandet av riskscenarier bör man för att undvika dubbelarbete ta hänsyn till relevanta unionsomfattande riskbedömningar och riskscenarier, såsom den riskbedömning och de riskscenarier som rådet efterlyste i sina slutsatser om utvecklingen av Europeiska unionens arbete på cyberområdet som utförs av kommissionen, unionens höga representanten för utrikes frågor och säkerhetspolitik (*den höga representanten*) och samarbetsgruppen för nät- och informationssäkerhet i samordning med relevanta civila och militära organ och byråer samt etablerade nätverk, inbegripet EU-CyCLONe, samt den riskbedömning av kommunikationsnät och kommunikationsinfrastruktur som begärts i den gemensamma uppmaningen från ministermötet i Nevers och som utförts av samarbetsgruppen för nät- och informationssäkerhet med stöd av kommissionen och Enisa, och i samarbete med Organet för europeiska regleringsmyndigheter för elektronisk kommunikation inrättat genom Europaparlamentets och rådets förordning (EU) 2018/1971[18], de samordnade säkerhetsriskbedömningar på unionsnivå av kritiska leveranskedjor som ska utföras enligt artikel 22 i direktiv (EU) 2022/2555 samt testningen av digital operativ motståndskraft i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554[19]. Sektorerna bör även väljas med beaktande av rådets rekommendation om en unionsomfattande samordnad strategi för att stärka den kritiska infrastrukturens motståndskraft.

---

[18] Europaparlamentets och rådets förordning (EU) 2018/1971 av den 11 december 2018 om inrättande av Organet för europeiska regleringsmyndigheter för elektronisk kommunikation (Berec) och Byrån för stöd till Berec (Berecbyrån), om ändring av förordning (EU) 2015/2120 och om upphävande av förordning (EG) nr 1211/2009 (EUT L 321, 17.12.2018, s. 1).

[19] Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1).

(35) Dessutom bör cybernödmekanismen stödja andra beredskapsåtgärder och beredskap inom andra sektorer som inte omfattas av den samordnade testningen av entiteter som är verksamma i högkritiska sektorer eller entiteter verksamma i andra kritiska sektorer. Det kan till exempel röra sig om olika typer av nationell beredskapsverksamhet.

(36) När medlemsstaterna får bidrag för att stödja beredskapsåtgärder kan entiteter i högkritiska sektorer delta i dessa åtgärder på frivillig basis. Det är god praxis att de deltagande entiteterna efter sådana åtgärder utarbetar en åtgärdsplan i syfte att genomföra eventuella resulterande rekommendationer om specifika åtgärder för att i största möjliga utsträckning dra nytta av beredskapsåtgärden. Även om det är viktigt att medlemsstaterna som en del av åtgärderna begär att deltagande entiteter utarbetar och genomför sådana åtgärdsplaner, är medlemsstaterna varken skyldiga eller bemyndigade att genom denna förordning se till att sådana begäranden verkställs. Sådana begäranden påverkar inte krav på entiteter och tillsynsbefogenheter för behöriga myndigheter i enlighet med direktiv (EU) 2022/2555.

(37) Cybernödmekanismen bör också stödja incidenthanteringsåtgärder för att mildra konsekvenserna av betydande cybersäkerhetsincidenter, storskaliga cybersäkerhetsincidenter och incidenter som är likvärdiga med en storskalig cybersäkerhetsincident, stödja initial återhämtning eller återställa samhällsviktiga tjänsters funktion. När så är lämpligt bör den komplettera civilskyddsmekanismen för att säkerställa ett heltäckande sätt att hantera incidenters konsekvenser för medborgarna.

(38) Cybernödmekanismen bör stödja tekniskt bistånd som en medlemsstat ger till en annan. Medlemsstater som påverkas av en betydande cybersäkerhetsincident eller storskalig cybersäkerhetsincident, även bistånd från CSIRT-enheter som avses i artikel 11.3 f i direktiv (EU) 2022/2555. Medlemsstater som ger sådant bistånd bör få begära ersättning för kostnader i samband med utsändning av expertgrupper inom ramen för ömsesidigt bistånd. Kostnader för exempelvis resor, inkvartering och dagtraktamenten för cybersäkerhetsexperter skulle kunna berättiga till ersättning.

(39) Med tanke på den viktiga roll som privata företag spelar för upptäckt, beredskap och hantering av storskaliga cybersäkerhetsincidenter och incidenter som är likvärdiga med en storskalig cybersäkerhetsincident, är det viktigt att erkänna värdet av ideellt samarbete med sådana företag, varigenom de erbjuder tjänster utan ersättning i samband med storskaliga cybersäkerhetsincidenter och kriser liksom incidenter som är likvärdiga med en storskalig cybersäkerhetsincident och kriser. Enisa skulle i samarbete med EU-CyCLONe kunna övervaka utvecklingen av sådana ideella initiativ och verka för att de uppfyller de kriterier som är tillämpliga på betrodda leverantörer av utlokaliserade säkerhetstjänster enligt denna förordning, inbegripet när det gäller privata företags tillförlitlighet, deras erfarenhet och förmåga att hantera känslig information på ett säkert sätt.

(40) Som en del av cybernödmekanismen bör en EU-cybersäkerhetsreserv gradvis inrättas, bestående av tjänster från betrodda leverantörer av utlokaliserade säkerhetstjänster för att stödja insatser och initiera återhämtningsåtgärder i händelse av betydande cybersäkerhetsincidenter, storskaliga cybersäkerhetsincidenter eller incidenter som är likvärdiga med en storskalig cybersäkerhetsincident som påverkar medlemsstater, unionens institutioner, organ eller byråer eller tredjeländer som är associerade till programmet för ett digitalt Europa. EU-cybersäkerhetsreserven bör säkerställa tjänsternas tillgänglighet och beredskap. Den bör därför omfatta tjänster som ställts till förfogande på förhand, till exempel beredskapskapacitet och kapacitet som kan sättas in med kort varsel. Tjänsterna från EU-cybersäkerhetsreserven bör stödja de nationella myndigheterna när det gäller att bistå berörda entiteter som är verksamma i högkritiska sektorer eller berörda entiteter som är verksamma i andra kritiska sektorer, som ett komplement till deras egna åtgärder på nationell nivå. Tjänsterna från EU-cybersäkerhetsreserven bör också kunna användas för att stödja unionens institutioner, organ och byråer på liknande villkor. EU-cybersäkerhetsreserven skulle också kunna bidra till att i hela den digitala ekonomin stärka konkurrensställningen för industri och tjänster i unionen, inbegripet mikroföretag och små och medelstora företag samt uppstartsföretag, bland annat genom att tillhandahålla incitament för investeringar i forskning och innovation. Det är viktigt att ta hänsyn till Enisas europeiska ram för cyberkompetens vid upphandling av tjänster till EU-cybersäkerhetsreserven. När användarna begär stöd från EU-cybersäkerhetsreserven bör de i sin ansökan inkludera lämplig information om den berörda entiteten och potentiella effekter, information om den begärda tjänsten från EU-cybersäkerhetsreserven och det stöd som ges till den berörda entiteten på nationell nivå, vilket bör beaktas vid bedömningen av den sökandes begäran. För att säkerställa komplementaritet med andra former av stöd som är tillgängliga för den berörda entiteten, bör begäran också inkludera, om den finns tillgänglig, information om avtalsarrangemang för tjänster som avser incidenthantering och initial återhämtning, samt försäkringsavtal som skulle kunna täcka sådana typer av incidenter.

(41) För att säkerställa en effektiv användning av unionsmedel bör tjänster som ställts till förfogande på förhand inom ramen för EU-cybersäkerhetsreserven, i enlighet med det relevanta avtalet, kunna omvandlas till beredskapstjänster som rör förebyggande och hantering av incidenter, om dessa tjänster som ställts till förfogande på förhand inte används för incidenthantering under den tid som de ställs till förfogande på förhand. Dessa tjänster bör komplettera varandra och inte överlappa de beredskapsåtgärder som ska förvaltas av Europeiska kompetenscentrumet för cybersäkerhet.

(42) Begäranden om stöd från EU-cybersäkerhetsreserven från medlemsstaternas cyberkrishanteringsmyndigheter och CSIRT-enheter, eller CERT-EU, på uppdrag av unionens institutioner, organ och byråer, bör bedömas av den upphandlande myndigheten. När Enisa har anförtrotts förvaltningen och driften av EU-cybersäkerhetsreserven är Enisa upphandlande myndighet. Begäranden om stöd från tredjeländer som är associerade till programmet för ett digitalt Europa bör bedömas av kommissionen. För att underlätta inlämning och bedömning av begäranden om stöd skulle Enisa kunna inrätta en säker plattform.

(43) Om flera parallella begäranden tas emot, bör dessa prioriteras i enlighet med de kriterier som fastställs i denna förordning. Mot bakgrund av de allmänna målen för denna förordning bör dessa kriterier inbegripa incidentens omfattning och allvarlighetsgrad, typ av berörd entitet, incidentens potentiella konsekvenser för medlemsstaterna och berörda användare, incidentens potentiella gränsöverskridande karaktär och risken för spridning samt de åtgärder som vidtagits av användaren för att bistå insatser och initial återhämtning. Mot bakgrund av dessa mål och med tanke på att begäranden från användare i medlemsstaterna uteslutande är avsedda att stödja, i hela unionen, entiteter som är verksamma inom högkritiska sektorer eller entiteter verksamma i andra kritiska sektorer, är det lämpligt att ge högre prioritet åt begäranden från användare i medlemsstaterna då dessa kriterier leder till att två eller flera begäranden bedöms vara likvärdiga. Detta påverkar inte eventuella skyldigheter att vidta åtgärder för att skydda och bistå unionens institutioner, organ och byråer som medlemsstaterna kan ha enligt relevanta värdtjänstavtal.

(44) Kommissionen bör ha det övergripande ansvaret för genomförandet av EU-cybersäkerhetsreserven. Med tanke på Enisas omfattande erfarenhet av stödåtgärden för cybersäkerhet är Enisa den lämpligaste byrån för att genomföra EU-cybersäkerhetsreserven. Därför bör kommissionen delvis eller, i de fall kommissionen anser det lämpligt, helt anförtro Enisa driften och förvaltningen av EU-cybersäkerhetsreserven. Detta bör ske i enlighet med de tillämpliga reglerna i förordning (EU, Euratom) 2024/2509 och bör i synnerhet omfattas av de relevanta villkoren för undertecknande av en överenskommelse om medverkan. Alla aspekter av driften och förvaltningen av EU-cybersäkerhetsreserven som inte anförtrotts Enisa bör förvaltas direkt av kommissionen, inbegripet innan överenskommelsen om medverkan undertecknas.

(45) Medlemsstaterna bör ha en nyckelroll när det gäller inrättandet, införandet och skedet efter införandet av EU-cybersäkerhetsreserven. Eftersom förordning (EU) 2021/694 är den relevanta grundläggande akten för åtgärder för genomförande av EU-cybersäkerhetsreserven, bör åtgärder inom ramen för EU-cybersäkerhetsreserven anges i de arbetsprogram som avses i artikel 24 i förordning (EU) 2021/694. Enligt punkt 6 i den artikeln ska dessa arbetsprogram antas av kommissionen genom genomförandeakter i enlighet med granskningsförfarandet. Dessutom bör kommissionen, i samordning med samarbetsgruppen för nät- och informationssäkerhet, fastställa prioriteringarna för och utvecklingen av EU-cybersäkerhetsreserven.

(46) De avtal som upprättas inom ramen för EU-cybersäkerhetsreserven bör inte påverka förhållandet mellan företag och befintliga skyldigheter mellan den berörda entiteten eller användare och tjänsteleverantören.

(47) För urvalet av privata tjänsteleverantörer som ska tillhandahålla tjänster inom ramen för EU-cybersäkerhetsreserven är det nödvändigt att fastställa ett antal minimikriterier och krav som bör ingå i anbudsinfordran för att välja ut dessa leverantörer, i syfte att säkerställa att behoven hos medlemsstaternas myndigheter, entiteter som är verksamma i högkritiska eller entiteter verksamma i andra kritiska sektorer tillgodoses. För att tillgodose medlemsstaternas särskilda behov vid upphandling av tjänster för EU-cybersäkerhetsreserven bör den upphandlande myndigheten, när så är lämpligt, utarbeta urvalskriterier och krav som går utöver dem som fastställs i denna förordning. Det är viktigt att uppmuntra mindre leverantörer som är verksamma på regional och lokal nivå att delta.

