EUROPA-
KOMMISSIONEN

Bruxelles, den 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om oprettelse af det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af nationale koordinationscentre

Europa-Kommissionens bidrag til mødet mellem lederne i Salzburg, den 19.-20. september 2018

{SEC(2018) 396 final} - {SWD(2018) 403 final} - {SWD(2018) 404 final}

BEGRUNDELSE

1. BAGGRUND FOR FORSLAGET

• Forslagets begrundelse og formål

I takt med at dagligdagen og økonomierne bliver mere og mere afhængige af digitale teknologier, udsættes borgerne i stadig større omfang for alvorlige cyberhændelser. Sikkerheden fremadrettet afhænger af at kunne beskytte EU bedre mod cybertrusler, da både den civile infrastruktur og den militære kapacitet er afhængige af sikre digitale systemer.

For at tackle de voksende udfordringer har EU støt øget sine aktiviteter på området med afsæt i strategien for cybersikkerhed fra 2013[1] og dens mål og principper om at fremme et pålideligt, sikkert og åbent cyberøkosystem. I 2016 vedtog EU de første foranstaltninger inden for cybersikkerhed gennem Europa-Parlamentets og Rådets direktiv (EU) 2016/1148[2] om sikkerheden i net- og informationssystemer.

På baggrund af et cybersikkerhedsområde under hastig forandring forelagde Kommissionen og EU's højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik i september 2017 en fælles meddelelse[3] "Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU" for yderligere at styrke EU's modstandsdygtighed over for, afskrækkelse af og reaktion på cyberangreb. Den fælles meddelelse, der også bygger på tidligere initiativer, skitserede en række foreslåede foranstaltninger, herunder bl.a. at styrke Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA), at skabe en frivillig EU-dækkende ramme for cybersikkerhedscertificering af produkter og tjenesteydelser i den digitale verden samt en plan for hurtig og koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser.

I den fælles meddelelse anerkendes det, at det også er i EU's strategiske interesse at sikre, at EU bevarer og udvikler afgørende teknologiske kapaciteter inden for cybersikkerhed til at sikre det digitale indre marked, og navnlig at beskytte kritiske netværk og informationssystemer og tilvejebringe vigtige cybersikkerhedstjenester. EU skal være i stand til på egen hånd at sikre sine digitale aktiver og konkurrere på globale marked for cybersikkerhed.

På nuværende tidspunkt er EU nettoimportør af cybersikkerhedsprodukter og -løsninger og er i vid udstrækning afhængig af ikke-europæiske leverandører[4]. Markedet for cybersikkerhed er på verdensplan et marked på 600 mia. EUR, som forventes at vokse i de næste fem år med i gennemsnit ca. 17 % målt på omsætning, antallet af virksomheder og beskæftigelsen. Men set ud fra et markedsperspektiv befinder kun 6 af EU's medlemsstater[5] sig blandt de 20 førende lande inden for cybersikkerhed .

---

1 FÆLLES MEDDELELSE TIL EUROPA-PARLAMENTET OG RÅDET: EU-strategi for cybersikkerhed: Et åbent, sikkert og beskyttet cyberspace, JOIN (2013) 1 final.

2 Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

3 FÆLLES MEDDELELSE TIL EUROPA-PARLAMENTET OG RÅDET Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU, JOIN(2017) 450 final.

4 Udkast til endelig rapport om markedsundersøgelsen af cybersikkerhed, 2018

5 Udkast til endelig rapport om markedsundersøgelsen af cybersikkerhed, 2018

Samtidig findes der i EU omfattende erfaring og ekspertise inden for cybersikkerhed - mere end 660 organisationer fra hele EU tilmeldte sig for nylig en kortlægning af ekspertisecentre for cybersikkerhed, som Kommissionen[6] stod for. Denne ekspertise kan, hvis den omsættes til kommercielle produkter og løsninger, gøre det muligt for EU at dække hele værdikæden inden for cybersikkerhed. Men forskernes og erhvervslivets indsats er fragmenteret og savner tilpasning og en fælles mission, hvilket hæmmer EU's konkurrenceevne på dette område samt dens evne til at sikre sine digitale aktiver. De relevante sektorer for cybersikkerhed (f.eks. energi, rumfart, forsvar, transport) og deres underområder er i dag ikke tilstrækkeligt understøttet[7]. Synergierne mellem de civile og militære cybersikkerhedssektorer udnyttes heller ikke fuldt ud i Europa.

Oprettelsen i 2016 af det offentlig-private partnerskab (OPP) for cybersikkerhed i EU var et reelt første skridt, der samler forskning, industri og den offentlige sektor om at fremme forskning og innovation inden for cybersikkerhed og inden for den finansielle ramme for 2014-2020, og burde munde ud i gode, mere målrettede resultater inden for forskning og innovation. OPP gjorde det muligt for industrielle partnere at give tilsagn om deres respektive udgifter på de områder, der er fastlagt i partnerskabets strategiske forsknings- og innovationsdagsorden.

