EUROPA-
KOMMISSIONEN

Strasbourg, den 18.4.2023
COM(2023) 209 final

2023/0109 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser

BEGRUNDELSE

1. BAGGRUND FOR FORSLAGET

• Forslagets begrundelse og formål

Denne begrundelse ledsager forslaget til en forordning om cybersolidaritet. Anvendelsen og afhængigheden af informations- og kommunikationsteknologier er blevet grundlæggende aspekter i alle sektorer af økonomien, da offentlige forvaltninger, virksomheder og borgere mere end nogensinde før er indbyrdes forbundne og afhængige af hinanden. Denne større udbredelse af digitale teknologier øger eksponeringen for cybersikkerhedshændelser og de mulige virkninger heraf. Samtidig står medlemsstaterne over for stigende cybersikkerhedsrisici og et generelt komplekst trusselsbillede med en klar risiko for, at cyberhændelser hurtigt kan spredes fra én medlemsstat til andre.

Cyberoperationer bliver desuden i stigende grad integreret i hybride strategier og krigsførelsesstrategier, og det har betydelige konsekvenser for de mål, operationerne sigter mod. Navnlig er der i forbindelse med Ruslands militære aggression mod Ukraine set forudgående og sideløbende fjendtlige cyberoperationer som en del af strategien, og det giver en ny baggrund for opfattelsen og vurderingen af EU's kollektive beredskab til håndtering af cybersikkerhedskriser og skaber behov for hurtig handling. Truslen om mulige omfattende hændelser, der kan forårsage betydelige forstyrrelser og skader på kritisk infrastruktur, kræver et øget beredskab på alle niveauer i EU's cybersikkerhedsøkosystem. Truslen rækker langt videre end Ruslands militære aggression mod Ukraine. Den omfatter fortsatte og formentlig blivende cybertrusler fra statslige og ikke-statslige aktører, når man tager de mange forskellige statslige, kriminelle og hacktivistiske aktører i betragtning, der er en del af de aktuelle geopolitiske spændinger. I de seneste år er antallet af cyberangreb steget dramatisk, herunder angreb i forsyningskæden rettet mod cyberspionage, ransomware eller forstyrrelser. I 2020 berørte angrebet på SolarWinds' forsyningskæde mere end 18 000 organisationer på verdensplan, herunder statslige organer og store virksomheder. Væsentlige cybersikkerhedshændelser kan skabe så omfattende forstyrrelser, at en enkelt eller flere berørte medlemsstater ikke kan håndtere dem alene. Derfor er der behov for at styrke solidariteten på EU-niveau for bedre at kunne opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser.

Med hensyn til at opdage cybertrusler og -hændelser er der et presserende behov for at øge udvekslingen af oplysninger og forbedre den samlede kapacitet og drastisk reducere den tid, der er nødvendig for at afsløre cybertrusler, før de kan forårsage omfattende skader og omkostninger[1]. Selv om mange cybersikkerhedstrusler og -hændelser har en mulig grænseoverskridende dimension på grund af sammenkoblingen af de digitale infrastrukturer, er udvekslingen af relevante oplysninger blandt medlemsstaterne fortsat begrænset.

[1] Ifølge en rapport fra Ponemon Institute og IBM Security var den gennemsnitlige tid i 2022 207 dage til at opdage et sikkerhedsbrud og yderligere 70 dage til at inddæmme angrebet. Brud på datasikkerheden med et forløb på over 200 dage havde i 2022 gennemsnitlige omkostninger på 4,86 mio. EUR sammenlignet med 3,74 mio. EUR for databrud på under 200 dage. ("Cost of a data breach 2022", https://www.ibm.com/reports/data-breach)

Opbygningen af et netværk af grænseoverskridende sikkerhedsoperationscentre (SOC'er) for dermed at øge kapaciteten til at opdage og reagere på trusler skal bidrage til at løse dette problem.

Med hensyn til beredskab og reaktion på cybersikkerhedshændelser er der i øjeblikket begrænset støtte på EU-niveau og begrænset solidaritet mellem medlemsstaterne. I Rådets konklusioner fra oktober 2021 blev behovet fremhævet for at afhjælpe disse mangler ved at opfordre Kommissionen til at forelægge et forslag om en ny beredskabsfond for cybersikkerhed[2].

Med denne forordning gennemføres ligeledes EU's strategi for cybersikkerhed, der blev vedtaget i december 2020[3], og som omfatter oprettelse af et europæisk cyberskjold, der skal styrke kapaciteten til at opdage og udveksle oplysninger om cybertrusler i Den Europæiske Union gennem en sammenslutning af nationale og grænseoverskridende SOC'er.

Denne forordning bygger på de første tiltag, der allerede er udviklet i et lukket samarbejde med de primære interessenter med støtte fra programmet for et digitalt Europa. Navnlig med hensyn til SOC'er blev der under arbejdsprogram for cybersikkerhed for 2021-2022 som en del af programmet for et digitalt Europa udsendt en indkaldelse af interessetilkendegivelser med henblik på fælles indkøb af værktøjer og infrastruktur til etablering af grænseoverskridende SOC'er og en indkaldelse vedrørende tilskud til kapacitetsopbygning af SOC'er, der betjener offentlige og private organisationer. Med hensyn til beredskab og reaktioner på hændelser har Kommissionen oprettet et kortsigtet program vedrørende støtte til medlemsstaterne i form af yderligere midler, der er afsat til Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), med henblik på omgående at styrke beredskabet og kapaciteten til at reagere på større cyberhændelser. Begge foranstaltninger er udarbejdet i tæt samarbejde med medlemsstaterne. Denne forordning skal afhjælpe mangler og integrere viden fra disse foranstaltninger.

Endelig understøtter dette forslag forpligtelserne i henhold til den fælles meddelelse om cyberforsvar[4], der blev vedtaget den 10. november, til at udarbejde et forslag til et EU-initiativ vedrørende cybersolidaritet med følgende målsætninger: styrke EU's fælles situationskendskab og kapacitet til opdage og reagere på hændelser med henblik på gradvist at opbygge en cybersikkerhedsreserve på EU-plan bestående af tjenester fra betroede private udbydere og støtte til test af kritiske enheder.

På den baggrund fremlægger Kommissionen nærværende forordning om cybersolidaritet med det mål at styrke solidariteten på EU-plan med henblik på bedre at kunne opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser og med følgende specifikke mål:

---

2 Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition, som blev godkendt af Rådet på samlingen den 23. maj 2022 (9364/22)

3 Fælles meddelelse til Europa-Parlamentet og Rådet: EU's strategi for cybersikkerhed for det digitale årti, JOIN202018 final.

4 Fælles meddelelse til Europa-Parlamentet og Rådet — EU's politik for cyberforsvar, JOIN(2022) 49 final.

- at styrke EU's fælles situationskendskab og kapacitet til at afsløre cybertrusler og -hændelser og dermed bidrage til europæisk teknologisk suverænitet på cybersikkerhedsområdet
- at styrke kritiske enheders beredskab i hele EU og styrke solidariteten ved at udvikle fælles indsatskapaciteter over for væsentlige eller omfattende cybersikkerhedshændelser, herunder ved at stille støtte til reaktioner på hændelser til rådighed for tredjelande, der er tilknyttet programmet for et digitalt Europa
- at øge Unionens modstandsdygtighed og bidrage til en effektiv indsats ved at gennemgå og vurdere væsentlige eller omfattende hændelser, herunder indhøstede erfaringer og eventuelle anbefalinger.

Målsætningerne opfyldes gennem følgende foranstaltninger:

- Etablering af en paneuropæisk infrastruktur for SOC'er (et europæisk cyberskjold) for at opbygge og styrke det fælles situationskendskab og den fælles kapacitet til at opdage hændelser.
- Oprettelse af en cyberberedskabsmekanisme som støtte til medlemsstaterne, så de bedre kan forberede sig og reagere på samt sikre omgående genopretning efter væsentlige eller omfattende cybersikkerhedshændelser. Støtte til reaktioner på hændelser stilles også til rådighed for EU's institutioner, organer, kontorer og agenturer (EUIBA).
- Oprettelse af en europæisk mekanisme til gennemgang af cybersikkerhedshændelser med henblik på at gennemgå og vurdere specifikke væsentlige eller omfattende hændelser.

Det europæiske cyberskjold og cyberberedskabsmekanismen støttes med midler fra programmet for et digitalt Europa, som dette lovgivningsinstrument indebærer en ændring af med henblik på at fastlægge ovennævnte foranstaltninger, yde finansiel støtte til deres udvikling og præcisere betingelserne for at modtage finansiel støtte.

•Sammenhæng med de gældende regler på samme område

EU-rammen omfatter flere love, der allerede er indført eller foreslået på EU-plan for at mindske sårbarheder, øge kritiske enheders modstandsdygtighed over for cybersikkerhedsrisici og støtte den koordinerede håndtering af omfattende cybersikkerhedshændelser og -kriser, navnlig direktivet om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS2)[5], forordningen om cybersikkerhed[6], direktivet om angreb på informationssystemer[7] og

[5] Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet).

[6] Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed).

[7] Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA.

Kommissionens henstilling (EU) 2017/1584 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser[8].

De foranstaltninger, der foreslås i henhold til forordningen om cybersolidaritet, omfatter situationskendskab, informationsudveksling samt støtte til beredskab og reaktion på cyberhændelser. Disse foranstaltninger er i overensstemmelse med og støtter målsætningerne for den gældende lovgivningsmæssige ramme på EU-plan, navnlig i henhold til direktiv (EU) 2022/2555 ("NIS 2-direktivet"). Forordningen om cybersolidaritet bygger især på og støtter de eksisterende operationelle samarbejds- og krisestyringsrammer for cybersikkerhed, navnlig det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe) og netværket af enheder, der håndterer IT-sikkerhedshændelser (CSIRT).

De grænseoverskridende SOC-platforme skal sikre en ny kapacitet, der supplerer CSIRT-netværket, ved at samle og dele data om cybersikkerhedstrusler fra offentlige og private enheder, øge værdien af sådanne data gennem ekspertanalyser og de nyeste værktøjer og bidrage til udviklingen af Unionens kapaciteter og teknologiske suverænitet.

Endelig er dette forslag i overensstemmelse med Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed[9], hvori medlemsstaterne opfordres til at træffe hurtige og effektive foranstaltninger og til at samarbejde loyalt, effektivt, i solidaritet og på en koordineret måde med hinanden, Kommissionen og andre relevante offentlige myndigheder samt de berørte enheder for at øge modstandsdygtigheden i den kritiske infrastruktur, der anvendes til at levere væsentlige tjenester på det indre marked.

- **Sammenhæng med Unionens politik på andre områder**

Forslaget er i overensstemmelse med andre kriseresponsmekanismer og -protokoller, såsom den integrerede mekanisme for politisk kriserespons (IPCR). Forordningen om cybersolidaritet supplerer ovennævnte krisestyringsrammer og -protokoller ved at yde målrettet støtte til beredskab og reaktion på cybersikkerhedshændelser. Forslaget er også i overensstemmelse med EU's eksterne reaktion på omfattende hændelser inden for rammerne af den fælles udenrigs- og sikkerhedspolitik (FUSP), herunder gennem EU's cyberdiplomatiske værktøjskasse. Forslaget supplerer foranstaltninger, der gennemføres inden for rammerne af artikel 42, stk. 7, i traktaten om Den Europæiske Union eller i situationer som defineret i artikel 222 i traktaten om Den Europæiske Unions funktionsmåde.

[8] Forslag til Europa-Parlamentets og Rådets forordning om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) 2019/1020 (COM/2022/454 final).

[9] Rådets henstilling af 8. december 2022 om en koordineret tilgang på EU-plan til styrkelse af kritisk infrastrukturs modstandsdygtighed (EØS-relevant tekst) 2023/C 20/01.

Det supplerer ligeledes EU's civilbeskyttelsesmekanisme[10], der blev oprettet i december 2013 og suppleret med en ny lovgivning, der blev vedtaget i maj 2021[11], og som styrker forebyggelses-, beredskabs- og indsatssøjlerne i EU's civilbeskyttelsesmekanisme og giver EU yderligere kapacitet til at reagere på nye risici i Europa og i verden og styrker rescEU-reserven.

2. RETSGRUNDLAG, NÆRHEDSPRINCIPPET OG PROPORTIONALITETSPRINCIPPET

• Retsgrundlag

Retsgrundlaget for dette forslag er artikel 173, stk. 3, og artikel 322, stk. 1, litra a), i traktaten om Den Europæiske Unions funktionsmåde (TEUF). I henhold til artikel 173 i TEUF skal Unionen og medlemsstaterne sørge for, at de nødvendige betingelser for udviklingen af EU-industriens konkurrenceevne er til stede. Denne forordning har til formål at styrke industriens og servicesektorernes konkurrenceevne i Europa i hele den digitaliserede økonomi og støtte deres digitale omstilling ved at styrke cybersikkerhedsniveauet på det digitale indre marked. Forordningen har navnlig til formål at øge modstandsdygtigheden hos borgere, virksomheder og enheder, der opererer i kritiske og meget kritiske sektorer, over for de tiltagende cybersikkerhedstrusler, som kan have ødelæggende samfundsmæssige og økonomiske virkninger.

Forslaget er også baseret på artikel 322, stk. 1, litra a), i TEUF, da det indeholder specifikke overførselsregler, der fraviger princippet om etårighed fastsat i Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046 ("finansforordningen")[12]. Med henblik på forsvarlig økonomisk forvaltning og i betragtning af det uforudsigelige, ekstraordinære og specifikke cybersikkerheds- og cybertrusselsbillede bør beredskabsmekanismen for cybersikkerhed have en vis grad af indbygget fleksibilitet med hensyn til budgetforvaltning, og navnlig bør det tillades, at uudnyttede forpligtelses- og betalingsbevillinger til foranstaltninger, der understøtter forordningens målsætninger, automatisk overføres til det følgende regnskabsår. Da denne nye regel rejser spørgsmål vedrørende finansforordningen, kan spørgsmålet behandles i forbindelse med de igangværende forhandlinger om omarbejdning af finansforordningen.

• Nærhedsprincippet (for områder, der ikke er omfattet af enekompetence)

Cybersikkerhedstruslernes udpræget grænseoverskridende karakter og det stigende antal risici og hændelser, som har afledte effekter på tværs af landegrænser, sektorer og produkter,

---

10 Europa-Parlamentets og Rådets afgørelse 1313/2013/EU af 17. december 2013 om en EU-civilbeskyttelsesmekanisme (EØS-relevant tekst).

11 Europa-Parlamentets og Rådets forordning (EU) 2021/836 af 20. maj 2021 om ændring af afgørelse nr. 1313/2013/EU om en EU-civilbeskyttelsesmekanisme (EØS-relevant tekst)

12 Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046 af 18. juli 2018 om de finansielle regler vedrørende Unionens almindelige budget (EUT L 193 af 30.7.2018, s. 1).

betyder, at målsætningerne for den nuværende indsats ikke effektivt kan opfyldes af medlemsstaterne alene; det kræver også fælles handling og solidaritet på EU-niveau.

Erfaringerne med at imødegå cybertrusler afledt af krigen mod Ukraine og erfaringerne fra en cybersikkerhedsøvelse, der blev gennemført under det franske formandskab (EU CyCLES), har vist, at der bør udvikles konkrete gensidige støttemekanismer, navnlig samarbejde med den private sektor, for at skabe solidaritet på EU-niveau. På denne baggrund opfordres Kommissionen i Rådets konklusioner af 23. maj 2022 om udviklingen af Den Europæiske Unions cyberposition til at forelægge et forslag om en ny beredskabsfond for cybersikkerhed.

Støtte og tiltag på EU-niveau for bedre at kunne afsløre cybersikkerhedstrusler og for at øge beredskabs- og indsatskapaciteten skaber merværdi, da dobbeltarbejde undgås på tværs af Unionen og i medlemsstaterne. Det vil sikre en bedre udnyttelse af eksisterende aktiver og en øget koordinering og udveksling af oplysninger om indhøstede erfaringer. Cyberberedskabsmekanismen har også til formål via EU's cybersikkerhedsreserve at yde støtte til tredjelande, der er tilknyttet programmet for et digitalt Europa.

Den støtte, der ydes gennem de forskellige initiativer, som skal oprettes og finansieres på EU-niveau, skal supplere og ikke overlappe det nationale situationskendskab og beredskab samt kapaciteten til at opdage og reagere på cybertrusler og -hændelser.

- **Proportionalitetsprincippet**

Foranstaltningerne går ikke videre end, hvad der er nødvendigt for at opfylde forordningens generelle og specifikke mål. Foranstaltningerne i denne forordning berører ikke medlemsstaternes ansvar for national sikkerhed, offentlig sikkerhed, forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger. De påvirker heller ikke de retlige forpligtelser for enheder, der opererer i kritiske og meget kritiske sektorer, til at vedtage cybersikkerhedsforanstaltninger i overensstemmelse med NIS 2-direktivet.

De foranstaltninger, der er omfattet af denne forordning, supplerer sådanne bestræbelser og foranstaltninger ved at støtte etableringen af infrastrukturer til bedre afsløring og analyse af trusler og ved at yde støtte til beredskabs- og indsatsforanstaltninger i tilfælde af væsentlige eller omfattende hændelser.

- **Valg af retsakt**

Forslaget har form af en forordning udstedt af Europa-Parlamentet og Rådet. Det er det mest hensigtsmæssige retlige instrument, da kun en forordning med direkte gældende retlige bestemmelser sikrer den nødvendige grad af ensartethed i oprettelse og drift af en europæisk cybersikrings- og cyberberedskabsmekanisme gennem støtte under programmet for et digitalt Europa til oprettelse heraf samt klare betingelser for anvendelse og tildeling af denne støtte.