(48) När den upphandlande myndigheten väljer leverantörer som ska ingå i EU-cybersäkerhetsreserven bör den sträva efter att säkerställa att EU-cybersäkerhetsreserven, betraktad som en helhet, innefattar leverantörer som kan tillgodose användarnas språkkrav. I detta syfte bör den upphandlande myndigheten, innan den utarbetar kravspecifikationerna, undersöka om de potentiella användarna av EU-cybersäkerhetsreserven har särskilda språkkrav, så att stödtjänster från EU-cybersäkerhetsreserven kan tillhandahållas på ett eller flera av unionens eller en medlemsstats officiella språk som sannolikt förstås av användaren eller den berörda entiteten. Om en användare kräver mer än ett språk för tillhandahållandet av stödtjänster från EU-cybersäkerhetsreserven och de tjänsterna har upphandlats på dessa språk för denna användare, bör användaren i begäran om stöd från reserven kunna ange på vilket av dessa språk som tjänsterna bör tillhandahållas i samband med den specifika incident som ligger till grund för begäran.

(49) För att stödja inrättandet av EU-cybersäkerhetsreserven är det viktigt att kommissionen begär att Enisa utarbetar en ordning för cybersäkerhetscertifiering för utlokaliserade säkerhetstjänster enligt förordning (EU) 2019/881 på de områden som omfattas av cybernödmekanismen.

(50) För att stödja denna förordnings mål att främja gemensam situationsmedvetenhet, öka unionens motståndskraft och möjliggöra effektiva insatser vid betydande cybersäkerhetsincidenter och storskaliga cybersäkerhetsincidenter bör kommissionen eller EU-CyCLONe kunna begära att Enisa, med stöd av CSIRT-nätverket och med den berörda medlemsstatens godkännande, granskar och analyserar cyberhot, kända sårbarheter som kan utnyttjas och begränsningsåtgärder med avseende på en specifik betydande cybersäkerhetsincident eller storskalig cybersäkerhetsincident. Efter avslutad granskning och analys av en incident bör Enisa utarbeta en incidentgranskningsrapport i samarbete med den berörda medlemsstaten, berörda parter såsom företrädare för den privata sektorn, kommissionen och andra relevanta unionsinstitutioner, -organ och -byråer. Med utgångspunkt i samarbetet med berörda parter, även från den privata sektorn, bör granskningsrapporten om specifika incidenter syfta till att analysera orsakerna till, konsekvenserna av och begränsningen av en incident efter det att den inträffat. Särskild uppmärksamhet bör ägnas de bidrag och lärdomar som delas av leverantörer av utlokaliserade säkerhetstjänster som uppfyller villkoren för högsta yrkesmässiga integritet, opartiskhet och erforderlig teknisk expertis enligt kraven i denna förordning. Rapporten bör överlämnas till EU-CyCLONe, CSIRT-nätverket och kommissionen och bör läggas till grund för deras arbete samt till Enisas arbete. När incidenten rör ett tredjeland som är associerat till programmet för ett digitalt Europa bör kommissionen också överlämna rapporten till den höga representanten.

(51) Med tanke på att cyberangrepp är oförutsägbara och sällan begränsade till ett visst geografiskt område, utan har en hög risk för spridningseffekter, bidrar förstärkningen av grannländernas resiliens och deras kapacitet att hantera betydande cybersäkerhetsincidenter och incidenter som är likvärdiga med en storskalig cybersäkerhetsincident på ett ändamålsenligt sätt till skyddet av unionen som helhet, och framför allt dess inre marknad och industri. Sådan verksamhet skulle kunna bidra ytterligare till unionens cyberdiplomati. Därför bör tredjeländer som är associerade till programmet för ett digitalt Europa kunna få stöd från EU-cybersäkerhetsreserven, på alla eller delar av deras territorier, när detta föreskrivs i det avtal genom vilket tredjelandet är associerat till programmet. Finansieringen för tredjeländer som är associerade till programmet för ett digitalt Europa bör stödjas av unionen inom ramen för relevanta partnerskap och finansieringsinstrument för dessa länder. Stödet bör omfatta tjänster på området insatser vid och initiera återhämtning från betydande cybersäkerhetsincidenter eller incidenter som är likvärdiga med en storskalig cybersäkerhetsincident.

(52) De villkor som fastställs för EU-cybersäkerhetsreserven och betrodda leverantörer av utlokaliserade säkerhetstjänster i denna förordning bör gälla vid tillhandahållande av stöd till tredjeländer som är associerade till programmet för ett digitalt Europa. Tredjeländer som är associerade till programmet för ett digitalt Europa bör kunna begära stöd från EU-cybersäkerhetsreserven när de entiteter som den riktar sig till och för vilka de begär stöd från EU-cybersäkerhetsreserven är entiteter som är verksamma inom högkritiska sektorer eller entiteter verksamma i andra kritiska sektorer och när de upptäckta incidenterna leder till betydande driftsstörningar eller kan ha spridningseffekter i unionen. Tredjeländer som är associerade till programmet för ett digitalt Europa bör endast vara berättigade till stöd om det avtal genom vilket de är associerade till programmet för ett digitalt Europa uttryckligen tillåter sådant stöd. Dessutom bör sådana tredjeländer fortsätta att vara berättigade till stöd endast så länge tre kriterier är uppfyllda. För det första bör tredjelandet fullt ut uppfylla de relevanta villkoren i det avtalet. För det andra bör tredjelandet, med tanke på EU-cybersäkehetsreservens kompletterande karaktär, ha vidtagit lämpliga åtgärder för att förbereda sig för betydande cybersäkerhetsincidenter eller incidenter som är likvärdiga med en storskalig cybersäkerhetsincident. För det tredje bör stödet från EU-cybersäkerhetsreserven vara förenligt med unionens politik gentemot och de övergripande förbindelserna med det landet och med annan unionspolitik på säkerhetsområdet. I samband med sin bedömning av huruvida detta tredje kriterium är uppfyllt bör kommissionen samråda med den höga representanten om att anpassa beviljandet av sådant stöd till den gemensamma utrikes- och säkerhetspolitiken.

(53) Tillhandahållandet av stöd till tredjeländer som är associerade till programmet för ett digitalt Europa kan påverka förbindelserna med tredjeländer och unionens säkerhetspolitik, inbegripet inom ramen för den gemensamma utrikes- och säkerhetspolitiken och den gemensamma säkerhets- och försvarspolitiken. Det är därför lämpligt att rådet ges genomförandebefogenheter för att godkänna och specificera den period under vilken sådant stöd kan tillhandahållas. Rådet bör agera på grundval av ett förslag från kommissionen, med vederbörligt beaktande av kommissionens bedömning av de tre kriterierna. Detsamma bör gälla för förnyelser och förförslag om ändring eller upphävande av sådana akter. Om rådet vid exceptionella omständigheter anser att det har skett en betydande förändring av omständigheterna när det gäller det tredje kriteriet, bör rådet kunna agera på eget initiativ för att ändra eller upphäva en genomförandeakt, utan att invänta ett förslag från kommissionen. Sådana betydande förändringar kommer sannolikt att kräva brådskande åtgärder, få särskilt betydande konsekvenser för förbindelserna med tredjeländer och inte kräva någon detaljerad förhandsbedömning från kommissionens sida. Kommissionen bör dessutom samarbeta med den höga representanten när det gäller begäranden om stöd från tredjeländer som är associerade till programmet för ett digitalt Europa och genomförandet av det stöd som beviljats sådana tredjeländer. Kommissionen bör också ta hänsyn till eventuella synpunkter från Enisa om sådana begäranden och sådant stöd. Kommissionen bör informera rådet om resultatet av bedömningen av begärandena, inbegripet relevanta överväganden i detta avseende, och de tjänster som används.

(54) I kommissionens meddelande av den 18 april 2023 om EU-akademin för cyberkompetens erkändes bristen på kvalificerad arbetskraft. Sådan kompetens är nödvändig för att uppfylla syftet med denna förordning. Unionen behöver snarast kvalificerad arbetskraft med de färdigheter och kompetenser som krävs för att förebygga, upptäcka och avskräcka från cyberattacker samt för att försvara unionen, inbegripet dess mest kritiska infrastruktur, mot sådana attacker och säkerställa dess resiliens. I detta syfte är det viktigt att uppmuntra samarbete mellan berörda parter, inbegripet från den privata sektorn, den akademiska världen och den offentliga sektorn. Det är lika viktigt att åstadkomma synergier inom alla unionens territorier för investeringar i utbildning i syfte att främja skapandet av skyddsåtgärder för att undvika kompetensflykt eller att kompetensgapet ökar mer i vissa regioner än i andra. Det är angeläget att eliminera kompetensklyftan på området för cybersäkerhet, med särskilt fokus på att minska könsklyftan bland arbetskraften inom cybersäkerhet för att främja kvinnors närvaro och deltagande i utformningen av den digitala förvaltningen.

(55) För att främja innovationen på den digitala inre marknaden är det viktigt att stärka forskning och innovation inom cybersäkerhet, i syfte att bidra till att öka medlemsstaternas resiliens och unionens öppna strategiska oberoende, vilka båda är mål för denna förordning. Synergier är avgörande för att stärka samarbetet och samordningen mellan de olika berörda parterna, inbegripet från den privata sektorn, det civila samhället och den akademiska världen.

(56) Denna förordning bör ta hänsyn till det åtagande som anges i Europaparlamentets, rådets och kommissionens gemensamma förklaring av den 26 januari 2022 med titeln Den europeiska förklaringen om digitala rättigheter och principer för det digitala decenniet, i syfte att skydda unionens demokratiers, människors, företags och offentliga institutioners intressen mot cybersäkerhetsrisker och it-brottslighet, inbegripet dataintrång och identitetsstöld eller identitetsmanipulering.

(57) I syfte att komplettera vissa icke väsentliga delar av denna förordning bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen för att fastställa vilken typ av och hur många insatstjänster som behövs för EU-cybersäkerhetsreserven. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning[20]. För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter systematiskt ges tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

[20] EUT L 123, 12.5.2016, s. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

(58) I syfte att säkerställa enhetliga villkor för genomförandet av denna förordning bör kommissionen tilldelas genomförandebefogenheter för att ytterligare specificera de närmare förfarandena för tilldelning av stödtjänster från EU-cybersäkerhetsreserven. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011[21].

(59) Utan att det påverkar tillämpningen av bestämmelserna om unionens årliga budget enligt fördragen bör kommissionen beakta de skyldigheter som följer av denna förordning när den bedömer Enisas budget- och personalbehov.

(60) Kommissionen bör regelbundet utvärdera de åtgärder som fastställs i denna förordning. Den första utvärderingen bör äga rum under de två första åren från och med den dag då denna förordning börjar tillämpas och minst vart fjärde år därefter, med beaktande av tidpunkten för översynen av den fleråriga budgetramen. Kommissionen bör överlämna en rapport om de framsteg som gjorts till Europaparlamentet och rådet. För att bedöma de olika inslag som krävs, inbegripet omfattningen av den information som utbyts inom det europeiska systemet med cybersäkerhetsvarningar, bör kommissionen uteslutande grunda sig på information som är lättillgänglig eller som tillhandahålls frivilligt. Med beaktande av den geopolitiska utvecklingen och för att säkerställa kontinuitet och fortsatt utveckling av de åtgärder som fastställs i denna förordning efter 2027, är det viktigt att kommissionen bedömer nödvändigheten av att i den fleråriga budgetramen tilldela en lämplig budget för perioden 2028–2034.

---

[21] Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(61) Eftersom målen för denna förordning, nämligen att stärka konkurrensställningen för industri och tjänster i unionen i hela den digitala ekonomin och att bidra till unionens tekniska suveränitet och öppna strategiska oberoende på cybersäkerhetsområdet, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning eller verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen artikel 5 i EU-fördraget. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå dessa mål.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Kapitel I
Allmänna bestämmelser

Artikel 1

Innehåll och mål

1. I denna förordning fastställs åtgärder för att stärka kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cyberincidenter, i synnerhet genom att inrätta

   a) ett europeiskt nätverk av cybernav (det europeiska systemet med cybersäkerhetsvarningar) för att bygga upp och förbättra samordnad kapacitet för upptäckt och gemensam kapacitet för situationsmedvetenhet,

   b) en cybernödmekanism för att stödja medlemsstaterna när det gäller att förbereda sig inför, hantera, mildra effekterna av och initiera återhämtning från betydande cybersäkerhetsincidenter och storskaliga cybersäkerhetsincidenter och att stödja andra användare när det gäller att hantera betydande cybersäkerhetsincidenter och incidenter som är likvärdiga med en storskalig cybersäkerhetsincident,

   c) en europeisk mekanism för utvärdering av cybersäkerhetsincidenter för att utvärdera och analysera betydande cybersäkerhetsincidenter eller storskaliga cybersäkerhetsincidenter.

