Europeiska unionens råd

Bryssel den 20 april 2023
(OR. en)

8512/23

Interinstitutionellt ärende:
2023/0109(COD)

CYBER 92
TELECOM 108
CADREFIN 51
FIN 448
BUDGET 6
IND 181
JAI 471
MI 314
DATAPROTECT 110
RELEX 481
CODEC 662

FÖRSLAG

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	19 april 2023
till:	Thérèse BLANCHET, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2023) 209 final
Ärende:	Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter

För delegationerna bifogas dokument – COM(2023) 209 final.

Bilaga: COM(2023) 209 final

EUROPEISKA
KOMMISSIONEN

Strasbourg den 18.4.2023
COM(2023) 209 final

2023/0109 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

Denna motivering åtföljer förslaget till en cybersolidaritetsakt. Användningen och beroendet av informations- och kommunikationsteknik har blivit grundläggande för alla sektorer av ekonomin i en tid när våra offentliga förvaltningar, företag och medborgare är mer sammanlänkade och ömsesidigt beroende än någonsin tidigare, över både sektors- och nationsgränser. Denna ökade användning av digital teknik ökar exponeringen för cybersäkerhetsincidenter och deras potentiella konsekvenser. Samtidigt står medlemsstaterna inför ökande cybersäkerhetsrisker och en överlag komplex hotbild, med en klar risk för att en cyberincident i en medlemsstat snabbt sprider sig till de andra.

Dessutom ingår cyberoperationer i allt högre grad i hybrid- och krigföringsstrategier, med betydande konsekvenser för måltavlan. Rysslands militära aggression mot Ukraina föregicks och åtföljs av systematiska fientliga cyberoperationer, vilket fullständigt har förändrat uppfattningen och bedömningen av EU:s kollektiva krishanteringsberedskap på cybersäkerhetsområdet och är en väckarklocka om behovet av brådskande åtgärder. Hotet om en eventuell storskalig incident som skulle orsaka betydande störningar och skador på kritisk infrastruktur kräver ökad beredskap på alla nivåer i EU:s cybersäkerhetsekosystem. Hotet gäller inte bara Rysslands militära aggression mot Ukraina, utan även kontinuerliga cyberhot från både statliga och icke-statliga aktörer vilka sannolikt kommer att fortgå, med tanke på det stora antalet statligt allierade, kriminella och hacktivister som är inblandade i dagens geopolitiska spänningar. Under de senaste åren har antalet cyberattacker ökat markant, t.ex. leverantörsattacker som syftar till cyberspionage, utpressning eller störningar. Leverantörsattacken mot SolarWinds 2020 drabbade över 18 000 organisationer runtom i världen, däribland statliga organ och stora företag. Allvarliga cybersäkerhetsincidenter kan påverka en enskild medlemsstat eller flera berörda medlemsstater så mycket att de inte kan hantera dem på egen hand. Därför krävs ökad solidaritet på unionsnivå för att vi bättre ska kunna upptäcka, förbereda oss inför och hantera cyberhot och cybersäkerhetsincidenter.

När det gäller upptäckt av cyberhot och cybersäkerhetsincidenter måste vi utan dröjsmål öka informationsutbytet och förbättra vår kollektiva kapacitet så att cyberhot kan upptäckas betydligt snabbare, innan de kan orsaka omfattande skador och kostnader[1]. Trots att många cyberhot och cybersäkerhetsincidenter har en potentiell gränsöverskridande dimension eftersom digitala infrastrukturer är sammankopplade är utbytet av relevant information mellan medlemsstaterna fortfarande begränsat. Den planerade lösningen på detta problem är att inrätta ett nätverk av gränsöverskridande säkerhetscentrum för att förbättra detektions- och insatskapaciteten.

[1] Enligt en rapport från Ponemon Institute och IBM Security tog det i genomsnitt 207 dagar att identifiera ett intrång 2022, och ytterligare 70 dagar att begränsa det. Samtidigt kostade dataintrång med en livscykel på mer än 200 dagar i genomsnitt 4,86 miljoner euro 2022, jämfört med 3,74 miljoner euro när de begränsades till mindre än 200 dagar. (*Cost of a data breach 2022*, https://www.ibm.com/reports/data-breach)

När det gäller beredskap och hantering av cybersäkerhetsincidenter finns det för närvarande begränsat unionsstöd och måttlig solidaritet mellan medlemsstaterna. Rådet lyfte i sina slutsatser från oktober 2021 fram behovet av att åtgärda dessa brister genom att uppmana kommissionen att lägga fram ett förslag om en ny fond för hantering av cybersäkerhetsincidenter[2].

Denna förordning syftar också till att genomföra EU:s strategi för cybersäkerhet[3], som antogs i december 2020 och som aviserade inrättandet av en europeisk cybersköld som ska förbättra förmågan att upptäcka cyberhot och utbyta information i Europeiska unionen genom en federation av nationella och gränsöverskridande säkerhetscentrum.

Denna förordning bygger på de första steg som redan tagits i nära samarbete med de viktigaste berörda parterna och med stöd av programmet för ett digitalt Europa. När det gäller säkerhetscentrum hölls en inbjudan att anmäla intresse för gemensam upphandling av verktyg och infrastruktur för att inrätta gränsöverskridande säkerhetscentrum och en ansökningsomgång för att möjliggöra kapacitetsuppbyggnad av säkerhetscentrum som betjänar offentliga och privata organisationer inom ramen för programmet för ett digitalt Europa och dess arbetsprogram för cybersäkerhet 2021–2022. När det gäller beredskap och incidenthantering har kommissionen inrättat ett korttidsprogram för att stödja medlemsstaterna genom ytterligare anslag till Europeiska unionens cybersäkerhetsbyrå (Enisa) i syfte att omedelbart stärka beredskapen och kapaciteten att hantera större cyberincidenter. Bägge åtgärderna har utarbetats i nära samordning med medlemsstaterna. Denna förordning avhjälper brister och integrerar lärdomar från dessa åtgärder.

Slutligen fullgörs genom detta förslag åtagandet i det gemensamma meddelandet om cyberförsvar[4], som antogs den 10 november, att utarbeta ett förslag till ett EU-cybersolidaritetsinitiativ med målen att stärka EU:s gemensamma upptäckts-, situationsmedvetenhets- och insatsförmåga, gradvis bygga upp en cybersäkerhetsreserv på EU-nivå med tjänster från betrodda privata leverantörer och stödja testning av kritiska entiteter.

Mot denna bakgrund lägger kommissionen fram denna cybersolidaritetsakt för att stärka solidariteten på unionsnivå så att vi bättre kan upptäcka, förbereda oss inför och hantera cyberhot och cybersäkerhetsincidenter genom följande specifika mål:

- Stärka EU:s gemensamma upptäckt av och situationsmedvetenhet om cyberhot och cyberincidenter och därmed bidra till europeisk teknisk suveränitet på cybersäkerhetsområdet.
- Förbättra beredskapen hos kritiska entiteter i hela EU och öka solidariteten genom att utveckla gemensam insatskapacitet mot betydande eller storskaliga

[2] Rådets slutsatser om utvecklingen av Europeiska unionens arbete på cyberområdet, godkända av rådet vid mötet den 23 maj 2022 (9364/22).

[3] Gemensamt meddelande till Europaparlamentet och rådet, *EU:s strategi för cybersäkerhet för ett digitalt decennium*, JOIN(2020)18 final.

[4] Gemensamt meddelande till Europaparlamentet och rådet, *EU:s politik för cyberförsvar*, JOIN(2022) 49 final.

cybersäkerhetsincidenter, bland annat genom att göra stöd för incidenthantering tillgängligt för tredjeländer som deltar i programmet för ett digitalt Europa.

- Öka unionens resiliens och bidra till effektiva insatser genom att granska och analysera betydande eller storskaliga incidenter för att bland annat dra lärdomar och utfärda rekommendationer, när så är lämpligt.

Dessa mål ska genomföras genom följande åtgärder:

- Utbyggnad av en europeisk infrastruktur av säkerhetscentrum (den europeiska cyberskölden) för att bygga upp och förbättra gemensam kapacitet för upptäckt och situationsmedvetenhet.
- Skapande av en cyberkrismekanism för att hjälpa medlemsstaterna att förbereda sig inför, hantera och omedelbart återhämta sig från betydande och storskaliga cybersäkerhetsincidenter. Stöd till incidenthantering ska också göras tillgängligt för unionens institutioner, organ och byråer.
- Inrättande av en europeisk mekanism för granskning av cybersäkerhetsincidenter för att granska och analysera specifika betydande eller storskaliga incidenter.

Den europeiska cyberskölden och cyberkrismekanismen kommer att stödjas genom finansiering från programmet för ett digitalt Europa, som kommer att ändras genom denna rättsakt för att inrätta ovannämnda åtgärder, föreskriva ekonomiskt stöd för deras utveckling och klargöra villkoren för att få ekonomiskt stöd.

• Förenlighet med befintliga bestämmelser inom området

EU-ramen består av flera rättsakter som redan införts eller föreslagits på unionsnivå för att minska sårbarheterna, öka kritiska entiteters resiliens mot cybersäkerhetsrisker och stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och cyberkriser, framför allt direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2-direktivet)[5], cybersäkerhetsakten[6], direktivet om angrepp mot informationssystem[7] samt kommissionens rekommendation (EU) 2017/1584 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser[8].

De åtgärder som föreslås i cybersolidaritetsakten omfattar situationsmedvetenhet, informationsutbyte och stöd till beredskap inför och hantering av cyberincidenter. Dessa åtgärder är förenliga med och stöder målen för det regelverk som redan finns på unionsnivå,

[5] 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).

[6] 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).

[7] 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.

[8] Förslag till Europaparlamentets och rådets förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020, COM(2022) 454 final.

framför allt direktiv (EU) 2022/2555 (*NIS 2-direktivet*). Cybersolidaritetsakten kommer särskilt att bygga på och stödja de befintliga ramarna för operativt samarbete och krishantering på cybersäkerhetsområdet, i synnerhet Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) och nätverket för enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter).

De gränsöverskridande säkerhetscentrumplattformarna bör utgöra en ny kapacitet som kompletterar CSIRT-nätverket, genom att samla och dela data om cyberhot från offentliga och privata entiteter, öka värdet av sådana data genom expertanalyser och toppmoderna verktyg och bidra till utvecklingen av unionens kapacitet och tekniska suveränitet.

Slutligen är detta förslag förenligt med rådets rekommendation om en unionsomfattande samordnad strategi för att stärka den kritiska infrastrukturens motståndskraft[9], där medlemsstaterna uppmanas att vidta brådskande och verkningsfulla åtgärder och att samarbeta lojalt, effektivt, solidariskt och samordnat 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.

- **Förenlighet med unionens politik inom andra områden**

Förslaget är förenligt med andra krismekanismer och protokoll, t.ex. EU-arrangemanget för integrerad politisk krishantering (IPCR). Cybersolidaritetsakten kommer att komplettera dessa krishanteringsramar och -protokoll genom att föreskriva särskilt stöd för beredskap inför och hantering av cybersäkerhetsincidenter. Förslaget är också förenligt med EU:s yttre åtgärder som svar på storskaliga incidenter inom ramen för den gemensamma utrikes- och säkerhetspolitiken (Gusp), bland annat genom EU:s verktygslåda för cyberdiplomati. Förslaget kommer att komplettera åtgärder som genomförs inom ramen för artikel 42.7 i fördraget om Europeiska unionen eller i situationer som anges i artikel 222 i fördraget om Europeiska unionens funktionssätt.

Det kompletterar också unionens civilskyddsmekanism[10], som inrättades i december 2013 och kompletterades med ny lagstiftning som antogs i maj 2021[11] och som stärker civilskyddsmekanismens pelare för förebyggande, beredskap och insatser, ger EU ytterligare kapacitet att hantera nya risker i Europa och resten av världen samt stärker rescEU-reserven.

---

[9] Rådets rekommendation av den 8 december 2022 om en unionsomfattande samordnad strategi för att stärka den kritiska infrastrukturens motståndskraft (Text av betydelse för EES), 2023/C 20/01.

[10] Europaparlamentets och rådets beslut nr 1313/2013/EU av den 17 december 2013 om en civilskyddsmekanism för unionen (Text av betydelse för EES).

[11] Europaparlamentets och rådets förordning (EU) 2021/836 av den 20 maj 2021 om ändring av beslut nr 1313/2013/EU om en civilskyddsmekanism för unionen (Text av betydelse för EES).

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

• Rättslig grund

Den rättsliga grunden för detta förslag är artiklarna 173.3 och 322.1 a i fördraget om Europeiska unionens funktionssätt (*EUF-fördraget*). Enligt artikel 173 i EUF-fördraget ska unionen och medlemsstaterna säkerställa att det finns nödvändiga förutsättningar för unionsindustrins konkurrensförmåga. Denna förordning syftar till att stärka den europeiska industrins och tjänstesektorns konkurrensställning i hela den digitaliserade ekonomin och stödja deras digitala omställning genom att öka cybersäkerheten på den digitala inre marknaden. Den syftar särskilt till att öka resiliensen hos enskilda, företag och entiteter som är verksamma i kritiska och högkritiska sektorer mot de växande cyberhoten, som kan få förödande samhälleliga och ekonomiska konsekvenser.

Förslaget grundar sig också på artikel 322.1 a i EUF-fördraget eftersom det innehåller särskilda överföringsregler som avviker från principen om ettårighet i Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046[12] (*budgetförordningen*). För att uppnå en sund ekonomisk förvaltning och med tanke på cybersäkerhetslandskapets och cyberhotens oförutsägbara, exceptionella och specifika karaktär bör cyberkrismekanismen ha en viss grad av flexibilitet i fråga om budgetförvaltningen, särskilt genom att tillåta att outnyttjade åtagande- och betalningsbemyndiganden för åtgärder som främjar förordningens mål automatiskt överförs till påföljande budgetår. Eftersom denna nya regel ger upphov till frågor i förhållande till budgetförordningen skulle denna fråga kunna tas upp i samband med de pågående förhandlingarna om omarbetningen av budgetförordningen.

• Subsidiaritetsprincipen (för icke-exklusiv befogenhet)

Cyberhotens starkt gränsöverskridande karaktär och det ökande antalet risker och incidenter, vars effekter kan sprida sig över gränser och mellan sektorer och produkter, innebär att målen med detta initiativ inte kan uppnås av medlemsstaterna på egen hand och kräver gemensamma åtgärder och solidaritet på unionsnivå.

Erfarenheterna av att motverka cyberhot under Rysslands krig mot Ukraina, tillsammans med lärdomarna från en cybersäkerhetsövning som genomfördes under det franska ordförandeskapet (EU CyCLES), har visat att konkreta mekanismer för ömsesidigt stöd, särskilt samarbete med den privata sektorn, bör utvecklas för att uppnå solidaritet på EU-nivå. Mot denna bakgrund uppmanades kommissionen i rådets slutsatser av den 23 maj 2022 om utvecklingen av Europeiska unionens arbete på cyberområdet att lägga fram ett förslag om en ny fond för hantering av cybersäkerhetsincidenter.

Stöd och åtgärder på unionsnivå för att bättre upptäcka cyberhot och för att öka beredskapen och insatskapaciteten ger ett mervärde eftersom man undviker dubbelarbete i unionen och medlemsstaterna. Det skulle leda till ett bättre utnyttjande av befintliga tillgångar och till

[12] Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046 av den 18 juli 2018 om finansiella regler för unionens allmänna budget (EUT L 193, 30.7.2018, s. 1).

bättre samordning och utbyte av information om lärdomar. Genom cyberkrismekanismen planeras också tredjeländer som är associerade till programmet för ett digitalt Europa att få stöd från EU-cybersäkerhetsreserven.