Men EU kan foretage langt større investeringer og har behov for en mere effektiv mekanisme til at opbygge varig kapacitet, samle indsatser og kompetencer og stimulere udviklingen af innovative løsninger på industriens udfordringer vedrørende cybersikkerhed inden for nye multifunktionelle teknologier (f.eks. kunstig intelligens, kvantedatabehandling, blockchain og sikre digitale identiteter) samt i kritiske sektorer (f.eks. transport, energi, sundhed, finans, offentlige myndigheder, telekommunikation, fremstilling, forsvar, rumfart).

Den fælles meddelelse så nærmere på muligheden for at styrke EU's cybersikkerhedskapacitet ved hjælp af et netværk af kompetencecentre for cybersikkerhed med et europæisk kompetencecenter for cybersikkerhed i centrum. Formålet hermed er at supplere den eksisterende kapacitetsopbygningsindsats på dette område på EU-plan og på nationalt plan. Den fælles meddelelse gav udtryk for Kommissionens intention om at iværksætte en konsekvensanalyse i 2018, der skal undersøge mulighederne for at oprette strukturen. Som et første skridt og for at bidrage til overvejelserne fremadrettet iværksatte Kommissionen en pilotfase under Horisont 2020, der skal være med til at samle nationale centre i et netværk, som vil skabe ny fremdrift inden for cybersikkerhedskompetence og teknologiudvikling.

Stats- og regeringscheferne på det digitale topmøde i Tallinn i september 2017 opfordrede EU til at blive en "global leder inden for cybersikkerhed senest i 2025 for at sikre tillid og beskyttelse af vores borgere, forbrugere og virksomheder på nettet og for at muliggøre et frit og lovstyret internet."

Rådets konklusioner[8], der blev vedtaget i november 2017, opfordrede Kommissionen til hurtigt at forelægge en konsekvensanalyse om og inden midten af 2018 at foreslå de relevante retlige instrumenter til gennemførelse af initiativet.

---

6 JRC's tekniske rapporter: "European Cybersecurity Centres of Expertise", 2018.

7 JRC's tekniske rapport: "Outcomes of the Mapping Exercise" (se bilag 4 og 5 for nærmere enkeltheder).

8 Rådets konklusioner om den fælles meddelelse til Europa-Parlamentet og Rådet: Modstandsdygtighed, afskrækkelse og forsvar: Opbygning af en stærk cybersikkerhed for EU, vedtaget af Rådet (almindelige anliggender) den 20. november 2017.

Programmet det digitale Europa, som Kommissionen fremsatte forslag om i juni 2018[9]*,* søger at udvide og maksimere fordelene ved digital omstilling for Europas borgere og virksomheder på alle EU's relevante politikområder, ved at styrke politikker og støtte ambitionerne for det digitale indre marked. Programmet foreslår en sammenhængende og overordnet tilgang, der skal sikre den bedst mulige anvendelse af avancerede teknologier og den rette kombination af teknisk kapacitet og menneskelig kompetence til den digitale omstilling - ikke kun inden for cybersikkerhed, men også med hensyn til intelligent datainfrastruktur, kunstig intelligens, avancerede færdigheder og anvendelser i industrien og inden for områder af offentlig interesse. Disse elementer er indbyrdes afhængige og gensidigt forstærkende og, når de fremmes samtidig, kan de opnå den fornødne størrelse, der kan få en dataøkonomi til at trives[10]. *Programmet Horisont Europa*[11] - EU's næste FoI-rammeprogram, har ligeledes cybersikkerhed som et af sine prioriterede indsatsområder.

I denne forbindelse foreslås det i nærværende forordning at oprette et europæisk industri-, teknologi- og forskningskompetencecenter for cybersikkerhed med et netværk af nationale koordinationscentre. For at stimulere Europas teknologiske og industrielle økosystem inden for cybersikkerhed bør denne formålsbestemte samarbejdsmodel fungere som følger: Kompetencecentret skal fremme og bistå netværkets arbejde, fremme kompetencefællesskabet for cybersikkerhed og derved fremme den teknologiske dagsorden for cybersikkerhed og lette adgangen til den indsamlede ekspertise. I denne forbindelse vil kompetencecentret navnlig gennemføre de relevante dele af programmet for det digitale Europa og Horisont Europa-programmet ved at yde tilskud og foretage indkøb. I lyset af de betragtelige cybersikkerhedsinvesteringer i andre dele af verden og behovet for at koordinere og sammenlægge ressourcer i Europa foreslås kompetencecentret som et europæisk partnerskab[12], der dermed kan fremme fælles investeringer fra EU, medlemsstaterne og/eller industrien. Forslaget pålægger derfor medlemsstaterne at bidrage med et forholdsmæssigt beløb til kompetencecentrets og netværkets initiativer. Bestyrelsen udgør det øverste beslutningsorgan, hvor alle medlemsstaterne har mulighed for at deltage, men hvor kun de medlemsstater, der deltager i finansieringen, har stemmeret. Stemmeordningen i bestyrelsen følger princippet om dobbelt flertal, hvor der kræves 75 % af det finansielle bidrag og 75 % af stemmerne. I betragtning af Kommissionens ansvar over for EU-budgettet råder Kommissionen over 50 % af stemmerne. I forbindelse med sit arbejde i bestyrelsen vil Kommissionen, når det er passende, benytte sig af ekspertisen fra Tjenesten for EU's Optræden Udadtil. Bestyrelsen bør bistås af et industrielt og videnskabeligt rådgivende organ, der kan sørge for en løbende dialog med den private sektor, forbrugerorganisationerne og andre relevante interessenter.