2. Denna förordning eftersträvar de allmänna målen att stärka konkurrensställningen för industri och tjänster i unionen i hela den digitala ekonomin, inbegripet mikroföretag och små och medelstora företag samt uppstartsföretag, och att bidra till unionens tekniska suveränitet och öppna strategiska oberoende på cybersäkerhetsområdet, bland annat genom att främja innovation på den digitala inre marknaden. Den strävar efter att uppnå dessa mål genom att stärka solidariteten på unionsnivå, förbättra cybersäkerhetsekosystemet, höja medlemsstaternas cyberresiliens och utveckla arbetskraftens färdigheter, kunnande, förmågor och kompetens när det gäller cybersäkerhet.

3. De allmänna mål som avses i punkt 2 ska uppnås genom följande specifika mål:

   a) Stärka den gemensamma samordnade upptäcktskapaciteten och den gemensamma situationsmedvetenheten i unionen när det gäller cyberhot och cyberincidenter.

   b) Förbättra beredskapen hos entiteter som är verksamma inom högkritiska sektorer eller entiteter som är verksamma i andra kritiska sektorer i hela unionen och stärka solidariteten genom att utveckla samordnad beredskapstestning och stärkt insats- och återhämtningskapacitet för att hantera betydande cybersäkerhetsincidenter, storskaliga cybersäkerhetsincidenter eller incidenter som är likvärdiga med en storskalig cybersäkerhetsincident, bland annat möjligheten att göra unionsstöd för hantering av cybersäkerhetsincidenter tillgängligt för tredjeländer som är associerade till programmet för ett digitalt Europa.

c) Öka unionens resiliens och bidra till effektiv hantering av incidenter genom att granska och analysera betydande cybersäkerhetsincidenter eller storskaliga cybersäkerhetsincidenter för att bland annat dra lärdomar av dessa och, när så är lämpligt, utfärda rekommendationer.

4. Åtgärderna enligt denna förordning ska genomföras med vederbörlig respekt för medlemsstaternas behörighet och ska komplettera den verksamhet som bedrivs av CSIRT-nätverket, EU-CyCLONe och samarbetsgruppen för nät- och informationssäkerhet.

5. Denna förordning påverkar inte medlemsstaternas väsentliga statliga funktioner, däribland att säkerställa statens territoriella integritet, upprätthålla lag och ordning och skydda den nationella säkerheten. I synnerhet ska den nationella säkerheten också i fortsättningen vara varje medlemsstats eget ansvar.

6. Utbyte av information enligt denna förordning som är konfidentiell i enlighet med unionsregler eller nationella regler ska begränsas till det som är relevant och står i proportion till ändamålet med utbytet. Vid sådant informationsutbyte ska informationens konfidentialitet bevaras och säkerhetsintressen och kommersiella intressen hos de berörda entiteterna skyddas. Det ska inte innebära tillhandahållande av information vars röjande skulle strida mot medlemsstaternas väsentliga intressen avseende nationell säkerhet, allmän säkerhet eller försvar.

Artikel 2

Definitioner

I denna förordning gäller följande definitioner:

1. *gränsöverskridande cybernav*: en flerlandsplattform, inrättad genom ett skriftligt konsortieavtal, som inom en samordnad nätverksstruktur för samman nationella cybernav från minst tre medlemsstater, och som är utformad för att förbättra övervakning, upptäckt och analys av cyberhot för att förhindra incidenter och stödja produktionen av underrättelseinformation om cyberhot, i synnerhet genom utbyte av relevanta data och relevant information, när så är lämpligt i anonymiserad form, samt genom utbyte av förstklassiga verktyg och gemensam utveckling av kapacitet för cyberrelaterad upptäckt, analys, förebyggande och skydd i en betrodd miljö.

2. *värdkonsortium*: ett konsortium som består av deltagande medlemsstater, som har kommit överens om att inrätta och bidra till förvärv av verktyg, infrastruktur eller tjänster för, och drift av, ett gränsöverskridande cybernav.

3. *CSIRT-enhet*: en CSIRT-enhet som utsetts eller inrättats enligt artikel 10 i direktiv (EU) 2022/2555.

4. *entitet*: en entitet enligt definitionen i artikel 6.38 i direktiv (EU) 2022/2555.

5. *entiteter som är verksamma inom högkritiska sektorer*: de typer av entiteter som förtecknas i bilaga I till direktiv (EU) 2022/2555.

6. *entiteter som är verksamma inom andra kritiska sektorer*: de typer av entiteter som förtecknas i bilaga II till direktiv (EU) 2022/2555.

7. *risk*: en risk enligt definitionen i artikel 6.9 i direktiv (EU) 2022/2555.

8. *cyberhot*: ett cyberhot enligt definitionen i artikel 2.8 i förordning (EU) 2019/881.

9. *incident*: en incident enligt definitionen i artikel 6.6 i direktiv (EU) 2022/2555.

10. *betydande cybersäkerhetsincident*: en incident som uppfyller kriterierna i artikel 23.3 i direktiv (EU) 2022/2555.

11. *större incident:* en större incident enligt definitionen i artikel 3.8 i Europaparlamentets och rådets förordning (EU, Euratom) 2023/2841[22].

12. *storskalig cybersäkerhetsincident*: en storskalig cybersäkerhetsincident enligt definitionen i artikel 6.7 i direktiv (EU) 2022/2555.

[22] Europaparlamentets och rådets förordning (EU, Euratom) 2023/2841 av den 13 december 2023 om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer (EUT L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

13. *incident som är likvärdig med en storskalig cybersäkerhetsincident*: när det gäller unionens institutioner, organ och byråer, en större incident och, när det gäller tredjeländer som är associerade till programmet för ett digitalt Europa, en incident som orsakar störningar som är så omfattande att de överskrider det berörda associerade tredjelandets kapacitet att hantera dem.

14. *tredjeland som är associerat till programmet för ett digitalt Europa*: ett tredjeland som är part i ett avtal med unionen som möjliggör dess deltagande i programmet för ett digitalt Europa enligt artikel 10 i förordning (EU) 2021/694.

15. *upphandlande myndighet*: kommissionen eller, i den mån driften och förvaltningen av EU-cybersäkerhetsreserven har anförtrotts Enisa enligt artikel 14.5 i denna förordning, Enisa.

16. *leverantör av utlokaliserade säkerhetstjänster*: en leverantör av utlokaliserade säkerhetstjänster enligt definitionen i artikel 6.40 i direktiv (EU) 2022/2555.

17. *betrodd leverantör av utlokaliserade säkerhetstjänster*: leverantör av utlokaliserade säkerhetstjänster som valts ut för att ingå i EU:s cybersäkerhetsreserv i enlighet med artikel 17.

Kapitel II

Det Europeiska systemet med cybersäkerhetsvarningar

Artikel 3

Inrättande av det europeiska systemet med cybersäkerhetsvarningar

1. Ett europeiskt nätverk av infrastruktur bestående av nationella cybernav och gränsöverskridande cybernav som frivilligt ansluter sig till det europeiska systemet med cybersäkerhetsvarningar ska inrättas för att stödja utvecklingen av avancerad kapacitet för unionen för att förbättra kapaciteten för upptäckt, analys och databehandling i samband med cyberhot och förebyggande av incidenter i unionen.

2. Det europeiska systemet med cybersäkerhetsvarningar ska

   a) bidra till bättre skydd och insatser mot cyberhot genom att stödja och samarbeta med, och stärka kapaciteten hos, relevanta entiteter, särskilt CSIRT-enheter, CSIRT-nätverket, EU-CyCLONe och de behöriga myndigheter som utsetts eller inrättats enligt artikel 8.1 i direktiv (EU) 2022/2555,

   b) föra samman relevanta data och relevant information om cyberhot och cyberincidenter från olika källor inom de gränsöverskridande cybernaven och dela analyserad eller aggregerad information via gränsöverskridande cybernav, i förekommande fall med CSIRT-nätverket,

c) samla in och stödja produktion av högkvalitativ och agerbar information samt underrättelseinformation om cyberhot, genom användning av förstklassiga verktyg och avancerad teknik, och dela denna information och underrättelseinformation om cyberhot,

d) bidra till en bättre samordnad upptäckt av cyberhot samt gemensam situationsmedvetenhet i hela unionen, och till att utfärda varningar, inbegripet, i förekommande fall, genom att tillhandahålla konkreta rekommendationer till entiteter,

e) tillhandahålla tjänster och verksamheter för cybersäkerhetssamfundet i unionen, inbegripet att bidra till utvecklingen av avancerade verktyg och avancerad teknik, såsom AI-verktyg och dataanalysverktyg.

3. Åtgärder för att genomföra det europeiska systemet med cybersäkerhetsvarningar ska stödjas med medel från programmet för ett digitalt Europa och genomföras i enlighet med förordning (EU) 2021/694, i synnerhet det specifika målet 3 i denna.

Artikel 4

Nationella cybernav

1. Om en medlemsstat beslutar att delta i det europeiska systemet med cybersäkerhetsvarningar ska den utse eller, i tillämpliga fall, inrätta ett nationellt cybernav för tillämpningen av denna förordning (nationellt cybernav).

2. Ett nationellt cybernav ska vara en enda entitet som agerar under en medlemsstats överinseende. Det kan vara en CSIRT-enhet eller, i tillämpliga fall, en nationell cyberkrishanteringsmyndighet eller en annan behörig myndighet som utsetts eller inrättats enligt artikel 8.1 i direktiv (EU) 2022/2555, eller en annan entitet. Det nationella cybernavet ska

   a) ha kapacitet att fungera som referenspunkt och gränssnitt mot andra offentliga och privata organisationer på nationell nivå för insamling och analys av information om cyberhot och cyberincidenter och att bidra till ett gränsöverskridande cybernav som avses i artikel 5, och

   b) kunna upptäcka, aggregera och analysera data och information som är relevanta för cyberhot och cyberincidenter, såsom underrättelseinformation om cyberhot, genom att framför allt använda förstklassig teknik, i syfte att förebygga incidenter.

3. Som en del av de funktioner som avses i punkt 2 i denna artikel får nationella cybernav samarbeta med entiteter i den privata sektorn för att utbyta relevanta data och relevant information i syfte att upptäcka och förebygga cyberhot och cyberincidenter, inbegripet med sektorsspecifika och sektorsövergripande grupper av väsentliga och viktiga entiteter som avses i artikel 3 i direktiv (EU) 2022/2555. När så är lämpligt och i enlighet med unionsrätten och nationell rätt får den information som begärs eller mottas av nationella cybernav omfatta telemetri-, sensor- och loggningsdata.

4. En medlemsstat som valts ut enligt artikel 9.1 ska förbinda sig till att ansöka om att dess nationella cybernav ska delta i ett gränsöverskridande cybernav.

Artikel 5

Gränsöverskridande cybernav

1. Om minst tre medlemsstater har åtagit sig att säkerställa att deras nationella cybernav samarbetar för att samordna sin cyberupptäckts- och hotövervakningsverksamhet, får dessa medlemsstater inrätta ett värdkonsortium för tillämpningen av denna förordning.

2. Ett värdkonsortium ska bestå av minst tre deltagande medlemsstater som har kommit överens om att inrätta och bidra till förvärv av verktyg, infrastruktur eller tjänster för, och drift av, ett gränsöverskridande cybernav i enlighet med punkt 4.

3. Om ett värdkonsortium väljs ut i enlighet med artikel 9.3 ska dess medlemmar ingå ett skriftligt konsortieavtal som

   a) anger de interna arrangemang för genomförandet av det värd- och användningsavtal som avses i artikel 9.3,

   b) inrättar värdkonsortiets gränsöverskridande cybernav, och

   c) innehåller de särskilda klausuler som krävs enligt artikel 6.1 och 6.2.

4. Ett gränsöverskridande cybernav ska vara en flerlandsplattform som inrättats genom ett skriftligt konsortieavtal enligt punkt 3. Det ska sammanföra de nationella cybernaven i värdkonsortiets medlemsstater i ett samordnat nätverk. Det ska vara utformat för att främja övervakning, upptäckt och analys av cyberhot, förhindra incidenter och stödja produktionen av underrättelseinformation om cyberhot, i synnerhet genom utbyte av relevanta data och relevant information, när så är lämpligt i anonymiserad form, samt genom utbyte av förstklassiga verktyg och gemensam utveckling av kapacitet för cyberrelaterad upptäckt, analys, förebyggande och skydd i en betrodd miljö.

5. Ett gränsöverskridande cybernav ska i rättsligt hänseende företrädas av en medlem av motsvarande värdkonsortium som fungerar som samordnare, eller av värdkonsortiet om det är en juridisk person. Ansvaret för att det gränsöverskridande cybernavet efterlever denna förordning och värd- och användningsavtalet ska fastställas i det skriftliga konsortieavtal som avses i punkt 3.