Det stöd som ges genom de olika initiativ som ska inrättas och finansieras på unionsnivå kommer att komplettera och inte överlappa nationell kapacitet när det gäller upptäckt, situationsmedvetenhet, beredskap och hantering av cyberhot och cyberincidenter.

• Proportionalitetsprincipen

Åtgärderna går inte utöver vad som är nödvändigt för att uppnå förordningens allmänna och specifika mål. Åtgärderna i denna förordning påverkar inte medlemsstaternas ansvar för nationell säkerhet, allmän säkerhet och förebyggande, utredning, upptäckt och lagföring av brott. De påverkar inte heller de rättsliga skyldigheterna för entiteter som är verksamma i kritiska och högkritiska sektorer att anta cybersäkerhetsåtgärder i enlighet med NIS 2-direktivet.

De åtgärder som omfattas av denna förordning kompletterar dessa insatser och åtgärder genom att stödja skapandet av infrastruktur för bättre upptäckt och analys av hot och genom att ge stöd för beredskaps- och insatsåtgärder vid betydande eller storskaliga incidenter.

• Val av instrument

Förslaget är utformat som Europaparlamentets och rådets förordning. Detta är det lämpligaste rättsliga instrumentet, eftersom endast en förordning med dess direkt tillämpliga rättsliga bestämmelser kan ge den grad av enhetlighet som krävs för inrättandet och driften av en europeisk cybersköld och cyberkrismekanism, genom att sörja för stöd från programmet för ett digitalt Europa för inrättandet och tydliga villkor för användning och tilldelning av detta stöd.

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

• Samråd med berörda parter

Åtgärderna i denna förordning kommer att stödjas genom programmet för ett digitalt Europa, som var föremål för ett brett samråd. Dessutom kommer de att bygga vidare på de första steg som har utarbetats i nära samarbete med de viktigaste berörda parterna. När det gäller säkerhetscentrum har kommissionen tagit fram ett konceptdokument om utvecklingen av gränsöverskridande säkerhetscentrumplattformar och en inbjudan att anmäla intresse, i nära samarbete med medlemsstaterna inom ramen för Europeiska kompetenscentrumet för cybersäkerhet. I detta sammanhang har en undersökning av kapaciteten hos nationella säkerhetscentrum genomförts, och gemensamma strategier och tekniska krav har diskuterats inom den tekniska arbetsgruppen av företrädare för medlemsstaterna vid Europeiska

kompetenscentrumet för cybersäkerhet. Dessutom har man diskuterat med industrin, särskilt genom den expertgrupp för säkerhetscentrum som inrättats av Enisa och Europeiska cybersäkerhetsorganisationen (Ecso).

När det gäller beredskap och incidenthantering har kommissionen inrättat ett korttidsprogram för att stödja medlemsstaterna genom ytterligare anslag till Enisa från programmet för ett digitalt Europa i syfte att omedelbart stärka beredskapen och kapaciteten att hantera större cyberincidenter. Medlemsstaternas och industrins synpunkter som samlats in under genomförandet av detta korttidsprogram har redan gett värdefulla insikter som har bidragit till utarbetandet av den föreslagna förordningen för att åtgärda identifierade brister. Detta var ett första steg i linje med rådets slutsatser om arbetet på cyberområdet, där kommissionen uppmanades att lägga fram ett förslag om en ny fond för hantering av cybersäkerhetsincidenter.

Dessutom hölls en workshop om cyberkrismekanismen med medlemsstaternas experter den 16 februari 2023 på grundval av ett diskussionsunderlag. Alla medlemsstater deltog i denna workshop och elva medlemsstater lämnade ytterligare skriftliga bidrag.

- **Konsekvensbedömning**

På grund av förslagets brådskande karaktär har ingen konsekvensbedömning gjorts. Åtgärderna i denna förordning kommer att stödjas genom programmet för ett digitalt Europa och är i linje med dem som fastställs i förordningen om det programmet, för vilken en särskild konsekvensbedömning gjordes. Denna förordning kommer inte att medföra några betydande administrativa eller miljömässiga konsekvenser utöver dem som redan bedömts i konsekvensbedömningen av förordningen om programmet för ett digitalt Europa.

Dessutom bygger den på de första åtgärder som tagits fram i nära samarbete med de viktigaste berörda parterna, som anges ovan, och följer upp medlemsstaternas uppmaning till kommissionen att lägga fram ett förslag om en ny fond för hantering av cybersäkerhetsincidenter senast i slutet av tredje kvartalet 2022.

När det specifikt gäller situationsmedvetenhet och upptäckt inom den europeiska cyberskölden hölls en inbjudan att anmäla intresse för gemensam upphandling av verktyg och infrastruktur för att inrätta gränsöverskridande säkerhetscentrum och en ansökningsomgång för att möjliggöra kapacitetsuppbyggnad av säkerhetscentrum som betjänar offentliga och privata organisationer inom ramen för programmet för ett digitalt Europa och dess arbetsprogram för cybersäkerhet 2021–2022.

På området beredskap och incidenthantering har kommissionen som nämns ovan inrättat ett korttidsprogram för att stödja medlemsstaterna genom programmet för ett digitalt Europa, vilket genomförs av Enisa. Tjänster som omfattas är bland annat beredskapsåtgärder, såsom penetrationstestning av kritiska entiteter för att upptäcka sårbarheter. Programmet förbättrar också möjligheterna att bistå medlemsstaterna i händelse av en större incident som påverkar kritiska entiteter. Enisa håller på att genomföra detta korttidsprogram, som redan gett relevanta insikter som har beaktats vid utarbetandet av denna förordning.

- **Grundläggande rättigheter**

Genom att öka säkerheten för digital information kommer detta förslag att bidra till att skydda rätten till frihet och säkerhet enligt artikel 6 i EU:s stadga om de grundläggande rättigheterna och rätten till respekt för privatlivet och familjelivet enligt artikel 7 i EU:s stadga om de grundläggande rättigheterna. Genom att skydda företag från ekonomiskt skadliga cyberattacker kommer förslaget också att bidra till näringsfriheten enligt artikel 16 i EU:s stadga om de grundläggande rättigheterna och rätten till egendom enligt artikel 17 i EU:s stadga om de grundläggande rättigheterna. Genom att skydda den kritiska infrastrukturens integritet vid cyberattacker kommer förslaget slutligen också att bidra till rätten till hälsovård enligt artikel 35 i EU:s stadga om de grundläggande rättigheterna och rätten till tillgång till tjänster av allmänt ekonomiskt intresse enligt artikel 36 i EU:s stadga om de grundläggande rättigheterna.

4. BUDGETKONSEKVENSER

Åtgärderna i denna förordning kommer att stödjas av finansiering inom ramen för det strategiska målet ”cybersäkerhet” i programmet för ett digitalt Europa.

I förordningen föreslås att den totala budgeten ökas med 100 miljoner euro genom en omfördelning från andra strategiska mål i programmet för ett digitalt Europa. Därmed kommer det nya totala belopp som finns tillgängligt för cybersäkerhetsåtgärder inom ramen för programmet för ett digitalt Europa att uppgå till 842,8 miljoner euro.

En del av tillskottet på 100 miljoner euro kommer att stärka den budget som förvaltas av Europeiska kompetenscentrumet för cybersäkerhet för åtgärder avseende säkerhetscentrum och beredskap som en del av centrumens arbetsprogram. Dessutom kommer tilläggsfinansieringen att användas för att stödja inrättandet av EU-cybersäkerhetsreserven.

Den kompletterar den budget som redan planerats för liknande åtgärder i huvudarbetsprogrammet för programmet för ett digitalt Europa och cybersäkerhetsdelen av programmet under perioden 2023–2027, vilket skulle leda till ett totalbelopp på 551 miljoner för 2023–2027, medan 115 miljoner euro redan har avsatts i form av pilotprojekt för 2021–2022. Medräknat medlemsstaternas bidrag skulle den totala budgeten kunna uppgå till 1 109 miljarder euro.

En översikt över kostnaderna finns i den finansieringsöversikt som åtföljer detta förslag.

5. ÖVRIGA INSLAG

- **Genomförandeplaner samt åtgärder för övervakning, utvärdering och rapportering**

Kommissionen kommer att övervaka genomförandet, tillämpningen och efterlevnaden av dessa nya bestämmelser i syfte att bedöma deras effektivitet. Kommissionen ska överlämna en

rapport om utvärderingen och översynen av denna förordning till Europaparlamentet och rådet senast fyra år efter den dag då den börjar tillämpas.

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

Allmänna mål, innehåll och definitioner (kapitel I)

I kapitel I fastställs förordningens mål, nämligen att stärka solidariteten på unionsnivå så att vi bättre kan upptäcka, förbereda oss inför och hantera cyberhot och cybersäkerhetsincidenter och i synnerhet att stärka unionens gemensamma förmåga att upptäcka och situationsmedvetenhet om cyberhot och cyberincidenter, att öka beredskapen hos entiteter som är verksamma i kritiska och högkritiska sektorer i hela unionen och stärka solidariteten genom att utveckla gemensam insatskapacitet mot betydande eller storskaliga cybersäkerhetsincidenter samt att öka unionens resiliens genom att granska och analysera betydande eller storskaliga incidenter. I detta kapitel anges också genom vilka åtgärder målen ska uppnås: införandet av en europeisk cybersköld, skapandet av en cyberkrismekanism och inrättandet av en mekanism för granskning av cybersäkerhetsincidenter. Det innehåller också de definitioner som används i hela instrumentet.

Den europeiska cyberskölden (kapitel II)

Genom kapitel II inrättas den europeiska cyberskölden, och dess olika delar och villkoren för deltagande fastställs. Till att börja med presenteras den europeiska cybersköldens allmänna mål, dvs. att utveckla avancerad kapacitet så att unionen ska kunna upptäcka, analysera och behandla data om cyberhot och cyberincidenter i unionen, samt de särskilda operativa målen. Det anges att unionens finansiering av den europeiska cyberskölden ska genomföras i enlighet med förordningen om programmet för ett digitalt Europa.

I kapitlet beskrivs dessutom den typ av entiteter som ska utgöra den europeiska cyberskölden. Skölden ska bestå av nationella säkerhetscentrum och gränsöverskridande säkerhetscentrum. Varje deltagande medlemsstat kommer att utse ett nationellt säkerhetscentrum. Det nationella säkerhetscentrumet fungerar som referenspunkt och gränssnitt mot andra offentliga och privata organisationer på nationell nivå för att samla in och analysera information om cyberhot och cybersäkerhetsincidenter och bidra till ett gränsöverskridande säkerhetscentrum. Efter en inbjudan att anmäla intresse kan ett nationellt säkerhetscentrum väljas ut av Europeiska kompetenscentrumet för cybersäkerhet för att delta i gemensam upphandling av verktyg och infrastruktur tillsammans med Europeiska kompetenscentrumet för cybersäkerhet och att motta ett bidrag för driften av verktygen och infrastrukturen. Om ett nationellt säkerhetscentrum får stöd från unionen måste det åta sig att ansöka om att delta i ett gränsöverskridande säkerhetscentrum inom två år.

Gränsöverskridande säkerhetscentrum utgörs av ett konsortium bestående av minst tre medlemsstater, företrädda av nationella säkerhetscentrum, som åtar sig att samarbeta för att samordna sin cyberupptäckts- och hotövervakningsverksamhet. Efter en inledande inbjudan att anmäla intresse kan ett värdkonsortium väljas ut av Europeiska kompetenscentrumet för

cybersäkerhet för att delta i en gemensam upphandling av verktyg och infrastruktur tillsammans med centrumet och för att få bidrag för driften av verktygen och infrastrukturen. Värdkonsortiets medlemmar ingår ett skriftligt konsortieavtal som anger deras interna arrangemang. I detta kapitel beskrivs sedan kraven för utbyte av information mellan deltagarna i ett gränsöverskridande säkerhetscentrum och för utbyte av information mellan ett gränsöverskridande säkerhetscentrum och andra gränsöverskridande säkerhetscentrum eller relevanta EU-entiteter. Nationella säkerhetscentrum som deltar i ett gränsöverskridande säkerhetscentrum måste dela relevant cyberhotrelaterad information med varandra, och detaljerna, inbegripet åtagandet att dela betydande mängder data och villkoren för detta, bör fastställas i ett konsortieavtal. Gränsöverskridande säkerhetscentrum måste säkerställa en hög grad av interoperabilitet sinsemellan. Gränsöverskridande säkerhetscentrum bör också ingå samarbetsavtal med andra gränsöverskridande säkerhetscentrum, där det fastställs principer för informationsutbyte. När gränsöverskridande säkerhetscentrum får information om en potentiell eller pågående storskalig cybersäkerhetsincident ska de ge relevant information till EU-CyCLONe, CSIRT-nätverket och kommissionen, så att de kan utöva sina respektive roller i samband med krishantering enligt direktiv (EU) 2022/2555. Kapitel II avslutas med fastställande av säkerhetsvillkoren för deltagande i den europeiska cyberskölden.

Cyberkrismekanismen (kapitel III)

I kapitel III inrättas cyberkrismekanismen för att förbättra unionens resiliens mot större cyberhot och i en anda av solidaritet förbereda sig inför och begränsa de kortsiktiga konsekvenserna av betydande och storskaliga cybersäkerhetsincidenter eller cyberkriser. Åtgärderna för att genomföra cyberkrismekanismen kommer att stödjas genom finansiering från programmet för ett digitalt Europa. Mekanismen omfattar åtgärder för att stödja beredskap (inbegripet samordnad testning av entiteter som är verksamma i högkritiska sektorer), insatser och omedelbar återhämtning vid betydande och storskaliga cybersäkerhetsincidenter eller för att begränsa betydande cyberhot och vidta ömsesidiga stödåtgärder.

Till beredskapsåtgärderna inom ramen för cyberkrismekanismen hör samordnad beredskapstestning av entiteter som är verksamma i högkritiska sektorer. Kommissionen bör, efter samråd med Enisa och samarbetsgruppen för nät- och informationssäkerhet, regelbundet identifiera relevanta sektorer eller delsektorer bland de högkritiska sektorer i bilaga I till direktiv (EU) 2022/2555 från vilka entiteter kan bli föremål för samordnad beredskapstestning på EU-nivå.

I syfte att genomföra de föreslagna incidenthanteringsåtgärderna inrättas genom denna förordning en EU-cybersäkerhetsreserv bestående av incidenthanteringstjänster från betrodda leverantörer som valts ut i enlighet med kriterierna i denna förordning. EU-cybersäkerhetsreservens tjänster är tänkta att användas av medlemsstaternas myndigheter för cyberkrishantering, medlemsstaternas CSIRT-enheter samt unionens institutioner, organ och byråer. Kommissionen kommer att ha det övergripande ansvaret för genomförandet av EU-cybersäkerhetsreserven och får helt eller delvis anförtro Enisa driften och förvaltningen av EU-cybersäkerhetsreserven.

För att få stöd från EU-cybersäkerhetsreserven bör användarna vidta egna åtgärder för att begränsa effekterna av den incident för vilken stöd begärs. Begäran om stöd från EU-cybersäkerhetsreserven bör innehålla nödvändig relevant information om incidenten och de åtgärder som redan vidtagits av användarna. I kapitlet beskrivs även formerna för genomförandet, inbegripet bedömningen av begäranden till EU-cybersäkerhetsreserven.

I förordningen föreskrivs också upphandlingsprinciper och urvalskriterier för betrodda leverantörer i EU-cybersäkerhetsreserven.

Tredjeländer får begära stöd från EU-cybersäkerhetsreserven när detta föreskrivs i associeringsavtal som ingåtts om deras deltagande i programmet för ett digitalt Europa. I kapitlet beskrivs ytterligare villkor och former för sådant deltagande.