3. RESULTATER AF EFTERFØLGENDE EVALUERINGER, HØRINGER AF INTERESSENTER OG KONSEKVENSANALYSER

- **Høringer af interessenter**

Foranstaltningerne i denne forordning støttes under programmet for et digitalt Europa, som har været genstand for en bred høring. Desuden bygger de videre på de første tiltag, der er udarbejdet i tæt samarbejde med de vigtigste interessenter. Med hensyn til SOC'er har Kommissionen udarbejdet et konceptdokument om udvikling af grænseoverskridende SOC-platforme og en indkaldelse af interessetilkendegivelser i tæt samarbejde med medlemsstaterne inden for rammerne af Det Europæiske Kompetencecenter for Cybersikkerhed (ECCC). I den forbindelse blev der gennemført en undersøgelse af SOC-kapaciteten i de enkelte lande, og fælles tilgange og tekniske krav er blevet drøftet i ECCC's tekniske arbejdsgruppe, der består af repræsentanter for medlemsstaterne. Desuden er der gennemført en dialog med industrien, navnlig gennem ekspertgruppen om SOC'er, der er nedsat af ENISA og Den Europæiske Organisation for Cybersikkerhed (ECSO).

For det andet, med hensyn til beredskab og reaktioner på hændelser har Kommissionen oprettet et kortsigtet program vedrørende støtte til medlemsstaterne i form af yderligere midler, der er afsat til ENISA under programmet for et digitalt Europa, med henblik på omgående at styrke beredskabet og kapaciteten til at reagere på større cyberhændelser. Tilbagemeldinger fra medlemsstaterne og industrien, der er indsamlet under gennemførelsen af dette kortsigtede program, giver allerede en værdifuld viden, der er anvendt ved udarbejdelse af den foreslåede forordning med henblik på at afhjælpe de konstaterede mangler. Det var første fase i henhold til Rådets konklusioner om EU's cyberposition, hvori Kommissionen anmodes om at fremsætte et forslag til en ny beredskabsfond for cybersikkerhed.

Desuden blev der afholdt en workshop med eksperter fra medlemsstaterne om cyberberedskabsmekanismen den 16. februar 2023 på grundlag af et debatoplæg. Alle medlemsstater deltog i workshoppen, og 11 medlemsstater indgav desuden skriftlige bidrag.

- **Konsekvensanalyse**

På grund af forslagets hastende karakter er der ikke foretaget nogen konsekvensanalyse. Foranstaltningerne i denne forordning støttes under programmet for et digitalt Europa og er i overensstemmelse med dem, der er fastsat i forordningen om programmet for et digitalt Europa, som var genstand for en særlig konsekvensanalyse. Denne forordning medfører ikke væsentlige administrative eller miljømæssige virkninger ud over dem, der allerede er vurderet i konsekvensanalysen af forordningen om programmet for et digitalt Europa.

Forordningen er desuden en videreførelse af de første foranstaltninger, der blev udviklet i tæt samarbejde med de vigtigste interessenter, jf. ovenfor, og en opfølgning på medlemsstaternes opfordring til Kommissionen om at fremlægge et forslag til en ny beredskabsfond for cybersikkerhed inden udgangen af tredje kvartal 2022.

Med hensyn til situationskendskab og afsløring af hændelser gennem det europæiske cyberskjold blev der specifikt udsendt en indkaldelse af interessetilkendegivelser med henblik på fælles indkøb af værktøjer og infrastruktur til etablering af grænseoverskridende SOC'er og en indkaldelse vedrørende tilskud til kapacitetsopbygning af SOC'er, der betjener offentlige og private organisationer.

Med hensyn til beredskab og reaktioner på hændelser har Kommissionen som nævnt ovenfor oprettet et kortsigtet program til støtte for medlemsstaterne under programmet for et digitalt Europa, der gennemføres af ENISA. Blandt de omfattede tjenester er beredskabsforanstaltninger såsom penetrationstest af kritiske enheder med henblik på at kortlægge sårbarheder. Det styrker også mulighederne for at bistå medlemsstaterne i tilfælde af en større hændelse, der påvirker kritiske enheder. ENISA er i gang med at gennemføre det kortsigtede program og har allerede fremlagt relevant viden, som er medtaget i udarbejdelsen af denne forordning.

- **Grundlæggende rettigheder**

Ved at bidrage til sikkerheden vedrørende digitale oplysninger skal forslaget bidrage til at beskytte retten til frihed og sikkerhed i overensstemmelse med artikel 6 i EU's charter om grundlæggende rettigheder og retten til respekt for privatliv og familieliv i overensstemmelse med artikel 7 i EU's charter om grundlæggende rettigheder. Ved at beskytte virksomhederne mod økonomisk skadelige cyberangreb bidrager forslaget også til friheden til at oprette og drive egen virksomhed i overensstemmelse med artikel 16 i EU's charter om grundlæggende rettigheder og ejendomsretten i overensstemmelse med artikel 17 i EU's charter om grundlæggende rettigheder. Endelig støtter forslaget ved at beskytte kritisk infrastrukturs robusthed over for cyberangreb retten til sundhedspleje i overensstemmelse med artikel 35 i EU's charter om grundlæggende rettigheder og retten til adgang til tjenesteydelser af almen økonomisk interesse i overensstemmelse med artikel 36 i EU's charter om grundlæggende rettigheder.

4. VIRKNINGER FOR BUDGETTET

Foranstaltningerne i denne forordning støttes med finansiering under den strategiske målsætning "cybersikkerhed" i programmet for et digitalt Europa.

Det samlede budget omfatter en forhøjelse på 100 mio. EUR, som i denne forordning foreslås omfordelt fra andre strategiske målsætninger for programmet for et digitalt Europa. Dermed bringes det nye samlede beløb, der er til rådighed til cybersikkerhedsforanstaltninger under programmet for et digitalt Europa, op på 842,8 mio. EUR.

En del af de supplerende 100 mio. EUR skal gå til at øge det budget, der forvaltes af ECCC, med henblik på at gennemføre foranstaltninger vedrørende SOC'er og beredskab som led i deres arbejdsprogram(mer). Desuden vil den supplerende finansiering indgå som støtte til oprettelse af EU's cybersikkerhedsreserve.

Den ekstra finansiering supplerer det budget, der allerede er afsat til lignende foranstaltninger i det primære arbejdsprogram for programmet for et digitalt Europa og programmet for cybersikkerhed fra perioden 2023-2027, hvilket bringer det samlede beløb op på 551 mio. for perioden 2023-2027, mens 115 mio. allerede var afsat i form af pilotprojekter i perioden 2021-2022. Når medlemsstaternes bidrag medregnes, kan det samlede budget blive på 1 109 mia. euro.

En oversigt over de omkostninger, der er forbundet hermed, findes i "finansieringsoversigten" til dette forslag.

5. ANDRE FORHOLD

- **Planer for gennemførelsen og foranstaltninger til overvågning, evaluering og rapportering**

Kommissionen vil overvåge gennemførelsen, anvendelsen og overholdelsen af disse nye bestemmelser med henblik på at vurdere deres effektivitet. Kommissionen forelægger Europa-Parlamentet og Rådet en rapport om evalueringen og revisionen af denne forordning senest fire år efter datoen for dens anvendelse.

- **Nærmere redegørelse for de enkelte bestemmelser i forslaget**

Generelle målsætninger, genstand og definitioner (kapitel I)

I kapitel I fastsættes forordningens målsætninger om at styrke solidariteten på EU-niveau med henblik på bedre at kunne afsløre, foregribe og reagere på cybersikkerhedstrusler og -hændelser, herunder navnlig at styrke Unionens samlede situationskendskab og afsløring af cybertrusler og -hændelser, styrke beredskabet i enheder, der opererer i kritiske og meget kritiske sektorer på tværs af Unionen, og styrke solidariteten ved at udvikle fælles indsatskapacitet over for væsentlige eller omfattende cybersikkerhedshændelser og styrke Unionens modstandsdygtighed ved at gennemgå og vurdere væsentlige eller omfattende hændelser. Kapitlet beskriver også de foranstaltninger, der sikrer opfyldelse af målsætningerne: indførelse af et europæisk cyberskjold, etablering af en cyberberedskabsmekanisme og etablering af en mekanisme til gennemgang af cybersikkerhedshændelser. Desuden fastsættes de definitioner, der anvendes i instrumentet.

Det europæiske cyberskjold (kapitel II)

I kapitel II beskrives det europæiske cyberskjold, de forskellige elementer og betingelserne for at deltage. Først beskrives den overordnede målsætning for det europæiske cyberskjold, som er at udvikle avancerede kapaciteter i Unionen med hensyn til at afsløre, analysere og behandle data om cybertrusler og -hændelser i Unionen, og dernæst de specifikke operationelle målsætninger. Det præciseres, at EU-finansiering af det europæiske cyberskjold skal gennemføres i overensstemmelse med forordningen om programmet for et digitalt Europa.

I kapitlet beskrives endvidere den type enheder, som skal udgøre det europæiske cyberskjold. Skjoldet består af nationale sikkerhedsoperationscentre ("nationale SOC'er") og grænseoverskridende sikkerhedsoperationscentre ("grænseoverskridende SOC'er"). Hver deltagende medlemsstat udpeger et nationalt SOC. Det skal fungerer som referencepunkt og portal til andre offentlige og private organisationer på nationalt plan med henblik på at indsamle og analysere oplysninger om cybersikkerhedstrusler og -hændelser og bidrage til et grænseoverskridende SOC. Efter en indkaldelse af interessetilkendegivelser kan ECCC udvælge et nationalt SOC, der deltager i fælles indkøb af værktøjer og infrastrukturer sammen med ECCC og modtager et tilskud til driften af værktøjerne og infrastrukturerne. Hvis et nationalt SOC modtager EU-støtte, skal det forpligte sig til at deltage i et grænseoverskridende SOC inden for to år.

Grænseoverskridende SOC'er skal bestå af et konsortium af mindst tre medlemsstater, repræsenteret ved de nationale SOC'er, som har forpligtet sig til at samarbejde om at koordinere cybersporings- og trusselsovervågningsaktiviteterne. Efter en indledende indkaldelse af interessetilkendegivelser kan ECCC udvælge et værtskonsortium, der deltager i et fælles indkøb af værktøjer og infrastrukturer sammen med ECCC og modtager tilskud til driften af værktøjerne og infrastrukturerne. Medlemmerne af værtskonsortiet indgår en skriftlig konsortieaftale, hvori de interne ordninger fastlægges. Kapitlet indeholder derefter en detaljeret beskrivelse af kravene til udveksling af oplysninger mellem deltagerne i et grænseoverskridende SOC og til udveksling af oplysninger mellem et grænseoverskridende SOC og andre grænseoverskridende SOC'er samt med relevante EU-enheder. Nationale SOC'er, der deltager i et grænseoverskridende SOC, udveksler relevante oplysninger om cybertrusler med hinanden, og detaljerne herfor, herunder forpligtelsen til at dele en betydelig mængde data og de tilhørende betingelserne, bør fastlægges i en konsortieaftale. Grænseoverskridende SOC'er sikrer en omfattende indbyrdes interoperabilitet. Grænseoverskridende SOC'er bør også indgå samarbejdsaftaler med andre grænseoverskridende SOC'er, hvori principperne for informationsudveksling beskrives. Hvis grænseoverskridende SOC'er indhenter oplysninger om en mulig eller igangværende væsentlig cybersikkerhedshændelse, forelægger de relevant information for EU-CyCLONe, CSIRT-netværket og Kommissionen med henblik på enhedernes respektive krisestyringsroller i henhold til direktiv (EU) 2022/2555. Kapitel II afsluttes med en præcisering af sikkerhedsbetingelserne for deltagelse i det europæiske cyberskjold.

Beredskabsmekanisme for cybersikkerhed (kapitel III)

Kapitel III omhandler beredskabsmekanismen for cybersikkerhed, der skal forbedre Unionens modstandsdygtighed over for større cybersikkerhedstrusler samt forberede og solidarisk afbøde de kortsigtede virkninger af væsentlige og omfattende cybersikkerhedshændelser eller -kriser. Foranstaltninger til gennemførelse af cyberberedskabsmekanismen støttes af midler fra programmet for et digitalt Europa. Mekanismen indeholder foranstaltninger til støtte for beredskab, herunder koordineret afprøvning af enheder, der opererer i meget kritiske sektorer, reaktion på og øjeblikkelig genopretning efter væsentlige eller omfattende cybersikkerhedshændelser eller afbødning af væsentlige cybertrusler og foranstaltninger til gensidig bistand.

Beredskabsforanstaltningerne under cyberberedskabsmekanismen omfatter koordineret beredskabstest af enheder, der opererer i meget kritiske sektorer. Kommissionen bør efter høring af ENISA og NIS-samarbejdsgruppen regelmæssigt udpege relevante sektorer eller delsektorer blandt de sektorer med høj kriminalitet, der er anført i bilag I til direktiv (EU) 2022/2555, hvor enhederne kan gennemgå en koordineret beredskabstest på EU-plan.

Med henblik på gennemførelsen af de foreslåede beredskabsforanstaltninger oprettes der ved denne forordning en EU-cybersikkerhedsreserve bestående af hændelsesberedskabstjenester, som varetages af betroede udbydere, der er udvalgt i overensstemmelse med de kriterier, der er fastsat i denne forordning. Brugerne af tjenesterne fra EU's cybersikkerhedsreserve omfatter medlemsstaternes cyberkrisestyringsmyndigheder og CSIRT'er samt Unionens institutioner, organer og agenturer. Kommissionen har det overordnede ansvar for gennemførelsen af EU's cybersikkerhedsreserve og kan helt eller delvist overdrage driften og administrationen af EU's cybersikkerhedsreserve til ENISA.

For at modtage støtte fra EU's cybersikkerhedsreserve bør brugerne træffe deres egne foranstaltninger for at afbøde virkningerne af den hændelse, der anmodes om støtte til. Anmodningerne om støtte fra EU's cybersikkerhedsreserve bør omfatte de nødvendige relevante oplysninger om hændelsen og om de foranstaltninger, som brugerne allerede har truffet. Kapitlet beskriver også gennemførelsesbestemmelserne, herunder vurdering af anmodninger til EU's cybersikkerhedsreserve.

Forordningen indeholder også bestemmelser om udbudsprincipper og udvælgelseskriterier vedrørende betroede udbydere under EU's cybersikkerhedsreserve.

Tredjelande kan anmode om støtte fra EU's cybersikkerhedsreserve, hvis de associeringsaftaler, der er indgået vedrørende deres deltagelse i programmet for et digitalt Europa, indeholder bestemmelser herom. I dette kapitel beskrives endvidere betingelser og nærmere bestemmelser for en sådan deltagelse.

Mekanisme til gennemgang af cybersikkerhedshændelser (kapitel IV)

Efter anmodning fra Kommissionen, EU-CyCLONe eller CSIRT-netværket gennemgår og vurderer ENISA trusler, sårbarheder og afbødende foranstaltninger ved specifikke, væsentlige eller omfattende cybersikkerhedshændelser. ENISA foretager gennemgang og vurdering og udarbejder en rapport herom til CSIRT-netværket, EU-CyCLONe og Kommissionen som støtte til udførelsen af deres opgaver. Når hændelsen vedrører et tredjeland, bør Kommissionen videresende rapporten til den højtstående repræsentant. Rapporten bør beskrive de indhøstede erfaringer og, hvor det er relevant, anbefalinger til forbedring af Unionens cyberposition.

Afsluttende bestemmelser (kapitel V)

Kapitel V indeholder ændringer af forordningen om programmet for et digitalt Europa og en forpligtelse for Kommissionen til at udarbejde regelmæssige rapporter til Europa-Parlamentet og Rådet til evaluering og revision af forordningen. Kommissionen har beføjelse til at vedtage

gennemførelsesretsakter efter undersøgelsesproceduren i artikel 21 med det formål at: præcisere betingelserne for interoperabilitet mellem grænseoverskridende SOC'er fastlægge de proceduremæssige ordninger for udveksling af oplysninger vedrørende en mulig eller igangværende væsentlig cybersikkerhedshændelse mellem grænseoverskridende SOC'er og EU-enheder fastsætte tekniske krav for at sikre et højt niveau af data og fysisk sikkerhed i infrastrukturen og beskytte Unionens sikkerhedsinteresser, når der udveksles oplysninger med enheder, der ikke er offentlige organer i medlemsstaterne præcisere, hvilke typer og hvor mange beredskabstjenester der er nødvendige i EU's cybersikkerhedsreserve og yderligere præcisere de detaljerede ordninger for tildeling af støttetjenesterne under EU's cybersikkerhedsreserve.

2023/0109 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 173, stk. 3, og artikel 322, stk. 1, litra a),

under henvisning til forslag fra Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Revisionsretten[1],

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg[2],

under henvisning til udtalelse fra Regionsudvalget[3],

efter den almindelige lovgivningsprocedure, og

ud fra følgende betragtninger:

(1) Anvendelsen og afhængigheden af informations- og kommunikationsteknologier er blevet grundlæggende aspekter i alle sektorer af økonomien, da offentlige forvaltninger, virksomheder og borgere mere end nogensinde før er indbyrdes forbundne og afhængige af hinanden.

(2) Cybersikkerhedshændelser er tiltagende både i omfang, hyppighed og virkning, herunder angreb mod forsyningskæden i form af cyberspionage, ransomware eller forstyrrelser. De udgør en alvorlig trussel mod netværks- og informationssystemernes funktion. Der ses et trusselsbillede i hastig udvikling, og truslen om mulige omfattende hændelser, der kan forårsage betydelige forstyrrelser og skader på kritisk infrastruktur, kræver et øget beredskab på alle niveauer i EU's cybersikkerhedsøkosystem. Truslen rækker langt videre end Ruslands militære aggression mod Ukraine og er formentlig blivende, når man tager de mange forskellige statslige, kriminelle og hacktivistiske aktører i betragtning, der er en del af de aktuelle geopolitiske spændinger. Sådanne hændelser kan hindre leveringen af offentlige tjenester og udøvelsen af økonomiske aktiviteter, herunder i kritiske eller meget kritiske sektorer, medføre betydelige finansielle tab, underminere brugernes tillid, forårsage betydelig skade på Unionens økonomi og muligvis få sundhedsmæssige eller livstruende konsekvenser. Desuden er cybersikkerhedshændelser uforudsigelige, fordi de ofte opstår og udvikler sig på meget kort tid, fordi de ikke er begrænsede til et specifikt geografisk område, og fordi de forekommer samtidig eller spredes hurtigt til mange lande.