6. En medlemsstat får ansluta sig till ett befintligt värdkonsortium med värdkonsortiets medlemmars godkännande. Det skriftliga konsortieavtal som avses i punkt 3 och värd- och användningsavtalet ska ändras i enlighet med detta. Detta ska inte påverka äganderätten för Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning (Europeiska kompetenscentrumet för cybersäkerhet) till de verktyg, infrastrukturer och tjänster som redan upphandlats gemensamt med värdkonsortiet.

Artikel 6

Samarbete och informationsutbyte inom och mellan gränsöverskridande cybernav

1. Medlemmar i ett värdkonsortium ska säkerställa att deras nationella cybernav, i enlighet med det skriftliga konsortieavtal som avses i artikel 5.3, utbyterrelevant information, när så är lämpligt i anonymiserad form, såsom information om cyberhot, tillbud, sårbarheter, tekniker och förfaranden, angreppsindikatorer, fientlig taktik, specifik information om fientliga aktörer, cybersäkerhetsvarningar och rekommendationer avseende konfiguration av cybersäkerhetsverktyg för att sinsemellan inom det gränsöverskridande cybernavet upptäcka cyberattacker, om detta informationsutbyte

   a) främjar och förbättrar upptäckten av cyberhot och stärker CSIRT-nätverkets kapacitet att förebygga och hantera incidenter eller begränsa deras effekter,

   b) höjer cybersäkerhetsnivån, till exempel genom att öka medvetenheten om cyberhot, begränsa eller hindra sådana hots förmåga att sprida sig, stödja en rad defensiva förmågor, avhjälpande av sårbarheter och delgivning av information om sårbarheter, metoder för att upptäcka och förebygga hot, strategier för begränsning av hot eller insats- och återhämtningsfaser, eller genom att främja offentliga och privata entiteters forskningssamverkan om cyberhot.

2. Det skriftliga konsortieavtal som avses i artikel 5.3 ska fastställa följande:

a) Ett åtagande att bland värdkonsortiets medlemmar utbyta information enligt punkt 1 och villkoren för hur detta utbyte av information ska ske.

b) En styrningsram som förtydligar och ger alla deltagare incitament att utbyta och relevant information, när så är lämpligt i anonymiserad form, enligt punkt 1.

c) Mål för bidrag till utvecklingen av avancerade verktyg och avancerad teknik, såsom AI-verktyg och dataanalysverktyg.

Det skriftliga konsortieavtalet får ange att den information som avses i punkt 1 ska utbytas i enlighet med unionsrätten och nationell rätt.

3. Gränsöverskridande cybernav ska ingå samarbetsavtal med varandra, och ange principer för interoperabilitet och informationsutbyte mellan de gränsöverskridande cybernaven. Gränsöverskridande cybernav ska informera kommissionen om de samarbetsavtal som ingåtts.

4. Det informationsutbyte som avses i punkt 1 mellan gränsöverskridande cybernav ska säkerställas genom en hög grad av interoperabilitet. För att stödja sådan interoperabilitet ska Enisai nära samråd med kommissionen, utan onödigt dröjsmål och under alla omständigheter senast den … [12 månader från dagen för ikraftträdandet av denna förordning], utfärda riktlinjer för interoperabilitet som särskilt anger format och protokoll för informationsutbyte, med beaktande av internationella standarder och bästa praxis, samt hur eventuella gränsöverskridande cybernav som inrättats ska fungera. Interoperabilitetskrav som föreskrivs i de gränsöverskridande cybernavens samarbetsavtal ska baseras på de riktlinjer som utfärdas av Enisa.

Artikel 7

Samarbete och informationsutbyte med nätverk på unionsnivå

1. De gränsöverskridande cybernaven och CSIRT-nätverket ska ha ett nära samarbete, särskilt för att utbyta information. I detta syfte ska de komma överens om förfaranden för samarbete och utbyte av relevant information och, utan att det påverkar tillämpningen av punkt 1, vilka typer av information som ska utbytas.

2. När gränsöverskridande cybernav får information om en potentiell eller pågående storskalig cybersäkerhetsincident ska de, i syfte att uppnå en gemensam situationsmedvetenhet, säkerställa att relevant information och tidiga varningar utan onödigt dröjsmål tillhandahålls medlemsstaternas myndigheter och kommissionen via EUCyCLONe och CSIRT-nätverket.

Artikel 8

Säkerhet

1. Medlemsstater som deltar i det europeiska systemet med cybersäkerhetsvarningar ska säkerställa en hög nivå av cybersäkerhet, inbegripet konfidentialitet och datasäkerhet samt fysisk säkerhet för det europeiska systemet med cybersäkerhetsvarningar och ska säkerställa att nätverket förvaltas på lämpligt sätt och kontrolleras på ett sådant sätt att det skyddas från hot och att dess och systemens säkerhet skyddas, inbegripet de data och den information som utbyts via nätverket.

2. Medlemsstater som deltar i det europeiska systemet med cybersäkerhetsvarningar ska säkerställa att utbytet av information som avses i artikel 6.1 inom det europeiska systemet med cybersäkerhetsvarningar med andra entiteter än offentliga myndigheter eller organ i en medlemsstat inte har en negativ inverkan på unionens eller medlemsstaternas säkerhetsintressen.

Artikel 9

Finansiering av det europeiska systemet med cybersäkerhetsvarningar

1. Efter en inbjudan att anmäla intresse för de medlemsstater som avser att delta i det europeiska systemet med cybersäkerhetsvarningar ska Europeiska kompetenscentrumet för cybersäkerhet välja ut medlemsstater för att tillsammans med Europeiska kompetenscentrumet för cybersäkerhet, delta i en gemensam upphandling, av verktyg, infrastruktur eller tjänster, i syfte att inrätta eller förbättra kapaciteten hos nationella cybernav som utsetts eller inrättats enligt artikel 4.1. Europeiska kompetenscentrumet för cybersäkerhet kan bevilja bidrag till de utvalda medlemsstaterna för att finansiera driften av sådana verktyg, sådan infrastruktur eller sådana tjänster. Unionens finansiella bidrag ska täcka upp till 50 % av kostnaderna för förvärv av verktyg, infrastruktur eller tjänster och upp till 50 % av driftskostnaderna. De utvalda medlemsstaterna ska täcka de återstående kostnaderna. Innan förfarandet för förvärv av verktyg, infrastruktur eller tjänster inleds ska Europeiska kompetenscentrumet för cybersäkerhet och de utvalda medlemsstaterna ingå ett värd- och användningsavtal som reglerar användningen av verktygen, infrastrukturen eller tjänsterna.

2. Om en medlemsstats nationella cybernav inte deltar i ett gränsöverskridande cybernav inom två år från den dag då verktygen, infrastrukturen eller tjänsterna förvärvades eller då det fick bidragsfinansiering, beroende på vilket som inträffade först, ska medlemsstaten inte vara berättigad till ytterligare unionsstöd i enlighet med detta kapitel förrän den har anslutit sig till ett gränsöverskridande cybernav.

3. Efter en inbjudan att anmäla intresse ska ett värdkonsortium väljas ut av Europeiska kompetenscentrumet för cybersäkerhet för att delta i en gemensam upphandling av verktyg, infrastruktur eller tjänster med kompetenscentrumet. Europeiska kompetenscentrumet för cybersäkerhet får tilldela värdkonsortiet ett bidrag för att finansiera driften av dessa verktyg, denna infrastruktur eller dessa tjänster. Unionens finansiella bidrag ska täcka upp till 75 % av kostnaderna för förvärv av verktyg, infrastruktur eller tjänster och upp till 50 % av driftskostnaderna. Återstående kostnader ska täckas av värdkonsortiet. Innan förfarandet för förvärv av verktyg, infrastruktur eller tjänster inleds ska Europeiska kompetenscentrumet för cybersäkerhet och värdkonsortiet ingå ett värd- och användningsavtal som reglerar användningen av verktygen, infrastrukturen eller tjänsterna.

4. Europeiska kompetenscentrumet för cybersäkerhet ska minst vartannat år kartlägga vilka verktyg, vilken infrastruktur eller vilka tjänster som är nödvändiga och av lämplig kvalitet för att inrätta eller förbättra kapaciteten hos nationella cybernav och gränsöverskridande cybernav och deras tillgänglighet, inbegripet från rättsliga enheter som är etablerade eller bedöms vara etablerade i medlemsstater och som kontrolleras av medlemsstater eller medborgare i medlemsstater. Vid kartläggningen ska Europeiska kompetenscentrumet för cybersäkerhet samråda med CSIRT-nätverket, eventuella befintliga gränsöverskridande cybernav, Enisa och kommissionen.

Kapitel III
Cybernödmekanism

Artikel 10

Inrättande av en cybernödmekanism

1. En cybernödmekanism inrättas för att stödja förbättringen av unionens resiliens mot cyberhot och, i en anda av solidaritet, förberedelsen inför och begränsningen av de kortsiktiga effekterna av betydande cybersäkerhetsincidenter, storskaliga cybersäkerhetsincidenter och incidenter som är likvärdiga med en storskalig cybersäkerhetsincident.

2. När det gäller medlemsstater ska åtgärder inom ramen för cybernödmekanismen tillhandahållas på begäran och komplettera medlemsstaternas insatser och åtgärder för att förbereda sig inför, hantera och återhämta sig från incidenter.

3. Åtgärderna för genomförande av cybernödmekanismen ska stödjas med medel från programmet för ett digitalt Europa och genomföras i enlighet med förordning (EU) 2021/694, i synnerhet det specifika målet 3 i denna.

4. Åtgärderna inom ramen för cybernödmekanismen ska främst genomföras genom Europeiska kompetenscentrumet för cybersäkerhet i enlighet med förordning (EU) 2021/887. Åtgärder för genomförandet av den EU-cybersäkerhetsreserv som avses i artikel 11.1 b i denna artikel ska emellertid genomföras av kommissionen och Enisa.

Artikel 11

Typer av åtgärder

Cybernödmekanismen ska stödja följande typer av åtgärder:

a) Beredskapsåtgärder, det vill säga

i) samordnad beredskapstestning av entiteter som är verksamma inom högkritiska sektorer i hela unionen, i enlighet med artikel 12,

ii) andra beredskapsåtgärder för entiteter som är verksamma inom högkritiska sektorer eller entiteter som är verksamma i andra kritiska sektorer, i enlighet med artikel 13.

b) Åtgärder som stöder hantering av och initiering av återhämtning från betydande cybersäkerhetsincidenter, storskaliga cybersäkerhetsincidenter och incidenter som är likvärdiga med en storskalig cybersäkerhetsincident, vilka ska tillhandahållas av betrodda leverantörer av utlokaliserade säkerhetstjänster som deltar i den EU-cybersäkerhetsreserv som inrättas enligt artikel 14.

c) Åtgärder till stöd för ömsesidigt bistånd som avses i artikel 18.

Artikel 12

Samordnad beredskapstestning av entiteter

1. Cybernödmekanismen ska stödja den frivilliga samordnade beredskapstestningen av entiteter som är verksamma i högkritiska sektorer.

2. Den samordnade beredskapstestningen kan bestå av beredskapsåtgärder, såsom penetrationstestning och hotbedömningar.

3. Stöd till beredskapsåtgärder enligt denna artikel ska i första hand ges till medlemsstaterna i form av bidrag och på de villkor som fastställs i de relevanta arbetsprogram som avses i artikel 24 i förordning (EU) 2021/694.

4. För att stödja den samordnade beredskapstestningen av entiteter som avses i artikel 11.1 a i) i denna förordning i hela unionen ska kommissionen, efter samråd med samarbetsgruppen för nät- och informationssäkerhet, EU-CyCLONe och Enisa, i förteckningen över högkritiska sektorer i bilaga I till direktiv (EU) 2022/2555 identifiera de berörda sektorer eller delsektorer för vilka en ansökningsomgång för att bevilja bidrag kan utlysas. Det ska vara frivilligt för medlemsstaterna att delta i ansökningsomgångarna.

5. När kommissionen identifierar sektorer eller delsektorer som avses i punkt 4 ska den beakta samordnade riskbedömningar och resilienstester på unionsnivå och resultaten av dessa.

6. Samarbetsgruppen för nät- och informationssäkerhet ska i samarbete med kommissionen, unionens höga representant för utrikes frågor och säkerhetspolitik (*den höga representanten*) och Enisa och, inom ramen för dess mandat, EU-CyCLONe, ta fram gemensamma riskscenarier och metoder för den samordnade beredskapstestningen enligt artikel 11.1 a i) och, när så är lämpligt, för andra beredskapsåtgärder enligt a ii) i den artikeln.

7. När en entitet som är verksam inom en högkritisk sektor frivilligt deltar i samordnad beredskapstestning och denna testning leder till rekommendationer om särskilda åtgärder, som den deltagande entiteten skulle kunna integrera i en åtgärdsplan, ska den myndighet i medlemsstaten som ansvarar för samordnad beredskapstestning, när så är lämpligt, se över de deltagande entiteternas uppföljning av dessa åtgärder i syfte att stärka beredskapen.