Ved at arbejde tæt sammen med netværket af nationale koordinationscentre og kompetencefælleskabet for cybersikkerhed (med en stor og varieret gruppe af aktører, der er involveret i teknologiudvikling af cybersikkerhed, som f.eks. forskningsenheder, industrier på udbudssiden, industrier på efterspørgselssiden, og den offentlige sektor), som er oprettet ved

---

9 COM (2018) 434 Forslag til Europa-Parlamentets og Rådets forordning programmet for et digitalt Europa for perioden 2021-2027

10 Se SWD(2018) 305

11 COM 2018) 435 Forslag til Europa-Parlamentets og Rådets forordning om oprettelse af Horisont Europa – rammeprogrammet for forskning og innovation og om reglerne for deltagelse og formidling.

12 Som defineret i COM 2018) 435 Forslag til Europa-Parlamentets og Rådets forordning om oprettelse af Horisont Europa – rammeprogrammet for forskning og innovation og om reglerne for deltagelse og formidling, og som omhandlet i COM (2018) 434 Forslag til Europa-Parlamentets og Rådets forordning programmet for et digitalt Europa for perioden 2021-2027

denne forordning, vil det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed blive det vigtigste gennemførelsesorgan for EU's finansielle ressourcer, der er afsat til cybersikkerhed under det foreslåede *program for et digitalt Europa* og *programmet Horisont Europa*.

En sådan samlet tilgang vil gøre det muligt at støtte cybersikkerhed på tværs af hele værdikæden, fra forskning til støtte til udvikling og indførelse af nøgleteknologier. Medlemsstaternes finansielle bidrag skal svare til EU's finansielle bidrag til dette initiativ og er en forudsætning for dets succes.

I betragtning af dens særlige ekspertise og brede og relevante repræsentation af interessenter bør den europæiske organisation for cybersikkerhed, som er Kommissionens modpart til det kontraktlige offentligt-private partnerskab for cybersikkerhed under Horisont 2020, indbydes til at bidrage til arbejdet i centret og netværket.

Desuden bør det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed også forsøge at skabe større synergier mellem de civile og militære dimensioner af cybersikkerhed. Det bør støtte medlemsstater og andre relevante aktører med rådgivning og udveksling af ekspertise og fremme samarbejde med hensyn til projekter og aktioner. På anmodning af medlemsstaterne kunne det også fungere som projektleder, navnlig for så vidt angår Den Europæiske Forsvarsfond. Dette initiativ tager sigte på at bidrage til håndtering af følgende problemer:

- **Utilstrækkeligt samarbejde mellem cybersikkerhedsindustrier på udbuds- og efterspørgselssiden.** De europæiske virksomheder står over for udfordringen med både fortsat at være sikre og samtidig tilbyde sikre produkter og tjenesteydelser til deres kunder. Dog er de imidlertid ofte ikke i stand til på passende vis at sikre deres eksisterende produkter, tjenester og aktiver eller til at udforme sikre innovative produkter og tjenesteydelser. Individuelle aktører, hvis hovedaktivitet ikke er knyttet til cybersikkerhed, har ofte ikke selv råd til at udvikle og etablere centrale cybersikkerhedsaktiver. Samtidig er relationerne mellem efterspørgsels- og udbudssiden af markedet for cybersikkerhed endnu ikke tilstrækkeligt udviklet, hvilket betyder, at tilvejebringelsen af europæiske produkter og løsninger, der er tilpasset de forskellige sektorers behov, ikke er optimal, og at der ikke eksisterer en utilstrækkelig grad af tillid mellem markedsaktørerne.
- **Manglende effektiv samarbejdsmekanisme mellem medlemsstaterne for industriel kapacitetsopbygning.** Der findes heller ikke i dag nogen effektiv samarbejdsmekanisme for medlemsstaterne til at arbejde sammen om at opbygge de nødvendige kapaciteter til støtte for innovation inden for cybersikkerhed på tværs af brancher og udbredelsen af avancerede europæiske cybersikkerhedsløsninger. De eksisterende samarbejdsmekanismer for medlemsstaterne inden for cybersikkerhed i direktiv (EU) 2016/1148 har ikke mandat til at tage højde for denne type aktiviteter.
- **Utilstrækkeligt samarbejde inden for og mellem forskere og erhvervsliv.** Trods Europas teoretiske kapacitet til at dække hele værdikæden inden for cybersikkerhed findes der relevante sektorer for cybersikkerhed (f.eks. energi, rumfart, forsvar, transport) og underområder, der i dag er dårligt understøttet af forskersamfundet, eller som kun støttes af et begrænset antal centre (f.eks. post-kvante- og kvantekryptografi, tillid og cybersikkerhed i KI). Selv om dette samarbejde tydeligvis eksisterer, er det meget ofte en kortsigtet, rådgivningsbaseret ordning, som ikke tillader indgåelse af langsigtede forskningsplaner til løsning af industriens udfordringer inden for cybersikkerhed.