---

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

(3) Det er nødvendigt at styrke industriens og servicesektorernes konkurrenceevne i Unionen på tværs af hele den digitaliserede økonomi og støtte den digitale omstilling i sektorerne ved at styrke cybersikkerhedsniveauet på det digitale indre marked. Som anbefalet i tre forskellige forslag fra konferencen om Europas fremtid[4] er der behov for at øge modstandsdygtigheden hos borgere, virksomheder og enheder, der driver kritisk infrastruktur, over for de tiltagende cybersikkerhedstrusler, som kan have ødelæggende samfundsmæssige og økonomiske konsekvenser. Der er derfor behov for investeringer i infrastrukturer og tjenester, der muliggør hurtigere opdagelse af og reaktion på cybersikkerhedstrusler og -hændelser, og medlemsstaterne har brug for hjælp til bedre at kunne forberede sig og reagere på væsentlige og omfattende cybersikkerhedshændelser. Unionen bør også øge sin kapacitet på disse områder, navnlig med hensyn til indsamling og analyse af data om cybersikkerhedstrusler og -hændelser.

(4) Unionen har allerede truffet en række foranstaltninger for at mindske sårbarheder og øge kritiske infrastrukturers og enheders modstandsdygtighed over for cybersikkerhedsrisici, navnlig Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[5], Kommissionens henstilling (EU) 2017/1584[6], Europa-Parlamentets og Rådets direktiv 2013/40/EU[7] og Europa-Parlamentets og Rådets forordning (EU) 2019/881[8]. Desuden opfordres medlemsstaterne i Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed til at træffe hurtige og effektive foranstaltninger og til at samarbejde loyalt, effektivt, i solidaritet og på en koordineret måde med hinanden, Kommissionen og andre relevante offentlige myndigheder samt de berørte enheder for at øge modstandsdygtigheden i den kritiske infrastruktur, der anvendes til at levere væsentlige tjenester på det indre marked.

(5) De voksende cybersikkerhedsrisici og det generelt komplekse trusselsbillede, hvor der er en klar risiko for, at cyberhændelser spreder sig fra én medlemsstat til andre og fra et tredjeland til Unionen, kræver styrket solidaritet på EU-niveau for bedre at kunne opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser. Medlemsstaterne har også opfordret Kommissionen til at fremsætte et forslag om en ny beredskabsfond for cybersikkerhed i Rådets konklusioner om EU's cyberposition[9].

(6) I den fælles meddelelse om EU's politik for cyberforsvar[10], der blev vedtaget den 10. november 2022, blev EU's cybersolidaritetsinitiativ beskrevet med følgende

---

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

5 Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (EUT L 333 af 27.12.2022).

6 Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (EUT L 239 af 19.9.2017, s. 36).

7 Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (EUT L 218 af 14.8.2013, s. 8).

8 Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15).

9 Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition, som blev godkendt af Rådet på samlingen den 23. maj 2022 (9364/22)

10 Fælles meddelelse til Europa-Parlamentet og Rådet — EU's politik for cyberforsvar JOIN/2022/49 final

målsætninger: styrke EU's fælles situationskendskab og kapacitet til at opdage og reagere på hændelser ved at fremme etableringen af en EU-infrastruktur for sikkerhedsoperationscentre ("SOC'er"), støtte en gradvis opbygning af en cybersikkerhedsreserve på EU-plan med brug af tjenester fra betroede private udbydere og teste kritiske enheder for potentielle sårbarheder baseret på EU's risikovurderinger.

(7) Det er nødvendigt at styrke situationskendskabet og kapaciteten til at opdage cybertrusler og -hændelser i hele Unionen og styrke solidariteten ved at øge medlemsstaternes og Unionens beredskab og kapacitet til at reagere på væsentlige og omfattende cybersikkerhedshændelser. Derfor bør en paneuropæisk infrastruktur af sikkerhedsoperationscentre (SOC'er) etableres (det europæiske cyberskjold) for at opbygge og styrke det fælles situationskendskab og den fælles kapacitet til at afsløre hændelser. Der bør etableres en beredskabsmekaniske for cybersikkerhed for dermed at styrke medlemsstaternes evne til at forberede sig og reagere på væsentlige eller omfattende cybersikkerhedshændelser og sikre en omgående efterfølgende genopretning. Der bør etableres en mekanisme til gennemgang af cybersikkerhedshændelser med henblik på at gennemgå og vurdere specifikke væsentlige eller omfattende hændelser. Disse foranstaltninger berører ikke artikel 107 og 108 i traktaten om Den Europæiske Unions funktionsmåde (TEUF).

(8) For at opfylde disse målsætninger er det også nødvendigt at ændre Europa-Parlamentets og Rådets forordning (EU) 2021/694[11] på visse områder. Denne forordning bør navnlig ændre forordning (EU) 2021/694 for så vidt angår tilføjelse af nye operationelle mål for det europæiske cyberskjold og cyberberedskabsmekanismen under specifikt mål nr. 3 i programmet for et digitalt Europa, hvis formål er at sikre det digitale indre markeds modstandsdygtighed, integritet og troværdighed, styrke kapaciteten til at overvåge cyberangreb og -trusler og reagere på dem og styrke det grænseoverskridende samarbejde om cybersikkerhed. De særlige betingelser, hvorunder der kan ydes finansiel støtte til disse aktioner, og de forvaltnings- og koordineringsmekanismer, der er nødvendige for at nå de fastsatte målsætninger, bør fastlægges. Andre ændringer af forordning (EU) 2021/694 bør omfatte beskrivelse af foreslåede foranstaltninger under de nye operationelle målsætninger og målbare indikatorer til overvågning af gennemførelsen heraf.

(9) Finansieringen af foranstaltninger under denne forordning bør fastsættes i forordning (EU) 2021/694, som fortsat bør være den relevante basisretsakt for disse foranstaltninger, der hører under specifik målsætning nr. 3 i programmet for et digitalt Europa. Der vil i de relevante arbejdsprogrammer blive fastsat særlige betingelser for deltagelse i de enkelte aktioner i overensstemmelse med den gældende bestemmelse i forordning (EU) 2021/694.

(10) Horisontale finansielle regler, der er vedtaget af Europa-Parlamentet og Rådet på grundlag af artikel 322 i TEUF, finder anvendelse på denne forordning. Disse regler er fastsat i finansforordningen og fastlægger navnlig proceduren for opstilling og gennemførelse af Unionens budget og indeholder bestemmelser om kontrol af de finansielle aktørers ansvar. Regler vedtaget på grundlag af artikel 322 i TEUF omfatter også en generel ordning vedrørende konditionalitet med henblik på beskyttelse af

[11] Europa-Parlamentets og Rådets forordning (EU) 2021/694 af 29. april 2021 om programmet for et digitalt Europa og om ophævelse af afgørelse (EU) 2015/2240 (EUT L 166 af 11.5.2021, s. 1).

Unionens budget som fastsat i Europa-Parlamentets og Rådets forordning (EU, Euratom) 2020/2092.

(11) Med henblik på forsvarlig økonomisk forvaltning bør særlige regler fastsættes for overførsel af uudnyttede forpligtelses- og betalingsbevillinger. Under overholdelse af princippet om, at Unionens budget fastsættes årligt, bør denne forordning på grund af det uforudsigelige, ekstraordinære og specifikke cybersikkerhedsbillede give mulighed for at overføre uudnyttede midler ud over dem, der er fastsat i finansforordningen, for derved at maksimere beredskabsmekanismens kapacitet til at støtte medlemsstaterne i effektivt at imødegå cybertrusler.

(12) For mere effektivt at forebygge, vurdere og reagere på cybertrusler og -hændelser er det nødvendigt at opbygge en mere omfattende viden om truslerne mod kritiske aktiver og infrastrukturer på Unionens område, herunder geografiske fordeling, sammenhæng og mulige virkninger i tilfælde af cyberangreb, der påvirker disse infrastrukturer. Der bør etableres en omfattende infrastruktur af SOC'er i EU ("det europæiske cyberskjold") bestående af flere interoperable grænseoverskridende platforme, som hver samler en række nationale SOC'er. Infrastrukturen bør tjene nationale og europæiske cybersikkerhedsinteresser og -behov. Den nyeste teknologi til avancerede dataindsamlings- og analyseværktøjer bør udnyttes, cyberdetektions- og -forvaltningskapaciteten bør udnyttes, og et situationskendskab i realtid bør opbygges. Infrastrukturen skal forbedre afsløring af cybersikkerhedstrusler og -hændelser og dermed supplere og støtte Unionens enheder og netværk med ansvar for krisestyring i Unionen, navnlig EU-netværket af forbindelsesorganisationer for cyberkriser ("EU-CyCLONe") som defineret i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555[12].

(13) De enkelte medlemsstater bør udpege et offentligt organ på nationalt plan, der har til opgave at koordinere aktiviteter til afsløring af cybertrusler i den pågældende medlemsstat. Disse nationale sikkerhedsoperationscentre (SOC'er) bør fungere som reference- og indgangspunkt på nationalt plan for deltagelse i det europæiske cyberskjold, og de bør sikre, at oplysninger om cybertrusler fra offentlige og private enheder deles og indsamles på nationalt plan på en effektiv og koordineret måde.

(14) Som en del af det europæiske cyberskjold bør der oprettes en række grænseoverskridende cybersikkerhedsoperationscentre ("grænseoverskridende SOC'er"). De skal samle de nationale SOC'er fra mindst tre medlemsstater, så fordelene ved grænseoverskridende trusselsdetektion og informationsdeling og -styring udnyttes fuldt ud. Den overordnede målsætning for de grænseoverskridende SOC'er bør være at styrke kapaciteten til at analysere, forebygge og opdage cybersikkerhedstrusler og støtte frembringelsen af efterretninger af høj kvalitet om cybersikkerhedstrusler, navnlig gennem deling af data fra forskellige offentlige eller private kilder samt gennem deling og fælles anvendelse af avancerede værktøjer og fælles udvikling af detektions-, analyse- og forebyggelseskapaciteter i et sikkert miljø. De bør stille ny supplerende kapacitet til rådighed, der bygger på og supplerer eksisterende SOC'er og IT-beredskabshold ("CSIRT'er") og andre relevante aktører.

[12] Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333 af 27.12.2022, s. 80).

(15) På nationalt plan sikres overvågning, opdagelse og analyse af cybertrusler typisk af offentlige og private enheders SOC'er i kombination med CSIRT'er. Desuden udveksler CSIRT'er oplysninger inden for rammerne af CSIRT-netværket i overensstemmelse med direktiv (EU) 2022/2555. De grænseoverskridende SOC'er skal udgøre en ny kapacitet, der supplerer CSIRT-netværket, ved at samle og dele data om cybersikkerhedstrusler fra offentlige og private enheder, værdiforøge data gennem ekspertanalyser, fælles etablerede infrastrukturer og de nyeste værktøjer, og derved bidrager de til udviklingen af Unionens kapaciteter og teknologiske suverænitet.

(16) De grænseoverskridende SOC'er bør fungere som et centralt knudepunkt, hvor relevante data og efterretninger om cybertrusler generelt sammenstilles, og de skal muliggøre udveksling af trusselsoplysninger blandt en lang række forskellige aktører (f.eks. IT-beredskabsenheder (CERT'er), CSIRT'er, informationsdelings- og analysecentre (ISAC'er) og operatører af kritisk infrastruktur). De oplysninger, der udveksles mellem deltagerne i en grænseoverskridende SOC, kan omfatte data fra netværk og sensorer, trusselsefterretningsfeeds, kompromitteringsindikatorer og kontekstualiserede oplysninger om hændelser, trusler og sårbarheder. Desuden bør grænseoverskridende SOC'er også indgå samarbejdsaftaler med andre grænseoverskridende SOC'er.

(17) At de relevante myndigheder opbygger et fælles situationskendskab er en nødvendig forudsætning for EU-dækkende beredskab og koordinering vedrørende væsentlige og omfattende cybersikkerhedshændelser. Ved direktiv (EU) 2022/2555 oprettes EU–CyCLONe for at støtte den koordinerede forvaltning af omfattende cybersikkerhedshændelser og -kriser på operationelt plan og for at sikre regelmæssig udveksling af relevante oplysninger mellem medlemsstaterne og EU's institutioner, organer, kontorer og agenturer. Henstilling (EU) 2017/1584 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser omhandler alle de relevante aktørers rolle. I direktiv (EU) 2022/2555 påpeges også Kommissionens ansvar i forbindelse med EU-civilbeskyttelsesmekanismen, der blev oprettet ved Europa-Parlamentets og Rådets afgørelse 1313/2013/EU, samt for at udarbejde analytiske rapporter om ordningerne under den integrerede mekanisme for politisk kriserespons ("IPCR") i henhold til gennemførelsesafgørelse (EU) 2018/1993. I situationer, hvor grænseoverskridende SOC'er indhenter oplysninger vedrørende en potentiel eller igangværende væsentlig cybersikkerhedshændelse, bør de derfor give relevante oplysninger til EU-CyCLONe, CSIRT-netværket og Kommissionen. Afhængigt af situationen kan de oplysninger, der skal udveksles, især omfatte tekniske oplysninger, oplysninger om angriberens eller den mulige angriberes kendetegn og motiver og ikke-tekniske oplysninger på overordnet niveau om en potentiel eller igangværende omfattende cybersikkerhedshændelse. I den sammenhæng bør der tages behørigt hensyn til, hvilke oplysninger der er nødvendige, og til den eventuelt følsomme karakter af de udvekslede oplysninger.

(18) Enheder, der deltager i det europæiske cyberskjold, bør sikre en høj grad af indbyrdes interoperabilitet, herunder, hvor det er relevant, for så vidt angår dataformater, taksonomi, datahåndterings- og dataanalyseværktøjer og sikre kommunikationskanaler, et minimumsniveau af sikkerhed i applikationslaget, oversigtstavle over situationskendskab samt indikatorer. Ved vedtagelse af en fælles taksonomi og udvikling af en skabelon til situationsrapporter til beskrivelse af den tekniske årsag til og virkningerne af cybersikkerhedshændelser bør der tages hensyn til det igangværende arbejde med underretning om hændelser i forbindelse med gennemførelsen af direktiv (EU) 2022/2555.

(19) For at muliggøre udveksling af data om cybersikkerhedstrusler fra forskellige kilder i stor skala i et pålideligt miljø bør enheder, der deltager i det europæiske cyberskjold, udstyres med avancerede og særligt sikre værktøjer, udstyr og infrastrukturer. Dermed bør det blive muligt at forbedre den kollektive detektionskapacitet og tilvejebringe rettidige advarsler til myndigheder og relevante enheder, navnlig ved at anvende de nyeste teknologier inden for kunstig intelligens og dataanalyse.

(20) Gennem indsamling, deling og udveksling af data bør det europæiske cyberskjold kunne styrke Unionens teknologiske suverænitet. Sammenlægning af udvalgte data af høj kvalitet bør også kunne bidrage til udviklingen af avancerede teknologier inden for kunstig intelligens og dataanalyse. Processen bør fremmes ved at forbinde det europæiske cyberskjold med den paneuropæiske infrastruktur til højtydende databehandling, der er oprettet ved Rådets forordning (EU) 2021/1173[13].

(21) Selv om det europæiske cyberskjold er et civilt projekt, kan cyberforsvarssektoren udnytte et større civilt situationskendskab og en stærkere civil detektionskapacitet, der er udviklet med henblik på beskyttelse af kritisk infrastruktur. Grænseoverskridende SOC'er bør med støtte fra Kommissionen og Det Europæiske Kompetencecenter for Cybersikkerhed ("ECCC") og i samarbejde med Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik ("den højtstående repræsentant") gradvist udvikle særlige protokoller og standarder for at muliggøre samarbejde med cyberforsvarssektoren, herunder kontrol sikkerhedsforhold. Udviklingen af det europæiske cyberskjold bør ledsages af overvejelser om at muliggøre et fremtidigt samarbejde med de netværk og platforme, der har ansvar for informationsudveksling i cyberforsvarssektoren, i tæt samarbejde med den højtstående repræsentant.

(22) Udveksling af oplysninger mellem deltagerne i det europæiske cyberskjold bør ske i overensstemmelse med eksisterende retlige krav og navnlig Unionens og den nationale databeskyttelseslovgivning samt Unionens konkurrenceregler vedrørende udveksling af oplysninger. Modtageren af oplysningerne bør, i det omfang behandlingen af personoplysninger er nødvendig, gennemføre tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og frihedsrettigheder og tilintetgøre data, så snart de ikke længere er nødvendige til det angivne formål, og underrette det organ, der stiller oplysningerne til rådighed, om, at oplysningerne er blevet destrueret.

(23) Med forbehold af artikel 346 i TEUF bør udvekslingen af oplysninger, der er fortrolige i henhold til EU-regler eller nationale regler, begrænses til det omfang, der er relevant og står i rimeligt forhold til formålet med denne udveksling. Udvekslingen af oplysninger skal bevare de pågældende oplysningers fortrolighed og beskytte de berørte enheders sikkerhed og kommercielle interesser med fuld fortrolighed vedrørende handels- og forretningshemmeligheder.

(24) I betragtning af de stigende risici og antallet af cyberhændelser, der påvirker medlemsstaterne, er det nødvendigt at oprette et krisestøtteinstrument for at forbedre Unionens modstandsdygtighed over for væsentlige og omfattende cybersikkerhedshændelser og supplere medlemsstaternes foranstaltninger gennem finansiel nødhjælp til beredskab, indsats og øjeblikkelig genopretning af væsentlige tjenester. Dette instrument bør muliggøre hurtig udsendelse af bistand under nærmere fastsatte omstændigheder og på klare betingelser og give mulighed for nøje

[13] Rådets forordning (EU) 2021/1173 af 13. juli 2021 om oprettelse af et fællesforetagende for europæisk højtydende databehandling og om ophævelse af forordning (EU) 2018/1488 (EUT L 256 af 19.7.2021, s. 3).

overvågning og evaluering af, hvordan ressourcerne er blevet anvendt. Mens medlemsstaterne har det primære ansvar for forebyggelse, beredskab og indsats i tilfælde af cybersikkerhedshændelser og -kriser, skal cyberberedskabsmekanismen øge solidariteten mellem medlemsstaterne i overensstemmelse med artikel 3, stk. 3, i traktaten om Den Europæiske Union (TEU).