Artikel 13

Andra beredskapsåtgärder

1. Cybernödmekanismen ska stödja beredskapsåtgärder som inte omfattas av artikel 12. Sådana åtgärder ska omfatta beredskapsåtgärder för entiteter i sektorer som inte identifierats för samordnad beredskapstestning enligt artikel 12. Sådana åtgärder kan stödja sårbarhetsövervakning, riskövervakning, övningar och fortbildning.

2. Stöd till beredskapsåtgärder enligt denna artikel ska ges till medlemsstaterna på begäran och i första hand i form av bidrag och med förbehåll för de villkor som anges i de relevanta arbetsprogram som avses i artikel 24 i förordning (EU) 2021/694.

Artikel 14

Inrättande av en EU-cybersäkerhetsreserv

1. En EU-cybersäkerhetsreserv inrättas för att på begäran bistå de användare som avses i punkt 3 när det gäller att hantera eller stödja hanteringen av betydande cybersäkerhetsincidenter, storskaliga cybersäkerhetsincidenter eller incidenter som är likvärdiga med en storskalig cybersäkerhetsincident, och initiera återhämtningen från sådana incidenter.

2. EU-cybersäkerhetsreserven ska bestå av insatstjänster från betrodda leverantörer av utlokaliserade säkerhetstjänster som valts ut i enlighet med kriterierna i artikel 17.2. EU-cybersäkerhetsreserven får omfatta tjänster som ställts till förfogande på förhand. Om de tjänster som ställs till förfogande på förhand av en betrodd leverantör av utlokaliserade säkerhetstjänster inte används för incidenthantering under den tid som de ställs till förfogande på förhand, ska de kunna omvandlas till beredskapstjänster som rör förebyggande och hantering av incidenter. EU-cybersäkerhetsreserven ska på begäran kunna sättas in i alla medlemsstater, i unionens institutioner, organ och byråer samt i tredjeländer som är associerade till programmet för ett digitalt Europa och som avses i artikel 19.1.

3. Användarna av de tjänster som tillhandahålls av EU-cybersäkerhetsreservens ska utgöras av följande:

a) Medlemsstaternas cyberkrishanteringsmyndigheter och CSIRT-enheter som avses i artikel 9.1 och 9.2 respektive artikel 10 i direktiv (EU) 2022/2555.

b) CERT-EU, i enlighet med artikel 13 i förordning (EU, Euratom) 2023/2841.

c) Behöriga myndigheter såsom CSIRT-enheter och cyberkrishanteringsmyndigheter i tredjeländer som är associerade till programmet för ett digitalt Europa i enlighet med artikel 19.8.

4. Kommissionen ska ha det övergripande ansvaret för genomförandet av EU-cybersäkerhetsreserven. Kommissionen ska fastställa EU-cybersäkerhetsreservens prioriteringar och utveckling, i samordning med samarbetsgruppen för nät- och informationssäkerhet och i linje med behoven hos de användare som avses i punkt 3, övervaka genomförandet och säkerställa komplementaritet, konsekvens, synergi och förbindelser med andra stödåtgärder enligt denna förordning samt andra unionsåtgärder och unionsprogram. Dessa prioriteringar ska ses över och, när så är lämpligt, ändras vartannat år. Kommissionen ska informera Europaparlamentet och rådet om de prioriteringarna och om eventuella ändringar av dessa.

5. Utan att det påverkar kommissionens övergripande ansvar för genomförandet av EU-cybersäkerhetsreserven enligt punkt 4 i denna artikel och med förbehåll för en överenskommelse om medverkan enligt definitionen i artikel 2.19 i förordning (EU, Euratom) 2024/2509, ska kommissionen helt eller delvis anförtro driften och förvaltningen av EU-cybersäkerhetsreserven åt Enisa. Aspekter som inte anförtrotts Enisa ska fortsatt förvaltas direkt av kommissionen.

6. Enisa ska minst vartannat år kartlägga vilka tjänster de användare som avses i punkt 3 a och b i denna artikel behöver. Kartläggningen ska också omfatta tillgängligheten för sådana tjänster, inbegripet från rättsliga enheter som är etablerade eller bedöms vara etablerade i medlemsstater och som kontrolleras av medlemsstater eller medborgare i medlemsstater. Vid kartläggningen av denna tillgänglighet ska Enisa bedöma den kompetens och kapacitet hos unionens cybersäkerhetsarbetskraft som är relevant för EU-cybersäkerhetsreservens mål. Vid kartläggningen ska Enisa samråda med samarbetsgruppen för nät- och informationssäkerhet, EU-CyCLONe, kommissionen och, i tillämpliga fall, interinstitutionella cybersäkerhetsstyrelsen, inrättad enligt artikel 10 i förordning (EU, Euratom) 2023/2841. Vid kartläggningen av tjänsternas tillgänglighet ska Enisa också samråda med berörda parter inom cybersäkerhetsbranschen, inbegripet leverantörer av utlokaliserade säkerhetstjänster. Enisa ska göra en liknande kartläggning, efter att ha informerat rådet och efter samråd med EU-CyCLONe, kommissionen och, när så är lämpligt, med den höga representanten, för att identifiera behoven hos de användare som avses i punkt 3 c i denna artikel.

7. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 23 för att komplettera denna förordning genom att specificera vilken typ av och hur många insatstjänster som behövs för EU-cybersäkerhetsreserven. När kommissionen utarbetar dessa delegerade akter ska den beakta den kartläggning som avses i punkt 6 i den här artikeln, och får utbyta råd och samarbeta med samarbetsgruppen för nät- och informationssäkerhet och Enisa.

Artikel 15

Begäran om stöd från EU-cybersäkerhetsreserven

1. De användare som avses i artikel 14.3 får begära tjänster från EU-cybersäkerhetsreserven för att stödja insatser vid och initiera återhämtning från betydande cybersäkerhetsincidenter, storskaliga cybersäkerhetsincidenter eller incidenter som är likvärdiga med en storskalig cybersäkerhetsincident.

2. För att få stöd från EU-cybersäkerhetsreserven ska de användare som avses i artikel 14.3 vidta alla lämpliga åtgärder för att mildra effekterna av den incident som begäran om stöd avser, vilket i förekommande fall innefattar tillhandahållande av direkt tekniskt bistånd och andra resurser för att bistå incidenthanteringen, samt återhämtningsinsatser.

3. En begäran om stöd ska lämnas till den upphandlande myndigheten på följande sätt:

   a) När det gäller de användare som avses i artikel 14.3 a i denna förordning, via den gemensamma kontaktpunkt som utsetts eller inrättats enligt artikel 8.3 i direktiv (EU) 2022/2555.

b) När det gäller den användare som avses i artikel 14.3 b, av den användaren.

c) När det gäller de användare som avses i artikel 14.3 c, via den gemensamma kontaktpunkt som avses i artikel 19.9.

4. När det gäller begäranden från de användare som avses i artikel 14.3 a ska medlemsstaterna informera CSIRT-nätverket och, när så är lämpligt, EU-CyCLONe om sina användares begäranden om stöd till incidenthantering och initial återhämtning enligt den här artikeln.

5. En begäran om stöd till incidenthantering och initial återhämtning ska omfatta följande:

a) Relevant information om den berörda entiteten och incidentens potentiella konsekvenser för

i) när det gäller de användare som avses i artikel 14.3 a i denna förordning, berörda medlemsstater och användare, inbegripet risken för spridning till en annan medlemsstat,

ii) när det gäller den användare som avses i artikel 14.3 b i denna förordning, berörda unionsinstitutioner, unionsorgan eller unionsbyråer,

iii) när det gäller de användare som avses i artikel 14.3 c i denna förordning, berörda tredjeländer som deltar i programmet för ett digitalt Europa.

b) Information om den begärda tjänsten, tillsammans med den planerade användningen av det begärda stödet, inbegripet en angivelse av de uppskattade behoven.

c) Relevant information om de åtgärder som vidtagits för att begränsa den incident som begäran om stöd avser, enligt punkt 2.

d) När så är lämpligt, tillgänglig information om andra former av stöd som finns att få för den berörda entiteten.

6. Enisa ska i samarbete med kommissionen och EU-CyCLONe utarbeta en mall för att underlätta inlämningen av begäranden om stöd från EU-cybersäkerhetsreserven.

7. Kommissionen får genom genomförandeakter ytterligare specificera närmare förfaranden för hur stödtjänster från EU-cybersäkerhetsreserven ska begäras och hur sådana begäranden ska besvaras enligt denna artikel samt artiklarna 16.1 och 19.10, inklusive förfaranden för inlämning av sådana begäranden och tillhandahållande av svaren samt mallarna för de rapporter som avses i artikel 16.9. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 24.2.

Artikel 16

Genomförande av stöd från EU-cybersäkerhetsreserven

1. När det gäller begäranden från de användare som avses i artikel 14.3 a och b ska begäranden om stöd från EU-cybersäkerhetsreserven bedömas av den upphandlande myndigheten. Ett svar ska sändas till de användare som avses i artikel 14.3 a och b utan dröjsmål och under alla omständigheter senast 48 timmar efter det att begäran lämnades för att säkerställa stödets effektivitet. Den upphandlande myndigheten ska informera rådet och kommissionen om resultatet av processen.

2. När det gäller information som utbyts i samband med begäran om och tillhandahållande av EU-cybersäkerhetsreservens tjänster ska alla parter som deltar i tillämpningen av denna förordning

   a) begränsa användningen och utbytet av denna information till vad som är nödvändigt för att de ska kunna fullgöra sina skyldigheter eller uppgifter enligt denna förordning,

   b) använda och utbyta information som är konfidentiell eller säkerhetsskyddsklassificerad unionsrätten och nationell rätt endast i enlighet med den rätten, och

   c) säkerställa ett ändamålsenligt, effektivt och säkert informationsutbyte, när så är lämpligt genom att använda och iaktta relevanta protokoll för informationsutbyte, inbegripet Traffic Light Protocol.

3. Vid bedömningen av enskilda begäranden enligt artiklarna 16.1 och 19.10 ska den upphandlande myndigheten eller kommissionen, beroende på vad som är tillämpligt, först bedöma om kriterierna i artikel 15.1 och 15.2 är uppfyllda. Om så är fallet ska de bedöma vilken varaktighet och form som lämpar sig för stödet, med beaktande av målet i artikel 1.3 b och följande kriterier, när så är lämpligt:

a) Incidentens omfattning och allvarlighetsgrad.

b) Typ av berörd entitet, där högre prioritet ges åt incidenter som påverkar väsentliga entiteter som avses i artikel 3.1 i direktiv (EU) 2022/2555.

c) De potentiella konsekvenserna av incidenten för berörda medlemsstater, unionsinstitutioner, unionsorgan eller unionsbyråer, eller tredjeländer som är associerade till programmet för ett digitalt Europa.

d) Incidentens potentiella gränsöverskridande karaktär och risken för spridning till andra medlemsstater, unionsinstitutioner, unionsorgan eller unionsbyråer, eller tredjeländer som är associerade till programmet för ett digitalt Europa.

e) De åtgärder som vidtagits av användaren för att bistå incidenthanteringen och de initiala återhämtningsinsatserna, enligt artikel 15.2.

4. När det gäller att prioritera begäranden ska, i de fall där begäranden inkommer samtidigt från användare som avses i artikel 14.3, de kriterier som anges i punkt 3 i den här artikeln beaktas, när så är lämpligt, utan att det påverkar principen om lojalt samarbete mellan medlemsstaterna och unionens institutioner, organ och byråer. Om två eller fler begäranden bedöms vara likvärdiga enligt de kriterierna, ska begäranden från medlemsstaternas användare ges högre prioritet. Om driften och förvaltningen av EU-cybersäkerhetsreserven helt eller delvis har anförtrotts åt Enisa enligt artikel 14.5 ska Enisa och kommissionen i nära samarbete prioritera begäranden i enlighet med denna punkt.

5. EU-cybersäkerhetsreservens tjänster ska tillhandahållas i enlighet med särskilda avtal mellan den betrodda leverantören av utlokaliserade säkerhetstjänster och den användare som tillhandahålls stödet inom ramen för EU-cybersäkerhetsreserven. Dessa tjänster får tillhandahållas i enlighet med särskilda avtal mellan den betrodda leverantören av utlokaliserade säkerhetstjänster, användaren och den berörda entiteten. Alla avtal som avses i denna punkt ska omfatta bland annat villkoren för skadeståndsansvar.

6. De avtal som avses i punkt 5 ska baseras på mallar som utarbetats av Enisa, efter samråd med medlemsstaterna och, när så är lämpligt, andra användare av EU-cybersäkerhetsreserven.