- **Utilstrækkeligt samarbejde mellem civile og forsvarsrelaterede cybersikkerhedsforsknings- og innovationsmiljøer.** Problemet med utilstrækkelige samarbejdsniveauer vedrører også civile og forsvarsmæssige fællesskaber. De eksisterende synergier, anvendes ikke i fuld udstrækning som følge af manglende effektive mekanismer, der gør det muligt for disse fællesskaber at samarbejde effektivt og skabe tillid, hvilket i endnu højere grad end på andre områder er en forudsætning for et vellykket samarbejde. Dette kombineres med begrænsede finansielle kapaciteter på EU's marked for cybersikkerhed, herunder utilstrækkelige midler til at støtte innovation.

- **Sammenhæng med gældende regler på samme område**

Kompetencenetværket for cybersikkerhed og det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed vil fungere som en supplerende støtte til eksisterende politikbestemmelser og aktører på cybersikkerhedsområdet. Mandatet for det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed vil være et supplement til ENISA's indsats, men har et forskelligt fokus og kræver et andet sæt af færdigheder. Hvor ENISA's mandat dækker en rådgivningsfunktion for forskning og innovation inden for cybersikkerhed i EU, fokuserer kompetencecentrets foreslåede mandat først og fremmest på andre opgaver, der er vigtige for at sætte EU bedre i stand til at øge cybersikkerheden i EU. ENISA's mandat omfatter heller ikke de former for aktiviteter, som ville falde ind under kompetencecentrets og netværkets primære opgaver - at stimulere udviklingen og anvendelsen af teknologi inden for cybersikkerhed og supplere kapacitetsopbygningsindsatsen på dette område på EU-plan og på nationalt plan.

Det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed vil , sammen med kompetencenetværket for cybersikkerhed ligeledes arbejde hen imod fremme af forskning for at lette og fremskynde standardiserings- og certificeringsprocesser, navnlig dem, der vedrører cybersikkerhedscertificeringsordninger som defineret i den foreslåede forordning om cybersikkerhed[13][14].

Det foreliggende initiativ er reelt en opskalering af det offentligt-private partnerskab (OPP) om cybersikkerhed, som var det første EU-dækkende forsøg på at samle cybersikkerhedsindustrien, efterspørgselssiden (købere af cybersikkerhedsprodukter og -løsninger, herunder offentlig forvaltning og kritiske sektorer som f.eks. transport, sundhed, energi, finans) og forskersamfundet om at etablere platformen for bæredygtig dialog og skabe betingelser for frivillig medfinansiering. OPP blev oprettet i 2016 og har udløst investeringer på op til 1,8 mia. EUR frem til 2020. Men omfanget af investeringer, der er på vej i andre dele af verden (f.eks. de investerede 19 mia. USD i cybersikkerhed i USA alene i 2017) viser, at EU skal gøre mere for at opnå kritisk masse af investeringer og for at overvinde fragmenteringen af kapaciteter spredt ud over hele EU.

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

---

13 Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om ENISA, "EU's Agentur for Cybersikkerhed", om ophævelse af forordning (EU) nr. 526/2013 og om cybersikkerhedscertificering af informations- og kommunikationsteknologi ("forordningen om cybersikkerhed", COM(2017) 477 final/3).

14 Dette berører ikke certificeringsmekanismerne i henhold til den generelle databeskyttelsesforordning, hvor databeskyttelsesmyndigheder spiller en rolle, i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF ("generel forordning om databeskyttelse")

Det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed vil fungere som et fælles gennemførelsesorgan for forskellige EU-programmer til støtte for cybersikkerhed (programmet for det digitale Europa og Horisont Europa) og øge sammenhæng og synergier mellem dem.