(25) Cyberberedskabsmekanismen bør yde støtte til medlemsstaterne som supplement til deres egne foranstaltninger og ressourcer og andre eksisterende støttemuligheder i tilfælde af reaktion på og øjeblikkelig genopretning efter væsentlige og omfattende cybersikkerhedshændelser såsom de tjenester, der leveres af Den Europæiske Unions Agentur for Cybersikkerhed ("ENISA") i overensstemmelse med dets mandat, den koordinerede indsats og bistanden fra CSIRT-netværket, støtten til afbødende foranstaltninger fra EU-CyCLONe samt gensidig bistand mellem medlemsstaterne, herunder i medfør af artikel 42, stk. 7, i TEU, PESCO's cyberberedskabshold[14] og hybride beredskabshold. Cyberberedskabsmekanismen bør indgå i løsning af behovet for at sikre, at der er specialiserede ressourcer til rådighed til støtte for beredskab og reaktion på cybersikkerhedshændelser i hele Unionen og i tredjelande.

(26) Dette instrument berører ikke procedurer og rammer for koordinering af kriserespons på EU-plan, navnlig EU-civilbeskyttelsesmekanismen[15], IPCR[16],, og direktiv (EU) 2022/2555. Instrumentet kan bidrage til eller supplere foranstaltninger, der gennemføres inden for rammerne af artikel 42, stk. 7, i TEU eller i situationer som defineret i artikel 222 i TEUF. Anvendelse af dette instrument bør også koordineres med gennemførelsen af foranstaltninger vedrørende cyberdiplomatiske værktøjskasser, hvor det er relevant.

(27) Den bistand, der ydes i henhold til denne forordning, bør støtte og supplere de foranstaltninger, som medlemsstaterne træffer på nationalt plan. Med henblik herpå bør der sikres et tæt samarbejde og samråd mellem Kommissionen og berørte medlemsstater. Når en medlemsstat anmoder om støtte i henhold til cyberberedskabsmekanismen, bør den fremlægge relevante oplysninger, der begrunder behovet for støtte.

(28) I henhold til direktiv (EU) 2022/2555 skal medlemsstaterne udpege eller oprette en eller flere cyberkrisestyringsmyndigheder og sikre, at de har tilstrækkelige ressourcer til at udføre deres opgaver effektivt og virkningsfuldt. I henhold til direktivet skal medlemsstaterne endvidere identificere kapaciteter, aktiver og procedurer, der kan indsættes i tilfælde af en krise, og vedtage en national omfattende beredskabsplan for cybersikkerhedshændelser og -kriser, hvor målsætningerne og ordningerne vedrørende håndtering af væsentlige cybersikkerhedshændelser og -kriser er fastsat. Medlemsstaterne skal også oprette et eller flere CSIRT'er, der har ansvar for håndtering af hændelser efter en veldefineret proces, der som minimum dækker de sektorer, delsektorer og typer af enheder, der er omfattet af nævnte direktivs anvendelsesområde, og sikre, at de har tilstrækkelige ressourcer til effektivt at udføre deres opgaver. Denne forordning berører ikke Kommissionens rolle med hensyn til at

---

14 RÅDETS AFGØRELSE (FUSP) 2017/2315 af 11. december 2017 om etablering af et permanent struktureret samarbejde (PESCO) og fastlæggelse af listen over deltagende medlemsstater.

15 Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU af 17. december 2013 om en EU-civilbeskyttelsesmekanisme (EUT L 347 af 20.12.2013, s. 924).

16 Integrerede ordninger for politisk kriserespons (IPCR) og i overensstemmelse med Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser.

sikre, at medlemsstaterne overholder forpligtelserne i direktiv (EU) 2022/2555. Cyberberedskabsmekanismen bør yde bistand til foranstaltninger, der har til formål at styrke beredskabet og indsatsen i forbindelse med hændelser for at afbøde virkningerne af væsentlige og omfattende cybersikkerhedshændelser, støtte øjeblikkelig genopretning og/eller genoprette væsentlige tjenesters funktion.

(29) For at fremme en konsekvent tilgang og styrke sikkerheden i hele Unionen og dens indre marked bør der som led i beredskabsforanstaltningerne ydes støtte til en strengt koordineret afprøvning og vurdering af cybersikkerheden i enheder, der opererer i de meget kritiske sektorer, der er udpeget i direktiv (EU) 2022/2555. Med henblik herpå bør Kommissionen med støtte fra ENISA og i samarbejde med NIS-samarbejdsgruppen, der er nedsat ved direktiv (EU) 2022/2555, regelmæssigt udpege relevante sektorer eller delsektorer, som bør være berettigede til at modtage finansiel støtte til koordineret testning på EU-plan. Sektorerne eller delsektorerne bør udvælges fra bilag I til direktiv (EU) 2022/2555 ("sektorer med høj kriminalitet"). De koordinerede test bør baseres på fælles risikoscenarier og -metoder. Udvælgelsen af sektorer og udarbejdelsen af risikoscenarier bør tage højde for relevante risikovurderinger og risikoscenarier på EU-plan, herunder behovet for at undgå overlapning, såsom den risikoevaluering og de risikoscenarier, der anbefales i Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition, der skal foretages af Kommissionen, den højtstående repræsentant og NIS-samarbejdsgruppen i samarbejde med relevante civile og militære organer og agenturer og etablerede netværk, herunder EU-CyCLONe, samt den risikovurdering af kommunikationsnet og -infrastrukturer, der er anmodet om i den fælles ministerielle Nevers-indkaldelse, og som gennemføres af NIS-samarbejdsgruppen med støtte fra Kommissionen og ENISA og i samarbejde med Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC), de koordinerede risikovurderinger, der skal foretages i henhold til artikel 22 i direktiv (EU) 2022/2555, og afprøvning af digital operationel modstandsdygtighed, jf. Europa-Parlamentets og Rådets forordning (EU) 2022/2554[17]. Ved udvælgelse af sektorer bør der også tages hensyn til Rådets henstilling om en EU-dækkende koordineret tilgang til styrkelse af kritisk infrastrukturs modstandsdygtighed.

(30) Derudover bør cyberberedskabsmekanismen yde støtte til andre beredskabsforanstaltninger og støtte beredskabet i andre sektorer, der ikke er omfattet af den koordinerede afprøvning af enheder, der opererer i meget kritiske sektorer. Disse foranstaltninger kan omfatte forskellige typer af nationale beredskabsaktiviteter.

(31) Cyberberedskabsmekanismen bør yde støtte til indsatsen i forbindelse med hændelser for at afbøde virkningerne af væsentlige og omfattende cybersikkerhedshændelser for at støtte øjeblikkelig genopretning og/eller genoprette væsentlige tjenesters funktion. Den bør, hvor det er relevant, supplere EU-civilbeskyttelsesmekanismen for at sikre en samlet tilgang til indsatsen over for følgerne af cyberhændelser for borgerne.

(32) Cyberberedskabsmekanismen bør støtte bistand fra andre medlemsstater til en medlemsstat, der er berørt af en væsentlig eller omfattende cybersikkerhedshændelse, herunder af CSIRT-netværket, jf. artikel 15 i direktiv (EU) 2022/2555. Medlemsstater, der yder bistand, bør have mulighed for at indgive anmodning om dækning af

[17] Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011

omkostninger i forbindelse med udsendelse af eksperthold inden for rammerne af gensidig bistand. De støtteberettigede omkostninger kan omfatte udgifter til rejser, indkvartering og daglige udgifter for cybersikkerhedseksperter.

(33) Der bør gradvist oprettes en cybersikkerhedsreserve på EU-plan bestående af tjenester fra private udbydere af administrerede sikkerhedstjenester til støtte for indsatsen og foranstaltninger til omgående genopretning i tilfælde af væsentlige eller omfattende cybersikkerhedshændelser. EU's cybersikkerhedsreserve bør sikre, at tjenesterne er tilgængelige og parate. Tjenesterne fra EU's cybersikkerhedsreserve bør tjene til at støtte de nationale myndigheder i at yde bistand til berørte enheder, der opererer i kritiske eller meget kritiske sektorer, som supplement til deres egne foranstaltninger på nationalt plan. Når medlemsstaterne anmoder om støtte fra EU's cybersikkerhedsreserve, bør de specificere hvilken støtte, der ydes til den berørte enhed på nationalt plan, og som bør tages i betragtning ved vurdering af medlemsstatens anmodning. Tjenesterne fra EU's cybersikkerhedsreserve kan også tjene til at støtte Unionens institutioner, organer og agenturer på lignende betingelser.

(34) Med henblik på at udvælge private tjenesteudbydere, der skal levere tjenester i forbindelse med EU's cybersikkerhedsreserve, er det nødvendigt at fastsætte et sæt minimumskriterier, der bør indgå i udbuddet til udvælgelse af udbyderne, for at sikre, at behovene opfyldes hos medlemsstaternes myndigheder og enheder, der opererer i kritiske eller meget kritiske sektorer.

(35) For at støtte etableringen af EU's cybersikkerhedsreserve kan Kommissionen overveje at anmode ENISA om at udarbejde et forslag til en certificeringsordning for kandidater i henhold til forordning (EU) 2019/881 for administrerede sikkerhedstjenester på de områder, der er omfattet af cyberberedskabsmekanismen.

(36) For at støtte målsætningerne i denne forordning om at fremme fælles situationskendskab, styrke Unionens modstandsdygtighed og muliggøre en effektiv reaktion på væsentlige og omfattende cybersikkerhedshændelser bør EU-CyCLONe, CSIRT-netværket eller Kommissionen kunne anmode ENISA om at gennemgå og vurdere trusler, sårbarheder og afbødende foranstaltninger i forbindelse med en specifik væsentlig eller omfattende cybersikkerhedshændelse. Efter gennemførelsen af en gennemgang og vurdering af en hændelse bør ENISA udarbejde en rapport om hændelsen i samarbejde med relevante interessenter, herunder repræsentanter fra den private sektor, medlemsstaterne, Kommissionen og andre relevante EU-institutioner, -organer og -agenturer. For så vidt angår den private sektor etablerer ENISA kanaler til udveksling af oplysninger med specialiserede udbydere, herunder udbydere af administrerede sikkerhedsløsninger og leverandører, med henblik på at bidrage til ENISA's opgave med at opnå et højt fælles cybersikkerhedsniveau i hele Unionen. På grundlag af samarbejdet med interessenter, herunder den private sektor, bør rapporten om gennemgang af specifikke hændelser have til formål at vurdere årsagerne til, virkningerne af og modvirkningen af en hændelse, efter at den er indtruffet. Der bør lægges særlig vægt på oplysninger og erfaringer, der indmeldes af udbydere af administrerede sikkerhedstjenester, som opfylder betingelserne om højeste faglige integritet, upartiskhed og den nødvendige tekniske ekspertise som krævet i denne forordning. Rapporten bør leveres og indgå i arbejdet i EU-CyCLONe, CSIRT-netværket og Kommissionen. Når hændelsen vedrører et tredjeland, videresender Kommissionen også rapporten til den højtstående repræsentant.

(37) I betragtning af cybersikkerhedsangrebenes uforudsigelige karakter og det forhold, at de ofte ikke kun berører et specifikt geografisk område og medrører høj risiko for

afsmittende virkninger, bidrager styrkelsen af nabolandenes modstandsdygtighed og deres evne til at reagere effektivt på væsentlige og omfattende cybersikkerhedshændelser til beskyttelsen af Unionen som helhed. Derfor kan tredjelande, der er associeret med programmet for et digitalt Europa, modtage støtte fra EU's cybersikkerhedsreserve, hvis dette er fastsat i den respektive associeringsaftale til programmet for et digitalt Europa. Finansieringen til associerede tredjelande bør støttes af Unionen inden for rammerne af relevante partnerskaber og finansieringsinstrumenter for disse lande. Støtten bør omfatte tjenester inden for reaktion på og omgående genopretning efter væsentlige eller omfattende cybersikkerhedshændelser. De betingelser, der er fastsat for EU's cybersikkerhedsreserve og betroede udbydere i denne forordning, bør finde anvendelse, når der ydes støtte til tredjelande, der er associeret med programmet for et digitalt Europa.

(38) For at sikre ensartede betingelser for gennemførelse af denne forordning bør Kommissionen tillægges gennemførelsesbeføjelser til at fastlægge betingelserne for interoperabilitet mellem grænseoverskridende SOC'er fastlægge de proceduremæssige ordninger for udveksling af oplysninger vedrørende en mulig eller igangværende væsentlig cybersikkerhedshændelse mellem grænseoverskridende SOC'er og EU-enheder fastsætte de tekniske krav med henblik på at garantere sikkerheden i forbindelse med det europæiske cyberskjold præcisere, hvilke typer og hvor mange beredskabstjenester der er nødvendige i EU's cybersikkerhedsreserve og yderligere præcisere de detaljerede ordninger for tildeling af støttetjenesterne under EU's cybersikkerhedsreserve. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011.

(39) Målsætningen for denne forordning kan bedre opfyldes på EU-plan end af medlemsstaterne hver især. Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet og proportionalitetsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. Denne forordning går ikke ud over, hvad der er nødvendigt for at opfylde denne målsætning —

VEDTAGET DENNE FORORDNING:

Kapitel I

GENERELLE FORMÅL, GENSTAND OG DEFINITIONER

Artikel 1

Genstand og formål

1. Ved denne forordning fastsættes foranstaltninger til styrkelse af Unionens kapacitet til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser, navnlig gennem følgende tiltag:

a) etablering af en paneuropæisk infrastruktur for sikkerhedsoperationscentre ("et europæisk cyberskjold") for at opbygge og styrke det fælles situationskendskab og den fælles kapacitet til at afsløre hændelser

b) oprettelse af en beredskabsmekanisme for cybersikkerhed som støtte til medlemsstaterne til at forberede sig og reagere på samt sikre omgående genopretning efter væsentlige eller omfattende cybersikkerhedshændelser

c) oprettelse af en europæisk mekanisme til gennemgang af cybersikkerhedshændelser med henblik på at gennemgå og vurdere væsentlige eller omfattende hændelser.

2. Formålet med denne forordning er at styrke solidariteten på EU-plan gennem følgende specifikke mål:

a) at styrke Unionens fælles situationskendskab og kapacitet til at opdage cybertrusler og -hændelser og dermed gøre det muligt at styrke industriens og servicesektorernes konkurrenceposition i Unionen i hele den digitale økonomi og bidrage til Unionens teknologiske suverænitet på cybersikkerhedsområdet

b) at styrke beredskabet hos enheder, der opererer i kritiske og meget kritiske sektorer i hele Unionen og styrke solidariteten ved at udvikle fælles indsatskapaciteter over for væsentlige eller omfattende cybersikkerhedshændelser, herunder ved at stille indsatsstøtte fra Unionen ved cybersikkerhedshændelser til rådighed for tredjelande, der er tilknyttet programmet for et digitalt Europa

c) at øge Unionens modstandsdygtighed og bidrage til en effektiv reaktion ved at gennemgå og vurdere væsentlige eller omfattende hændelser, herunder ved at trække på indhøstede erfaringer og henstillinger, hvor det er relevant.

3. Denne forordning berører ikke medlemsstaternes primære ansvar for national sikkerhed, offentlig sikkerhed samt for forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger.

Artikel 2

Definitioner

I denne forordning forstås ved:

1) "**grænseoverskridende sikkerhedsoperationscenter**" ("**grænseoverskridende SOC**"): en platform for flere lande, der i en koordineret netværksstruktur samler nationale SOC'er fra mindst tre medlemsstater, der fungerer som værtskonsortium, og som er udformet med henblik på at forebygge cybertrusler og -hændelser og støtte tilvejebringelse af efterretninger af høj kvalitet, navnlig gennem udveksling af data fra forskellige offentlige og private kilder samt gennem deling af avancerede værktøjer og fælles udvikling af cyberkapacitet til opdagelse, analyse, forebyggelse af hændelser og beskyttelse i et sikkert miljø

2) "**offentligt organ**": et offentligretligt organ som defineret i artikel 2, stk. 1, nr. 4), i Europa-Parlamentets og Rådets direktiv 2014/24/EU[18]

3) "**værtskonsortium**": et konsortium bestående af deltagende stater repræsenteret ved nationale SOC'er, der har indvilliget i at etablere og bidrage til erhvervelse af værktøjer og infrastruktur til og drift af et grænseoverskridende SOC

4) "**enhed**": en enhed som defineret i artikel 6, nr. 38), i direktiv (EU) 2022/2555

5) "**enheder, der opererer i kritiske eller meget kritiske sektorer**": den type enheder, der er opført i bilag I og II til direktiv (EU) 2022/2555

6) "**cybertrussel**": en cybertrussel som defineret i artikel 2, nr. 8), i forordning (EU) 2019/881

7) "**væsentlig cybersikkerhedshændelse**": en cybersikkerhedshændelse, der opfylder kriterierne i artikel 23, stk. 3, i direktiv (EU) 2022/2555

8) "**omfattende cybersikkerhedshændelse**": en hændelse som defineret i artikel 6, nr. 7), i direktiv (EU) 2022/2555

9) "**beredskab**": en tilstand ved en væsentlig eller omfattende cybersikkerhedshændelse af parathed og kapacitet til at sikre en effektiv hurtig reaktion gennem forudgående risikovurderings- og overvågningsforanstaltninger

10) "**indsats**": tiltag i forbindelse med, under eller efter en væsentlig eller omfattende cybersikkerhedshændelse for at håndtere dens umiddelbare og kortsigtede negative konsekvenser

11) "**betroede udbydere**": udbydere af administrerede sikkerhedstjenester som defineret i artikel 6, nr. 40), i direktiv (EU) 2022/2555, der er udvalgt i overensstemmelse med artikel 16 i denne forordning.

Kapitel II

DET EUROPÆISKE CYBERSKJOLD

Artikel 3

Etablering af det europæiske cyberskjold

1. Der oprettes en sammenkoblet paneuropæisk infrastruktur af sikkerhedsoperationscentre ("det europæiske cyberskjold") med henblik på at udvikle avancerede kapaciteter for Unionen til at opdage, analysere og behandle data om cybertrusler og -hændelser i Unionen. Skjoldet består af nationale sikkerhedsoperationscentre ("nationale SOC'er") og grænseoverskridende sikkerhedsoperationscentre ("grænseoverskridende SOC'er").