Mekanismen för granskning av cybersäkerhetsincidenter (kapitel IV)

På begäran av kommissionen, EU-CyCLONe eller CSIRT-nätverket bör Enisa granska och analysera hot, sårbarheter och begränsningsåtgärder med avseende på en viss betydande eller storskalig cybersäkerhetsincident. Enisa bör lägga fram granskningen och analysen i form av en incidentgranskningsrapport till CSIRT-nätverket, EU-CyCLONe och kommissionen så att de kan utföra sina uppgifter. När incidenten rör ett tredjeland bör kommissionen dela rapporten med den höga representanten. Rapporten bör innehålla lärdomar och, när så är lämpligt, rekommendationer för att förbättra unionens säkerhetsstatus.

Slutbestämmelser (kapitel V)

Kapitel V innehåller ändringar av förordningen om programmet för ett digitalt Europa och en skyldighet för kommissionen att utarbeta regelbundna rapporter till Europaparlamentet och rådet för utvärdering och översyn av förordningen. Kommissionen ges befogenhet att anta genomförandeakter i enlighet med det granskningsförfarande som avses i artikel 21 för att specificera villkoren för interoperabiliteten mellan gränsöverskridande säkerhetscentrum, fastställa förfarandena för informationsutbyte mellan gränsöverskridande säkerhetscentrum och unionsentiteter om en potentiell eller pågående storskalig cybersäkerhetsincident, ange tekniska krav för att säkerställa en hög nivå av dataskydd och fysiskt skydd för infrastrukturen och för att skydda unionens säkerhetsintressen vid utbyte av information med entiteter som inte är offentliga organ i medlemsstaterna, fastställa vilken typ av och hur många insatstjänster som behövs för EU-cybersäkerhetsreserven samt ytterligare specificera de närmare arrangemangen för tilldelning av stödtjänsterna från EU-cybersäkerhetsreserven.

2023/0109 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter

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, och

av följande skäl:

1) Användningen och beroendet av informations- och kommunikationsteknik har blivit grundläggande för alla sektorer av ekonomin i en tid när våra offentliga förvaltningar, företag och medborgare är mer sammanlänkade och ömsesidigt beroende än någonsin tidigare, över både sektors- och nationsgränser.

2) Cybersäkerhetsincidenternas omfattning, frekvens och konsekvenser ökar, även när det gäller leverantörsattacker som syftar till cyberspionage, utpressning eller störningar. De utgör ett allvarligt hot mot nätverks- och informationssystemens funktion. Med tanke på det snabbt föränderliga hotlandskapet innebär hotet om eventuella storskaliga incidenter som skulle orsaka betydande störningar eller skador på kritisk infrastruktur att det krävs ökad beredskap på alla nivåer i EU:s cybersäkerhetsram. Hotet gäller inte bara Rysslands militära aggression mot Ukraina och kommer sannolikt att fortgå, med tanke på det stora antalet statligt allierade, kriminella och hacktivister som är inblandade i dagens geopolitiska spänningar. Sådana incidenter kan hindra tillhandahållandet av offentliga tjänster och utövandet av ekonomisk verksamhet, även i kritiska eller högkritiska sektorer, leda till betydande ekonomiska förluster, undergräva användarnas förtroende, orsaka stora skador på unionens ekonomi och till och med få hälsomässiga eller livshotande konsekvenser. Dessutom är cybersäkerhetsincidenter oförutsägbara, eftersom de ofta uppstår och utvecklas på mycket kort tid, inte är begränsade till något specifikt

[1] EUT C […], […], s. […].
[2] EUT C , , s. .
[3] EUT C , , s. .

geografiskt område och inträffar samtidigt i flera länder eller sprids omedelbart över landsgränserna.

3) Det är nödvändigt att stärka den unionsbaserade industrins och tjänstesektorns konkurrensställning i hela den digitaliserade ekonomin och stödja deras digitala omställning genom att stärka cybersäkerhetsnivån på den digitala inre marknaden. Som rekommenderades i tre olika förslag från konferensen om Europas framtid[4] är det nödvändigt att öka resiliensen hos enskilda, företag 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 som kommer att stödja snabbare upptäckt och hantering av cyberhot och cybersäkerhetsincidenter, och medlemsstaterna behöver hjälp med att bättre förbereda sig inför och hantera betydande och storskaliga cybersäkerhetsincidenter. Unionen bör 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 cybersäkerhetsrisker hos kritiska infrastrukturer och entiteter, framför allt Europaparlamentets och rådets direktiv (EU) 2022/2555[5], kommissionens rekommendation (EU) 2017/1584[6], Europaparlamentets och rådets direktiv 2013/40/EU[7] och Europaparlamentets och rådets förordning (EU) 2019/881[8]. I rådets rekommendation om en unionsomfattande samordnad strategi för att stärka den kritiska infrastrukturens motståndskraft uppmanas medlemsstaterna dessutom att vidta brådskande och verkningsfulla åtgärder och att samarbeta lojalt, effektivt, solidariskt och samordnat 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) De ökande cybersäkerhetsriskerna och ett överlag sett komplext hotlandskap, med en tydlig risk för att cyberincidenter snabbt sprider sig från en medlemsstat till de andra och från ett tredjeland till unionen, kräver ökad solidaritet på unionsnivå för att vi bättre ska kunna upptäcka, förbereda oss inför och hantera cyberhot och cybersäkerhetsincidenter. I rådets slutsatser om EU:s arbete på cyberområdet[9] uppmanade medlemsstaterna också kommissionen att lägga fram ett förslag om en ny fond för hantering av cybersäkerhetsincidenter.

---

4 https://futureu.europa.eu/sv/

5 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).

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

7 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).

8 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).

9 Rådets slutsatser om utvecklingen av Europeiska unionens arbete på cyberområdet, godkända av rådet vid mötet den 23 maj 2022 (9364/22).

6) I det gemensamma meddelandet om EU:s politik för cyberförsvar[10], som antogs den 10 november 2022, 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 hantera betydande och storskaliga cybersäkerhetsincidenter. Därför bör en europeisk infrastruktur av säkerhetscentrum (den europeiska cyberskölden) inrättas för att bygga upp och förbättra gemensam kapacitet för upptäckt och situationsmedvetenhet, en cyberkrismekanism bör skapas för att hjälpa medlemsstaterna att förbereda sig inför, hantera och omedelbart återhämta sig från betydande och storskaliga cybersäkerhetsincidenter och en mekanism för granskning av cybersäkerhetsincidenter bör inrättas för att granska och analysera specifika betydande eller storskaliga incidenter. Dessa åtgärder bör inte påverka tillämpningen av artiklarna 107 och 108 i fördraget om Europeiska unionens funktionssätt (*EUF-fördraget*).

8) För att uppnå dessa mål är det också nödvändigt att ändra Europaparlamentets och rådets förordning (EU) 2021/694[11] på vissa områden. Denna förordning bör ändra förordning (EU) 2021/694 i synnerhet genom att lägga till nya operativa mål med anknytning till den europeiska cyberskölden och cyberkrismekanismen 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 cybersäkerhet. Detta bör kompletteras genom att man fastställer de särskilda villkor enligt vilka ekonomiskt stöd kan beviljas för dessa åtgärder och definierar de styrnings- och samordningsmekanismer som krävs för att uppnå de avsedda målen. Förordning (EU) 2021/694 bör också ändras genom att man inför beskrivningar av föreslagna åtgärder inom ramen för de nya operativa målen samt mätbara indikatorer för att övervaka genomförandet av dessa nya operativa mål.

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

10) 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 budgetförordningen 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-

[10] Gemensamt meddelande till Europaparlamentet och rådet, *EU:s politik för cyberförsvar*, JOIN(2022) 49 final.

[11] 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).

fördraget märks även en generell villkorlighetsordning för skydd av unionsbudgeten som fastställs i Europaparlamentets och rådets förordning (EU, Euratom) 2020/2092.

11) För att uppnå en sund ekonomisk förvaltning bör särskilda regler fastställas för överföring av outnyttjade åtagande- och betalningsbemyndiganden. Samtidigt som principen om att unionens budget fastställs årligen iakttas bör denna förordning, på grund av cybersäkerhetslandskapets oförutsägbara, exceptionella och specifika karaktär, göra det möjligt att överföra outnyttjade medel utöver dem som anges i budgetförordningen för att maximera cyberkrismekanismens kapacitet att hjälpa medlemsstaterna att effektivt bekämpa cyberhot.

12) För att mer effektivt förebygga, analysera och hantera 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. Det bör inrättas en storskalig unionsinfrastruktur av säkerhetscentrum (*den europeiska cyberskölden*), som består av flera interoperativa gränsöverskridande plattformar som var och en omfattar flera nationella säkerhetscentrum. Denna infrastruktur bör tjäna nationella och europeiska cybersäkerhetsintressen och cybersäkerhetsbehov genom att utnyttja den senaste tekniken för avancerad datainsamling och dataanalys, förbättra kapaciteten för upptäckt och hantering av cyberhot och tillhandahålla situationsmedvetenhet i realtid. Denna infrastruktur bör tjäna till att öka upptäckten av cyberhot och cybersäkerhetsincidenter och därigenom komplettera och stödja unionens entiteter och nätverk med ansvar för krishantering i unionen, särskilt EU:s kontaktnätverk för cyberkriser (EU-CyCLONe), enligt definitionen i Europaparlamentets och rådets direktiv (EU) 2022/2555[12].

13) Varje medlemsstat bör utse ett offentligt organ som på nationell nivå har uppgiften att samordna åtgärder för att upptäcka cyberhot i den medlemsstaten. Dessa nationella säkerhetscentrum bör fungera som referenspunkt och gränssnitt på nationell nivå för deltagande i den europeiska cyberskölden och bör säkerställa att information om cyberhot från offentliga och privata entiteter delas och samlas in på nationell nivå på ett effektivt och enhetligt sätt.

14) Som en del av den europeiska cyberskölden bör ett antal gränsöverskridande säkerhetscentrum inrättas. Dessa bör sammanföra nationella säkerhetscentrum från minst tre medlemsstater, så att alla fördelar med gränsöverskridande hotupptäckt och informationsutbyte och hantering kan utnyttjas. Det allmänna målet med gränsöverskridande säkerhetscentrum bör vara att stärka kapaciteten att analysera, förebygga och upptäcka cyberhot och stödja produktionen av högkvalitativa underrättelser om cyberhot, främst genom delning av data 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 miljö. De bör tillhandahålla ny ytterligare kapacitet som bygger på och kompletterar befintliga säkerhetscentrum och enheter för hantering av it-säkerhetsincidenter (*CSIRT-enheter*) och andra relevanta aktörer.

[12] 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).

15) På nationell nivå säkerställs övervakning, upptäckt och analys av cyberhot vanligtvis av offentliga och privata entiteters säkerhetscentrum, i kombination med CSIRT-enheter. Dessutom utbyter CSIRT-enheterna information inom CSIRT-nätverket, i enlighet med direktiv (EU) 2022/2555. De gränsöverskridande säkerhetscentrumen bör utgöra en ny kapacitet som kompletterar CSIRT-nätverket, genom att samla och dela data om cyberhot från offentliga och privata entiteter, öka värdet av sådana data genom expertanalyser och gemensamt upphandlade infrastrukturer och toppmoderna verktyg samt bidra till utvecklingen av unionens kapacitet och tekniska suveränitet.

16) De gränsöverskridande säkerhetscentrumen bör fungera som en central punkt som möjliggör en bred sammanslagning av relevanta data och underrättelser om cyberhot samt göra det möjligt att sprida hotinformation till en mängd olika typer av aktörer (t.ex. incidenthanteringsorganisationer (Cert), CSIRT-enheter, informations- och analyscentraler (ISAC) och operatörer av kritisk infrastruktur). Exempel på information som kan utbytas mellan deltagarna i ett gränsöverskridande säkerhetscentrum är data från nätverk och sensorer, hotunderrättelseflöden, angreppsindikatorer och kontextualiserad information om incidenter, hot och sårbarheter. Dessutom bör gränsöverskridande säkerhetscentrum också ingå samarbetsavtal med andra gränsöverskridande säkerhetscentrum.

17) Gemensam situationsmedvetenhet mellan berörda myndigheter är en nödvändig förutsättning för unionsomfattande beredskap och samordning när det gäller betydande och storskaliga cybersäkerhetsincidenter. Genom direktiv (EU) 2022/2555 inrättas 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. Rekommendation (EU) 2017/1584 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser tar upp alla relevanta aktörers roll. 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, samt ansvar för att tillhandahålla analytiska rapporter för arrangemangen för integrerad politisk krishantering (IPCR) enligt genomförandebeslut (EU) 2018/1993. I situationer där gränsöverskridande säkerhetscentrum får information om en potentiell eller pågående storskalig cybersäkerhetsincident bör de därför ge relevant information till EU-CyCLONe, CSIRT-nätverket och kommissionen. Beroende på situationen skulle man t.ex. kunna dela teknisk information, information 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 karaktär.

18) Entiteter som deltar i den europeiska cyberskölden 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 – samt säkra kommunikationskanaler, en miniminivå av säkerhet i applikationslagret, informationspanel för situationsmedvetenhet och indikatorer. Vid antagandet av en gemensam taxonomi och utarbetandet av en mall för situationsrapporter för att beskriva de tekniska orsakerna till och konsekvenserna av cybersäkerhetsincidenter bör man beakta det pågående arbetet med incidentanmälan i samband med genomförandet av direktiv (EU) 2022/2555.

19) För att möjliggöra utbyte av data om cybersäkerhetshot från olika källor i stor skala i en tillförlitlig miljö bör entiteter som deltar i den europeiska cyberskölden utrustas med förstklassiga verktyg, utrustning och infrastrukturer som har hög säkerhet. 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.

20) Genom att samla in, dela och utbyta data bör den europeiska cyberskölden förbättra unionens tekniska suveränitet. Sammanslagningen av högkvalitativa kurerade data bör också bidra till utvecklingen av avancerad AI-teknik och dataanalysteknik. Den bör underlättas genom att den europeiska cyberskölden kopplas samman med den europeiska infrastruktur för högpresterande datorsystem som inrättades genom rådets förordning (EU) 2021/1173[13].

21) Även om den europeiska cyberskölden är ett civilt projekt skulle cyberförsvarsgemenskapen gynnas av starkare civil kapacitet för upptäckt och situationsmedvetenhet vilken utvecklats för att skydda kritisk infrastruktur. Gränsöverskridande säkerhetscentrum bör, med stöd av kommissionen och Europeiska kompetenscentrumet för cybersäkerhet och i samarbete med unionens höga representant för utrikes frågor och säkerhetspolitik (*den höga representanten*), gradvis utarbeta särskilda protokoll och standarder för att möjliggöra samarbete med cyberförsvarsgemenskapen, inbegripet säkerhetsprövning och säkerhetsvillkor. Utvecklingen av den europeiska cyberskölden bör åtföljas av en reflektion som möjliggör framtida samarbete med nätverk och plattformar som ansvarar för informationsutbyte inom cyberförsvarsgemenskapen, i nära samarbete med den höga representanten.

22) Informationsutbytet mellan deltagarna i den europeiska cyberskölden 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, förstöra uppgifterna så snart de inte längre är nödvändiga för det angivna ändamålet och informera det organ som tillhandahöll uppgifterna om att uppgifterna har förstörts.

23) Utan att det påverkar tillämpningen av artikel 346 i EUF-fördraget bör utbyte av information som är konfidentiell i enlighet med unionsregler eller nationella regler begränsas till det som är relevant och står i proportion till ändamålet med utbytet. Vid utbyte av sådan information bör informationens konfidentialitet bevaras och de berörda entiteternas säkerhet och kommersiella intressen skyddas, med full respekt för företags- och affärshemligheter.