Dette initiativ vil også give mulighed for at supplere medlemsstaternes indsats ved at tilvejebringe relevant input til uddannelsespolitiske beslutningstagere for at forbedre færdigheder i cybersikkerhed (f.eks. ved at udvikle cybersikkerhedsundervisningsplaner i civile og militære uddannelsessystemer), der skal være med til at udvikle en kvalificeret arbejdsstyrke inden for cybersikkerhed i EU - et centralt aktiv for cybersikkerhedsvirksomheder samt andre industrier, der er involveret i cybersikkerhed. For så vidt angår cybersikkerhedsuddannelse vil dette initiativ være i overensstemmelse med det igangværende arbejde med den platform for cybersikkerhedsuddannelse og cybersikkerhedsøvelser, som blev oprettet ved Det Europæiske Sikkerheds- og Forsvarsakademi.

Dette initiativ vil supplere og støtte indsatsen i de digitale innovationsknudepunkter under programmet for det digitale Europa. Digitale innovationsknudepunkter er almennyttige organisationer, der hjælper virksomheder - navnlig nystartede virksomheder, SMV'er og midcapselskaber med at blive mere konkurrencedygtige ved at forbedre deres forretnings-/produktionsprocesser, produkter og tjenesteydelser gennem intelligent innovation ved hjælp af digital teknologi. Digitale innovationsknudepunkter leverer forretningsorienterede innovationstjenester, såsom markedsoplysninger, finansieringsrådgivning, adgang til relevante test- og forsøgsfaciliteter, uddannelse og kompetenceudvikling med det formål at bidrage til, at nye produkter eller tjenester kan nå ud på markedet, eller at indføre bedre produktionsprocesser. Nogle digitale innovationsknudepunkter, med specifik cybersikkerhedsekspertise kan inddrages direkte i kompetencefællesskabet for cybersikkerhed, der oprettes ved dette initiativ. I de fleste tilfælde vil digitale innovationsknudepunkter, som ikke har nogen specifik cybersikkerhedsprofil, imidlertid lette deres aktørers adgang til den ekspertise, viden og kapacitet inden for cybersikkerhed, der findes i kompetencefællesskabet for cybersikkerhed ved at arbejde tæt sammen med netværket af nationale koordinationscentre og det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed. Digitale innovationsknudepunkter vil også kunne støtte indførelsen af innovative cybersikkerhedsprodukter og -løsninger, der lever op til behovene hos virksomheder og andre slutbrugere, de betjener. Sidst, men ikke mindst, kunne sektorspecifikke digitale innovationsknudepunkter dele deres viden om konkrete sektorspecifikke behov med netværket og centret for at bidrage til overvejelserne om den forsknings- og innovationsdagsorden, der imødekommer industriens krav.

Der vil blive tilstræbt synergier med relevante videns- og innovationsfælleskaber under Det Europæiske Institut for Innovation og Teknologi, og navnlig med EIT Digital.

2. RETSGRUNDLAG, NÆRHEDSPRINCIPPET OG PROPORTIONALITETSPRINCIPPET

• Retsgrundlag

Kompetencecentret bør oprettes på et dobbelt retsgrundlag på grund af dets art og specifikke mål. Kompetencecentret kan med udgangspunkt i artikel 187 i TEUF om oprettelse af strukturer til effektiv gennemførelse af programmerne for forskning, teknologisk udvikling og demonstration i Unionen, skabe synergier og samle ressourcer til at investere i de nødvendige kapaciteter på medlemsstatsniveau og udvikle fælles, europæiske aktiver (f.eks. ved fælles

indkøb af nødvendig cybersikkerhedstest- og forsøgsinfrastruktur). Artikel 188, stk. 1, foreskriver vedtagelsen af sådanne foranstaltninger. Ikke desto mindre ville første afsnit af artikel 188 som eneste retsgrundlag alene ikke gøre det muligt at træffe foranstaltninger, der går videre end aktiviteter inden for forskning og udvikling, som er nødvendige for at opfylde alle kompetencecentrets mål som fastsat i denne forordning til støtte for indførelsen på markedet af cybersikkerhedsprodukter og -løsninger og hjælpe den europæiske cybersikkerhedsindustri med at blive mere konkurrencedygtig og øge dens markedsandel og tilføre merværdi til den nationale indsats for at finde løsninger på kvalifikationsunderskuddet. For at nå disse mål er det nødvendigt at føje artikel 173, stk. 3, til som et retsgrundlag, som gør det muligt for EU at træffe foranstaltninger til støtte for industriens konkurrenceevne.

- **En begrundelse for forslaget set i lyset af nærheds- og proportionalitetsprincipperne**

Cybersikkerhed er et anliggende af fælles interesse i EU, som bekræftet af ovennævnte konklusioner fra Rådet. Omfanget og den grænseoverskridende karakter af hændelser såsom *WannaCry* eller *NonPetya* er et glimrende eksempel på dette. Arten og omfanget af de teknologiske udfordringer, samt utilstrækkelig koordinering af indsatsen inden for og på tværs af erhvervslivet, den offentlige sektor og forskningsverden kræver, at EU yderligere støtter koordineringsindsatser for både at samle kritisk masse af ressourcer og sikre bedre viden og forvaltning af aktiver. Dette er påkrævet på grund af de ressourcemæssige krav vedrørende visse kapaciteter for forskning i, udvikling og udbredelse af cybersikkerhed behovet for at give adgang til tværfaglig cybersikkerhedsknowhow på tværs af forskellige fagområder (ofte kun delvist tilgængelige på nationalt plan) den globale karakter af industrielle værdikæder samt aktiviteten hos globale konkurrenter, der arbejder på tværs af markederne.