[18] Europa-Parlamentets og Rådets direktiv 2014/24/EU af 26. februar 2014 om offentlige udbud og om ophævelse af direktiv 2004/18/EF (EUT L 94 af 28.3.2014, s. 65).

Tiltag til gennemførelse af det europæiske cyberskjold støttes med midler fra programmet for et digitalt Europa og gennemføres i overensstemmelse med forordning (EU) 2021/694, navnlig specifikt mål nr. 3.

2. Det europæiske cyberskjold skal:

a) samle og dele data om cybertrusler og -hændelser fra forskellige kilder gennem grænseoverskridende SOC'er

b) tilvejebringe anvendelige oplysninger af høj kvalitet og efterretninger om cybertrusler ved hjælp af de nyeste værktøjer, navnlig kunstig intelligens og dataanalyseteknologier

c) bidrage til bedre beskyttelse mod og reaktion på cybertrusler

d) bidrage til hurtigere opdagelse af cybertrusler og større situationskendskab i hele Unionen

e) levere tjenester og aktiviteter til cybersikkerhedssektoren i Unionen, herunder bidrage til udviklingen af værktøjer inden for avanceret kunstig intelligens og dataanalyse.

Det europæiske cyberskjold udvikles i samarbejde med den paneuropæiske højtydende databehandlingsinfrastruktur, der er etableret i henhold til forordning (EU) 2021/1173.

Artikel 4

Nationale sikkerhedsoperationscentre

1. For at deltage i det europæiske cyberskjold udpeger hver medlemsstat mindst ét nationalt SOC. Det nationale SOC skal være et offentligt organ.

Det skal have kapacitet til at fungere som referencepunkt og portal til andre offentlige og private organisationer på nationalt plan med henblik på at indsamle og analysere oplysninger om cybersikkerhedstrusler og -hændelser og bidrage til et grænseoverskridende SOC. Det skal være udstyret med avancerede teknologier, der gør det muligt at finde, aggregere og analysere data, der er relevante for cybersikkerhedstrusler og -hændelser.

2. Efter en indkaldelse af interessetilkendegivelser udvælges de nationale SOC'er af Det Europæiske Kompetencecenter for Cybersikkerhed ("ECCC") til at deltage i fælles indkøb af værktøjer og infrastrukturer i samarbejde med ECCC. ECCC kan yde tilskud til de udvalgte nationale SOC'er til finansiering af driften af disse værktøjer og infrastrukturer. Unionens finansielle bidrag dækker op til 50 % af omkostningerne ved erhvervelse af værktøjer og infrastrukturer og op til 50 % af driftsomkostningerne, mens de resterende omkostninger afholdes af medlemsstaten. Inden iværksættelsen af proceduren for erhvervelse af værktøjer og infrastrukturer indgår ECCC og det nationale SOC en hosting- og brugsaftale, der regulerer brugen af værktøjerne og infrastrukturerne.

3. Et nationalt SOC, der er udvalgt i henhold til stk. 2, forpligter sig til at ansøge om at deltage i et grænseoverskridende SOC senest to år efter den dato, hvor værktøjerne og infrastrukturerne erhverves, eller hvor det modtager tilskudsfinansiering, alt efter hvad der indtræffer først. Hvis et national SOC ikke deltager i et grænseoverskridende SOC på det tidspunkt, er det ikke berettiget til yderligere EU-støtte i henhold til denne forordning.

Artikel 5

Grænseoverskridende sikkerhedsoperationscentre

1. Et værtskonsortium bestående af mindst tre medlemsstater, repræsenteret ved nationale SOC'er, der har forpligtet sig til at samarbejde om at koordinere deres cybersporings- og trusselsovervågningsaktiviteter, er berettiget til at deltage i foranstaltninger til oprettelse af et grænseoverskridende SOC.

2. Efter en indkaldelse af interessetilkendegivelser udvælges et værtskonsortium af ECCC til at deltage i fælles indkøb af værktøjer og infrastrukturer i samarbejde med ECCC. ECCC kan yde tilskud til værtskonsortiet til finansiering af driften af disse værktøjer og infrastrukturer. Unionens finansielle bidrag dækker op til 75 % af omkostningerne ved erhvervelse af værktøjer og infrastrukturer og op til 50 % af driftsomkostningerne, mens de resterende omkostninger afholdes af værtskonsortiet. Inden iværksættelsen af proceduren for erhvervelse af værktøjer og infrastrukturer indgår ECCC og værtskonsortiet en hosting- og brugsaftale, der regulerer brugen af værktøjerne og infrastrukturerne.

3. Medlemmerne af værtskonsortiet indgår en skriftlig konsortieaftale, hvori de interne ordninger for gennemførelse af værts- og brugsaftalen fastlægges.

4. Et grænseoverskridende SOC repræsenteres i juridisk henseende af et nationalt SOC, der fungerer som koordinerende SOC, eller af værtskonsortiet, hvis det har status som juridisk person. Det koordinerende SOC er ansvarligt for overholdelse af kravene i værts- og brugsaftalen og af denne forordning.

Artikel 6

Samarbejde og informationsudveksling inden for og mellem grænseoverskridende SOC'er

1. Medlemmerne af et værtskonsortium udveksler indbyrdes relevante oplysninger inden for den grænseoverskridende SOC, herunder oplysninger om cybertrusler, nærvedhændelser, sårbarheder, teknikker og procedurer, indikatorer for kompromittering, fjendtlige taktikker, trusselsspecifikke oplysninger, cybersikkerhedsadvarsler og anbefalinger vedrørende konfiguration af cybersikkerhedsværktøjer til afsløring af cyberangreb, hvor en sådan informationsudveksling:

a) har til formål at forebygge, opdage, reagere på eller reetablere sig efter hændelser eller afbøde deres virkninger

b) øger cybersikkerhedsniveauet, navnlig ved at øge kendskabet til cybertrusler, begrænse eller hindre muligheden for, at sådanne trusler spreder sig, støtte en række forsvarskapaciteter, afhjælpe og afsløre sårbarheder, støtte teknikker til opdagelse, begrænsning og forebyggelse af trusler, støtte afbødningsstrategier eller indsats- og genopretningsfaserne eller fremme samarbejde mellem offentlige og private enheder om forskning i trusler.

2. Den skriftlige konsortieaftale i henhold til artikel 5, stk. 3, skal indeholde:

a) en forpligtelse til at dele en betydelig mængde data, jf. stk. 1, og betingelserne for udveksling af disse oplysninger

b) en forvaltningsramme, der tilskynder alle deltagere til at udveksle oplysninger

c) mål for bidrag til udvikling af værktøjer inden for avanceret kunstig intelligens og dataanalyse.

3. For at tilskynde til udveksling af oplysninger mellem grænseoverskridende SOC'er skal disse sikre en høj grad af indbyrdes interoperabilitet. For at sikre interoperabilitet mellem de grænseoverskridende SOC'er kan Kommissionen ved hjælp af gennemførelsesretsakter efter høring af ECCC fastsætte betingelserne for interoperabilitet. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i denne forordnings artikel 21, stk. 2.

4. Grænseoverskridende SOC'er indgår samarbejdsaftaler med hinanden, hvor principperne for informationsudveksling mellem de grænseoverskridende platforme fastlægges.

Artikel 7

Samarbejde og informationsudveksling med EU-enheder

1. Hvis grænseoverskridende SOC'er indhenter oplysninger om en potentiel eller igangværende væsentlig cybersikkerhedshændelse, forelægger de uden unødig forsinkelse de relevante oplysninger for EU-CyCLONe, CSIRT-netværket og Kommissionen i betragtning af deres respektive krisestyringsroller i overensstemmelse med direktiv (EU) 2022/2555.

2. Kommissionen kan ved hjælp af gennemførelsesretsakter fastlægge de proceduremæssige ordninger for den udveksling af oplysninger, der er omhandlet i stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i denne forordnings artikel 21, stk. 2.

Artikel 8

Sikkerhed

1. De medlemsstater, der deltager i det europæiske cyberskjold, sikrer et højt niveau af datasikkerhed og fysisk sikkerhed i den infrastruktur, der udgør det europæiske cyberskjold, og sikrer, at infrastrukturen forvaltes og styres hensigtsmæssigt, så den beskyttes mod trusler og så sikkerheden i infrastrukturen og i systemerne, herunder data, der udveksles via infrastrukturen, garanteres.

2. Medlemsstater, der deltager i det europæiske cyberskjold, sikrer, at udvekslingen af oplysninger inden for det europæiske cyberskjold med enheder, der ikke er offentlige organer i medlemsstaterne, ikke har en negativ indvirkning på Unionens sikkerhedsinteresser.

3. Kommissionen kan vedtage gennemførelsesretsakter, der fastsætter tekniske krav til medlemsstaternes opfyldelse af forpligtelserne i stk. 1 og 2. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i denne forordnings artikel 21, stk. 2. I den forbindelse tager Kommissionen med støtte fra den højtstående repræsentant hensyn til relevante sikkerhedsstandarder på forsvarsniveau for at lette samarbejdet med militære aktører.

Kapitel III

CYBERBEREDSKABSMEKANISME

Artikel 9

Etablering af cyberberedskabsmekanismen

1. Der etableres en beredskabsmekanisme for cybersikkerhed for at forbedre Unionens modstandsdygtighed over for større cybersikkerhedstrusler samt forberede Unionen på og solidarisk afbøde de kortsigtede virkninger af væsentlige og omfattende cybersikkerhedshændelser eller -kriser ("mekanismen").

2. Aktioner til gennemførelse af cyberberedskabsmekanismen støttes med midler fra programmet for et digitalt Europa og gennemføres i overensstemmelse med forordning (EU) 2021/694, navnlig specifikt mål nr. 3.

Artikel 10

Foranstaltningstyper

1. Under mekanismen støttes følgende typer foranstaltninger:

a) beredskabsforanstaltninger, herunder koordineret beredskabstest af enheder, der opererer i meget kritiske sektorer i EU

b) beredskabsforanstaltninger, der støtter reaktion på og øjeblikkelig genopretning efter væsentlige og omfattende cybersikkerhedshændelser, der leveres af betroede udbydere, der deltager i EU's cybersikkerhedsreserve, som er oprettet i henhold til artikel 12

c) gensidige bistandsaktioner i form af bistand fra en medlemsstats nationale myndigheder til en anden medlemsstat, navnlig som omhandlet i artikel 11, stk. 3, litra f), i direktiv (EU) 2022/2555.

Artikel 11

Koordineret beredskabstest af enheder

1. Med henblik på at støtte den koordinerede beredskabstest af de enheder, der er omhandlet i artikel 10, stk. 1, litra a), i hele Unionen identificerer Kommissionen efter høring af NIS-samarbejdsgruppen og ENISA de berørte sektorer eller delsektorer blandt de sektorer af særlig kritisk betydning, der er anført i bilag I til direktiv (EU) 2022/2555, hvor enheder kan gøres til genstand for koordineret beredskabstest, under hensyntagen til eksisterende og planlagte koordinerede risikovurderinger og prøvning af modstandsdygtighed på EU-plan.

2. NIS-samarbejdsgruppen udarbejder i samarbejde med Kommissionen, ENISA og den højtstående repræsentant fælles risikoscenarier og metoder til gennemførelse af de koordinerede test.

Artikel 12

Etablering af EU's cybersikkerhedsreserve

1. Der oprettes en EU-cybersikkerhedsreserve med henblik på at bistå de brugere, der er omhandlet i stk. 3, med at reagere på eller yde støtte til at reagere på væsentlige eller omfattende cybersikkerhedshændelser og omgående genopretning efter sådanne hændelser.

2. EU's cybersikkerhedsreserve består af hændelsesberedskabstjenester fra betroede udbydere, der er udvalgt i overensstemmelse med kriterierne i artikel 16. Reserven omfatter tjenester omfattet af forhåndsforpligtelser. Tjenesterne kan indsættes i alle medlemsstater.

3. Brugere af tjenester fra EU's cybersikkerhedsreserve omfatter:

a) medlemsstaternes cyberkrisestyringsmyndigheder og CSIRT'er som anført i henholdsvis artikel 9, stk. 1 og 2, og artikel 10 i direktiv (EU) 2022/2555

b) EU's institutioner, organer og agenturer.

4. Brugerne, som er nævnt i stk. 3, litra a), anvender tjenesterne fra EU's cybersikkerhedsreserve til at reagere på eller støtte indsatsen mod og den omgående genopretning efter væsentlige eller omfattende hændelser, der påvirker enheder, der opererer i kritiske eller meget kritiske sektorer.

5. Kommissionen har det overordnede ansvar for gennemførelsen af EU's cybersikkerhedsreserve. Kommissionen fastlægger prioriteterne for og udviklingen af EU's cybersikkerhedsreserve i overensstemmelse med kravene til de brugere, der er omhandlet i stk. 3, overvåger gennemførelsen og sikrer komplementaritet, sammenhæng, synergi og forbindelser med andre støtteaktioner i henhold til denne forordning samt andre EU-foranstaltninger og -programmer.

6. Kommissionen kan helt eller delvist overdrage driften og administrationen af EU's cybersikkerhedsreserve til ENISA ved hjælp af bidragsaftaler.

7. For at støtte Kommissionen i etableringen af EU's cybersikkerhedsreserve udarbejder ENISA en kortlægning af de nødvendige tjenester efter høring af medlemsstaterne og Kommissionen. ENISA udarbejder efter høring af Kommissionen en lignende kortlægning for at identificere behovene i de tredjelande, der er berettiget til støtte fra EU's cybersikkerhedsreserve i henhold til artikel 17. Kommissionen hører, hvor det er relevant, den højtstående repræsentant.

8. Kommissionen kan i gennemførelsesretsakter præcisere de typer og det antal af beredskabstjenester, der kræves i EU's cybersikkerhedsreserve. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 21, stk. 2.

Artikel 13

Anmodninger om støtte fra EU's cybersikkerhedsreserve

1. De brugere, der er omhandlet i artikel 12, stk. 3, kan anmode om tjenester fra EU's cybersikkerhedsreserve til støtte for en reaktion på og en øjeblikkelig genopretning efter væsentlige eller omfattende cybersikkerhedshændelser.

2. For at modtage støtte fra EU's cybersikkerhedsreserve træffer de brugere, der er omhandlet i artikel 12, stk. 3, foranstaltninger til at afbøde virkningerne af den hændelse, der er årsag til anmodningen om støtte, herunder ydelse af direkte teknisk bistand og andre ressourcer som en del af reaktionen på hændelsen og den omgående genopretningsindsats.

3. Anmodninger om støtte fra de brugere, der er omhandlet i denne forordnings artikel 12, stk. 3, litra a), sendes til Kommissionen og ENISA via det centrale kontaktpunkt, der er udpeget eller oprettet af medlemsstaten i overensstemmelse med artikel 8, stk. 3, i direktiv (EU) 2022/2555.

4. Medlemsstaterne underretter CSIRT-netværket og, hvor det er relevant, EU-CyCLONe om deres anmodninger om støtte til reaktioner på hændelser og omgående genopretning i henhold til denne artikel.

5. Anmodninger om støtte til reaktioner på hændelser og omgående genopretning omfatter:

a) relevante oplysninger om den berørte enhed og mulige virkninger af hændelsen samt den planlagte anvendelse af den støtte, der anmodes om, herunder en angivelse af de anslåede behov

b) oplysninger om foranstaltninger, der er truffet for at afbøde den hændelse, der er årsag til anmodningen om støtte, jf. stk. 2

c) oplysninger om andre former for støtte, der er til rådighed for den berørte enhed, herunder indgåede kontrakter vedrørende reaktioner på hændelser og tjenester til omgående genopretning, samt forsikringsaftaler, der muligvis dækker hændelsestypen.

6. ENISA udarbejder i samarbejde med Kommissionen og NIS-samarbejdsgruppen en skabelon for at lette indgivelsen af anmodninger om støtte fra EU's cybersikkerhedsreserve.

7. Kommissionen kan i gennemførelsesretsakter yderligere præcisere de detaljerede ordninger for tildeling af støtte fra EU's cybersikkerhedsreserve. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 21, stk. 2.

Artikel 14

Gennemførelse af støtte fra EU's cybersikkerhedsreserve

1. Anmodninger om støtte fra EU's cybersikkerhedsreserve vurderes af Kommissionen med støtte fra ENISA eller som defineret i bidragsaftaler i henhold til artikel 12, stk. 6, og et svar sendes straks til de brugere, der er omhandlet i artikel 12, stk. 3.

2. Hvis flere anmodninger indgives samtidig, skal der ved prioritering heraf tages hensyn til følgende kriterier, hvor det er relevant:

a) alvorligheden af cybersikkerhedshændelsen

b) typen af berørt enhed, idet der gives højere prioritet til hændelser, der påvirker væsentlige enheder som defineret i artikel 3, stk. 1, i direktiv (EU) 2022/2555

c) mulig indvirkning på den eller de berørte medlemsstater eller brugere

d) hændelsens mulige grænseoverskridende karakter og risikoen for afledte effekter for andre medlemsstater eller brugere

e) foranstaltninger truffet af brugeren for at medvirke til reaktionen herpå og den umiddelbare genopretningsindsats, jf. artikel 13, stk. 2, og artikel 13, stk. 5, litra b).

3. Tjenesterne under EU's cybersikkerhedsreserve leveres i overensstemmelse med særaftaler mellem tjenesteudbyderen og den bruger, som støtten under EU's cybersikkerhedsreserve ydes til. Aftalerne skal indeholde ansvarsbetingelser.

4. De i stk. 3 omhandlede aftaler kan baseres på skabeloner udarbejdet af ENISA efter høring af medlemsstaterne.

5. Kommissionen og ENISA bærer intet kontraktligt ansvar for skader påført tredjepart som følge af de tjenester, der leveres inden for rammerne af gennemførelsen af EU's cybersikkerhedsreserve.

6. Senest én måned efter afslutningen af støtteforanstaltningen forelægger brugerne Kommissionen og ENISA en sammenfattende rapport om den leverede tjeneste, de opnåede resultater og de indhøstede erfaringer. Når brugeren er fra et tredjeland, jf. artikel 17, videresendes rapporten til den højtstående repræsentant.