24) Med tanke på de ökande riskerna och antalet cyberincidenter som påverkar medlemsstaterna är det nödvändigt att inrätta ett krisstödsinstrument för att förbättra unionens resiliens mot betydande och storskaliga cybersäkerhetsincidenter och komplettera medlemsstaternas åtgärder genom ekonomiskt krisstöd för beredskap, insatser och omedelbar återställning av samhällsviktiga tjänster. Det instrumentet bör göra det möjligt att snabbt sätta in bistånd under fastställda omständigheter och på

[13] Rådets förordning (EU) 2021/1173 av den 13 juli 2021 om bildande av det gemensamma företaget för ett europeiskt högpresterande datorsystem och om upphävande av förordning (EU) 2018/1488 (EUT L 256, 19.7.2021, s. 3).

tydliga villkor samt möjliggöra en noggrann övervakning och utvärdering av hur resurserna har använts. Cyberkrismekanismen 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 cybersäkerhetsincidenter och cyberkriser.

25) Cyberkrismekanismen bör ge medlemsstaterna stöd som kompletterar deras egna åtgärder och resurser och andra befintliga stödalternativ vid insatser mot och omedelbar återhämtning från betydande och storskaliga cybersäkerhetsincidenter, såsom de tjänster som tillhandahålls av Europeiska unionens cybersäkerhetsbyrå (*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, Pescos snabbinsatsteam för cybersäkerhet[14] och snabbinsatsteam för hybridhot. Den bör vara ett svar på behovet av att säkerställa att särskilda medel finns tillgängliga för att stödja beredskap och insatser vid cybersäkerhetsincidenter i hela unionen och i tredjeländer.

26) Detta instrument påverkar inte förfaranden och ramar för samordning av krishantering på unionsnivå, såsom civilskyddsmekanismen[15], IPCR[16,] och direktiv (EU) 2022/2555. Det kan bidra till eller komplettera åtgärder som genomförs inom ramen för artikel 42.7 i EU-fördraget eller i situationer som definieras i artikel 222 i EUF-fördraget. Användningen av detta instrument bör också samordnas med genomförandet av åtgärderna i verktygslådan för cyberdiplomati, när så är lämpligt.

27) 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 och den berörda medlemsstaten säkerställas. När en medlemsstat begär stöd inom ramen för cyberkrismekanismen bör den tillhandahålla relevant information som motiverar behovet av stöd.

28) 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

---

14 RÅDETS BESLUT (Gusp) 2017/2315 av den 11 december 2017 om upprättande av permanent strukturerat samarbete och om fastställande av förteckningen över deltagande medlemsstater.

15 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).

16 EU-arrangemang för integrerad politisk krishantering (IPCR) och i enlighet med kommissionens rekommendation (EU) 2017/1584 av den 13 september 2017 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser.

medlemsstaterna fullgör sina skyldigheter enligt direktiv (EU) 2022/2555. Cyberkrismekanismen bör ge bistånd till beredskapshöjande åtgärder och incidenthanteringsåtgärder för att minska konsekvenserna av betydande och storskaliga cybersäkerhetsincidenter, stödja omedelbar återhämtning och/eller återställa samhällsviktiga tjänsters funktion.

29) För att främja en konsekvent strategi och stärka säkerheten i hela unionen och 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. I detta syfte bör kommissionen, med stöd av Enisa och i samarbete med samarbetsgruppen för nät- och informationssäkerhet som inrättats genom direktiv (EU) 2022/2555, regelbundet identifiera relevanta sektorer eller delsektorer som bör vara berättigade till ekonomiskt stöd för samordnad testning på unionsnivå. Sektorerna eller delsektorerna bör väljas från bilaga I till direktiv (EU) 2022/2555 (”Högkritiska sektorer”). De samordnade testerna 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 i sina slutsatser om utvecklingen av Europeiska unionens arbete på cyberområdet uppmanade kommissionen, den höga representanten och samarbetsgruppen för nät- och informationssäkerhet att utarbeta 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 (Berec), de samordnade riskbedömningar 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[17]. Sektorerna bör även väljas med beaktande av rådets rekommendation om en unionsomfattande samordnad strategi för att stärka den kritiska infrastrukturens motståndskraft.

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

31) Cyberkrismekanismen bör också stödja incidenthanteringsåtgärder för att minska konsekvenserna av betydande och storskaliga cybersäkerhetsincidenter, stödja omedelbar återhämtning eller återställa samhällsviktiga tjänsters funktion. När så är lämpligt bör den komplettera civilskyddsmekanismen för att säkerställa ett heltäckande sätt att hantera cyberincidenters konsekvenser för medborgarna.

32) Cyberkrismekanismen bör stödja bistånd som medlemsstaterna ger till en medlemsstat som påverkas av en betydande eller storskalig cybersäkerhetsincident, även bistånd som ges genom det CSIRT-nätverk som beskrivs i artikel 15 i direktiv (EU) 2022/2555. Medlemsstater som ger bistånd bör få begära ersättning för kostnader i

[17] 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.

samband med utsändning av expertgrupper inom ramen för ömsesidigt bistånd. Kostnader för exempelvis resor, inkvartering och dagtraktamenten för cybersäkerhetsexperter skulle kunna berättiga till ersättning.

33) En cybersäkerhetsreserv på unionsnivå bör gradvis inrättas, bestående av tjänster från privata leverantörer av förvaltade säkerhetstjänster, för att stödja insatser och omedelbara återhämtningsåtgärder i händelse av betydande eller storskaliga cybersäkerhetsincidenter. EU-cybersäkerhetsreserven bör säkerställa tjänsternas tillgänglighet och beredskap. Tjänsterna från EU-cybersäkerhetsreserven bör stödja de nationella myndigheterna när det gäller att bistå berörda entiteter som är verksamma i kritiska eller högkritiska sektorer, som ett komplement till deras egna åtgärder på nationell nivå. När medlemsstaterna begär stöd från EU-cybersäkerhetsreserven bör de ange vilket stöd som ges till den berörda entiteten på nationell nivå, vilket bör beaktas vid bedömningen av medlemsstatens begäran. Tjänsterna från EU-cybersäkerhetsreserven kan också användas för att stödja unionens institutioner, organ och byråer på liknande villkor.

34) För urvalet av privata tjänsteleverantörer som ska tillhandahålla tjänster inom ramen för EU-cybersäkerhetsreserven är det nödvändigt att fastställa ett antal minimikriterier som bör ingå i anbudsinfordran för att välja ut dessa leverantörer, i syfte att säkerställa att behoven hos medlemsstaternas myndigheter och entiteter som är verksamma i kritiska eller högkritiska sektorer tillgodoses.

35) För att stödja inrättandet av EU-cybersäkerhetsreserven skulle kommissionen kunna överväga att begära att Enisa utarbetar ett förslag till certifieringssystem för sökande i enlighet med förordning (EU) 2019/881 för förvaltade säkerhetstjänster på de områden som omfattas av cyberkrismekanismen.

36) För att stödja denna förordnings mål att främja gemensam situationsmedvetenhet, öka unionens resiliens och möjliggöra effektiva insatser vid betydande och storskaliga cybersäkerhetsincidenter bör EU-CyCLONe, CSIRT-nätverket och kommissionen kunna be Enisa att granska och analysera hot, sårbarheter och begränsningsåtgärder med avseende på en specifik betydande eller storskalig cybersäkerhetsincident. Efter avslutad granskning och analys av en incident bör Enisa utarbeta en incidentgranskningsrapport i samarbete med berörda parter såsom företrädare för den privata sektorn, medlemsstaterna, kommissionen och andra relevanta EU-institutioner, EU-organ och EU-byråer. När det gäller den privata sektorn håller Enisa på att utveckla kanaler för informationsutbyte med specialiserade leverantörer, däribland leverantörer av förvaltade säkerhetslösningar och försäljare, för att bidra till Enisas uppdrag att uppnå en hög gemensam cybersäkerhetsnivå i hela unionen. Med utgångspunkt i samarbetet med berörda parter, även 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 förvaltade säkerhetstjänster som uppfyller villkoren för högsta yrkesmässiga integritet, opartiskhet och erforderlig teknisk expertis enligt kraven i denna förordning. Rapporten bör läggas fram och bidra till arbetet inom EU-CyCLONe, CSIRT-nätverket och kommissionen. När incidenten rör ett tredjeland kommer kommissionen också att dela rapporten med den höga representanten.

37) Med tanke på att cyberangrepp är oförutsägbara och sällan begränsade till ett visst geografiskt område, utan har hög risk för spridningseffekter, bidrar förstärkningen av grannländernas resiliens och deras kapacitet att hantera betydande och storskaliga

cybersäkerhetsincidenter på ett ändamålsenligt sätt till skyddet av unionen som helhet. Tredjeländer som är associerade till programmet för ett digitalt Europa kan därför få stöd från EU-cybersäkerhetsreserven, när detta föreskrivs i respektive avtal om associering till programmet. Finansieringen för associerade tredjeländer bör stödjas av unionen inom ramen för relevanta partnerskap och finansieringsinstrument för dessa länder. Stödet bör omfatta tjänster på området insatser vid och omedelbar återhämtning från betydande eller storskaliga cybersäkerhetsincidenter. De villkor som fastställs för EU-cybersäkerhetsreserven och betrodda leverantörer i denna förordning bör gälla vid tillhandahållande av stöd till tredjeländer som är associerade till programmet för ett digitalt Europa.

38) I syfte att säkerställa enhetliga villkor för genomförandet av denna förordning bör kommissionen tilldelas genomförandebefogenheter för att fastställa villkoren för interoperabilitet mellan gränsöverskridande säkerhetscentrum, fastställa förfarandena för informationsutbyte mellan gränsöverskridande säkerhetscentrum och unionsentiteter om en potentiell eller pågående storskalig cybersäkerhetsincident, ange tekniska krav för att säkerställa den europeiska cybersköldens säkerhet, fastställa vilken typ av och hur många insatstjänster som behövs för EU-cybersäkerhetsreserven samt ytterligare specificera de närmare arrangemangen för tilldelning av stödtjänsterna från EU-cybersäkerhetsreserven. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011.

39) Målet för denna förordning kan bättre uppnås på unionsnivå än av medlemsstaterna. Unionen får därmed vidta åtgärder i enlighet med subsidiaritetsprincipen och proportionalitetsprincipen i artikel 5 i fördraget om Europeiska unionen. Denna förordning går inte utöver vad som är nödvändigt för att uppnå detta mål.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Kapitel I

ALLMÄNNA MÅL, INNEHÅLL OCH DEFINITIONER

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 cybersäkerhetsincidenter, i synnerhet genom följande åtgärder:

a) Utbyggnad av en europeisk infrastruktur av säkerhetscentrum (*den europeiska cyberskölden*) för att bygga upp och förbättra gemensam kapacitet för upptäckt och situationsmedvetenhet.

b) Skapande av en cyberkrismekanism för att hjälpa medlemsstaterna att förbereda sig inför, hantera och omedelbart återhämta sig från betydande och storskaliga cybersäkerhetsincidenter.

c) Inrättande av en europeisk mekanism för granskning av cybersäkerhetsincidenter för att granska och analysera betydande eller storskaliga incidenter.

2. Denna förordning syftar till att stärka solidariteten på unionsnivå genom följande särskilda mål:

a) Stärka den gemensamma upptäcktsförmågan och situationsmedvetenheten i unionen när det gäller cyberhot och cyberincidenter och därigenom göra det möjligt att stärka konkurrenskraften för unionens industri- och tjänstesektorer i hela den digitala ekonomin och bidra till unionens tekniska suveränitet på cybersäkerhetsområdet.

b) Förbättra beredskapen hos entiteter som är verksamma inom kritiska och högkritiska sektorer i hela unionen och stärka solidariteten genom att utveckla gemensam insatskapacitet mot betydande eller storskaliga cybersäkerhetsincidenter, bland annat genom att göra unionsstöd för hantering av cybersäkerhetsincidenter tillgängligt för tredjeländer som deltar i programmet för ett digitalt Europa.

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

3. Denna förordning påverkar inte medlemsstaternas primära ansvar för nationell säkerhet, allmän säkerhet och förebyggande, utredning, upptäckt och lagföring av brott.

Artikel 2

Definitioner

I denna förordning gäller följande definitioner:

1) ***gränsöverskridande säkerhetscentrum***: en flerlandsplattform som inom en samordnad nätverksstruktur för samman nationella säkerhetscentrum från minst tre medlemsstater vilka bildar ett värdkonsortium, och som är utformad för att förhindra cyberhot och cyberincidenter och stödja produktionen av högkvalitativ underrättelseinformation, i synnerhet genom utbyte av data från olika offentliga och privata källor samt genom utbyte av förstklassiga verktyg och gemensam utveckling av kapacitet för cyberdetektering, analys, förebyggande och skydd i en betrodd miljö.

2) ***offentligt organ***: ett offentligrättsligt organ enligt definitionen i artikel 2.1.4 i Europaparlamentets och rådets direktiv 2014/24/EU[18].

3) ***värdkonsortium***: ett konsortium som består av deltagande stater, företrädda av nationella säkerhetscentrum, som har kommit överens om att inrätta och bidra till förvärv av verktyg och infrastruktur för, och drift av, ett gränsöverskridande säkerhetscentrum.

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

5) ***entiteter som är verksamma inom kritiska eller högkritiska sektorer***: typ av entitet som förtecknas i bilaga I och bilaga II till direktiv (EU) 2022/2555.

[18] 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).

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

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

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

9) ***beredskap***: ett tillstånd där man är redo och har kapacitet att säkerställa en effektiv och snabb insats vid en betydande eller storskalig cybersäkerhetsincident, där tillståndet uppnås genom riskbedömnings- och övervakningsåtgärder som vidtagits i förväg.

10) ***insats***: åtgärd i samband med att en betydande eller storskalig cybersäkerhetsincident inträffar, eller under eller efter en sådan incident, för att hantera dess omedelbara och kortsiktiga negativa konsekvenser.

11) ***betrodd leverantör***: leverantör av hanterade säkerhetstjänster enligt definitionen i artikel 6.40 i direktiv (EU) 2022/2555, utvalda i enlighet med artikel 16 i denna förordning.

Kapitel II

DEN EUROPEISKA CYBERSKÖLDEN

Artikel 3

Inrättande av en europeisk cybersköld

1. En sammankopplad europeisk infrastruktur av säkerhetscentrum (*den europeiska cyberskölden*) ska inrättas för att utveckla avancerad kapacitet för unionen att upptäcka, analysera och behandla data om cyberhot och cyberincidenter i unionen. Den ska bestå av alla nationella säkerhetscentrum (*nationella SOC*) och gränsöverskridande säkerhetscentrum (*gränsöverskridande SOC*).

Åtgärder för att genomföra den europeiska cyberskölden ska stödjas med medel från programmet för ett digitalt Europa och genomföras i enlighet med förordning (EU) 2021/694, i synnerhet specifikt mål 3.

2. Den europeiska cyberskölden ska

a) föra samman och dela data om cyberhot och cyberincidenter från olika källor via gränsöverskridande säkerhetscentrum,

b) producera högkvalitativ och agerbar information samt underrättelseinformation om cyberhot, genom användning av förstklassiga verktyg, i synnerhet artificiell intelligens och dataanalysteknik,

b) bidra till bättre skydd mot och hantering av cyberhot,

d) bidra till snabbare upptäckt av cyberhot samt situationsmedvetenhet i hela unionen, och

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

Detta ska utvecklas i samarbete med den europeiska infrastrukturen för högpresterande datorsystem, som inrättades i enlighet med förordning (EU) 2021/1173.

Artikel 4

Nationella säkerhetscentrum

1. För att delta i den europeiska cyberskölden ska varje medlemsstat utse minst ett nationellt säkerhetscentrum. Det nationella säkerhetscentrumet ska vara ett offentligt organ.