Dette kræver ressourcer og ekspertise i et omfang, der næppe kan modsvares af en individuel foranstaltning i nogen medlemsstat. Eksempelvis kunne et paneuropæisk kvantekommunikationsnetværk kræve investering på ca. 900 mio. EUR, afhængigt af investeringerne fra medlemsstaterne (der skal forbindes indbyrdes/suppleres) og af i hvilket omfang teknologi giver mulighed for genbrug af eksisterende infrastrukturer. Initiativet vil være vigtigt for at samle finansiering og tillade, at denne type investeringer kommer til at foregå i EU.

Medlemsstaterne kan ikke alene nå målene med dette initiativ i fuldt omfang. Som det fremgår af ovenstående, lader de sig bedre gennemføre på EU-niveau ved at sammenlægge indsatsen, og undgå unødvendigt dobbeltarbejde, hvilket er med til at opnå kritisk masse af investeringer og sikre, at offentlige finansieringer udnyttes optimalt. I overensstemmelse med proportionalitetsprincippet går denne forordning samtidigt ikke videre, end hvad der er nødvendigt for at nå dette mål. En EU-indsats er således begrundet i nærhedsprincippet og proportionalitetsprincippet.

Dette instrument indeholder ingen nye forpligtelser for erhvervslivet. Samtidig forventes virksomheder og navnlig SMV'er at ville reducere omkostningerne til deres bestræbelser på at udforme innovative cybersikre produkter, da initiativet åbner mulighed for at sammenlægge ressourcer til at investere i de nødvendige kapaciteter på medlemsstatsplan eller udvikle fælles, europæiske aktiver (f.eks. ved fælles indkøb af nødvendige cybersikkerhedstest og forsøgsinfrastruktur). Disse aktiver kan anvendes af industrier og SMV'er på tværs af forskellige sektorer, så det sikres, at deres produkter er cybersikre, og cybersikkerhed gøres til en konkurrencefordel for dem.

- **Valg af retsakt**

Der oprettes ved det foreslåede instrument et organ til gennemførelse af cybersikkerhedsaktioner under programmet for det digitale Europa og programmet for Horisont Europa. Heri beskrives organets mandat, opgaver og forvaltningsstruktur. Oprettelsen af et sådant EU-organ kræver vedtagelse af en forordning.

3. HØRINGER AF INTERESSEREDE PARTER OG KONSEKVENSANALYSER

Forslaget om at skabe et kompetencenetværk for cybersikkerhed med et europæisk industri-, teknologi- og forskningskompetencecenter for cybersikkerhed er et nyt initiativ. Det fungerer som en videreførelse og udbygning af det offentligt-private partnerskab om cybersikkerhed, som blev oprettet i 2016.

- **Høring af interesserede parter**

Cybersikkerhed er et bredt, tværfagligt emne. Kommissionen gjorde brug af forskellige høringsmetoder for at sikre, at EU's almene interesse - i modsætning til en smal vifte af interessentgruppers særinteresser - er godt tilgodeset i dette initiativ. Denne metode sikrer gennemsigtighed og ansvarlighed i Kommissionens arbejde. Selv om der ikke blev afholdt nogen offentlig høring specielt til dette initiativ i betragtning af målgruppen (industrien og forskersamfundet og medlemsstaterne), var temaerne allerede behandlet i flere andre åbne offentlige høringer:

- en generel åben offentlig høring i 2018 om emnet investering, forskning og innovation, SMV'er og det indre marked.
- en 12-ugers online offentlig høring i 2017 for at indhente synspunkter fra offentligheden (ca. 90 deltagere) om ENISA's evaluering og revision.
- en 12-ugers online offentlig høring i 2016 i anledning af lanceringen af det kontraktlige offentligt-private partnerskab om cybersikkerhed (ca. 240 deltagere).

Kommissionen har ligeledes afholdt specifikke høringer om dette initiativ, herunder workshopper, møder og særlige anmodninger om input (fra ENISA og Det Europæiske Forsvarsagentur). Høringsperioden varede 6 måneder og med start i november 2017 frem til marts 2018. Kommissionen har også foretaget en kortlægning af ekspertisecentre, som gjorde det muligt at indsamle input fra 665 ekspertisecentre for cybersikkerhed om deres knowhow, aktivitet, arbejdsområder, internationalt samarbejde. Undersøgelsen blev lanceret i januar, og undersøgelser fremsendt senest den 8. marts 2018 indgik i rapportens analyse.