7. Kommissionen aflægger regelmæssigt rapport til NIS-samarbejdsgruppen om anvendelsen og resultaterne af støtten.

Artikel 15

Koordinering med krisestyringsmekanismer

1. I tilfælde, hvor væsentlige eller omfattende cybersikkerhedshændelser skyldes eller resulterer i katastrofer som defineret i afgørelse 1313/2013/EU[19], supplerer støtten til reaktioner på sådanne hændelser i henhold til denne forordning foranstaltninger i henhold til afgørelse 1313/2013/EU uden at berøre denne afgørelse.

2. I tilfælde af en omfattende, grænseoverskridende cybersikkerhedshændelse, hvor integrerede ordninger for politisk kriserespons (IPCR) udløses, skal støtten i henhold til denne forordning til at reagere på en sådan hændelse håndteres i overensstemmelse med de relevante protokoller og procedurer i henhold til IPCR.

3. I samråd med den højtstående repræsentant kan støtte under cyberberedskabsmekanismen supplere den bistand, der ydes inden for rammerne af den fælles udenrigs- og sikkerhedspolitik og den fælles sikkerheds- og forsvarspolitik, herunder gennem cyberberedskabsholdene. Den kan også supplere eller bidrage til den bistand, som en medlemsstat yder til en anden medlemsstat inden for rammerne af artikel 42, stk. 7, i traktaten om Den Europæiske Union.

4. Støtte under cyberberedskabsmekanismen kan indgå i den fælles indsats mellem Unionen og medlemsstaterne i de situationer, der er omhandlet i artikel 222 i traktaten om Den Europæiske Unions funktionsmåde.

[19] Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU af 17. december 2013 om en EU-civilbeskyttelsesmekanisme (EUT L 347 af 20.12.2013, s. 924).

Artikel 16

Betroede udbydere

1. I forbindelse med udbudsprocedurer med henblik på etablering af EU's cybersikkerhedsreserve handler den ordregivende myndighed i overensstemmelse med principperne i forordning (EU, Euratom) 2018/1046 og i overensstemmelse med følgende principper:

a) sikre, at EU's cybersikkerhedsreserve omfatter tjenester, der kan udrulles i alle medlemsstater, idet der navnlig tages hensyn til nationale krav til levering af sådanne tjenester, herunder certificering eller akkreditering

b) sikre beskyttelse af Unionens og dens medlemsstaters væsentlige sikkerhedsinteresser

c) sikre, at EU's cybersikkerhedsreserve skaber merværdi for EU ved at bidrage til de målsætninger, der er fastsat i artikel 3 i forordning (EU) 2021/694, herunder ved at fremme udviklingen af cybersikkerhedsfærdigheder i EU.

2. Ved indkøb af tjenesteydelser til EU's cybersikkerhedsreserve medtager den ordregivende myndighed følgende udvælgelseskriterier i udbudsdokumenterne:

a) udbyderen skal påvise, at personalet har den højeste grad af faglig integritet, selvstændighed og ansvar samt den nødvendige tekniske kompetence til at udføre aktiviteterne inden for de specifikke områder, og udbyderen skal sikre, at ekspertisen samt de nødvendige tekniske ressourcer er permanent til rådighed uden afbrydelse

b) udbyderen og dennes datterselskaber og underleverandører skal have indført en ramme til beskyttelse af følsomme oplysninger vedrørende tjenesten, navnlig dokumentation, undersøgelser og rapporter, og arbejde i overensstemmelse med Unionens sikkerhedsregler om beskyttelse af EU's klassificerede informationer

c) udbyderen skal fremlægge tilstrækkelig dokumentation for en transparent ledelsesstruktur, hvor der ikke er sandsynlighed for, at upartiskheden og kvaliteten af tjenesterne kan anfægtes eller interessekonflikter opstå

d) udbyderen skal have en passende sikkerhedsgodkendelse, i det mindste for personale, der arbejder med udrulning af tjenesterne

e) udbyderens IT-systemer skal være sikret med et relevant sikkerhedsniveau

f) udbyderen skal være udstyret med den nødvendige hardware og software til at understøtte den ønskede tjeneste

g) udbyderen skal kunne dokumentere erfaring med at levere lignende tjenester til relevante nationale myndigheder eller enheder, der opererer i kritiske eller meget kritiske sektorer

h) udbyderen skal være i stand til at levere tjenesten hurtigt i den eller de medlemsstater, hvor udbyderen kan levere tjenesten

i) udbyderen skal kunne levere tjenesten på det lokale sprog i den eller de medlemsstater, hvor udbyderen kan levere tjenesten

j) når en EU-certificeringsordning for administrerede sikkerhedstjenester i henhold til forordning (EU) 2019/881 er indført, skal udbyderen certificeres i overensstemmelse med denne ordning.

Artikel 17

Støtte til tredjelande

1. Tredjelande kan anmode om støtte fra EU's cybersikkerhedsreserve, hvis de associeringsaftaler, der er indgået vedrørende deres deltagelse i programmet for et digitalt Europa, indeholder bestemmelser herom.

2. Støtte fra EU's cybersikkerhedsreserve er i overensstemmelse med denne forordning og opfylder eventuelle specifikke betingelser, der er fastsat i de associeringsaftaler, der er omhandlet i stk. 1.

3. Brugere fra associerede tredjelande, der er berettigede til levering af tjenester fra EU's cybersikkerhedsreserve, omfatter kompetente myndigheder såsom CSIRT'er og cyberkrisestyringsmyndigheder.

4. Tredjelande, der er berettiget til støtte fra EU's cybersikkerhedsreserve, udpeger en myndighed, der skal fungere som et centralt kontaktpunkt med henblik på denne forordning.

5. Forud for modtagelse af støtte fra EU's cybersikkerhedsreserve forelægger tredjelande Kommissionen og den højtstående repræsentant oplysninger om deres cyberrobusthed og risikostyringskapacitet, herunder som minimum oplysninger om nationale foranstaltninger, der er truffet for at forberede sig på væsentlige eller omfattende cybersikkerhedshændelser, samt oplysninger om ansvarlige nationale enheder, herunder CSIRT'er eller tilsvarende enheder, deres kapaciteter og de ressourcer, de har fået tildelt. Når bestemmelserne i artikel 13 og 14 i denne forordning henviser til medlemsstaterne, finder de anvendelse på tredjelande som fastsat i stk. 1.

6. Kommissionen koordinerer behandlingen af de modtagne anmodninger med den højtstående repræsentant og gennemførelsen af den støtte, der ydes til tredjelande fra EU's cybersikkerhedsreserve.

Kapitel IV

MEKANISME TIL GENNEMGANG AF CYBERSIKKERHEDSHÆNDELSER

Artikel 18

Mekanisme til gennemgang af cybersikkerhedshændelser

1. Efter anmodning fra Kommissionen, EU-CyCLONe eller CSIRT-netværket gennemgår og vurderer ENISA trusler, sårbarheder og afbødende foranstaltninger ved specifikke, væsentlige eller omfattende cybersikkerhedshændelser. Efter afsluttet gennemgang og vurdering af en hændelse fremsender ENISA en rapport om hændelsen til CSIRT-netværket, EU-CyCLONe og Kommissionen som støtte til udførelsen af deres opgaver, navnlig opgaver i henhold til artikel 15 og 16 i direktiv (EU) 2022/2555. Hvis det er relevant, videresender Kommissionen rapporten med den højtstående repræsentant.

2. Ved udarbejdelse af den i stk. 1 omhandlede rapport om gennemgang af en hændelse samarbejder ENISA med alle relevante interessenter, herunder repræsentanter for medlemsstaterne, Kommissionen, andre relevante EU-institutioner, -organer og -agenturer, udbydere af administrerede sikkerhedstjenester og brugere af cybersikkerhedstjenester. Hvor det er relevant, samarbejder ENISA også med enheder, der er berørt af væsentlige eller

omfattende cybersikkerhedshændelser. Som støtte for gennemgangen kan ENISA også høre andre typer interessenter. De hørte repræsentanter skal oplyse om eventuelle interessekonflikter.

3. Rapporten omfatter en gennemgang og analyse af den specifikke væsentlige eller omfattende cybersikkerhedshændelse, herunder de vigtigste årsager, sårbarheder og indhøstede erfaringer. Fortrolige oplysninger beskyttes i overensstemmelse med EU-retten eller national ret vedrørende beskyttelse af følsomme eller klassificerede informationer.

4. Rapporten skal, hvor det er relevant, indeholde anbefalinger til forbedring af Unionens cyberposition.

5. Hvis det er muligt, offentliggøres en udgave af rapporten. Denne udgave indeholder kun de oplysninger, der kan offentliggøres.

Kapitel V

AFSLUTTENDE BESTEMMELSER

Artikel 19

Ændringer af forordning (EU) 2021/694

I forordning (EU) 2021/694 foretages følgende ændringer:

1) Artikel 6 ændres således:

a) Stk. 1 ændres således:

1) Følgende indsættes som litra aa):

"aa) støtte udviklingen af et EU-cyberskjold, herunder udvikling, udrulning og drift af nationale og grænseoverskridende SOC-platforme, der bidrager til et øget situationskendskab i Unionen og til at styrke Unionens efterretningskapacitet vedrørende cybertrusler".

2) Følgende tilføjes som litra g):

"g) etablere og drive en cyberberedskabsmekanisme for at hjælpe medlemsstaterne med at forberede sig og reagere på væsentlige cybersikkerhedshændelser som supplement til nationale ressourcer og kapaciteter og andre former for støtte, der er til rådighed på EU-plan, herunder etablering af en EU-cybersikkerhedsreserve".

a) Stk. 2 affattes således:

"2. Foranstaltningerne under specifikt mål nr. 3 gennemføres primært gennem det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og

netværket af nationale koordinationscentre i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2021/887[20] med undtagelse af foranstaltninger til gennemførelse af EU's cybersikkerhedsreserve, som gennemføres af Kommissionen og ENISA."

2) Artikel 9 ændres således:

a) Stk. 2, litra b), c) og d), affattes således:

"b), 1 776 956 000 EUR til specifikt mål nr. 2 — Kunstig intelligens

c), 1 629 566 000 EUR til specifikt mål nr. 3 — Cybersikkerhed og tillid

d), 482 347 000 EUR til specifikt mål nr. 4 — Højtudviklede digitale færdigheder

b) Følgende tilføjes som stk. 8:

"8. Uanset artikel 12, stk. 4, i forordning (EU, Euratom) 2018/1046 overføres uudnyttede forpligtelses- og betalingsbevillinger til foranstaltninger, der forfølger de mål, der er fastsat i nærværende forordnings artikel 6, stk. 1, litra g), automatisk, og der kan indgås forpligtelser og betales frem til den 31. december i det følgende regnskabsår."

3) Artikel 14, stk. 2, affattes således:

"2. Programmet kan yde finansiering i enhver af de former, der er fastsat i finansforordningen, herunder navnlig gennem udbud som den primære form eller tilskud og priser.

Hvor det er nødvendigt at indkøbe innovative varer og tjenester for at opfylde målsætningen for en foranstaltning, må der kun ydes tilskud til støttemodtagere, der er ordregivende myndigheder eller ordregivende enheder som defineret i Europa-Parlamentets og Rådets direktiv 2014/24/EU [27] og 2014/25/EU [28].

Hvor levering af innovative varer eller tjenester, som endnu ikke er kommercielt tilgængelige i stor skala, er nødvendig for at opfylde målsætningen for en foranstaltning, kan den ordregivende myndighed eller den ordregivende enhed godkende tildelingen af flere kontrakter inden for samme udbudsprocedure.

Ud fra behørigt begrundede hensyn til den offentlige sikkerhed kan den ordregivende myndighed eller den ordregivende enhed kræve, at kontraktens opfyldelsessted skal være inden for Unionens område.

Ved gennemførelse af udbudsprocedurer vedrørende EU's cybersikkerhedsreserve, der er oprettet ved artikel 12 i forordning (EU) 2023/XX, kan Kommissionen og ENISA fungere som indkøbscentral på vegne af tredjelande, der er associeret til programmet,

[20] Europa-Parlamentets og Rådets forordning (EU) 2021/887 af 20. maj 2021 om oprettelse af Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed og Netværket af Nationale Koordinationscentre (EUT L 202 af 8.6.2021, s. 1).

jf. artikel 10. Kommissionen og ENISA kan også fungere som grossist ved at købe, oplagre og videresælge eller donere varer og tjenesteydelser, herunder leje, til disse tredjelande. Uanset artikel 169, stk. 3, i forordning (EU) XXX/XXXX [omarbejdning af finansforordningen] er en anmodning fra et enkelt tredjeland tilstrækkelig til at give Kommissionen eller ENISA mandat til at handle.

Ved gennemførelse af udbudsprocedurer vedrørende EU's cybersikkerhedsreserve, der etableres ved artikel 12 i forordning (EU) 2023/XX, kan Kommissionen og ENISA fungere som indkøbscentral på vegne af EU's institutioner, organer og agenturer. Kommissionen og ENISA kan også fungere som grossist ved at købe, oplagre og videresælge eller donere varer og tjenesteydelser, herunder leje, til EU's institutioner, organer og agenturer. Uanset artikel 169, stk. 3, i forordning (EU) XXX/XXXX [omarbejdning af finansforordningen] er en anmodning fra en enkelt EU-institution, et enkelt EU-organ eller et enkelt EU-agentur tilstrækkeligt til at give Kommissionen eller ENISA mandat til at handle.

Programmet kan også stille finansiering til rådighed i form af finansielle instrumenter under blandingsoperationer."

4) Følgende tilføjes som artikel 16a:

For så vidt angår foranstaltninger til gennemførelse af det europæiske cyberskjold, der er oprettet ved artikel 3 i forordning (EU) 2023/XX, er reglerne fastsat i artikel 4 og 5 i forordning (EU) 2023/XX gældende. I tilfælde af konflikt mellem bestemmelserne i denne forordning og artikel 4 og 5 i forordning (EU) 2023/XX har sidstnævnte forrang og finder anvendelse på disse specifikke foranstaltninger.

5) Artikel 19 affattes således:

"Tilskud i henhold til programmet tildeles og forvaltes i overensstemmelse med finansforordningens afsnit VIII og kan dække op til 100 % af de støtteberettigede omkostninger, uden at dette berører samfinansieringsprincippet i finansforordningens artikel 190. Sådanne tilskud tildeles og forvaltes som nærmere angivet for hvert specifikt mål.

Støtte i form af tilskud kan ydes direkte af ECCC uden forslagsindkaldelse til de nationale SOC'er, der er omhandlet i artikel 4 i forordning XXXX, og værtskonsortiet, der er omhandlet i artikel 5 i forordning XXXX, i overensstemmelse med finansforordningens artikel 195, stk. 1, litra d).

Støtte i form af tilskud til cyberberedskabsmekanismen, jf. artikel 10 i forordning XXXX, kan tildeles direkte af ECCC til medlemsstaterne uden forslagsindkaldelse i overensstemmelse med finansforordningens artikel 195, stk. 1, litra d).

For så vidt angår foranstaltninger omhandlet i artikel 10, stk. 1, litra c), i forordning 202X/XXXX underretter ECCC Kommissionen og ENISA om medlemsstaternes anmodninger om direkte tilskud uden indkaldelse af forslag.

Med henblik på støtte til gensidig bistand til en reaktion på en væsentlig eller omfattende cybersikkerhedshændelse som defineret i artikel 10, litra c), i forordning XXXX og i overensstemmelse med finansforordningens artikel 193, stk. 2, andet afsnit, litra a), kan omkostningerne i behørigt begrundede tilfælde betragtes som støtteberettigede, selv om de blev afholdt, inden ansøgningen om tilskud blev indgivet."

6) Bilag I og II ændres som anført i bilaget til denne forordning.

Artikel 20

Evaluering

Senest [fire år efter datoen for denne forordnings anvendelse] forelægger Kommissionen Europa-Parlamentet og Rådet en rapport om evaluering og revision af denne forordning.

Artikel 21

Udvalgsprocedure

1. Kommissionen bistås af Koordinationsudvalget for Programmet for et Digitalt Europa, der er nedsat i medfør af forordning (EU) 2021/694. Dette udvalg er et udvalg som omhandlet i forordning (EU) nr. 182/2011.
2. Når der henvises til dette stykke, finder artikel 5 i forordning (EU) nr. 182/2011 anvendelse.

Artikel 22

Ikrafttræden

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende.*

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i enhver medlemsstat.

Udfærdiget i Strasbourg, den […].

På Europa-Parlamentets vegne	*På Rådets vegne*
Formand	*Formand*

FINANSIERINGSOVERSIGT

1. FORSLAGETS/INITIATIVETS RAMME

1.1 Forslagets/initiativets betegnelse

1.2 Berørt(e) politikområde(r)

1.3 Forslaget/initiativet vedrører:

1.4 Mål

1.4.1 Generelt/generelle mål

1.4.2 Specifikt/specifikke mål

1.4.3 Forventet/forventede resultat(er) og virkning(er)

1.4.4 Resultatindikatorer

1.5 Begrundelse for forslaget/initiativet

1.5.1 Behov, der skal opfyldes på kort eller lang sigt, herunder en detaljeret tidsplan for iværksættelsen af initiativet

1.5.2 Merværdien ved et EU-tiltag (f.eks. som følge af koordineringsfordele, retssikkerhed, større effekt eller komplementaritet). Ved "merværdien ved et EU-tiltag" forstås her merværdien af EU's intervention i forhold til den værdi, som medlemsstaterne ville have skabt enkeltvis

1.5.3 Erfaringer fra tidligere foranstaltninger af lignende art

1.5.4 Forenelighed med den flerårige finansielle ramme og mulige synergivirkninger med andre relevante instrumenter

1.5.5 Vurdering af de forskellige finansieringsmuligheder, der er til rådighed, herunder muligheden for omfordeling

1.6 Forslagets/initiativets varighed og finansielle virkninger

1.7 Planlagt(e) budgetgennemførelsesmetode(r)

2 FORVALTNINGSFORANSTALTNINGER

2.1 Bestemmelser om overvågning og rapportering

2.2 Forvaltnings- og kontrolsystem(er)

2.2.1 Begrundelse for den/de påtænkte forvaltningsmetode(r), finansieringsmekanisme(r), betalingsvilkår og kontrolstrategi

2.2.2 Oplysninger om de konstaterede risici og det/de interne kontrolsystem(er), der etableres for at afbøde dem

2.2.3 Vurdering af og begrundelse for kontrolforanstaltningernes omkostningseffektivitet (forholdet mellem kontrolomkostningerne og værdien af de forvaltede midler) samt vurdering af den forventede risiko for fejl (ved betaling og ved afslutning)

2.3 Foranstaltninger til forebyggelse af svig og uregelmæssigheder

3 FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

3.1 Berørt(e) udgiftsområde(r) i den flerårige finansielle ramme og udgiftspost(er) på budgettet

3.2 Forslagets anslåede finansielle virkninger for bevillingerne

3.2.1 Sammenfatning af de anslåede virkninger for aktionsbevillingerne

3.2.2 Anslåede resultater finansieret med aktionsbevillinger

3.2.3 Sammenfatning af de anslåede virkninger for administrationsbevillingerne

3.2.3.1. Anslået behov for menneskelige ressourcer

3.2.4 Forenelighed med indeværende flerårige finansielle ramme

3.2.5 Bidrag fra tredjemand

3.3 Anslåede virkninger for indtægterne

1 FORSLAGETS/INITIATIVETS RAMME

1.1 Forslagets/initiativets betegnelse

Europa-Parlamentets og Rådets forordning om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser

1.2 Berørt(e) politikområde(r)

Et Europa klar til den digitale tidsalder

Europæiske strategiske investeringer

Aktivitet: Europas digitale fremtid i støbeskeen.