Det ska ha kapacitet att fungera som referenspunkt och gränssnitt mot andra offentliga och privata organisationer på nationell nivå för insamling och analys av information om cybersäkerhetshot och cybersäkerhetsincidenter och ska bidra till ett gränsöverskridande säkerhetscentrum. Det ska vara utrustat med förstklassig teknik som klarar att upptäcka, aggregera och analysera data av relevans för cybersäkerhetshot och cybersäkerhetsincidenter.

2. Efter en inbjudan att anmäla intresse ska nationella säkerhetscentrum väljas ut av Europeiska kompetenscentrumet för cybersäkerhet för att delta i en gemensam upphandling av verktyg och infrastrukturer med kompetenscentrumet. Europeiska kompetenscentrumet för cybersäkerhet kan bevilja bidrag till de utvalda nationella säkerhetscentrumen för att finansiera driften av dessa verktyg och infrastrukturer. Unionens finansiella bidrag ska täcka upp till 50 % av kostnaderna för förvärv av verktyg och infrastrukturer och upp till 50 % av driftskostnaderna, och de återstående kostnaderna ska täckas av den berörda medlemsstaten. Innan förfarandet för förvärv av verktyg och infrastrukturer inleds ska Europeiska kompetenscentrumet för cybersäkerhet och de nationella säkerhetscentrumen ingå ett värd- och användningsavtal som reglerar användningen av verktygen och infrastrukturerna.

3. Ett nationellt säkerhetscentrum som utvalts i enlighet med punkt 2 ska förbinda sig att ansöka om att delta i ett gränsöverskridande säkerhetscentrum inom två år från den dag då verktygen och infrastrukturerna förvärvas eller då det erhåller bidragsfinansiering, beroende på vad som inträffar först. Om ett nationellt säkerhetscentrum inte blivit deltagare i ett gränsöverskridande säkerhetscentrum vid den tidpunkten ska det inte ha rätt till ytterligare unionsstöd inom ramen för denna förordning.

Artikel 5

Gränsöverskridande säkerhetscentrum

1. Ett värdkonsortium bestående av minst tre medlemsstater, företrädda av nationella säkerhetscentrum, som åtar sig att samarbeta för att samordna sin cyberupptäckts- och hotövervakningsverksamhet ska ha rätt att delta i åtgärder för att inrätta ett gränsöverskridande säkerhetscentrum.

2. 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

och infrastrukturer med kompetenscentrumet. Europeiska kompetenscentrumet för cybersäkerhet får tilldela värdkonsortiet ett bidrag för att finansiera driften av dessa verktyg och infrastrukturer. Unionens finansiella bidrag ska täcka upp till 75 % kostnaderna för förvärv av verktyg och infrastrukturer och upp till 50 % av driftskostnaderna, och de återstående kostnaderna ska täckas av värdkonsortiet. Innan förfarandet för förvärv av verktyg och infrastrukturer inleds ska Europeiska kompetenscentrumet för cybersäkerhet och värdkonsortiet ingå ett värd- och användningsavtal som reglerar användningen av verktygen och infrastrukturerna.

3. Värdkonsortiets medlemmar ska ingå ett skriftligt konsortieavtal som anger deras interna arrangemang för genomförandet av värd- och användningsavtalet.

4. Ett gränsöverskridande säkerhetscentrum ska för rättsliga ändamål företrädas av ett nationellt säkerhetscentrum som fungerar som samordnande säkerhetscentrum, eller av värdkonsortiet om det är en juridisk person. Det samordnande säkerhetscentrumet ska ansvara för uppfyllandet av kraven i värd- och användningsavtalet och i denna förordning.

Artikel 6

Samarbete och informationsutbyte inom och mellan gränsöverskridande säkerhetscentrum

1. Medlemmar i ett värdkonsortium ska utbyta relevant information sinsemellan inom det gränsöverskridande säkerhetscentrumet, inbegripet 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 upptäcka cyberattacker, om detta informationsutbyte

a) syftar till att förebygga, upptäcka, reagera på eller återhämta sig från incidenter eller begränsa deras inverkan,

b) höjer cybersäkerhetsnivån, särskilt 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 utbyta en betydande mängd data enligt punkt 1 och villkoren för detta informationsutbyte.

b) En styrningsram som ger alla deltagare incitament att utbyta information.

c) Mål för bidrag till utvecklingen av avancerade AI-verktyg och dataanalysverktyg.

3. För att uppmuntra informationsutbyte mellan gränsöverskridande säkerhetscentrum ska dessa gränsöverskridande säkerhetscentrum säkerställa en hög nivå av interoperabilitet sinsemellan. För att främja interoperabiliteten mellan de gränsöverskridande säkerhetscentrumen får kommissionen, genom genomförandeakter och efter samråd med

Europeiska kompetenscentrumet för cybersäkerhet, specificera villkoren för denna interoperabilitet. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 21.2 i denna förordning.

4. Gränsöverskridande säkerhetscentrum ska ingå samarbetsavtal med varandra, och specificera principer för informationsutbyte mellan de gränsöverskridande plattformarna.

Artikel 7

Samarbete och informationsutbyte med unionsentiteter

1. När gränsöverskridande säkerhetscentrum får information om en potentiell eller pågående storskalig cybersäkerhetsincident ska de ge relevant information till EU-CyCLONe, CSIRT-nätverket och kommissionen, så att de kan utöva sina respektive roller i samband med krishantering enligt direktiv (EU) 2022/2555 utan onödigt dröjsmål.

2. Kommissionen får genom genomförandeakter fastställa förfarandena för det informationsutbyte som föreskrivs i punkt 1. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 21.2 i denna förordning.

Artikel 8

Säkerhet

1. Medlemsstater som deltar i den europeiska cyberskölden ska säkerställa en hög nivå av datasäkerhet och fysisk säkerhet för den europeiska cybersköldens infrastruktur och ska säkerställa att infrastrukturen förvaltas på lämpligt sätt och kontrolleras på ett sådant sätt att den skyddas från hot och att infrastrukturens och systemens säkerhet skyddas, inbegripet de data som utbyts via infrastrukturen.

2. Medlemsstater som deltar i den europeiska cyberskölden ska säkerställa att utbytet av information inom den europeiska cyberskölden med andra entiteter än medlemsstaternas offentliga organ inte har en negativ inverkan på unionens säkerhetsintressen.

3. Kommissionen får anta genomförandeakter som fastställer de tekniska kraven för medlemsstaternas uppfyllande av sina skyldigheter enligt punkterna 1 och 2. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 21.2 i denna förordning. När kommissionen gör detta ska den, med stöd av den höga representanten, beakta relevanta säkerhetsstandarder på försvarsnivå, för att främja samarbete med militära aktörer.

Kapitel III

CYBERKRISMEKANISM

Artikel 9

Inrättande av en cyberkrismekanism

1. En cyberkrismekanism inrättas för att förbättra unionens resiliens mot större cyberhot och i en anda av solidaritet förbereda sig inför och begränsa de kortsiktiga effekterna av betydande och storskaliga cybersäkerhetsincidenter (*cyberkrismekanismen*).

2. Åtgärder för att genomföra cyberkrismekanismen ska stödjas med medel från programmet för ett digitalt Europa och genomföras i enlighet med förordning (EU) 2021/694, i synnerhet specifikt mål 3.

Artikel 10

Typ av åtgärder

1. Cyberkrismekanismen ska stödja följande typer av åtgärder:

a) Beredskapsåtgärder, i synnerhet samordnad beredskapstestning av entiteter som är verksamma inom högkritiska sektorer i unionen.

b) Incidenthanteringsåtgärder, som stöder hanteringen av och den omedelbara återhämtningen från betydande och storskaliga cybersäkerhetsincidenter, vilka ska tillhandahållas av betrodda leverantörer som deltar i den EU-cybersäkerhetsreserv som inrättas enligt artikel 12.

c) Ömsesidiga stödåtgärder som utgörs av stöd från de nationella myndigheterna i en medlemsstat till en annan medlemsstat, i synnerhet i enlighet med artikel 11.3 f i direktiv (EU) 2022/2555.

Artikel 11

Samordnad beredskapstestning av entiteter

1. För att stödja den samordnade beredskapstestningen av entiteter enligt artikel 10.1 a i unionen ska kommissionen, efter samråd med samarbetsgruppen för nät- och informationssäkerhet och Enisa, i förteckningen över högkritiska sektorer i bilaga I till direktiv (EU) 2022/2555 identifiera de berörda sektorer eller delsektorer från vilka entiteter kan bli föremål för samordnad beredskapstestning, med beaktande av befintliga och planerade samordnade riskbedömningar och resilienstester på unionsnivå.

2. Samarbetsgruppen för nät- och informationssäkerhet ska i samarbete med kommissionen, Enisa och den höga representanten ta fram gemensamma riskscenarier och metoder för de samordnade testerna.

Artikel 12

Inrättande av en EU-cybersäkerhetsreserv

1. En EU-cybersäkerhetsreserv ska inrättas, för att bistå de användare som avses i punkt 3, när det gäller att hantera eller stödja hanteringen av betydande eller storskaliga cybersäkerhetsincidenter, och en omedelbar återhämtning från sådana incidenter.

2. EU-cybersäkerhetsreserven ska bestå av incidenthanteringstjänster från betrodda leverantörer som valts ut i enlighet med kriterierna i artikel 16. Cybersäkerhetsreserven ska omfatta tjänster som ställts till förfogande på förhand. Tjänsterna ska kunna sättas in i alla medlemsstater.

3. Exempel på användare av tjänster från EU-cybersäkerhetsreserven är

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

b) unionens institutioner, organ och byråer.

4. De användare som avses i punkt 3 a ska använda EU-cybersäkerhetsreservens tjänster för insatser eller stöd till insatser till följd av, och omedelbar återhämtning från, betydande eller storskaliga incidenter som påverkar entiteter som är verksamma inom kritiska eller högkritiska sektorer.

5. Kommissionen ska ha det övergripandet ansvaret för genomförandet av EU-cybersäkerhetsreserven. Kommissionen ska fastställa EU-cybersäkerhetsreservens prioriteringar och utveckling, i linje med behoven hos de användare som avses i punkt 3, och ska övervaka genomförandet och säkerställa komplementaritet, konsekvens, synergi och förbindelser med andra stödåtgärder enligt denna förordning samt andra unionsåtgärder och unionsprogram.

6. Kommissionen får helt eller delvis anförtro driften och förvaltningen av EU-cybersäkerhetsreserven åt Enisa, genom överenskommelser om medverkan.

7. För att stödja kommissionen i inrättandet av EU-cybersäkerhetsreserven ska Enisa kartlägga vilka tjänster som behövs, efter samråd med medlemsstaterna och kommissionen. Enisa ska göra en liknande kartläggning, efter samråd med kommissionen, för att identifiera behoven hos tredjeländer som är berättigade till stöd från EU-cybersäkerhetsreserven i enlighet med artikel 17. Kommissionen ska vid behov samråda med den höga representanten.

8. Kommissionen får genom genomförandeakter specificera typerna av insatstjänster och antalet insatstjänster som behövs för EU-cybersäkerhetsreserven. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 21.2.

Artikel 13

Begäran om stöd från EU-cybersäkerhetsreserven

1. De användare som avses i artikel 12.3 får begära tjänster från EU-cybersäkerhetsreserven för att stödja insatser till följd av och omedelbar återhämtning från betydande eller storskaliga cybersäkerhetsincidenter.

2. För att få stöd från EU-cybersäkerhetsreserven ska de användare som avses i artikel 12.3 vidta åtgärder för att begränsa konsekvenserna av den incident som begäran om stöd avser, vilket innefattar tillhandahållande av direkt tekniskt bistånd och andra resurser som bistånd till incidenthanteringen, samt omedelbara återhämtningsinsatser.

3. En begäran om stöd som kommer från de användare som avses i artikel 12.3 a i denna förordning ska lämnas till kommissionen och Enisa via den gemensamma kontaktpunkt som utsetts eller inrättats av medlemsstaten i enlighet med artikel 8.3 i direktiv (EU) 2022/2555.

4. Medlemsstaterna ska informera CSIRT-nätverket och, när så är lämpligt, EU-CyCLONe om sin begäran om stöd till incidenthantering och omedelbar återhämtning i enlighet med denna artikel.

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

a) Ändamålsenlig information om den påverkade entiteten och incidentens potentiella konsekvenser samt den planerade användningen av det begärda stödet, inbegripet en angivelse av de uppskattade behoven.

b) Information om de åtgärder som vidtagits för att begränsa den incident som begäran om stöd avser, enligt punkt 2.

c) Information om andra former av stöd som är tillgängliga för den berörda entiteten, inbegripet avtalsarrangemang för tjänster som avser incidenthantering och omedelbar återhämtning, samt försäkringsavtal som skulle kunna täcka sådana typer av incidenter.

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

7. Kommissionen får genom genomförandeakter ytterligare specificera närmare bestämmelser för tilldelningen av stödtjänster från EU-cybersäkerhetsreserven. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 21.2.

Artikel 14

Genomförande av stöd från EU-cybersäkerhetsreserven

1. Begäran om stöd från EU-cybersäkerhetsreserven ska bedömas av kommissionen med stöd från Enisa eller i enlighet med överenskommelser om medverkan enligt artikel 12.6 och ett svar ska utan dröjsmål sändas till de användare som avses i artikel 12.3.

2. Om många begäranden inkommer samtidigt ska följande kriterier beaktas för prioriteringen, när så är relevant:

a) Cybersäkerhetsincidentens allvarlighetsgrad.

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

c) De potentiella konsekvenserna för påverkade medlemsstater eller användare.

d) Incidentens potentiella gränsöverskridande karaktär och risken för spridning till andra medlemsstater eller användare.

e) De åtgärder som vidtagits av användaren för att bistå incidenthanteringen och de omedelbara återhämtningsinsatserna, enligt artikel 13.2 och 13.5 b.

3. EU-cybersäkerhetsreservens tjänster ska tillhandahållas i enlighet med särskilda avtal mellan tjänsteleverantören och den användare som tillhandahålls stödet inom ramen för EU-cybersäkerhetsreserven. Dessa avtal ska omfatta villkoren för skadeståndsansvar.

4. De avtal som avses i punkt 3 kan baseras på mallar som utarbetats av Enisa, efter samråd med medlemsstaterna.

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

6. Inom en månad från det att stödåtgärden avslutats ska användarna förse kommissionen och Enisa med en sammanfattande rapport om den tjänst som tillhandahållits, de resultat som uppnåtts och lärdomar som dragits. När användaren är från ett tredjeland enligt artikel 17 ska denna rapport delas med den höga representanten.

7. Kommissionen ska regelbundet rapportera till samarbetsgruppen för nät- och informationssäkerhet om användningen och resultaten av stödet.

Artikel 15

Samordning med krishanteringsmekanismer

1. I de fall då betydande eller storskaliga cybersäkerhetsincidenter har sitt ursprung eller resulterar i katastrofer enligt definitionen i beslut 1313/2013/EU[19] ska stödet inom ramen för denna förordning för att hantera sådana incidenter komplettera åtgärder som vidtas enligt och inte påverka tillämpningen av beslut 1313/2013/EU.

2. Vid storskaliga, gränsöverskridande cybersäkerhetsincidenter som utlöser EU-arrangemangen för integrerad politisk krishantering (IPCR) ska stödet enligt denna förordning för incidenthanteringen hanteras i enlighet med relevanta protokoll och förfaranden inom ramen för IPCR.

3. I samråd med den höga representanten får stöd inom ramen för cyberkrismekanismen komplettera det bistånd som ges inom ramen för den gemensamma utrikes- och säkerhetspolitiken och den gemensamma säkerhets- och försvarspolitiken, däribland genom snabbinsatsteam för cybersäkerhet. Det kan också komplettera eller bidra till bistånd som en medlemsstat tillhandahåller en annan medlemsstat inom ramen för artikel 42.7 i fördraget om Europeiska unionen.