7. Kommissionen, Enisa och andra användare av EU-cybersäkerhetsreserven ska inte ha något avtalsrättsligt ansvar för skador som åsamkas tredje part av de tjänster som tillhandahålls inom ramen för genomförandet av EU-cybersäkerhetsreserven.

8. Användare får nyttja de tjänster från EU-cybersäkerhetsreserven som tillhandahålls som svar på en begäran enligt artikel 15.1 endast för att stödja insatser vid och initiera återhämtning från betydande cybersäkerhetsincidenter, storskaliga cybersäkerhetsincidenter eller incidenter som är likvärdiga med en storskalig cybersäkerhetsincident. De får nyttja dessa tjänster endast med avseende på

   a) entiteter som är verksamma inom högkritiska sektorer eller entiteter som är verksamma i andra kritiska sektorer, när det gäller de användare som avses i artikel 14.3 a, samt likvärdiga entiteter när det gäller de användare som avses i artikel 14.3 c, och

   b) unionens institutioner, organ och byråer, när det gäller den användare som avses i artikel 14.3 b.

9. Inom två månader från det att stöd avslutats ska användare som har mottagit stöd lämna en sammanfattande rapport om den tjänst som tillhandahållits, de resultat som uppnåtts och lärdomar som dragits till

   a) kommissionen, Enisa, CSIRT-nätverket och EU-CyCLONe, när det gäller de användare som avses i artikel 14.3 a,

   b) kommissionen, Enisa och interinstitutionella cybersäkerhetsstyrelsen, när det gäller den användare som avses i artikel 14.3 b,

c) kommissionen, när det gäller de användare som avses i artikel 14.3 c.

Kommissionen ska översända eventuella sammanfattande rapporter som den enligt första stycket c i denna punkt har tagit emot från användare som avses i artikel 14.3 till rådet och den höga representanten.

10. Om driften och förvaltningen av EU-cybersäkerhetsreserven helt eller delvis har anförtrotts åt Enisa enligt artikel 14.5 i denna förordning ska Enisa regelbundet rapportera till och samråda med kommissionen i detta avseende. I detta sammanhang ska Enisa till kommissionen omedelbart sända alla begäranden som tas emot från de användare som avses i artikel 14.3 c i denna förordning och, om så krävs för prioriteringen enligt den här artikeln, alla begäranden som tas emot från de användare som avses i artikel 14.3 a eller b i denna förordning. Skyldigheterna i denna punkt ska inte påverka tillämpningen av artikel 14 i förordning (EU) 2019/881.

11. När det gäller de användare som avses i artikel 14.3 a och b ska den upphandlande myndigheten till samarbetsgruppen för nät- och informationssäkerhet regelbundet och minst två gånger om året rapportera om användningen och resultaten av stödet.

12. När det gäller de användare som avses i artikel 14.3 c ska kommissionen regelbundet och minst två gånger om året rapportera till rådet och informera den höga representanten om användningen och resultaten av stödet.

Artikel 17

Betrodda leverantörer av utlokaliserade säkerhetstjänster

1. I upphandlingsförfarandena i samband med inrättandet av EU-cybersäkerhetsreserven ska den upphandlande myndigheten agera i enlighet med principerna i förordning (EU, Euratom) 2024/2509 och i enlighet med följande principer:

   a) Säkerställa att de tjänster som ingår i EU-cybersäkerhetsreserven som helhet innebär att EU-cybersäkerhetsreserven omfattar tjänster som kan användas i alla medlemsstater, med beaktande av i synnerhet nationella krav på tillhandahållandet av sådana tjänster, inbegripet i fråga om språk, certifiering eller ackreditering.

   b) Säkerställa skyddet av unionens och dess medlemsstaters väsentliga säkerhetsintressen.

   c) Säkerställa att EU-cybersäkerhetsreserven tillför unionsmervärde, genom att bidra till de mål som fastställs i artikel 3 i förordning (EU) 2021/694, inbegripet att främja utvecklingen av cybersäkerhetskompetens i unionen.

2. Vid upphandlingen av tjänster för EU-cybersäkerhetsreserven ska den upphandlande myndigheten inkludera följande kriterier och krav i upphandlingsdokumenten:

a) Leverantören ska visa att dess personal har högsta grad av yrkesmässig integritet, oberoende och ansvar och den tekniska kompetens som krävs för att utföra arbetet på sitt specifika område samt säkerställa expertisens varaktighet och kontinuitet och de tekniska resurser som krävs.

b) Leverantören och eventuella relevanta dotterföretag och underleverantörer ska följa tillämpliga regler om skydd av säkerhetsskyddsklassificerad information och ha lämpliga åtgärder, inbegripet, när så är lämpligt, avtal sinsemellan, för att skydda konfidentiell information som rör tjänsten, i synnerhet faktaunderlag, resultat och rapporter.

c) Leverantören ska på ett tillfredsställande sätt styrka att styrningsstrukturen är transparent och inte riskerar att undergräva dess opartiskhet och tjänstekvaliteten eller orsaka intressekonflikter.

d) Leverantören ska ha en lämplig säkerhetsprövning, åtminstone för personal som är avsedd för utförandet av tjänsterna, när medlemsstaterna kräver detta.

e) Leverantören ska ha den relevanta säkerhetsnivån för sina it-system.

f) Leverantören ska vara utrustad med den hårdvara och programvara som behövs för den efterfrågade tjänsten, och som inte får ha några kända sårbarheter som kan utnyttjas, som ska ha de senaste säkerhetsuppdateringarna och som under alla omständigheter ska vara förenlig med tillämpliga bestämmelser i Europaparlamentets och rådets förordning (EU) 2024/…[23+].

g) Leverantören ska kunna visa att den har erfarenhet av att leverera liknande tjänster till relevanta nationella myndigheter, entiteter som är verksamma inom högkritiska sektorer eller entiteter som är verksamma inom andra kritiska sektorer.

h) Leverantören ska kunna tillhandahålla tjänsten inom en kort tidsram i den eller de medlemsstater där den kan tillhandahålla tjänsten.

i) Leverantören ska kunna tillhandahålla tjänsten på ett eller flera av unionens institutioners eller en medlemsstats officiella språk enligt vad som eventuellt efterfrågas av den eller de medlemsstater eller de användare enligt artikel 14.3 b och c där leverantören kan tillhandahålla tjänsten.

j) När en europeisk ordning för cybersäkerhetscertifiering för utlokaliserade säkerhetstjänster enligt förordning (EU) 2019/881 införts ska leverantören vara certifierad i enlighet med den ordningen inom två år från den dag då ordningen börjar tillämpas.

---

[23] Europaparlamentets och rådets förordning (EU) 2024/… av den … om … (EUT L, …, ELI: …).

[+] EUT: För in numret på den förordning som finns i dokument PE-CONS 100/23 (2022/0272 (COD)) och för in den förordningens nummer, datum, titel, EUT-hänvisning och ELI-hänvisning i fotnoten.

k) Leverantören ska i anbudet ange omvandlingsvillkoren för eventuella outnyttjade incidenthanteringstjänster som skulle kunna omvandlas till beredskapstjänster med nära anknytning till incidenthantering, såsom övningar eller fortbildning.

3. I syfte att upphandla tjänster för EU-cybersäkerhetsreserven får den upphandlande myndigheten, när så är lämpligt, utarbeta kriterier och krav utöver dem som avses i punkt 2, i nära samarbete med medlemsstaterna.

Artikel 18

Åtgärder till stöd för ömsesidigt bistånd

1. Cybernödmekanismen ska stödja tekniskt bistånd som en medlemsstat ger till en annan medlemsstat som påverkas av en betydande cybersäkerhetsincident eller storskalig cybersäkerhetsincident, även i de fall som avses i artikel 11.3 f i direktiv (EU) 2022/2555.

2. Stödet till det tekniska ömsesidiga bistånd som avses i punkt 1 i denna artikel ska ges i form av bidrag och med förbehåll för de villkor som anges i de relevanta arbetsprogram som avses i artikel 24 i förordning (EU) 2021/694.

Artikel 19

Stöd till tredjeländer som är associerade till programmet för ett digitalt Europa

1. Ett tredjeland som är associerat till programmet för ett digitalt Europa får begära stöd från EU-cybersäkerhetsreserven om det avtal genom vilket det är associerat till programmet för ett digitalt Europa föreskriver deltagande i EU-cybersäkerhetsreserven. Detta avtal ska innehålla bestämmelser som ålägger det berörda tredjeland som är associerat till programmet för ett digitalt Europa att fullgöra skyldigheterna i punkterna 2 och 9 i denna artikel. När det gäller ett tredjelands deltagande i EU-cybersäkerhetsreserven får den partiella associeringen av ett tredjeland till programmet för ett digitalt Europa innebära en associering som är begränsad till det operativa mål som anges i artikel 6.1 g i förordning (EU) 2021/694.

2. Inom tre månader efter att det avtal som avses i punkt 1 har ingåtts och under alla omständigheter innan stöd mottas från EU-cybersäkerhetsreserven ska det tredjeland som är associerat till programmet för ett digitalt Europa förse kommissionen med information om sin cyberresiliens och riskhanteringskapacitet, inbegripet åtminstone information om nationella åtgärder som vidtagits som förberedelse inför betydande cybersäkerhetsincidenter, storskaliga cybersäkerhetsincidenter eller incidenter som är likvärdiga med en storskalig cybersäkerhetsincident, samt information om ansvariga nationella entiteter, inbegripet enheter för hantering av it-säkerhetsincidenter eller motsvarande entiteter, deras kapacitet och de resurser som de tilldelats. De tredjeländer som är associerade till programmet för ett digitalt Europa ska regelbundet och minst en gång om året tillhandahålla uppdateringar av denna information. Kommissionen ska tillhandahålla denna information till den höga representanten och Enisa i syfte att underlätta tillämpningen av punkt 11.

3. Kommissionen ska med avseende på varje tredjeland som är associerat till programmet för ett digitalt Europa och som avses i punkt 1 regelbundet och minst en gång om året bedöma följande kriterier:

a) Huruvida landet uppfyller villkoren i det avtal som avses i punkt 1, i den mån dessa villkor gäller deltagande i EU-cybersäkerhetsreserven.

b) Huruvida landet har vidtagit lämpliga åtgärder som förberedelse inför betydande cybersäkerhetsincidenter eller incidenter som är likvärdiga med en storskalig cybersäkerhetsincident, på grundval av den information som avses i punkt 2.

c) Huruvida tillhandahållandet av stöd är förenligt med unionens politik gentemot och de övergripande förbindelserna med landet och huruvida det är förenligt med annan unionspolitik på säkerhetsområdet.

Med avseende på kriteriet i led c i första stycket ska kommissionen samråda med den höga representanten när den gör den bedömning som avses i det stycket.

Om kommissionen konstaterar att ett tredjeland som är associerat till programmet för ett digitalt Europa uppfyller alla de villkor som avses i första stycket ska kommissionen lägga fram ett förslag för rådet om att i enlighet med punkt 4 anta en genomförandeakt genom vilken tillhandahållandet av stöd från EU-cybersäkerhetsreserven till det landet godkänns.

4. Rådet får anta de genomförandeakter som avses i punkt 3. Dessa genomförandeakter ska tillämpas i högst ett år. De får förnyas. De får omfatta en gräns, som inte får understiga 75 dagar, för antalet dagar under vilka stöd kan ges som svar på en enskild begäran.

   Vid tillämpning av denna artikel ska rådet agera snabbt och, som regel, anta de genomförandeakter som avses i den här punkten inom åtta veckor efter det att antagandet av det relevanta förslag som avses i punkt 3 tredje stycket.

5. Rådet får när som helst på förslag av kommissionen ändra eller upphäva en genomförandeakt som antagits enligt punkt 4.

   Om rådet anser att det har skett en betydande förändring i fråga om det kriterium som anges i punkt 3 första stycket c får rådet ändra eller upphäva en genomförandeakt som antagits enligt punkt 4 på vederbörligen motiverat initiativ av en eller flera medlemsstater.

6. När rådet utövar sina genomförandebefogenheter enligt denna artikel ska det tillämpa de kriterier som avses i punkt 3 första stycket och redogöra för sin bedömning av dessa kriterier. I synnerhet ska rådet, när det agerar på eget initiativ enligt punkt 5 andra stycket, redogöra för den betydande förändring som avses i det stycket.

7. Stöd från EU-cybersäkerhetsreserven till ett tredjeland som är associerat till programmet för ett digitalt Europa ska uppfylla alla särskilda villkor som fastställs i det avtal som avses i punkt 1.

8. Användare från tredjeländer som är associerade till programmet för ett digitalt Europa och som är berättigade att erhålla tjänster från EU-cybersäkerhetsreserven ska inbegripa behöriga myndigheter såsom enheter för hantering av it-säkerhetsincidenter eller motsvarande entiteter, och cyberkrishanteringsmyndigheter.