Interesserede parter fra industri- og forskersamfundene fandt, at kompetencecentret og netværket kan tilføje merværdi til den nuværende indsats på nationalt plan ved at hjælpe med til at skabe et "økosystem" for cybersikkerhed på europæisk plan, der muliggør et bedre samarbejde mellem forsknings- og erhvervskredse. De mente også, at det var nødvendigt, at EU og medlemsstaterne anlægger et proaktivt, mere langsigtet og strategisk perspektiv til cybersikkerhed i industripolitik, der går videre end blot forskning og innovation. Interessenter har udtrykt behov for at få adgang til nøglekapaciteter såsom test- og forsøgsfaciliteter og for at være mere ambitiøs med hensyn til at indhente kvalifikationsunderskuddet på cybersikkerhedsområdet, f.eks. gennem omfattende europæiske projekter, der skal tiltrække de bedste talenter. Alle ovennævnte forslag blev også fundet nødvendige for EU for at blive internationalt anerkendt som førende inden for cybersikkerhed.

Medlemsstaterne tilsluttede sig som led i de høringsaktiviteter, der er pågået siden sidste september[15] og i Rådets særlige konklusioner[16], intentionen om at etablere et kompetencenetværk for cybersikkerhed, der skal stimulere udvikling og anvendelse af cybersikkerhedsteknologier og understregede behovet for at involvere alle medlemsstater og deres eksisterende ekspertise- og kompetencecentre med særligt fokus på komplementaritet. Specifikt med hensyn til det kommende kompetencecenter understregede medlemsstaterne betydningen af dets koordinerende rolle i forbindelse med støtte til netværket. Navnlig med hensyn til nationale aktiviteter og behov inden for cyberforsvar viste kortlægningsøvelsen angående medlemsstaternes cyberforsvarsbehov, som blev udført af Tjenesten for EU's Optræden Udadtil i marts 2018, at de fleste medlemsstaterne anerkender merværdien af EU-støtte til cyberuddannelse og støtte til industrien gennem forskning og udvikling[17]. Initiativet vil blive gennemført sammen med medlemsstater eller enheder, som støttes af dem. Samarbejder mellem industri, forskning og/eller den offentlige sektor vil samle og styrke eksisterende enheder og indsatser for at etablere nye. Medlemsstaterne vil også blive inddraget i fastlæggelsen af specifikke foranstaltninger rettet mod den offentlige sektor som direkte bruger af cybersikkerhedsteknologi og -knowhow.

- **Konsekvensanalyse**

Der blev den 11. april 2017 fremsendt en konsekvensanalyse til støtte for dette projekt til Udvalget for Forskriftskontrol, som afgav en positiv udtalelse med forbehold. Konsekvensanalysen blev derefter gennemgået på baggrund af udvalgets kommentarer. Udvalgets udtalelse og det bilag, der forklarer, hvordan bestyrelsens bemærkninger er blevet behandlet, offentliggøres sammen med nærværende forslag.

Der er overvejet en række politiske løsningsmodeller i konsekvensanalysen af både lovgivningsmæssig og ikkelovgivningsmæssig art. Følgende modeller blev valgt ud til en indgående vurdering:

- Referencescenarie - Samarbejdsmodel - tager udgangspunkt i en videreførelse af den nuværende strategi for opbygning af cybersikkerhed med hensyn til industriel og teknologisk kapacitet i EU ved at støtte forskning og innovation og dermed forbundne samarbejdsmekanismer under RP9.
- Løsningsmodel 1: Kompetencenetværk for cybersikkerhed i kombination med et europæisk industri-, teknologi- og forskningskompetencecenter for cybersikkerhed med et dobbelt mandat til fremme af foranstaltninger til støtte for industrielle teknologier samt inden for forskning og innovation.
- Løsningsmodel 2: Kompetencenetværk for cybersikkerhed med et europæisk forsknings- og kompetencecenter for cybersikkerhed med fokus på forsknings- og innovationsaktiviteter

De løsningsmodeller, der blev kasseret på et tidligt tidspunkt, omfattede 1) modellen med ikke at træffe nogen foranstaltninger overhovedet, 2) modellen med kun at oprette kompetencenetværket for cybersikkerhed, 3) modellen med kun at oprette en centraliseret struktur samt 4) modellen med at bruge et eksisterende agentur (Den Europæiske Unions

[15] F.eks. rundbordsmøde på højt niveau med medlemsstaterne, næstformand Andrus Ansip, kommissær Mariya Gabriel, den 5. december 2017

[16] Rådet (almindelige anliggender): Rådets konklusioner om den fælles meddelelse til Europa-Parlamentet og Rådet: Modstandsdygtighed, afskrækkelse og forsvar: Opbygning af en stærk cybersikkerhed for EU (20. november 2017)

[17] EEAS, marts 2018

Agentur for Net- og Informationssikkerhed (ENISA), Forvaltningsorganet for Forskning (REA) eller Forvaltningsorganet for Innovation og Netværk (INEA).