4. Stöd inom ramen för cyberkrismekanismen får vara ett led i unionens och medlemsstaternas gemensamma insatser i situationer som avses i artikel 222 i fördraget om Europeiska unionens funktionssätt.

Artikel 16

Betrodda leverantörer

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

1. I upphandlingsförfarandena i samband med inrättandet av EU-cybersäkerhetsreserven ska den upphandlande myndigheten agera i enlighet med principerna i förordning (EU, Euratom) 2018/1046 och i enlighet med följande principer:

a) Säkerställa att EU-cybersäkerhetsreserven omfattar tjänster som kan användas i alla medlemsstater, med beaktande av i synnerhet nationella krav för tillhandahållandet av sådana tjänster, inbegripet certifiering eller ackreditering.

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

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

2. Vid upphandlingen av tjänster för EU-cybersäkerhetsreserven ska den upphandlande myndigheten inkludera följande urvalskriterier 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/kontinuitet och de tekniska resurser som krävs.

b) Leverantören och dess dotterbolag och underleverantörer ska ha en ram för att skydda känslig information som rör tjänsten, i synnerhet faktaunderlag, resultat och rapporter, och ska efterleva unionens säkerhetsbestämmelser om skydd av säkerhetsskyddsklassificerade EU-uppgifter.

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.

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

f) Leverantören ska vara utrustad med den tekniska hårdvaru- och programvaruutrustning som behövs för den efterfrågade tjänsten.

g) Leverantören ska kunna visa att den har erfarenhet av att leverera liknande tjänster till relevanta nationella myndigheter eller entiteter som är verksamma inom kritiska eller högkritiska 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 det lokala språket i den eller de medlemsstater där den kan tillhandahålla tjänsten.

j) När ett EU-certifieringssystem för hanterade säkerhetstjänster enligt förordning (EU) 2019/881 införts ska leverantören vara certifierad i enlighet med det systemet.

Artikel 17

Stöd till tredjeländer

1. Tredjeländer får begära stöd från EU-cybersäkerhetsreserven när detta föreskrivs i associeringsavtal som ingåtts om deras deltagande i programmet för ett digitalt Europa.

2. Stöd från EU-cybersäkerhetsreserven ska vara förenligt med denna förordning och ska uppfylla alla särskilda villkor som fastställs i de associeringsavtal som avses i punkt 1.

3. Användare från associerade tredjeländer som har rätt att ta emot tjänster från EU-cybersäkerhetsreserven ska inbegripa behöriga myndigheter, såsom CSIRT-enheter och myndigheter för hantering av cyberkriser.

4. Varje tredjeland som är berättigat till stöd från EU-cybersäkerhetsreserven ska utse en myndighet som ska fungera som gemensam kontaktpunkt vid tillämpningen av denna förordning.

5. Innan stöd ges från EU-cybersäkerhetsreserven ska tredjeländer förse kommissionen och den höga representanten med information om sin cyberresiliens och riskhanteringskapacitet, inbegripet åtminstone information om nationella åtgärder som vidtagits som förberedelse inför betydande eller storskaliga cybersäkerhetsincidenter, samt information om ansvariga nationella entiteter, inbegripet CSIRT-enheter eller motsvarande entiteter, deras kapacitet och de resurser som de tilldelats. De bestämmelser i artiklarna 13 och 14 i denna förordning som avser medlemsstater ska tillämpas på tredjeländer enligt punkt 1.

6. Kommissionen ska samordna med den höga representanten när det gäller begäranden som mottagits och genomförandet av stöd som beviljats tredjeländer från EU-cybersäkerhetsreserven.

Kapitel IV

MEKANISM FÖR GRANSKNING AV CYBERSÄKERHETSINCIDENTER

Artikel 18

Mekanism för granskning av cybersäkerhetsincidenter

1. På begäran av kommissionen, EU-CyCLONe eller CSIRT-nätverket ska Enisa granska och analysera hot, sårbarheter och begränsningsåtgärder med avseende på en viss betydande eller storskalig cybersäkerhetsincident. När granskningen och analysen av en incident har slutförts ska Enisa lämna en incidentgranskningsrapport till CSIRT-nätverket, EU-CyCLONe 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 så är relevant ska kommissionen dela rapporten med den höga representanten.

2. Vid utarbetandet av den incidentgranskningsrapport som avses i punkt 1 ska Enisa samarbeta med alla relevanta intressenter, inbegripet företrädare för medlemsstaterna, kommissionen, andra berörda EU-institutioner, EU-organ och EU-byråer, leverantörer av hanterade säkerhetstjänster och användare av cybersäkerhetstjänster. När så är lämpligt ska Enisa också samarbeta med entiteter som påverkas av betydande eller storskaliga cybersäkerhetsincidenter. Enisa får också samråda med andra typer av intressenter som ett led i granskningen. Rådfrågade företrädare ska redovisa alla potentiella intressekonflikter.

3. Rapporten ska omfatta en granskning och analys av den specifika betydande eller storskaliga cybersäkerhetsincidenten, inbegripet de huvudsakliga orsakerna, sårbarheterna och lärdomarna. Konfidentiella uppgifter ska skyddas i enlighet med unionsrätten eller nationell rätt om skydd av känsliga eller säkerhetsskyddsklassificerade uppgifter.

4. När så är lämpligt ska rapporten omfatta rekommendationer för att förbättra unionens säkerhetsstatus.

5. När så är möjligt ska en version av rapporten göras tillgänglig för allmänheten. Den versionen ska endast omfatta offentlig information.

Kapitel V

SLUTBESTÄMMELSER

Artikel 19

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:

1) Följande led ska införas som led aa:

”aa) Stödja utvecklingen av en EU-cybersköld, vilket innefattar utveckling, inrättande och drift av nationella och gränsöverskridande säkerhetscentrumplattformar som bidrar till situationsmedvetenhet i unionen och till att förbättra unionens underrättelsekapacitet när det gäller cyberhot.”

2) Följande led ska läggas till som led g:

”g) Inrätta och driva en cyberkrismekanism för att stödja medlemsstaternas beredskap inför och insatser vid betydande cybersäkerhetsincidenter, som kompletterar nationella resurser och kapaciteter och andra stöd som finns tillgängliga på unionsnivå, inbegripet inrättandet av en EU-cybersäkerhetsreserv.”

a) 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[20], med undantag för åtgärder för genomförandet av EU-cybersäkerhetsreserven, som ska genomföras av kommissionen och Enisa.**”**

[20] 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).

2) Artikel 9 ska ändras på följande sätt:

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

”b) 1 776 956 000 EUR för specifikt mål 2 – Artificiell intelligens.

c) 1 629 566 000 EUR för specifikt mål 3 – Cybersäkerhet och förtroende.

d) 482 347 000 EUR för specifikt mål 4 – Avancerade digitala färdigheter.”

b) Följande punkt ska läggas till som punkt 8:

”8. Genom undantag från artikel 12.4 i förordning (EU, Euratom) 2018/1046 ska outnyttjade åtagande- och betalningsbemyndiganden för åtgärder som syftar till att uppnå målen i artikel 6.1 g i denna förordning automatiskt överföras och får ingås och utbetalas fram till och med den 31 december påföljande budgetår.”

3) I artikel 14 ska punkt 2 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[27] och 2014/25/EU[28].

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 den EU-cybersäkerhetsreserv som inrättats genom artikel 12 i förordning (EU) 2023/XX får kommissionen och Enisa agera som inköpscentral för upphandling på uppdrag av tredjeländer som är associerade till programmet i linje med artikel 10 eller i deras namn. Kommissionen och Enisa får också agera som grossister genom att köpa, lagra och sälja eller donera varor och tjänster, inbegripet hyror, till dessa tredjeländer. Genom undantag från artikel 169.3 i förordning (EU) XXX/XXXX [budgetförordningen omarbetning] räcker en begäran från ett enda tredjeland för att ge kommissionen eller Enisa mandat att agera.

Vid genomförandet av upphandlingsförfaranden för den EU-cybersäkerhetsreserv som inrättats genom artikel 12 i förordning (EU) 2023/XX får kommissionen och Enisa

agera som inköpscentral för upphandling på uppdrag av unionens institutioner, organ och byråer eller i deras namn. Kommissionen och Enisa får också agera som grossister genom att köpa, lagra och sälja eller donera varor och tjänster, inbegripet hyror, inbegripet uthyrning, till unionens institutioner, organ och byråer. Genom undantag från artikel 169.3 i förordning (EU) XXX/XXXX [budgetförordningen omarbetning], räcker 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.”

4) Följande artikel ska läggas till som artikel 16a:

”Vid åtgärder för genomförandet av den europeiska cybersköld som inrättats genom artikel 3 i förordning (EU) 2023/XX ska de tillämpliga reglerna vara de som anges i artiklarna 4 och 5 i förordning (EU) 2023/XX. Om bestämmelserna i denna förordning står i strid med artiklarna 4 och 5 i förordning (EU) 2023/XX ska de sistnämnda ha företräde och tillämpas på dessa specifika åtgärder.”

5) Artikel 19 ska ersättas med följande:

”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 nationella säkerhetscentrum som avses i artikel 4 i förordning XXXX och det värdkonsortium som avses i artikel 5 i förordning XXXX, i enlighet med artikel 195.1 d i budgetförordningen.

Stöd i form av bidrag för cyberkrismekanismen enligt artikel 10 i förordning XXXX får beviljas direkt utan ansökningsomgång av Europeiska kompetenscentrumet för cybersäkerhet till medlemsstater, i enlighet med artikel 195.1 d i budgetförordningen.

För åtgärder som anges i artikel 10.1 c i förordning 202X/XXXX ska Europeiska kompetenscentrumet för cybersäkerhet informera kommissionen och Enisa om medlemsstaternas ansökningar om direkta bidrag utan ansökningsomgång.

För att stödja ömsesidigt bistånd för insatser vid en betydande eller storskalig cybersäkerhetsincident enligt definitionen i artikel 10 c i förordning XXXX 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.”

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

Artikel 20

Utvärdering

Kommissionen ska senast den [fyra år efter denna förordnings tillämpningsdatum] överlämna en rapport om utvärderingen och översynen av denna förordning till Europaparlamentet och rådet.

Artikel 21

Kommittéförfarande

1. Kommissionen ska biträdas av samordningskommittén för programmet för ett digitalt Europa som inrättats genom 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 22

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 Strasbourg den

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

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets titel

1.2. Berörda politikområden

1.3. Förslaget eller initiativet avser

1.4. Mål

1.4.1. Allmänt/allmänna mål:

1.4.2. Specifikt/specifika mål:

1.4.3. Verkan eller resultat som förväntas

1.4.4. Prestationsindikatorer

1.5. Grunder för förslaget eller initiativet

1.5.1. Krav som ska uppfyllas på kort eller lång sikt, inbegripet en detaljerad tidsplan för genomförandet av initiativet

1.5.2. Mervärdet av en åtgärd på unionsnivå (som kan följa av flera faktorer, t.ex. samordningsfördelar, rättssäkerhet, ökad effektivitet eller komplementaritet). Med ”mervärdet av en åtgärd på unionsnivå” i denna punkt avses det värde en åtgärd från unionens sida tillför utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.

1.5.3. Erfarenheter från tidigare liknande åtgärder

1.5.4. Förenlighet med den fleråriga budgetramen och eventuella synergieffekter med andra relevanta instrument

1.5.5. En bedömning av de olika finansieringsalternativ som finns att tillgå, inbegripet möjligheter till omfördelning

1.6. Beräknad varaktighet för och beräknade budgetkonsekvenser av förslaget eller initiativet

1.7. Planerad(e) genomförandemetod(er)

2. FÖRVALTNING

2.1. Regler om uppföljning och rapportering

2.2. Förvaltnings- och kontrollsystem

2.2.1. Motivering av den genomförandemetod, de finansieringsmekanismer, de betalningsvillkor och den kontrollstrategi som föreslås

2.2.2. Uppgifter om identifierade risker och om det eller de interna kontrollsystem som inrättats för att begränsa riskerna

2.2.3. Beräkning och motivering av kontrollernas kostnadseffektivitet (dvs. förhållandet mellan kostnaden för kontrollerna och värdet av de medel som förvaltas) och en bedömning av den förväntade risken för fel (vid betalning och vid avslutande)

2.3. Åtgärder för att förebygga bedrägeri och oriktigheter

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

3.2. Förslagets beräknade budgetkonsekvenser på anslagen

3.2.1. Sammanfattning av beräknad inverkan på driftsanslagen

3.2.2. Beräknad output som finansieras med driftsanslag

3.2.3. Sammanfattning av beräknad inverkan på de administrativa anslagen

3.2.3.1. Beräknat personalbehov

3.2.4. Förenlighet med den gällande fleråriga budgetramen

3.2.5. Bidrag från tredje part

3.3. Beräknad inverkan på inkomsterna

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets titel

Europaparlamentets och rådets förordning om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter

1.2. Berörda politikområden

Ett Europa rustat för den digitala tidsåldern

Europeiska strategiska investeringar

Verksamhet: Att forma EU:s digitala framtid

1.3. Förslaget eller initiativet avser

☒ **en ny åtgärd**

☐ **en ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd**[33]

☐ **en förlängning av en befintlig åtgärd**

☐ **en sammanslagning eller omdirigering av en eller flera åtgärder mot en annan/en ny åtgärd**

1.4. Mål

1.4.1. Allmänt/allmänna mål:

Cybersolidaritetsakten kommer att stärka solidariteten på unionsnivå så att vi bättre kan upptäcka, förbereda oss inför och hantera cyberhot och cybersäkerhetsincidenter. Den har följande syften:

a) Stärka EU:s gemensamma upptäcktsförmåga och situationsmedvetenhet när det gäller cyberhot och cyberincidenter.

b) Förbättra beredskapen hos kritiska entiteter i hela EU och öka solidariteten genom att utveckla den gemensamma kapaciteten att hantera betydande eller storskaliga cybersäkerhetsincidenter, bland annat genom att göra stöd för incidenthantering tillgängligt för tredjeländer som deltar i programmet för ett digitalt Europa.

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

1.4.2. Specifikt/specifika mål:

Cybersolidaritetsaktens mål kommer att uppnås på följande sätt:

a) Utbyggnad av en europeisk infrastruktur av säkerhetscentrum (den europeiska cyberskölden) för att bygga upp och förbättra gemensam kapacitet för upptäckt och situationsmedvetenhet.

[33] I den mening som avses i artikel 58.2 a eller b i budgetförordningen.

b) Skapande av en cyberkrismekanism för att hjälpa medlemsstaterna att förbereda sig inför, hantera och omedelbart återhämta sig från betydande och storskaliga cybersäkerhetsincidenter. Stöd till incidenthantering ska också göras tillgängligt för unionens institutioner, organ och byråer.

Dessa åtgärder kommer att stödjas genom finansiering från programmet för ett digitalt Europa, som kommer att ändras genom denna rättsakt för att inrätta ovannämnda åtgärder, omfatta ekonomiskt stöd för utveckling av dem och klargöra villkoren för ekonomiskt stöd.

c) Inrättande av en europeisk mekanism för granskning av cybersäkerhetsincidenter för att granska och analysera betydande eller storskaliga incidenter.

1.4.3. Verkan eller resultat som förväntas

Beskriv den verkan som förslaget eller initiativet förväntas få på de mottagare eller den del av befolkningen som berörs.

Förslaget skulle ge betydande fördelar för de olika intressenterna. Den europeiska cyberskölden kommer att förbättra medlemsstaternas förmåga att upptäcka cyberhot. Cyberkrismekanismen kommer att komplettera medlemsstaternas åtgärder genom krisstöd för beredskap, incidenthantering och omedelbar återhämtning/återställning av samhällsviktiga tjänsters funktion.