1.3 Forslaget/initiativet vedrører:

☒ **en ny foranstaltning**

☐ **en ny foranstaltning som opfølgning på et pilotprojekt/en forberedende foranstaltning**[33]

☐ **en forlængelse af en eksisterende foranstaltning**

☐ **en sammenlægning eller en omlægning af en eller flere foranstaltninger til en anden/en ny foranstaltning**

1.4 Mål

1.4.1 Generelt/generelle mål

Forordningen om cybersolidaritet styrker solidariteten på EU-plan for bedre at kunne opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser. Foranstaltningens formål:

a) at styrke EU's fælles situationskendskab og kapacitet til at afsløre cybertrusler og -hændelser

b) at styrke kritiske enheders beredskab i hele EU og styrke solidariteten ved at udvikle fælles indsatskapaciteter over for væsentlige eller omfattende cybersikkerhedshændelser, herunder ved at stille støtte til håndtering af hændelser til rådighed for tredjelande, der er tilknyttet programmet for et digitalt Europa

c) at øge Unionens modstandsdygtighed og bidrage til en effektiv indsats ved at gennemgå og vurdere væsentlige eller omfattende hændelser, herunder indhøstede erfaringer og eventuelle anbefalinger.

1.4.2 Specifikt/specifikke mål

Forordningen om cybersolidaritet opfylder de fastsatte målsætninger gennem:

[33] Jf. finansforordningens artikel 58, stk. 2, litra a) hhv. b).

a) etablering af en paneuropæisk infrastruktur for sikkerhedsoperationscentre ("et europæisk cyberskjold") for at opbygge og styrke det fælles situationskendskab og den fælles kapacitet til at afsløre hændelser.

b) oprettelse af en cyberberedskabsmekanisme som støtte til medlemsstaterne, så de bedre kan forberede sig og reagere på samt sikre omgående genopretning efter væsentlige eller omfattende cybersikkerhedshændelser. Støtte til reaktioner på hændelser stilles også til rådighed for EU's institutioner, organer, kontorer og agenturer (EUIBA).

Foranstaltningerne støttes med midler fra programmet for et digitalt Europa, som dette lovgivningsinstrument indebærer en ændring af med henblik på at fastlægge ovennævnte foranstaltninger, yde finansiel støtte til deres udvikling og præcisere betingelserne for at modtage finansiel støtte.

c) oprettelse af en europæisk mekanisme til gennemgang af cybersikkerhedshændelser med henblik på at gennemgå og vurdere væsentlige eller omfattende hændelser.

1.4.3 Forventet/forventede resultat(er) og virkning(er)

Angiv, hvilke virkninger forslaget/initiativet forventes at få for modtagerne/målgrupperne.

Forslaget vil medføre betydelige fordele for de forskellige interessenter. Det europæiske cyberskjold forbedrer medlemsstaternes kapacitet til at afsløre cybertrusler. Cyberberedskabsmekanismen supplerer medlemsstaternes foranstaltninger gennem nødhjælp til beredskab, indsats og øjeblikkelig genopretning/genetablering af væsentlige tjenesters funktion.

Foranstaltningerne styrker industriens og virksomhedernes konkurrenceevne i Europa i hele den digitaliserede økonomi og støtter deres digitale omstilling ved at styrke cybersikkerhedsniveauet på det digitale indre marked. Forordningen har navnlig til formål at øge modstandsdygtigheden hos borgere, virksomheder og enheder, der opererer i kritiske eller meget kritiske sektorer, over for de voksende cybersikkerhedstrusler, som kan have ødelæggende samfundsmæssige og økonomiske virkninger. Det sker gennem investeringer i værktøjer, der muliggør hurtigere opdagelse og reaktion på cybersikkerhedstrusler og -hændelser, og medlemsstaterne sikres hjælp til at forberede sig bedre og reagere på væsentlige og omfattende cybersikkerhedshændelser. Det skal ligeledes sikre Europa en øget kapacitet på disse områder, navnlig med hensyn til indsamling og analyse af data om cybersikkerhedstrusler og -hændelser.

1.4.4 Resultatindikatorer

Angiv indikatorerne til overvågning af fremskridt og resultater.

For at fremme solidariteten på EU-plan kan en række indikatorer benyttes:

1) Antallet af cybersikkerhedsinfrastrukturer eller værktøjer eller begge dele, som er indkøbt i fællesskab

2) Antallet af foranstaltninger til støtte for beredskab og reaktion på cybersikkerhedshændelser inden for rammerne af cyberberedskabsmekanismen.

1.5 Begrundelse for forslaget/initiativet

1.5.1 Behov, der skal opfyldes på kort eller lang sigt, herunder en detaljeret tidsplan for iværksættelsen af initiativet

Denne forordning bør træde i kraft umiddelbart efter vedtagelsen, dvs. på tyvendedagen efter offentliggørelsen i Den Europæiske Unions Tidende.

1.5.2 Merværdien ved et EU-tiltag (f.eks. som følge af koordineringsfordele, retssikkerhed, større effekt eller komplementaritet). Ved "merværdien ved et EU-tiltag" forstås her merværdien af EU's intervention i forhold til den værdi, som medlemsstaterne ville have skabt enkeltvis

Cybersikkerhedstruslernes udpræget grænseoverskridende karakter generelt og det stigende antal risici og hændelser, som har afledte effekter på tværs af landegrænser, sektorer og produkter, betyder, at målsætningerne for den nuværende indsats ikke effektivt kan opfyldes af medlemsstaterne alene; det kræver også fælles handling og solidaritet på EU-niveau. Erfaringerne med at imødegå cybertrusler afledt af krigen mod Ukraine og erfaringerne fra en cybersikkerhedsøvelse, der blev gennemført under det franske formandskab (EU CyCLES), har vist, at der bør udvikles konkrete gensidige støttemekanismer, navnlig samarbejde med den private sektor, for at skabe solidaritet på EU-niveau. På denne baggrund opfordres Kommissionen i Rådets konklusioner af 23. maj 2022 om udviklingen af Den Europæiske Unions cyberposition til at forelægge et forslag om en ny beredskabsfond for cybersikkerhed. Støtte og tiltag på EU-niveau for bedre at kunne afsløre cybersikkerhedstrusler og for at øge beredskabs- og indsatskapaciteten skaber merværdi, da dobbeltarbejde undgås på tværs af Unionen og i medlemsstaterne. Det vil sikre en bedre udnyttelse af eksisterende aktiver og en øget koordinering og udveksling af oplysninger om indhøstede erfaringer.

1.5.3 Erfaringer fra tidligere foranstaltninger af lignende art

Med hensyn til situationskendskab og afsløring af hændelser gennem det europæiske cyberskjold blev der udsendt en indkaldelse af interessetilkendegivelser med henblik på fælles indkøb af værktøjer og infrastruktur til etablering af grænseoverskridende SOC'er og en indkaldelse vedrørende tilskud til kapacitetsopbygning af SOC'er, der betjener offentlige og private organisationer, inden for rammerne af arbejdsprogrammet vedrørende cybersikkerhed for 2021-2022 under programmet for et digitalt Europa.

Med hensyn til beredskab og reaktioner på hændelser har Kommissionen oprettet et kortsigtet program vedrørende støtte til medlemsstaterne i form af yderligere midler, der er afsat til ENISA, med henblik på omgående at styrke beredskabet og kapaciteten til at reagere på større cyberhændelser. Blandt de omfattede tjenester er beredskabsforanstaltninger såsom penetrationstest af kritiske enheder med henblik på at kortlægge sårbarheder. Det styrker også mulighederne for at bistå medlemsstaterne i tilfælde af en større hændelse, der påvirker kritiske enheder. ENISA er i gang med at gennemføre det kortsigtede program og har allerede fremlagt værdifuld relevant viden, som er medtaget i udarbejdelsen af denne forordning.

1.5.4 Forenelighed med den flerårige finansielle ramme og mulige synergivirkninger med andre relevante instrumenter

Forordningen om cybersolidaritet bygger på foranstaltninger, der i øjeblikket støttes af Unionen og medlemsstaterne, med henblik på at øge situationskendskabet og

kapaciteten til at afsløre cybertrusler og reagere på omfattende og grænseoverskridende cybersikkerhedshændelser. Desuden er instrumentet i overensstemmelse med andre krisestyringsrammer, herunder IPCR, den fælles sikkerheds- og forsvarspolitik, herunder cyberberedskabshold, og den bistand, som en medlemsstat yder til en anden medlemsstat inden for rammerne af artikel 42, stk. 7, i traktaten om Den Europæiske Union. Det nye forslag supplerer og støtter endvidere de strukturer, der er udviklet under andre cybersikkerhedsinstrumenter såsom direktiv (EU) 2022/2555 (NIS 2-direktivet) eller forordning 2019/881 (forordningen om cybersikkerhed).

1.5.5 Vurdering af de forskellige finansieringsmuligheder, der er til rådighed, herunder muligheden for omfordeling

Forvaltningen af de indsatsområder, der er tildelt ENISA, ligger inden for rammerne af agenturets eksisterende mandat og generelle opgaver. Disse indsatsområder kan kræve særlige profiler eller nye opgaver, men disse kan finansieres ved brug af ENISA's eksisterende ressourcer og ved omfordeling eller sammenkobling af forskellige opgaver. ENISA gennemfører i øjeblikket et kortsigtet program, som Kommissionen oprettede i 2022 for omgående at styrke beredskabet og kapaciteten til at reagere på større cyberhændelser. Tjenesterne omfatter muligheder for at bistå medlemsstaterne i tilfælde af en større hændelse, der påvirker kritiske enheder. ENISA er i gang med at gennemføre det kortsigtede program og har allerede fremlagt værdifuld relevant viden, som er medtaget i udarbejdelsen af denne forordning. De ressourcer, der er afsat til det kortsigtede program, kan også anvendes i sammenhæng med denne forordning.

1.6 Forslagets/initiativets varighed og finansielle virkninger

☒ **Begrænset varighed**

– ☒ gældende fra datoen for vedtagelsen af forslaget til Europa-Parlamentets og Rådets forordning om styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser ("forordningen om cybersolidaritet")

– ☒ Finansielle virkninger fra 2023 til 2027 for forpligtelsesbevillinger og fra 2023 til 2031 for betalingsbevillinger[34].

☐ **Ubegrænset varighed**

– — iværksættelse med en indkøringsperiode fra ÅÅÅÅ til ÅÅÅÅ

– — derefter gennemførelse i fuldt omfang

1.7 Planlagt(e) budgetgennemførelsesmetode(r)[35]

☒ **Direkte forvaltning** ved Kommissionen

– ☒ i dens tjenestegrene, herunder ved dens personale i EU's delegationer

– ☐ i forvaltningsorganerne

☐ **Delt forvaltning** i samarbejde med medlemsstaterne

☒ **Indirekte forvaltning** ved at overlade budgetgennemførelsesopgaver til:

– ☐ tredjelande eller organer, som tredjelande har udpeget

– ☐ internationale organisationer og deres agenturer (angives nærmere)

– ☐ Den Europæiske Investeringsbank og Den Europæiske Investeringsfond

– ☒ de organer, der er omhandlet i finansforordningens artikel 70 og 71

– ☐ offentligretlige organer

– ☐ privatretlige organer, der har fået overdraget offentlige tjenesteydelsesopgaver, i det omfang de har fået stillet tilstrækkelige finansielle garantier

– ☐ privatretlige organer undergivet lovgivningen i en medlemsstat, som har fået overdraget gennemførelsen af et offentlig-privat partnerskab, og som har fået stillet tilstrækkelige finansielle garantier

– ☐ organer eller personer, der har fået overdraget gennemførelsen af specifikke aktioner i den fælles udenrigs- og sikkerhedspolitik i henhold til afsnit V i traktaten om Den Europæiske Union, og som er anført i den relevante basisretsakt

– *Hvis der angives flere forvaltningsmetoder, gives der en nærmere forklaring i afsnittet "Bemærkninger".*

Bemærkninger

Foranstaltningerne vedrørende det europæiske cyberskjold bliver gennemført af ECCC. Indtil ECCC har kapacitet til at gennemføre sit eget budget, gennemfører Europa-Kommissionen aktionerne under direkte forvaltning på vegne af ECCC. ECCC kan udvælge enheder på

[34] Retsaktens foranstaltninger bør støttes under den næste flerårige finansielle ramme.

[35] Nærmere oplysninger om budgetgennemførelsesmetoder og henvisninger til finansforordningen findes på webstedet BUDGpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx

grundlag af indkaldelser af interessetilkendegivelser til at deltage i fælles indkøb af værktøjer. ECCC kan yde tilskud til driften af disse værktøjer.

Desuden kan ECCC yde tilskud til beredskabsforanstaltninger inden for rammerne af cyberberedskabsmekanismen.

Kommissionen har det overordnede ansvar for gennemførelsen af EU's cybersikkerhedsreserve. Kommissionen kan helt eller delvist ved hjælp af bidragsaftaler overdrage driften og administrationen af EU's cybersikkerhedsreserve til ENISA. De foranstaltninger, der i henhold til denne forordning tildeles ENISA, er i overensstemmelse med dets eksisterende mandat. Det gælder følgende foranstaltninger: i) støtte til NIS-samarbejdsgruppen til udvikling af beredskabsforanstaltninger i overensstemmelse med risikovurderinger ii) støtte til Kommissionen til etablering af og tilsyn med gennemførelsen af EU's cybersikkerhedsreserve, herunder modtagelse og behandling af anmodninger om støtte iii) udarbejdelse af skabeloner for at lette indgivelse af anmodninger om støtte og særaftaler, der skal indgås mellem tjenesteudbyderen og den bruger, som støtten under EU's cybersikkerhedsreserve ydes til iv) gennemgang og vurdering af trusler, sårbarheder og afbødende foranstaltninger i forbindelse med specifikke væsentlige eller omfattende cybersikkerhedshændelser og udarbejdelse af rapporter herom.

Opgaverne anslås tilsammen til ca. 7 fuldtidsækvivalenter ud af ENISA's eksisterende ressourcer og bygger allerede på den ekspertise og det forberedende arbejde, som ENISA i øjeblikket udfører inden for rammerne af pilotprojektet om nødhjælp til beredskab og reaktioner på hændelser.

2 FORVALTNINGSFORANSTALTNINGER

2.1 Bestemmelser om overvågning og rapportering

Angiv hyppighed og betingelser.

Kommissionen overvåger gennemførelsen, anvendelsen og overholdelsen af disse nye bestemmelser med henblik på at vurdere deres effektivitet. Kommissionen forelægger Europa-Parlamentet og Rådet en rapport om evalueringen og revisionen af denne forordning senest fire år efter datoen for dens anvendelse.

2.2 Forvaltnings- og kontrolsystem(er)

2.2.1 Begrundelse for den/de påtænkte forvaltningsmetode(r), finansieringsmekanisme(r), betalingsvilkår og kontrolstrategi

Med forordningen indføres en ramme for gennemførelse af EU-finansiering med henblik på at øge cyberrobustheden gennem tiltag, der forbedrer kapaciteten til at opdage, reagere på og sikre genopretning i tilfælde af væsentlige og omfattende cybersikkerhedshændelser. Det kontor i GD CNECT, der har ansvaret for det politiske område, står for gennemførelsen af direktivet.

For at kunne løse de nye opgaver er det nødvendigt at afsætte tilstrækkelige ressourcer til Kommissionens tjenestegrene. Håndhævelsen af den nye forordning anslås at kræve 6 FTE'er (3 AD-stillinger og 3 KA-stillinger) til varetagelse af følgende opgaver:

- fastlæggelse af beredskabsforanstaltninger i henhold til risikovurderinger
- sikring af interoperabilitet mellem grænseoverskridende SOC-platforme
- udarbejdelse af mulige gennemførelsesretsakter (to for SOC'er og to for cybersikkerhedsberedskabsmekanismen)
- Forvaltning af hosting- og brugsaftaler for SOC'er
- Etablering og forvaltning af EU's cybersikkerhedsreserve, enten direkte eller via en bidragsaftale til ENISA. I tilfælde af bidragsaftale til ENISA skal der udarbejdes og føres tilsyn med gennemførelsen af bidragsaftalen for de opgaver, der er tildelt ENISA
- Deltagelse i de høringsgrupper, som ENISA har indkaldt vedrørende gennemgang og vurdering af væsentlige og omfattende cybersikkerhedshændelser samt udarbejdelse af rapporter.

2.2.2 Oplysninger om de konstaterede risici og det/de interne kontrolsystem(er), der etableres for at afbøde dem

En identificeret risiko i forbindelse med det europæiske cyberskjold er, at medlemsstaterne muligvis ikke deler en tilstrækkelig mængde af relevante oplysninger om cybertrusler, hverken inden for de grænseoverskridende SOC-platforme eller mellem grænseoverskridende platforme og andre relevante enheder på EU-plan. For at fjerne denne risiko sker tildelingen af midler efter en indkaldelse af interessetilkendegivelser, hvor medlemsstaterne forpligter sig til at dele en given mængde oplysninger på EU-niveau. Denne forpligtelse bliver derefter formaliseret i en værtsaftale og brugsaftale, og ECCC får beføjelse til at foretage revisioner for at sikre, at de fælles indkøbte værktøjer og infrastrukturer anvendes i overensstemmelse

med aftalen. Forpligtelsen til at dele en omfattende mængde oplysninger inden for de grænseoverskridende SOC'er bliver formaliseret i en konsortieaftale.