9. Varje tredjeland som är associerat till programmet för ett digitalt Europa och som är berättigat till stöd från EU-cybersäkerhetsreserven ska utse en myndighet som ska fungera som gemensam kontaktpunkt vid tillämpning av denna förordning.

10. Begäranden om stöd från EU-cybersäkerhetsreserven enligt denna artikel ska bedömas av kommissionen. Den upphandlande myndigheten får ge stöd till ett tredjeland endast om och så länge som en genomförandeakt från rådet, antagen enligt punkt 4 i denna artikel, som godkänner sådant stöd med avseende på det landet är i kraft. Ett svar ska utan onödigt dröjsmål sändas till de användare som avses i artikel 14.3 c.

11. När kommissionen tar emot en begäran om stöd enligt denna artikel ska den omedelbart underrätta rådet. Kommissionen ska hålla rådet underrättat om bedömningen av begäran. Kommissionen ska också samarbeta med den höga representanten när det gäller begäranden som mottagits och genomförandet av stöd från EU-cybersäkerhetsreserven som beviljats tredjeländer som är associerade till programmet för ett digitalt Europa. Kommissionen ska också ta hänsyn till eventuella synpunkter från Enisa avseende dessa begäranden.

Artikel 20

Samordning med unionens krishanteringsmekanismer

1. I de fall där en betydande cybersäkerhetsincident, en storskalig cybersäkerhetsincident eller en incident som är likvärdig med en storskalig cybersäkerhetsincident har sitt ursprung eller resulterar i en katastrof enligt definitionen i artikel 4.1 i beslut nr 1313/2013/EU ska det stöd som ges enligt denna förordning för att hantera en sådan incident komplettera åtgärder som vidtas enligt det beslutet, utan att tillämpningen av det beslutet påverkas.

2. I de fall där en storskalig cybersäkerhetsincident eller incident som är likvärdig med en storskalig cybersäkerhetsincident aktiverar EU-arrangemangen för integrerad politisk krishantering (IPCR) enligt genomförandebeslut (EU) 2018/1993 ska det stöd som ges enligt denna förordning för att hantera en sådan incident hanteras i enlighet med relevanta förfaranden inom ramen för IPCR.

Kapitel IV

Europeisk mekanism för utvärdering av cybersäkerhetsincidenter

Artikel 21

Europeisk mekanism för utvärdering av cybersäkerhetsincidenter

1. På begäran av kommissionen eller EU-CyCLONe ska Enisa, med stöd av CSIRT-nätverket och med de berörda medlemsstaternas godkännande, granska och analysera cyberhot, kända sårbarheter som kan utnyttjas och begränsningsåtgärder med avseende på en viss betydande cybersäkerhetsincident eller storskalig cybersäkerhetsincident. När granskningen och analysen av en incident har slutförts, och i syfte att dra lärdomar för att undvika eller begränsa framtida incidenter, ska Enisa lämna en incidentgranskningsrapport till EU-CyCLONe, CSIRT-nätverket, de berörda medlemsstaterna och kommissionen så att de kan utföra sina uppgifter, i synnerhet de uppgifter som anges i artiklarna 15 och 16 i direktiv (EU) 2022/2555. När en incident påverkar ett tredjeland som är associerat till programmet för ett digitalt Europa ska Enisa tillhandahålla denna rapport till rådet. I sådana fall ska kommissionen tillhandahålla rapporten till den höga representanten.

2. Vid utarbetandet av den incidentgranskningsrapport som avses i punkt 1 i denna artikel ska Enisa samarbeta med och samla in återkoppling från alla berörda parter, inbegripet medlemsstaternas företrädare, kommissionen, andra berörda unionsinstitutioner, unionsorgan och unionsbyråer, industrin, inbegripet leverantörer av utlokaliserade säkerhetstjänster, och användare av cybersäkerhetstjänster. När så är lämpligt ska Enisa, tillsammans med CSIRT-enheterna och när så är relevant de behöriga myndigheter som utsetts eller inrättats enligt artikel 8.1 i direktiv (EU) 2022/2555, också samarbeta med entiteter som påverkas av betydande cybersäkerhetsincidenter eller storskaliga cybersäkerhetsincidenter. De företrädare med vilka samråd sker ska redovisa alla potentiella intressekonflikter.

3. Den incidentgranskningsrapport som avses i punkt 1 i denna artikel ska omfatta en granskning och en analys av den specifika betydande cybersäkerhetsincidenten eller storskaliga cybersäkerhetsincidenten, inbegripet de huvudsakliga orsakerna, de kända sårbarheter som kan utnyttjas och lärdomar som dragits. Enisa ska säkerställa att rapporten är förenlig med unionsrätten eller nationell rätt om skydd av känsliga eller säkerhetsskyddsklassificerade uppgifter. Om den eller de berörda medlemsstaterna eller andra användare som avses i artikel 14.3 som påverkas av incidenten begär det ska de data och den information som rapporten innehåller anonymiseras. Rapporten får inte innehålla några uppgifter om aktivt utnyttjade sårbarheter som inte har avhjälpts.

4. När så är lämpligt ska incidentgranskningsrapporten innehålla rekommendationer som syftar till att förbättra unionens arbete på cyberområdet, och den får innehålla bästa praxis och lärdomar från berörda parter.

5. Enisa får utfärda en offentligt tillgänglig version av incidentgranskningsrapporten. Den versionen av rapporten ska endast innehålla tillförlitlig offentlig information eller annan tillförlitlig information med den eller de berörda medlemsstaternas samtycke och, när det gäller information om en användare enligt artikel 14.3 b eller c, med den användarens samtycke.

Kapitel V

Slutbestämmelser

Artikel 22

Ändringar av förordning (EU) 2021/694

Förordning (EU) 2021/694 ska ändras på följande sätt:

1. Artikel 6 ska ändras på följande sätt:

   a) Punkt 1 ska ändras på följande sätt:

      i) Följande led ska införas:

”aa) Stödja utvecklingen av det europeiska system med cybersäkerhetsvarningar som inrättats genom artikel 3 i Europaparlamentets och rådets förordning (EU) …/…[*+] (europeiska systemet med cybersäkerhetsvarningar), vilket innefattar utveckling, inrättande och drift av nationella cybernav och gränsöverskridande cybernav som bidrar till situationsmedvetenhet i unionen och till att förbättra unionens underrättelsekapacitet när det gäller cyberhot.

---

[*] Europaparlamentets och rådets förordning (EU) …/… om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter och om ändring av förordning (EU) 2021/694 (cybersolidaritetsakten) (EUT L, …, ELI: …)”

[+] EUT: vänligen inför numret på förordningen i dokument PE-CONS 94/24 (2023/0109(COD)) och infoga den förordningens nummer, datum, EUT-referens och ELI-referens i fotnoten.

ii) Följande led ska läggas till:

”g) Inrätta och driva den cybernödmekanism som inrättats genom artikel 10 i förordning (EU) …/…[+], inklusive den EU-cybersäkerhetsreserv som inrättats genom artikel 14 i den förordningen (*EU-cybersäkerhetsreserven)* för att stödja medlemsstaternas beredskap för och insatser vid betydande cybersäkerhetsincidenter och storskaliga cybersäkerhetsincidenter, som kompletterar nationella resurser och kapaciteter och andra former av stöd som finns tillgängliga på unionsnivå, och för att stödja andra användares insatser vid betydande cybersäkerhetsincidenter och storskaliga cybersäkerhetsincidenter.”

b) Punkt 2 ska ersättas med följande:

”2. Åtgärderna inom ramen för specifikt mål 3 ska främst genomföras genom Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och nätverket av nationella samordningscentrum i enlighet med Europaparlamentets och rådets förordning (EU) 2021/887[*]. EU-cybersäkerhetsreserven ska emellertid genomföras av kommissionen och, i enlighet med artikel 14.6 i förordning (EU) …/…[+] av Enisa.

---

[*] Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum (EUT L 202, 8.6.2021, s. 1).

[+] EUT: vänligen inför numret på förordningen i dokument PE-CONS 94/24 (2023/0109(COD)).

2. Artikel 9 ska ändras på följande sätt:

a) I punkt 2 ska leden b, c och d ersättas med följande:

”b) 1 760 806 000 EUR för specifikt mål 2 – Artificiell intelligens.

c) 1 372 020 000 EUR för specifikt mål 3 – Cybersäkerhet och förtroende.

d) 482 640 000 EUR för specifikt mål 4 – Avancerade digitala färdigheter.”

b) Följande punkt ska läggas till:

”8. Med avvikelse från artikel 12.1 i budgetförordningen gäller att outnyttjade åtagande- och betalningsbemyndiganden för åtgärder inom ramen för genomförandet av EU-cybersäkerhetsreserven och åtgärder till stöd för ömsesidigt bistånds enligt förordning (EU) …/…[+] som syftar till att uppnå målen i artikel 6.1 g i den här förordningen ska överföras automatiskt och får ingås och utbetalas fram till och med den 31 december påföljande budgetår. Europaparlamentet och rådet ska informeras om de anslag som har överförts enligt artikel 12.6 i budgetförordningen.”

[+] EUT: vänligen inför numret på förordningen i dokument PE-CONS 94/24 (2023/0109(COD)).

3. Artikel 12 ska ändras på följande sätt:

a) Följande punkter ska införas:

”5a. Punkt 5 ska, när det gäller rättsliga enheter som är etablerade i unionen men kontrolleras från tredjeländer, inte tillämpas på en åtgärd för genomförandet av det europeiska systemet med cybersäkerhetsvarningar om båda följande villkor är uppfyllda med avseende på den berörda åtgärden:

”a) Med beaktande av resultaten av den kartläggning som genomförs enligt artikel 9.4 i förordning (EU) …/…[+] finns det en verklig risk för att verktyg, infrastruktur eller tjänster som är nödvändiga och tillräckliga för att åtgärden på ett adekvat sätt ska kunna bidra till målet för det europeiska systemet med cybersäkerhetsvarningar inte kommer att finnas tillgängliga hos rättsliga enheter som är etablerade eller bedöms vara etablerade i medlemsstater och som kontrolleras av medlemsstater eller medborgare i medlemsstater.

b) Säkerhetsrisken med upphandling från sådana rättsliga enheter inom det europeiska systemet med cybersäkerhetsvarningar står i proportion till fördelarna och undergräver inte unionens och dess medlemsstaters väsentliga säkerhetsintressen.

[+] EUT: För in numret på den förordning som finns i dokument PE-CONS 94/24 (2023/0109(COD)).

5b. Punkt 5 ska, när det gäller rättsliga enheter som är etablerade i unionen men kontrolleras från tredjeländer, inte tillämpas på åtgärder för genomförandet av EU-cybersäkerhetsreserven om båda följande villkor är uppfyllda med avseende på den berörda åtgärden:

”a) Med beaktande av resultaten av den kartläggning som genomförs enligt artikel 14.6 i förordning (EU) …/…[+] finns det en verklig risk för att teknik, expertis eller kapacitet som är nödvändig och tillräcklig för att EU-cybersäkerhetsreserven på ett adekvat sätt ska kunna fylla sina funktioner inte kommer att finnas tillgängliga hos rättsliga enheter som är etablerade eller bedöms vara etablerade i medlemsstater och som kontrolleras av medlemsstater eller medborgare i medlemsstater.

b) Säkerhetsrisken med att inkludera sådana rättsliga enheter i EU-cybersäkerhetsreserven står i proportion till fördelarna och undergräver inte unionens och dess medlemsstaters väsentliga säkerhetsintressen.”

b) Punkt 6 ska ersättas med följande:

”6. Om det är vederbörligen motiverat av säkerhetsskäl får arbetsprogrammet också föreskriva att rättsliga enheter som är etablerade i associerade länder och rättsliga enheter som är etablerade i unionen men kontrolleras från tredjeländer kan vara berättigade att delta i alla eller vissa åtgärder inom ramen för de specifika målen 1 och 2 endast om de uppfyller de krav som dessa rättsliga enheter ska uppfylla för att garantera skydd av unionens och medlemsstaternas väsentliga säkerhetsintressen och säkerställa skydd av uppgifter i säkerhetsskyddsklassificerade handlingar. Dessa krav ska anges i arbetsprogrammet.”

Första stycket ska också tillämpas, när det gäller rättsliga enheter som är etablerade i unionen men kontrolleras från tredjeländer, på åtgärder inom ramen för specifikt mål 3

a) för att genomföra det europeiska systemet med cybersäkerhetsvarningar när punkt 5 är tillämplig, och

b) för att genomföra EU-cybersäkerhetsreserven punkt 5b är tillämplig.”

4. Artikel 14.2 ska ersättas med följande:

”2. Programmet får tillhandahålla finansiering i alla former som anges i budgetförordningen, inbegripet i synnerhet genom upphandling som primär form, eller bidrag och priser.