Dessa åtgärder kommer att stärka konkurrensställningen för europeisk industri och europeiska företag i hela den digitaliserade ekonomin och stödja deras digitala omställning genom att öka cybersäkerheten på den digitala inre marknaden. Förslaget syftar särskilt till att öka resiliensen hos enskilda, företag och entiteter som är verksamma inom kritiska eller högkritiska sektorer mot de växande cyberhoten, som kan få förödande samhälleliga och ekonomiska konsekvenser. Detta kommer att uppnås genom investering i verktyg som kommer att stödja snabbare upptäckt och hantering av cyberhot och cybersäkerhetsincidenter, och genom hjälp till medlemsstaterna så att de bättre kan förbereda sig inför och hantera betydande och storskaliga cybersäkerhetsincidenter. Detta bör också bidra till att öka unionens kapacitet på dessa områden, särskilt när det gäller insamling och analys av data om cyberhot och cybersäkerhetsincidenter.

1.4.4. Prestationsindikatorer

Ange indikatorer för övervakning av framsteg och resultat.

För att främja solidaritet på unionsnivå skulle flera olika indikatorer kunna beaktas:

1) Antal cybersäkerhetsinfrastrukturer eller cybersäkerhetsverktyg eller båda som upphandlas gemensamt.

2) Antal åtgärder som stöder beredskap inför och hantering av cybersäkerhetsincidenter inom ramen för cyberkrismekanismen.

1.5. Grunder för förslaget eller initiativet

1.5.1. Krav som ska uppfyllas på kort eller lång sikt, inbegripet en detaljerad tidsplan för genomförandet av initiativet

Förordningen bör tillämpas fullt ut kort efter dess antagande, dvs. den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

1.5.2. Mervärdet av en åtgärd på unionsnivå (som kan följa av flera faktorer, t.ex. samordningsfördelar, rättssäkerhet, ökad effektivitet eller komplementaritet). Med ”mervärdet av en åtgärd på unionsnivå” i denna punkt avses det värde en åtgärd från unionens sida tillför utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.

Cyberhotens i allmänhet starka gränsöverskridande karaktär och det ökande antalet risker och incidenter, vars effekter kan sprida sig över gränser och mellan sektorer och produkter, innebär att målen med detta initiativ inte kan uppnås av medlemsstaterna på egen hand och kräver gemensamma åtgärder och solidaritet på unionsnivå. Erfarenheterna av att motverka cyberhot under Rysslands krig mot Ukraina, tillsammans med lärdomarna från en cybersäkerhetsövning som genomfördes under det franska ordförandeskapet (EU CyCLES), har visat att konkreta mekanismer för ömsesidigt stöd, särskilt samarbete med den privata sektorn, bör utvecklas för att uppnå solidaritet på EU-nivå. Mot denna bakgrund uppmanades kommissionen i rådets slutsatser av den 23 maj 2022 om utvecklingen av Europeiska unionens arbete på cyberområdet att lägga fram ett förslag om en ny fond för hantering av cybersäkerhetsincidenter. Stöd och åtgärder på unionsnivå för att bättre upptäcka cyberhot och för att öka beredskapen och insatskapaciteten ger ett mervärde eftersom man undviker dubbelarbete i unionen och medlemsstaterna. Det skulle leda till ett bättre utnyttjande av befintliga tillgångar och till bättre samordning och utbyte av information om lärdomar.

1.5.3. Erfarenheter från tidigare liknande åtgärder

När det gäller situationsmedvetenhet och upptäckt inom den europeiska cyberskölden hölls en inbjudan att anmäla intresse för gemensam upphandling av verktyg och infrastruktur för att inrätta gränsöverskridande säkerhetscentrum och en ansökningsomgång för att möjliggöra kapacitetsuppbyggnad av säkerhetscentrum som betjänar offentliga och privata organisationer inom ramen för programmet för ett digitalt Europa och dess arbetsprogram för cybersäkerhet för 2021–2022.

När det gäller beredskap och incidenthantering har kommissionen inrättat ett korttidsprogram för att stödja medlemsstaterna genom ytterligare anslag till Enisa i syfte att omedelbart stärka beredskapen och kapaciteten att hantera större cyberincidenter. Tjänster som omfattas är bland annat beredskapsåtgärder, såsom penetrationstestning av kritiska entiteter för att upptäcka sårbarheter. Programmet förbättrar också möjligheterna att bistå medlemsstaterna i händelse av en större incident som påverkar kritiska entiteter. Enisa håller på att genomföra detta korttidsprogram, som redan gett relevanta och värdefulla insikter som har beaktats vid utarbetandet av denna förordning.

1.5.4. Förenlighet med den fleråriga budgetramen och eventuella synergieffekter med andra relevanta instrument

Cybersolidaritetsakten kommer att bygga vidare på sådana åtgärder som unionen och medlemsstaterna för närvarande stöder för att förbättra situationsmedvetenheten och förmågan att upptäcka cyberhot och hantera storskaliga och gränsöverskridande cybersäkerhetsincidenter. Instrumentet är också förenligt med andra krishanteringsramar såsom IPCR, den gemensamma säkerhets- och försvarspolitiken, inbegripet snabbinsatsteam för cybersäkerhet, och det bistånd som en medlemsstat ger en annan inom ramen för artikel 42.7 i fördraget om Europeiska unionen. Det nya förslaget skulle också komplettera och stödja strukturer som utvecklats inom ramen

för andra cybersäkerhetsinstrument såsom direktiv (EU) 2022/2555 (NIS 2-direktivet) eller förordning 2019/881 (cybersäkerhetsakten).

1.5.5. En bedömning av de olika finansieringsalternativ som finns att tillgå, inbegripet möjligheter till omfördelning

Förvaltningen av de verksamhetsområden som Enisa får ansvaret för är anpassade till Enisas befintliga mandat och allmänna uppgifter. Dessa verksamhetsområden kan kräva särskilda profiler eller nya uppdrag, men de kan absorberas av Enisas befintliga resurser och lösas genom omfördelning eller sammankoppling av olika uppdrag. Enisa håller för närvarande på att genomföra ett korttidsprogram som kommissionen inrättade 2022 för att omedelbart stärka beredskapen och kapaciteten att hantera större cyberincidenter. De tjänster som ingår omfattar möjligheter att bistå medlemsstaterna i händelse av en större incident som påverkar kritiska entiteter. Enisas genomförande av detta korttidsprogram pågår och har redan gett relevanta och värdefulla insikter som har beaktats vid utarbetandet av denna förordning. Resurser som tilldelats korttidsprogrammet skulle också kunna användas för denna förordning.

1.6. Beräknad varaktighet för och beräknade budgetkonsekvenser av förslaget eller initiativet

☒ begränsad varaktighet

– ☒ i praktiken från och med dagen för antagandet av förslaget till Europaparlamentets och rådets förordning om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter (*cybersolidaritetsakten*)

– ☒ Budgetkonsekvenser från och med 2023 till och med 2027 för åtagandebemyndiganden och från och med 2023 till och med 2031 för betalningsbemyndiganden[34].

☐ obegränsad varaktighet

– Efter en inledande period ÅÅÅÅ–ÅÅÅÅ,

– beräknas genomförandetakten nå en stabil nivå.

1.7. Planerad(e) genomförandemetod(er)[35]

☒ **Direkt förvaltning** som sköts av kommissionen

– ☒ av dess avdelningar, vilket också inbegriper personalen vid unionens delegationer;

– ☐ av genomförandeorgan

☐ **Delad förvaltning** med medlemsstaterna

☒ **Indirekt förvaltning** genom att uppgifter som ingår i budgetgenomförandet anförtros

– ☐ tredjeländer eller organ som de har utsett

– ☐ internationella organisationer och organ kopplade till dem (ange vilka)

– ☐ EIB och Europeiska investeringsfonden

– ☒ organ som avses i artiklarna 70 och 71 i budgetförordningen

– ☐ offentligrättsliga organ

– ☐ privaträttsliga organ som har anförtrotts offentliga förvaltningsuppgifter i den utsträckning som de har försetts med tillräckliga ekonomiska garantier

– ☐ organ som omfattas av privaträtten i en medlemsstat, som anförtrotts genomförandeuppgifter inom ramen för ett offentlig-privat partnerskap och som har försetts med tillräckliga ekonomiska garantier

– ☐ organ eller personer som anförtrotts genomförandet av särskilda åtgärder inom Gusp enligt avdelning V i fördraget om Europeiska unionen och som fastställs i den relevanta grundläggande rättsakten

– *Vid fler än en metod, ange kompletterande uppgifter under ”Anmärkningar”.*

---

34 Rättsaktens åtgärder bör stödjas genom nästa fleråriga budgetram.

35 Närmare förklaringar av de olika genomförandemetoderna med hänvisningar till respektive bestämmelser i budgetförordningen återfinns på webbplatsen Budgpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx

Anmärkningar

De åtgärder som rör den europeiska cyberskölden kommer att genomföras av Europeiska kompetenscentrumet för cybersäkerhet. Till dess att Europeiska kompetenscentrumet för cybersäkerhet har kapacitet att genomföra sin egen budget kommer Europeiska kommissionen att genomföra åtgärderna genom direkt förvaltning för kompetenscentrumets räkning Europeiska kompetenscentrumet för cybersäkerhet får välja ut entiteter genom inbjudningar att anmäla intresse att delta i gemensam upphandling av verktyg. Europeiska kompetenscentrumet för cybersäkerhet får bevilja bidrag för driften av dessa verktyg. Det får också bevilja bidrag för beredskapsåtgärder inom ramen för cyberkrismekanismen. Kommissionen ska ha det övergripande ansvaret för genomförandet av EU-cybersäkerhetsreserven. Kommissionen får, helt eller delvis och genom överenskommelser om medverkan, anförtro Enisa driften och förvaltningen av EU-cybersäkerhetsreserven. De uppgifter som Enisa tilldelas genom denna förordning är i linje med dess befintliga mandat. Det handlar bland annat om följande uppgifter: i) Stöd till samarbetsgruppen för nät- och informationssäkerhet vid utvecklingen av beredskapsåtgärder i enlighet med riskbedömningar. ii) Stöd till kommissionen vid inrättandet av och tillsynen över genomförandet av EU-cybersäkerhetsreserven, inbegripet att ta emot och behandla begäranden om stöd. iii) Utarbetande av mallar för att underlätta inlämningen av begäranden om stöd och särskilda avtal som ska ingås mellan tjänsteleverantören och användare som får stöd inom ramen för EU-cybersäkerhetsreserven. iv) Granskning och analys av hot, sårbarheter och begränsningsåtgärder med avseende på en viss betydande eller storskalig cybersäkerhetsincident och utarbetande av rapporter om detta. Alla dessa uppgifter beräknas till omkring 7 heltidsekvivalenter från Enisas befintliga resurser och bygger på expertis och förberedande arbete som redan görs av Enisa inom pilotprojektet för krisstöd för beredskap och incidenthantering.

2. FÖRVALTNING

2.1. Regler om uppföljning och rapportering

Ange intervall och andra villkor för sådana åtgärder:

Kommissionen kommer att övervaka genomförandet, tillämpningen och efterlevnaden av dessa nya bestämmelser i syfte att bedöma deras effektivitet. Kommissionen ska överlämna en rapport om utvärderingen och översynen av denna förordning till Europaparlamentet och rådet senast fyra år efter den dag då den börjar tillämpas.

2.2. Förvaltnings- och kontrollsystem

2.2.1. Motivering av den genomförandemetod, de finansieringsmekanismer, de betalningsvillkor och den kontrollstrategi som föreslås

Genom förordningen införs en ram för genomförande av EU-finansiering som syftar till att öka cybersäkerhetsresiliensen genom åtgärder som förbättrar kapaciteten för upptäckt, hantering och återhämtning i samband med betydande och storskaliga cybersäkerhetsincidenter. De enheter inom GD CNECT som ansvarar för politikområdet kommer att ansvara för genomförandet av direktivet.

För att klara av de nya uppgifterna är det nödvändigt att på lämpligt sätt förse kommissionens avdelningar med resurser. Kontrollen av efterlevnaden av den nya förordningen beräknas kräva 6 heltidsekvivalenter (3 tjänstemän och 3 kontraktsanställda) för att göra följande:

- Fastställa beredskapsåtgärder i enlighet med riskbedömningar.
- Säkerställa interoperabilitet mellan gränsöverskridande säkerhetscentrumplattformar.
- Utarbeta potentiella genomförandeakter (två för gränsöverskridande säkerhetscentrum och två för cyberkrismekanismen).
- Administrera värdtjänstavtal och användningsavtal för säkerhetscentrum.
- Inrätta och förvalta EU-cybersäkerhetsreserven, direkt eller via en överenskommelse om medverkan med Enisa. Om det finns en överenskommelse om medverkan med Enisa, utarbeta och övervaka genomförandet av denna överenskommelse för de uppgifter som tilldelats Enisa.
- Delta i de samrådsgrupper som sammankallats av Enisa för att granska och analysera betydande och storskaliga cybersäkerhetsincidenter och utarbeta rapporterna.

2.2.2. Uppgifter om identifierade risker och om det eller de interna kontrollsystem som inrättats för att begränsa riskerna

En risk som identifierats för den europeiska cyberskölden är att medlemsstaterna inte delar med sig av tillräckligt mycket relevant information om cyberhot vare sig inom de gränsöverskridande säkerhetscentrumplattformarna eller mellan gränsöverskridande plattformar och andra entiteter på EU-nivå. För att begränsa dessa risker kommer tilldelningen av medel att ske efter en inbjudan att anmäla intresse där medlemsstaterna åtar sig att dela en viss mängd information med EU-

nivån. Detta åtagande kommer sedan att formaliseras genom ett värdtjänst- och användningsavtal, som kommer att ge Europeiska kompetenscentrumet för cybersäkerhet befogenhet att genomföra revisioner och säkerställa att de gemensamt upphandlade verktygen och infrastrukturerna används i enlighet med avtalet. Åtaganden om en hög nivå av informationsutbyte inom gränsöverskridande säkerhetscentrumplattformar kommer att formaliseras i ett konsortieavtal.

En risk som identifierats för cyberkrismekanismen är att användare som deltar i mekanismen inte vidtar tillräckliga åtgärder för att säkerställa beredskap inför cyberattacker. Därför åläggs användarna att vidta sådana beredskapsåtgärder för att kunna få stöd från EU-cybersäkerhetsreserven. När användare lämnar en begäran om stöd till EU-cybersäkerhetsreserven måste de förklara vilka åtgärder som redan har vidtagits för att hantera incidenten, vilket sedan kommer att beaktas vid analysen av begäran till EU-cybersäkerhetsreserven.

2.2.3. Beräkning och motivering av kontrollernas kostnadseffektivitet (dvs. förhållandet mellan kostnaden för kontrollerna och värdet av de medel som förvaltas) och en bedömning av den förväntade risken för fel (vid betalning och vid avslutande)

Eftersom de regler för deltagande i programmet för ett digitalt Europa som är tillämpliga på stödet inom ramen för cybersolidaritetsakten liknar dem som kommissionen kommer att använda i sina arbetsprogram, och med en grupp av stödmottagare med en riskprofil som liknar den hos program med direkt förvaltning, kan man förvänta sig att felmarginalen kommer att vara ungefär densamma som den som kommissionen förutser för programmet för ett digitalt Europa, det vill säga ge rimlig säkerhet om att risken för fel under den fleråriga utgiftsperioden på årsbasis kommer att ligga inom ett intervall på 2–5 % med det slutliga målet att uppnå en kvarstående felfrekvens som ligger så nära 2 % som möjligt i samband med avslutandet av de fleråriga programmen, när de finansiella konsekvenserna av alla revisioner, korrigeringar och åtgärder för återkrav har beaktats.