En identificeret risiko i forbindelse med cyberberedskabsmekanismen er, at brugere, der deltager i mekanismen, ikke træffer tilstrækkelige foranstaltninger til at sikre beredskabet over for cyberangreb. Derfor er brugerne forpligtede til at træffe sådanne beredskabsforanstaltninger for at kunne modtage støtte fra EU's cybersikkerhedsreserve. Når brugerne indgiver anmodninger om støtte til EU's cybersikkerhedsreserve, skal de redegøre for de foranstaltninger, der allerede er truffet for at kunne reagere på en hændelse, og de oplysninger indgår ved vurdering af anmodningerne til EU's cybersikkerhedsreserve.

2.2.3 Vurdering af og begrundelse for kontrolforanstaltningernes omkostningseffektivitet (forholdet mellem kontrolomkostningerne og værdien af de forvaltede midler) samt vurdering af den forventede risiko for fejl (ved betaling og ved afslutning)

Da reglerne for deltagelse i programmet for et digitalt Europas, som også gælder for støtte i henhold til forordningen om cybersolidaritet, svarer til de regler, som Kommissionen bruger i sit arbejdsprogram, og da støttemodtagerne har samme risikoprofil som for programmerne under direkte forvaltning, kan det forventes, at fejlprocenten vil være den samme som den, Kommissionen har fastsat for programmet for et digitalt Europa, dvs. at der gives en rimelig forsikring om, at risikoen for fejl i den flerårige udgiftsperiode på årsbasis vil ligge inden for 2-5 % med det ultimative mål at opnå en tilbageværende fejlprocent så tæt som muligt på 2 % ved afslutningen af de flerårige programmer, når der først er taget hensyn til den økonomiske effekt af alle revisioner, korrektioner og tilbagesøgningsforanstaltninger.

2.3 Foranstaltninger til forebyggelse af svig og uregelmæssigheder

Angiv eksisterende eller påtænkte forebyggelses- og beskyttelsesforanstaltninger, f.eks. fra strategien til bekæmpelse af svig.

For så vidt angår det europæiske cyberskjold har ECCC beføjelse til på grundlag af adgang til oplysninger og kontrol på stedet at revidere de værktøjer og infrastrukturer, der er indkøbt i fællesskab, i overensstemmelse med den hosting- og brugsaftale, der skal indgås mellem værtskonsortiet og ECCC.

De eksisterende foranstaltninger til forebyggelse af svig, der gælder for EU's institutioner, organer og agenturer, dækker de supplerende bevillinger, der er nødvendige i forbindelse med denne forordning.

3 FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

3.1 Berørt(e) udgiftsområde(r) i den flerårige finansielle ramme og udgiftspost(er) på budgettet

- Eksisterende budgetposter

I samme rækkefølge som udgiftsområderne i den flerårige finansielle ramme og budgetposterne.

Udgiftsområde i den flerårige finansielle ramme	Budgetpost	Udgiftens art	Bidrag			
	Nummer	OB/IOB[36]	fra EFTA-lande[37]	fra kandidatlande og potentielle kandidatlande[38]	fra andre tredjelande	andre formålsbestemte indtægter
1	02 04 01 10 Programmet for et digitalt Europa — Cybersikkerhed	OB	JA	JA	NEJ	NEJ
1	02 04 01 11 Programmet for et digitalt Europa — Industri-, teknologi- og forskningskompetencecentret	Opdelte	JA	JA	NEJ	NEJ
1	02 04 03 Programmet for et digitalt Europa — kunstig intelligens	Opdelte	JA	JA	NEJ	NEJ
1	02 04 04 Programmet for et digitalt Europa — færdigheder	Opdelte	JA	JA	NEJ	NEJ
1	02 01 30 Udgifter til støttefunktioner i forbindelse med programmet for et digitalt Europa	IOB	JA	JA	NEJ	NEJ

[36] OB = opdelte bevillinger/IOB = ikke-opdelte bevillinger.
[37] EFTA: Den Europæiske Frihandelssammenslutning.
[38] Kandidatlande og, hvis det er relevant, potentielle kandidatlande.

3.2 Forslagets anslåede finansielle virkninger for bevillingerne

3.2.1 Sammenfatning af de anslåede virkninger for aktionsbevillingerne

– ☐ Forslaget/initiativet medfører ikke anvendelse af aktionsbevillinger

– ☒ Forslaget/initiativet medfører anvendelse af aktionsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

Udgiftsområde i den flerårige finansielle ramme	Nummer	1 **Det indre marked, innovation og det digitale område**

Forslaget øger ikke det samlede niveau af forpligtelser under programmet for et digitalt Europa. Bidraget til dette initiativ er en omfordeling af forpligtelserne fra SO2 og SO4 for at styrke budgettet for SO3 og ECCC. Enhver forhøjelse af forpligtelserne under programmet for et digitalt Europa som følge af en revision af FFR kan anvendes til dette initiativ.

GD CONNECT			År **2025**	År **2026**	År **2027**	År **2028 og derefter**	Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)			**I ALT**
○ Aktionsbevillinger										
Budgetpost[39] 02.040110 (omfordeling fra 02.0403 og 02.0404)	Forpligtelser	1a	15,000	15,000	6,000	p.m.				**36,000**
	Betalinger	2a	15,000	15,000	6,000					**36,000**
Budgetpost 02.040111.02 (omfordeling fra 02.0403 og 02.0404)	Forpligtelser	1b	13,000	23,000	28,000	p.m.				**64,000**
	Betalinger	2b	8,450	18,200	25,250	12,100				**64,000**
Administrationsbevillinger finansieret over bevillingsrammen for særprogrammer[40]										

39 Ifølge den officielle budgetkontoplan.

40 Teknisk og/eller administrativ bistand og udgifter til støtte for gennemførelsen af EU's programmer og/eller foranstaltninger (tidligere BA-poster), indirekte forskning, direkte forskning.

Budgetpost 02.0130		3)	0,150	0,150	0,150	p.m.				0,450
Bevillinger I ALT vedrørende GD CONNECT	Forpligtelser	=1a+1b +3	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Betalinger	=2a+2b +3	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

○ Aktionsbevillinger I ALT	Forpligtelser	4)	28,000	38,000	34,000	p.m.				**100,000**
	Betalinger	5)	23,450	33,200	31,250	12,100				**100,000**
○ Administrationsbevillinger finansieret over bevillingsrammen for særprogrammer I ALT		6)	0,150	0,150	0,150	p.m.				**0,450**
Bevillinger I ALT under UDGIFTSOMRÅDE 1 i den flerårige finansielle ramme	Forpligtelser	=4+6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Betalinger	=5+6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Hvis flere aktionsrelaterede udgiftsområder berøres af forslaget/initiativet, indsættes der et tilsvarende afsnit for hvert udgiftsområde

○ Aktionsbevillinger I ALT (alle aktionsrelaterede udgiftsområder)	Forpligtelser	4)	28,000	38,000	34,000	p.m.				**100,000**
	Betalinger	5)	23,450	33,200	31,250	12,100				**100,000**
Administrationsbevillinger finansieret over bevillingsrammen for særprogrammer I ALT (alle aktionsrelaterede udgiftsområder)		6)	0,150	0,150	0,150					**0,450**
Bevillinger I ALT under UDGIFTSOMRÅDE 1 til 6 i den flerårige finansielle ramme (referencebeløb)	Forpligtelser	=4+6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Betalinger	=5+6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Udgiftsområde i den flerårige finansielle ramme	7	"Administrationsudgifter"

Dette afsnit skal udfyldes ved hjælp af arket vedrørende administrative budgetoplysninger, der først skal indføres i bilaget til finansieringsoversigten (bilag 5 til Kommissionens afgørelse om de interne regler for gennemførelse af Den Europæiske Unions almindelige budget (afsnittet om Kommissionen), som uploades til DECIDE med henblik på høring af andre tjenestegrene.

i mio. EUR (tre decimaler)

		År **2025**	År **2026**	År **2027**	År **2028 og derefter**	Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)			**I ALT**
GD: ETABLERING AF FORBINDELSER									
○ Menneskelige ressourcer		0,786	0,786	0,786	p.m.				**2,358**
○ Andre administrationsudgifter		0,035	0,035	0,035	p.m.				**0,105**
I ALT GD CONNECT	Bevillinger	**0,821**	**0,821**	**0,821**					**2 463**

Bevillinger I ALT under UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme	(Forpligtelser i alt = betalinger i alt)	**0,821**	**0,821**	**0,821**					**2 463**

i mio. EUR (tre decimaler)

		År **2025**	År **2026**	År **2027**	År **2028 og derefter**	Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)			**I ALT**
Bevillinger I ALT	Forpligtelser	**28,971**	**38,971**	**34,971**	**p.m.**				**102,913**

under UDGIFTSOMRÅDE 1 til 7 i den flerårige finansielle ramme	Betalinger	**24,421**	**34,171**	**32,221**	**12,100**				**102,913**

3.2.2 Anslåede resultater finansieret med aktionsbevillinger

Forpligtelsesbevillinger i mio. EUR (tre decimaler)

Angiv målsætninger og resultater ⇩			År **n**		År **n+1**		År **n+2**		År **n+3**		Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)						**I ALT**	
	RESULTATER																	
	Type[41]	Gnsntl. omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal resultater i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 1[42]																		
— Resultat																		
— Resultat																		
— Resultat																		
Subtotal for specifikt mål nr. 1																		
SPECIFIKT MÅL NR. 2																		
— Resultat																		
Subtotal for specifikt mål nr. 2																		
I ALT																		

41 Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks.: antal finansierede studenterudvekslinger, antal km bygget vej osv.).

42 Som beskrevet i punkt 1.4.2 "Specifikt/specifikke mål"

3.2.3 Sammenfatning af de anslåede virkninger for administrationsbevillingerne

– ☐ Forslaget/initiativet medfører ikke anvendelse af administrationsbevillinger

– ☒ Forslaget/initiativet medfører anvendelse af administrationsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

	År 2025	År r 2026	År 2027	År n+3	Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)			**I ALT**
UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme								
Menneskelige ressourcer	0,786	0,786	0,786					**2 358**
Andre administrationsudgifter	0,035	0,035	0,035					**0,105**
Subtotal UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme	**0,821**	**0,821**	**0,821**					**2 463**

Uden for UDGIFTSOMRÅDE 7[43] i den flerårige finansielle ramme								
Menneskelige ressourcer								
Andre administrationsudgifter	0,150	0,150	0,150					**0,450**
Subtotal uden for UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme	**0,150**	**0,150**	**0,150**					**0,450**

I ALT	**0,971**	**0,971**	**0,971**					**2 913**

Bevillingerne til menneskelige ressourcer og andre administrationsudgifter vil blive dækket ved hjælp af de bevillinger, som generaldirektoratet allerede har afsat til forvaltning af foranstaltningen, og/eller ved intern omfordeling i generaldirektoratet, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige generaldirektorat i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

[43] Teknisk og/eller administrativ bistand og udgifter til støtte for gennemførelsen af EU's programmer og/eller foranstaltninger (tidligere BA-poster), indirekte forskning, direkte forskning.

3.2.3.1. Anslået behov for menneskelige ressourcer

– ☐ Forslaget/initiativet medfører ikke anvendelse af menneskelige ressourcer

– ☒ Forslaget/initiativet medfører anvendelse af menneskelige ressourcer som anført herunder:

Overslag angives i årsværk

		År **2025**	År **2026**	År 2027	År **n+3**	Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)		
○ Stillinger i stillingsfortegnelsen (tjenestemænd og midlertidigt ansatte)								
20 01 02 01 (i hovedsædet og i Kommissionens repræsentationskontorer)		3	3	3				
20 01 02 03 (i delegationerne)								
01 01 01 01 (indirekte forskning)								
01 01 01 11 (direkte forskning)								
Andre budgetposter (skal angives)								
○ Eksternt personale (i årsværk: FTE)[44]								
20 02 01 (KA, UNE, V under den samlede bevillingsramme)		3	3	3				
20 02 03 (KA, LA, UNE, V og JMD i delegationerne)								
XX 01 xx **yy zz** [45]	— i hovedsædet							
	— i delegationer							
01 01 01 02 (KA, UNE, V — indirekte forskning)								
01 01 01 12 (KA, UNE, V — direkte forskning)								
Andre budgetposter (skal angives)								
I ALT		**6**	**6**	**6**				

XX angiver det berørte politikområde eller budgetafsnit.

Personalebehovet vil blive dækket ved hjælp af det personale, som generaldirektoratet allerede har afsat til forvaltning af foranstaltningen, og/eller ved interne rokader i generaldirektoratet, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige generaldirektorat i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

Opgavebeskrivelse:

Tjenestemænd og midlertidigt ansatte	- fastlæggelse af beredskabsforanstaltninger i henhold til risikovurderinger (artikel 11) - Udarbejdelse af mulige gennemførelsesretsakter (to for SOC'er og to for cybersikkerhedsberedskabsmekanismen) - Forvaltning af hosting- og brugsaftaler for SOC'er - Etablering og forvaltning af EU's cybersikkerhedsreserve, enten direkte eller via en bidragsaftale til ENISA.
Eksternt personale	Under tilsyn af en tjenestemand - fastlæggelse af beredskabsforanstaltninger i henhold til risikovurderinger (artikel 11) - Udarbejdelse af mulige gennemførelsesretsakter (to for SOC'er og to for

[44] KA: kontraktansatte, LA: lokalt ansatte, UNE: udstationerede nationale eksperter, V: vikarer, JMD: juniormedarbejdere i delegationerne.

[45] Delloft for eksternt personale under aktionsbevillingerne (tidligere BA-poster).

	cybersikkerhedsberedskabsmekanismen) - Forvaltning af hosting- og brugsaftaler for SOC'er - Etablering og forvaltning af EU's cybersikkerhedsreserve, enten direkte eller via en bidragsaftale til ENISA.

3.2.4 *Forenelighed med indeværende flerårige finansielle ramme*

Forslaget/initiativet:

– [X] kan finansieres fuldt ud gennem omfordeling inden for det relevante udgiftsområde i den flerårige finansielle ramme (FFR)

Gør rede for omlægningen med angivelse af de berørte budgetposter og de beløb, der er tale om. I tilfælde af omfattende omlægning gives oplysningerne i form af en exceltabel.

	2023	2024	2025	2026	2027	total
SO1	16.232.897	20.528.765	17.406.899	16.223.464	10.022.366	80.414.391
SO2 initial	226.316.819	295.067.000	195.649.000	221.809.000	246.608.000	1.185.449.819
To CYBER initiative			18.000.000	28.000.000	19.000.000	65.000.000
NEW 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
Fom SO2-SO4			15.000.000	15.000.000	6.000.000	36.000.000
New SO3	**24.361.553**	**35.596.172**	**18.638.000**	**18.638.000**	**17.175.000**	**114.408.725**
ECCC initial	176.222.303	208.374.879	104.228.130	90.704.986	84.851.497	664.381.795
From SO2-SO4			13.000.000	23.000.000	28.000.000	64.000.000
New ECCC	**176.222.303**	**208.374.879**	**117.228.130**	**113.704.986**	**112.851.497**	**728.381.795**
SO4 initial	66.902.708	64.892.032	56.577.977	70.477.245	72.107.201	330.957.163
To CYBER initiative			10.000.000	10.000.000	15.000.000	35.000.000
NEW SO4	**66.902.708**	**64.892.032**	**46.577.977**	**60.477.245**	**57.107.201**	**295.957.163**

– [ ] kræver anvendelse af den uudnyttede margen under det relevante udgiftsområde i FFR og/eller anvendelse af særlige instrumenter som fastlagt i FFR-forordningen

Gør rede for behovet med angivelse af de berørte udgiftsområder og budgetposter, de beløb, der er tale om, og de instrumenter, der foreslås anvendt.

– [ ] kræver en revision af FFR.

Gør rede for behovet med angivelse af de berørte udgiftsområder og budgetposter og de beløb, der er tale om.

3.2.5 *Bidrag fra tredjemand*

Forslaget/initiativet:

– [X] indeholder ikke bestemmelser om samfinansiering med tredjemand

– [ ] indeholder bestemmelser om samfinansiering med tredjemand, jf. følgende overslag:

Bevillinger i mio. EUR (tre decimaler)

	År **n**[46]	År **n+1**	År **n+2**	År **n+3**	Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)	I alt

[46] År n er det år, hvor gennemførelsen af forslaget/initiativet påbegyndes. Erstat "n" med det forventede første gennemførelsesår (f.eks.: 2021). Dette gælder også for de efterfølgende år.

Angiv det organ, der deltager i samfinansieringen								
Samfinansierede bevillinger I ALT								

3.3 Anslåede virkninger for indtægterne

– ☒ Forslaget/initiativet har ingen finansielle virkninger for indtægterne

– ☐ Forslaget/initiativet har følgende finansielle virkninger:

– – ☐ for egne indtægter

– – ☐ for andre indtægter

– – Angiv, om indtægterne er formålsbestemte ☐

i mio. EUR (tre decimaler)

Indtægtspost på budgettet:	Bevillinger til rådighed i indeværende regnskabsår	Forslagets/initiativets virkninger[47]						
		År **n**	År **n+1**	År **n+2**	År **n+3**	Indsæt så mange år som nødvendigt for at vise virkningernes varighed (jf. punkt 1.6)		
Artikel …								

For indtægter, der er formålsbestemte, angives det, hvilke af budgettets udgiftsposter der berøres.

[…]

Andre bemærkninger (f.eks. om hvilken metode, der er benyttet til at beregne virkningerne for indtægterne).

[…]

[47] Med hensyn til EU's traditionelle egne indtægter (told og sukkerafgifter) opgives beløbene netto, dvs. bruttobeløb, hvorfra der er trukket opkrævningsomkostninger på 20 %.