Om upphandling av innovativa varor och tjänster krävs för att uppnå målet med en åtgärd får bidrag endast beviljas bidragsmottagare som är upphandlande myndigheter eller upphandlande enheter enligt definitionen i Europaparlamentets och rådets direktiv 2014/24/EU* och 2014/25/EU**.

Om tillhandahållande av innovativa varor eller tjänster som ännu inte är kommersiellt tillgängliga i stor skala krävs för att uppnå målet med en åtgärd får den upphandlande myndigheten eller den upphandlande enheten tillåta att flera kontrakt tilldelas inom samma upphandlingsförfarande.

Om det är vederbörligen motiverat av hänsyn till den allmänna säkerheten får den upphandlande myndigheten eller den upphandlande enheten kräva att platsen för kontraktets fullgörande ska ligga inom unionens territorium.

Vid genomförandet av upphandlingsförfaranden för EU-cybersäkerhetsreserven får kommissionen och Enisa agera som inköpscentral för upphandling på uppdrag av tredjeländer som är associerade till programmet i enlighet med artikel 10 i denna förordning, eller i deras namn. Kommissionen och Enisa får också agera som grossister genom att köpa, lagra och sälja eller donera varor och tjänster, inbegripet uthyrning, till dessa tredjeländer. Med avvikelse från artikel 168.3 i Europaparlamentets och rådets förordning (EU, Euratom) 2024/2509*** är det tillräckligt med en begäran från ett enda tredjeland för att ge kommissionen eller Enisa mandat att agera.

Vid genomförandet av upphandlingsförfaranden för EU-cybersäkerhetsreserven får kommissionen och Enisa agera som inköpscentral för upphandling på uppdrag av unionens institutioner, organ eller byråer eller i deras namn. Kommissionen och Enisa får också agera som grossist genom att köpa, lagra och sälja eller donera varor och tjänster, inbegripet uthyrning, till unionens institutioner, organ eller byråer. Med avvikelse från artikel 168.3 i förordning (EU, Euratom) 2024/2509+ är det tillräckligt med en begäran från en enda av unionens institutioner, organ eller byråer för att ge kommissionen eller Enisa mandat att agera.

Programmet får också tillhandahålla finansiering i form av finansiella instrument inom ramen för blandfinansieringsinsatser.

---

* Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG (EUT L 94, 28.3.2014, s. 65).

** Europaparlamentets och rådets direktiv 2014/25/EU av den 26 februari 2014 om upphandling av enheter som är verksamma på områdena vatten, energi, transporter och posttjänster och om upphävande av direktiv 2004/17/EG (EUT L 94, 28.3.2014, s. 243).

*** Europaparlamentets och rådets förordning (EU, Euratom) 2024/2509 av den 23 september 2024 om finansiella regler för unionens allmänna budget (EUT L, 2024/2509, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).”

5. Följande artikel ska införas:

”*Artikel 16a*

Regelkonflikter

Vid åtgärder för genomförandet av det europeiska systemet med cybersäkerhetsvarningar ska de tillämpliga reglerna vara de som anges i artiklarna 4, 5 och 9 i förordning (EU) …/…[+]. Om bestämmelserna i den här förordningen står i strid med artiklarna 4, 5 och 9 i förordning (EU) …/… ska de sistnämnda ha företräde och tillämpas på dessa specifika åtgärder.

[+] EUT: För in numret på den förordning som finns i dokument PE-CONS 94/24 (2023/0109(COD)).

När det gäller EU-cybersäkerhetsreserven anges särskilda regler för deltagande av tredjeländer som är associerade till programmet i artikel 19 i förordning (EU) …/…[+]. Om bestämmelserna i den här förordningen står i strid med artikel 19 i förordning (EU) …/…[+] ska den sistnämnda ha företräde och tillämpas på dessa specifika åtgärder.”

6. Artikel 19 ska ersättas med följande:

”*Artikel 19*
Bidrag

Bidrag inom programmet ska tilldelas och förvaltas i enlighet med avdelning VIII i budgetförordningen och får täcka upp till 100 % av de stödberättigande kostnaderna, utan att det påverkar principen om medfinansiering i artikel 190 i budgetförordningen. Sådana bidrag ska tilldelas och förvaltas i enlighet med vad som anges för varje specifikt mål.

Stöd i form av bidrag får beviljas direkt utan ansökningsomgång av Europeiska kompetenscentrumet för cybersäkerhet till de medlemsstater som valts ut enligt artikel 9 i förordning (EU) …/…[+] och det värdkonsortium som avses i artikel 5 i förordning (EU) …/…[+], i enlighet med artikel 195.1 d i budgetförordningen.

Stöd i form av bidrag för cybernödmekanismen får beviljas direkt utan ansökningsomgång av Europeiska kompetenscentrumet för cybersäkerhet till medlemsstater, i enlighet med artikel 195.1 d i budgetförordningen.

[+] EUT: Vänligen för in numret för förordningen i dokument PE-CONS 94/24 (2023/0109 (COD)).

När det gäller åtgärder till stöd för ömsesidigt bistånd som föreskrivs i artikel 18 i förordning (EU) …/…[+] ska Europeiska kompetenscentrumet för cybersäkerhet informera kommissionen och Enisa om medlemsstaternas ansökningar om direkta bidrag utan ansökningsomgång.

När det gäller åtgärder till stöd för ömsesidigt bistånd som föreskrivs i artikel 18 i förordning (EU) …/…[+] och i enlighet med artikel 193.2 andra stycket a i budgetförordningen får kostnaderna i vederbörligen motiverade fall anses stödberättigande även om de uppkom innan bidragsansökan lämnades in.”

7. Bilagorna I och II ska ändras i enlighet med bilagan till den här förordningen.

Artikel 23

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artikel 14.7 ska ges till kommissionen för en period på fem år från och med den … [den dag då den grundläggande lagstiftningsakten träder i kraft], med möjlighet till förlängning. Kommissionen ska utarbeta en rapport om delegeringen av befogenhet senast nio månader före utgången av perioden på fem år. Delegeringen av befogenhet ska genom tyst medgivande förlängas med perioder av samma längd, såvida inte Europaparlamentet eller rådet motsätter sig en sådan förlängning senast tre månader före utgången av perioden i fråga.

[+] EUT: Vänligen inför numret på förordningen i dokument PE-CONS 94/24 (2023/0109(COD)).

3. Den delegering av befogenhet som avses i artikel 14.7 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artikel 14.7 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 24

Kommittéförfarande

1. Kommissionen ska biträdas av samordningskommittén för programmet för ett digitalt Europa, som avses i artikel 31.1 i förordning (EU) 2021/694. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

Artikel 25

Utvärdering och översyn

1. Kommissionen ska senast den … [två år från den dag då denna förordning träder i kraft] och därefter minst vart fjärde år utvärdera hur de åtgärder som föreskrivs i denna förordning har fungerat och överlämna en rapport till Europaparlamentet och rådet.

2. I den utvärdering som avses i punkt 1 ska i synnerhet följande bedömas:

a) Antalet nationella cybernav och gränsöverskridande cybernav som inrättats, omfattningen av den information som utbytts, inbegripet, om möjligt, inverkan på CSIRT-nätverkets arbete, och den utsträckning i vilken de har bidragit till att stärka den gemensamma upptäckten och situationsmedvetenheten i unionen när det gäller cyberhot och cyberincidenter och till att utveckla den senaste tekniken, samt användningen av finansiering från programmet för ett digitalt Europa för gemensamt upphandlade verktyg, infrastruktur eller tjänster inom cybersäkerhet och, om informationen finns tillgänglig, graden av samarbete mellan nationella cybernav och sektorsspecifika och sektorsövergripande grupper av väsentliga och viktiga entiteter som avses i artikel 3 i direktiv (EU) 2022/2555.

b) Användningen av och effektiviteten hos åtgärder inom ramen för cybernödmekanismen till stöd för beredskap, inbegripet fortbildning, insatser vid och initial återhämtning från betydande cybersäkerhetsincidenter, storskaliga cybersäkerhetsincidenter och incidenter som är likvärdiga med en storskalig cybersäkerhetsincident, inbegripet användningen av finansiering från programmet för ett digitalt Europa och lärdomar och rekommendationer från genomförandet av cybernödmekanismen.

c) Användningen av och effektiviteten hos EU-cybersäkerhetsreserven med avseende på typen av användare, inbegripet användningen av finansiering från programmet för ett digitalt Europa, användningen av tjänster, inbegripet typen av tjänster, den genomsnittliga tid det tagit att besvara begärandena och sätta in EU-cybersäkerhetsreserven, andelen tjänster som omvandlats till beredskapstjänster som rör förebyggande och hantering av incidenter samt lärdomar och rekommendationer från genomförandet av EU-cybersäkerhetsreserven.

d) Denna förordnings bidrag till att i hela den digitala ekonomin stärka konkurrensställningen för industri och tjänster i unionen, inbegripet mikroföretag och små och medelstora företag samt uppstartsföretag, och bidrag till det övergripande målet att stärka arbetskraftens cybersäkerhetskompetens och cybersäkerhetskapacitet.

3. På grundval av de rapporter som avses i punkt 1 ska kommissionen när så är lämpligt lägga fram ett lagstiftningsförslag om ändring av denna förordning för Europaparlamentet och rådet.

Artikel 26

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den …

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

BILAGA

Förordning (EU) 2021/694 ska ändras på följande sätt:

1. I bilaga I ska avsnittet ”Specifikt mål 3 – Cybersäkerhet och förtroende” ersättas med följande:

”Specifikt mål 3 – Cybersäkerhet och förtroende

Programmet ska stimulera förstärkningen, uppbyggnaden och förvärvet av väsentlig kapacitet för att trygga unionens digitala ekonomi, samhälle och demokrati genom att stärka unionens industriella potential och konkurrenskraft på cybersäkerhetsområdet, och förbättra såväl den privata som den offentliga sektorns kapacitet att skydda medborgare och företag från cyberhot, inbegripet genom att stödja genomförandet av direktiv (EU) 2016/1148.

Inledande och, i förekommande fall, senare åtgärder inom ramen för detta mål ska inbegripa följande:

1. Saminvesteringar med medlemsstater i sådan avancerad utrustning, infrastruktur och know-how på cybersäkerhetsområdet som är avgörande för att skydda kritisk infrastruktur och den digitala inre marknaden i stort. Sådana saminvesteringar kan inbegripa investeringar i kvantdatorsystem och dataresurser för cybersäkerhet, situationsmedvetenhet i cyberrymden, inbegripet nationella cybernav och gränsöverskridande cybernav som utgör det europeiska systemet med cybersäkerhetsvarningar, samt andra verktyg som ska göras tillgängliga för offentlig och privat sektor i hela Europa.

2. Utöka den befintliga tekniska kapaciteten och skapa nätverk mellan medlemsstaternas kompetenscentrum och se till att den kapaciteten tillgodoser den offentliga sektorns och industrins behov, inbegripet genom produkter och tjänster som stärker cybersäkerheten och förtroendet på den digitala inre marknaden.

3. Säkerställa ett brett införande av de senaste effektiva cybersäkerhets- och förtroendelösningarna i alla medlemsstater. Detta införande inbegriper att stärka produkternas säkerhet och trygghet, från utformning till kommersialisering.

4. Stöd för att överbrygga kompetensgapet inom cybersäkerhet, med beaktande av en jämn könsfördelning, till exempel genom att samordna programmen för cybersäkerhetskompetens, anpassa dem till sektorsspecifika behov och underlätta tillgången till riktad specialiserad utbildning.

5. Främja solidaritet mellan medlemsstaterna när det gäller att förbereda sig inför och hantera betydande cybersäkerhetsincidenter och storskaliga cybersäkerhetsincidenter genom införande av cybersäkerhetstjänster över gränserna, inbegripet stöd till ömsesidigt bistånd mellan offentliga myndigheter och inrättande av en reserv av betrodda leverantörer av utlokaliserade säkerhetstjänster på unionsnivå.”

2. I bilaga II ska avsnittet/kapitlet ”Specifikt mål 3 – Cybersäkerhet och förtroende” ersättas med följande:

”Specifikt mål 3 – Cybersäkerhet och förtroende

3.1. Antal cybersäkerhetsinfrastrukturer eller cybersäkerhetsverktyg eller båda som upphandlas gemensamt, inbegripet i samband med det europeiska systemet med cybersäkerhetsvarningar.

3.2. Antal användare och användargrupper som får tillgång till europeiska cybersäkerhetssystem.

3.3 Antal åtgärder som stöder beredskap för och hantering av cybersäkerhetsincidenter inom ramen för cybernödmekanismen.”

Ett uttalande har gjorts med avseende på denna akt och återfinns i [Publikationsbyrån: EUT C XXX, XX.XX.2024, s. XX] och genom följande länk [Publikationsbyrån: för in länken till uttalandet]