2.3. Åtgärder för att förebygga bedrägeri och oriktigheter

Beskriv förebyggande åtgärder (befintliga eller planerade), t.ex. från strategi för bedrägeribekämpning.

När det gäller den europeiska cyberskölden kommer Europeiska kompetenscentrumet för cybersäkerhet att ha revisionsbefogenheter, på grundval av tillgång till information och kontroller på plats, över de gemensamt upphandlade verktygen och infrastrukturerna, i enlighet med det värdtjänst- och användningsavtal som kommer att undertecknas mellan värdkonsortiet och Europeiska kompetenscentrumet för cybersäkerhet.

De befintliga bedrägeriförebyggande åtgärder som är tillämpliga på unionens institutioner, organ och byråer kommer att täcka de ytterligare anslag som krävs för denna förordning.

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

- Befintliga budgetrubriker (även kallade ”budgetposter”)

Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd

Rubrik i den fleråriga budgetramen	Budgetrubrik	Typ av utgift	Bidrag			
	Nummer	Diff./Icke-diff[36].	från Efta-länder[37]	från kandidatländer och potentiella kandidater [38]	från andra tredjeländer	övriga inkomster avsatta för särskilda ändamål
1	02 04 01 10 – Programmet för ett digitalt Europa – Cybersäkerhet	Diff.	JA	JA	NEJ	NEJ
1	02 04 01 11 – programmet för ett digitalt Europa – Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning	Diff.	JA	JA	NEJ	NEJ
1	02 04 03 – programmet för ett digitalt Europa – Artificiell intelligens	Diff.	JA	JA	NEJ	NEJ
1	02 04 04 – programmet för ett digitalt Europa – Kompetens	Diff.	JA	JA	NEJ	NEJ
1	02 01 30 – Stödutgifter för programmet för ett digitalt Europa	Icke-diff. anslag	JA	JA	NEJ	NEJ

[36] Differentierade respektive icke-differentierade anslag.
[37] Efta: Europeiska frihandelssammanslutningen.
[38] Kandidatländer och i förekommande fall potentiella kandidatländer.

3.2. Förslagets beräknade budgetkonsekvenser på anslagen

3.2.1. Sammanfattning av beräknad inverkan på driftsanslagen

– ☐ Förslaget/initiativet kräver inte att driftsanslag tas i anspråk

– ☒ Förslaget/initiativet kräver att driftsanslag tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

Rubrik i den fleråriga budgetramen	Nummer	1 **Inre marknaden, innovation och digitalisering**

Förslaget kommer inte att öka den totala nivån av åtaganden inom programmet för ett digitalt Europa. Bidraget till detta initiativ utgörs nämligen av en omfördelning av åtaganden från specifikt mål 2 och specifikt mål 4 för att stärka budgeten för specifikt mål 3 och Europeiska kompetenscentrumet för cybersäkerhet. Varje ökning av åtaganden inom ramen för programmet för ett digitalt Europa till följd av en ändring av den fleråriga budgetramen skulle kunna användas för detta initiativs syfte.

GD CONNECT			År **2025**	År **2026**	År **2027**	År **2028+**	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)			**TOTALT**
○ Driftsanslag										
Budgetrubrik[39] 02.040110 (omfördelning från 02.0403 och 02.0404)	Åtaganden	(1a)	15,000	15,000	6,000	p.m.				**36,000**
	Betalningar	(2a)	15,000	15,000	6,000					**36,000**
Budgetrubrik 02.040111.02 (omfördelning från 02.0403 och 02.0404)	Åtaganden	(1b)	13,000	23,000	28,000	p.m.				**64,000**
	Betalningar	(2b)	8,450	18,200	25,250	12,100				**64,000**
Anslag av administrativ natur som finansieras genom ramanslagen för särskilda program[40]										

[39] Enligt den officiella kontoplanen.

[40] Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

Budgetrubrik 02.0130		3)	0,150	0,150	0,150	p.m.				0,450
TOTALA anslag för GD CONNECT	Åtaganden	=1a+1b +3	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Betalningar	=2a+2b +3	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

○ TOTALA driftsanslag	Åtaganden	4)	28,000	38,000	34,000	p.m.				**100,000**
	Betalningar	5)	23,450	33,200	31,250	12,100				**100,000**
○ TOTALA anslag av administrativ natur som finansieras genom ramanslagen för särskilda program		6)	0,150	0,150	0,150	p.m.				**0,450**
TOTALA anslag för RUBRIK 1 i den fleråriga budgetramen	Åtaganden	=4+ 6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Betalningar	=5+ 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Upprepa avsnittet ovan om flera rubriker avseende driftsanslag i budgetramen påverkas av förslaget eller initiativet:

○ TOTALA driftsanslag (alla rubriker avseende driftsanslag)	Åtaganden	4)	28,000	38,000	34,000	p.m.				**100,000**
	Betalningar	5)	23,450	33,200	31,250	12,100				**100,000**
TOTALA anslag av administrativ natur som finansieras genom ramanslagen för särskilda program (alla driftsrelaterade rubriker)		6)	0,150	0,150	0,150					**0,450**
TOTALA anslag för RUBRIK 1 till 6 i den fleråriga budgetramen (Referensbelopp)	Åtaganden	=4+ 6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Betalningar	=5+ 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Rubrik i den fleråriga budgetramen	**7**	”Administrativa utgifter”

Detta avsnitt ska fyllas i med hjälp av det datablad för budgetuppgifter av administrativ natur som först ska föras in i bilagan till finansieringsöversikt för rättsakt (bilaga 5 till kommissionens beslut om interna bestämmelser för genomförandet av kommissionens avsnitt av Europeiska unionens allmänna budget), vilken ska laddas upp i DECIDE som underlag för samråden mellan kommissionens avdelningar.

Miljoner euro (avrundat till tre decimaler)

		År **2025**	År **2026**	År **2027**	År **2028+**	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)			**TOTALT**
GD: CONNECT									
○ Personalresurser		0,786	0,786	0,786	p.m.				**2,358**
○ Övriga administrativa utgifter		0,035	0,035	0,035	p.m.				**0,105**
GD CONNECT TOTALT	Anslag	**0,821**	**0,821**	**0,821**					**2,463**

TOTALA anslag för RUBRIK 7 i den fleråriga budgetramen	(summa åtaganden = summa betalningar)	**0,821**	**0,821**	**0,821**					**2,463**

Miljoner euro (avrundat till tre decimaler)

		År **2025**	År **2026**	År **2027**	År **2028+**	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)			**TOTALT**
TOTALA anslag för RUBRIK 1 till 7 i den fleråriga budgetramen	Åtaganden	**28,971**	**38,971**	**34,971**	**p.m.**				**102,913**
	Betalningar	**24,421**	**34,171**	**32,221**	**12,100**				**102,913**

3.2.2. Beräknad output som finansieras med driftsanslag

Åtagandebemyndiganden i miljoner euro (avrundat till tre decimaler)

Ange mål och output ⇩			År **N**		År **N+1**		År **N+2**		År **N+3**		För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)						**TOTALT**	
	OUTPUT																	
	Typ[41]	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 1[42]…																		
- Output																		
- Output																		
- Output																		
Delsumma för specifikt mål nr 1																		
SPECIFIKT MÅL nr 2…																		
- Output																		
Delsumma för specifikt mål nr 2																		
TOTALT																		

[41] Output är produkter och tjänster som ska levereras (t.ex. antal studentutbyten som finansierats, antal km vägar som byggts osv.).

[42] Mål som redovisats under punkt 1.4.2: ”Specifikt/specifika mål…”.

3.2.3. Sammanfattning av beräknad inverkan på de administrativa anslagen

– ☐ Förslaget/initiativet kräver inte att anslag av administrativ natur tas i anspråk

– ☒ Förslaget/initiativet kräver att anslag av administrativ natur tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

	År 2025	År r 2026	År 2027	År N+3	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)			**TOTALT**
RUBRIK 7 i den fleråriga budgetramen								
Personalresurser	0,786	0,786	0,786					**2,358**
Övriga administrativa utgifter	0,035	0,035	0,035					**0,105**
Delsumma RUBRIK 7 i den fleråriga budgetramen	**0,821**	**0,821**	**0,821**					**2,463**
Utanför RUBRIK 7[43] i den fleråriga budgetramen								
Personalresurser								
Andra anslag av administrativ natur	0,150	0,150	0,150					**0,450**
Delsumma utanför RUBRIK 7 i den fleråriga budgetramen	**0,150**	**0,150**	**0,150**					**0,450**
TOTALT	**0,971**	**0,971**	**0,971**					**2,913**

Personalbehov och andra administrativa kostnader ska täckas genom anslag inom generaldirektoratet vilka redan har avdelats för förvaltningen av åtgärden i fråga, eller genom en omfördelning av anslag inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

[43] Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

3.2.3.1. Beräknat personalbehov

– ☐ Förslaget/initiativet kräver inte att personalresurser tas i anspråk

– ☒ Förslaget/initiativet kräver att personalresurser tas i anspråk enligt följande:

Beräkningarna ska anges i heltidsekvivalenter

		År **2025**	År **2026**	År 2027	År **n+3**	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)		
O Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)								
20 01 02 01 (vid huvudkontoret eller vid kommissionens kontor i medlemsstaterna)		3	3	3				
20 01 02 03 (vid delegationer)								
01 01 01 01 (indirekta forskningsåtgärder)								
01 01 01 11 (direkta forskningsåtgärder)								
Annan budgetrubrik (ange vilken)								
O Extern personal (i heltidsekvivalenter)[44]								
20 02 01 (kontraktsanställda, nationella experter och vikarier finansierade genom ramanslaget)		3	3	3				
20 02 03 (kontraktsanställda, lokalanställda, nationella experter, vikarier och unga experter som tjänstgör vid delegationerna)								
XX 01 xx **yy zz** [45]	- vid huvudkontoret							
	- vid delegationer							
01 01 01 02 (kontraktsanställda, vikarier och nationella experter som arbetar med indirekta forskningsåtgärder)								
01 01 01 12 (kontraktsanställda, vikarier och nationella experter som arbetar med direkta forskningsåtgärder)								
Annan budgetrubrik (ange vilken)								
TOTALT		**6**	**6**	**6**				

XX motsvarar det politikområde eller den avdelning i budgeten som avses.

Personalbehoven ska täckas med personal inom generaldirektoratet vilka redan har avdelats för förvaltningen av åtgärden i fråga, eller genom en omfördelning av personal inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

Beskrivning av arbetsuppgifter:

Tjänstemän och tillfälligt anställda	- Fastställa beredskapsåtgärder i enlighet med riskbedömningar (artikel 11). - Utarbeta potentiella genomförandeakter (två för säkerhetscentrum och två för cyberkrismekanismen). - Administrera värdtjänstavtal och användningsavtal för säkerhetscentrum. - Inrätta och förvalta EU-cybersäkerhetsreserven, direkt eller via en överenskommelse om medverkan med Enisa.
Extern personal	Under tillsyn av en tjänsteman - Fastställa beredskapsåtgärder i enlighet med riskbedömningar (artikel 11). - Utarbeta potentiella genomförandeakter (två för säkerhetscentrum och två för cyberkrismekanismen).

44 [Denna fotnot förklarar vissa initialförkortningar som inte används i den svenska versionen].

45 Särskilt tak för finansiering av extern personal genom driftsanslag (tidigare s.k. BA-poster).

	- Administrera värdtjänstavtal och användningsavtal för säkerhetscentrum. - Inrätta och förvalta EU-cybersäkerhetsreserven, direkt eller via en överenskommelse om medverkan med Enisa.

3.2.4. *Förenlighet med den gällande fleråriga budgetramen*

Förslaget/initiativet

– [X] kan finansieras fullständigt genom omfördelningar inom den berörda rubriken i den fleråriga budgetramen.

Förklara i förekommande fall vilka omfördelningar som krävs, och ange berörda budgetrubriker och motsvarande belopp. Bifoga en Excel-tabell om det gäller en större omfördelning.

	23	24	25	26	27	totalt
SO1	16,232,897	20,528,765	17,406,899	16,223,464	10,022,366	80,414,391
SO2 initialt	226,316,819	295,067,000	195,649,000	221,809,000	246,608,000	1,185,449,819
Till cyberinitiativ			18,000,000	28,000,000	19,000,000	65,000,000
NYTT SO2	**226,316,819**	**295,067,000**	**177,649,000**	**193,809,000**	**227,608,000**	**1,120,449,819**
SO3 DB 24	24,361,553	35,596,172	3,638,000	3,638,000	11,175,000	78,408,725
Från SO2-SO4			15,000,000	15,000,000	6,000,000	36,000,000
Nytt SO3	**24,361,553**	**35,596,172**	**18,638,000**	**18,638,000**	**17,175,000**	**114,408,725**
ECCC initia	176,222,303	208,374,879	104,228,130	90,704,986	84,851,497	664,381,795
Från SO2-4			13,000,000	23,000,000	28,000,000	64,000,000
Nytt ECCC	**176,222,303**	**208,374,879**	**117,228,130**	**113,704,986**	**112,851,497**	**728,381,795**
SO4 initialt	66,902,708	64,892,032	56,577,977	70,477,245	72,107,201	330,957,163
Till cyberinitiativ			10,000,000	10,000,000	15,000,000	35,000,000
Nytt SO4	**66,902,708**	**64,892,032**	**46,577,977**	**60,477,245**	**57,107,201**	**295,957,163**

– [ ] kräver användning av den outnyttjade marginalen under den relevanta rubriken i den fleråriga budgetramen och/eller användning av särskilda instrument enligt definitionen i förordningen om den fleråriga budgetramen.

Beskriv vad som krävs, ange berörda rubriker och budgetrubriker, motsvarande belopp och de instrument som är föreslagna för användning.

– [ ] kräver en översyn av den fleråriga budgetramen.

Beskriv behovet av sådana åtgärder, och ange berörda rubriker i budgetramen, budgetrubriker i den årliga budgeten samt de motsvarande beloppen.

3.2.5. *Bidrag från tredje part*

Förslaget/initiativet

– [X] innehåller inga bestämmelser om samfinansiering från tredje parter

– [ ] innehåller bestämmelser om samfinansiering från tredje parter enligt följande uppskattning:

Anslag i miljoner euro (avrundat till tre decimaler)

	År **N**[46]	År **N+1**	År **N+2**	År **N+3**	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)			Totalt
Ange vilket organ som deltar i samfinansieringen								
TOTALA anslag som tillförs genom samfinansiering								

[46] Med år n avses det år då förslaget eller initiativet ska börja genomföras. Ersätt ”n” med det förväntade första genomförandeåret (till exempel 2021). Detsamma för följande år.

3.3. Beräknad inverkan på inkomsterna

– ☒ Förslaget/initiativet påverkar inte budgetens inkomstsida.

– ☐ Förslaget/initiativet påverkar inkomsterna på följande sätt:

  – ☐ Påverkan på egna medel

  – ☐ Påverkan på andra inkomster

  – ange om inkomsterna har avsatts för utgiftsposter☐

Miljoner euro (avrundat till tre decimaler)

Budgetrubrik i den årliga budgetens inkomstdel:	Belopp som förts in för det innevarande budgetåret	Förslagets/initiativets inverkan på inkomsterna[47]						
		År **N**	År **N+1**	År **N+2**	År **N+3**	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)		
Artikel …….								

För inkomster avsatta för särskilda ändamål, ange vilka budgetrubriker i utgiftsdelen som berörs.

[…]

Övriga anmärkningar (t.ex. vilken metod/formel som har använts för att beräkna inverkan på inkomsterna eller andra relevanta uppgifter).

[…]

[47] Vad gäller traditionella egna medel (tullar, sockeravgifter) ska nettobeloppen anges, dvs. bruttobeloppen minus 20 % avdrag för uppbördskostnader.