Analysen konkluderede, at løsningsmodel 1 er den bedst egnede til at nå initiativets mål og samtidig sikre den størst mulige økonomiske, samfundsmæssige og miljømæssige virkning og beskyttelse af EU's interesser. De vigtigste argumenter for denne model gik på evnen til at skabe en reel cybersikkerhedsindustripolitik ved at støtte aktiviteter, der ikke kun vedrører forskning og udvikling, men også markedsintroduktion fleksibiliteten til at tillade forskellige modeller for samarbejde med netværket af kompetencecentre med henblik på at optimere anvendelsen af eksisterende viden og ressourcer evne til at strukturere samarbejdet og fælles forpligtelser for de offentlige og private aktører fra alle relevante sektorer, herunder forsvaret. Sidst, men ikke mindst, giver løsningsmodel 1 også mulighed for at øge synergierne og kan fungere som en mekanisme for gennemførelse af to forskellige EU-cyberfinansieringsstrømme under den næste flerårige finansielle ramme (programmet for det digitale Europa, Horisont Europa).

- **Grundlæggende rettigheder**

Dette initiativ vil gøre det muligt for offentlige myndigheder og virksomheder i medlemsstaterne mere effektivt at forebygge og reagere på cybertrusler ved at tilbyde og udstyre sig selv med mere sikre produkter og løsninger. Dette er særlig relevant for beskyttelsen af adgang til væsentlige tjenester (f.eks. transport, sundhed, bankvæsen og finansielle tjenesteydelser).

Øget kapacitet i EU til selvstændigt at sikre sine varer og tjenesteydelser kan ligeledes forventes at hjælpe borgerne med at udøve deres demokratiske rettigheder og værdier (f.eks. bedre beskytte deres informationsrelaterede rettigheder i chartret om grundlæggende rettigheder, navnlig retten til beskyttelse af personoplysninger og privatlivets fred) og dermed øge deres tillid til det digitale samfund og den digitale økonomi.

4. VIRKNINGER FOR BUDGETTET

Det europæiske industri-, teknologi- og forskningskompetencecenter vil i samarbejde med kompetencenetværket for cybersikkerhed være det vigtigste organ for gennemførelsen af EU's finansielle ressourcer til cybersikkerhed under programmet for det digitale Europa og Horisont Europa.

De budgetmæssige virkninger i forbindelse med gennemførelsen af det digitale Europa er beskrevet detaljeret i finansieringsoversigten, der er vedlagt dette forslag. Bidraget fra finansieringsrammen for klyngen "Rummeligt og sikkert samfund" i søjle II "Globale udfordringer og industriel konkurrenceevne" i Horisont Europa (samlet rammebeløb 2 800 000 000 EUR) omhandlet i artikel 21, stk. 1, litra b), vil blive foreslået af Kommissionen i løbet af lovgivningsprocessen, og under alle omstændigheder før der er opnået politisk enighed. Forslaget vil være baseret på resultaterne af den strategiske planlægningsproces som defineret i artikel 6, stk. 6, i forordning XXX [rammeprogrammet Horisont Europa].

5. ANDRE FORHOLD

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

En udtrykkelig bestemmelse om evaluering, som pålægger Kommissionen af foretage en uafhængig evaluering, er foreskrevet i dette forslag (artikel 38). Kommissionen rapporterer efterfølgende til Europa-Parlamentet og Rådet om evalueringen, i givet fald ledsaget af et forslag til revision, for at måle virkningen af instrumentet og dets merværdi. Kommissionens evalueringsmetode med henblik på bedre lovgivning anvendes.

Den administrerende direktør bør hvert andet år forelægge bestyrelsen en efterfølgende evaluering aktiviteterne hos det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværkets aktiviteter, jf. artikel 17 i dette forslag. Den administrerende direktør bør ligeledes udarbejde en handlingsplan, der følger op på konklusionerne på efterfølgende evalueringer, og hvert andet år aflægge en statusrapport til Kommissionen. Bestyrelsen bør være ansvarlig for at overvåge den passende opfølgning af disse konklusioner, som fastsat i artikel 16 i dette forslag.

Påståede tilfælde af fejl eller forsømmelser i forbindelse med den juridiske enheds aktiviteter kan være underlagt Den Europæiske Ombudsmands undersøgelser i overensstemmelse med traktatens artikel 228.

2018/0328 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om oprettelse af det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af nationale koordinationscentre

Europa-Kommissionens bidrag til mødet mellem lederne i Salzburg, den 19.-20. september 2018

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 188, stk. 1,

under henvisning til forslag fra Europa-Kommissionen,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg[18],

under henvisning til udtalelse fra Regionsudvalget[19],

efter den almindelige lovgivningsprocedure, og

ud fra følgende betragtninger:

(1) Vores dagligdag og økonomier bliver mere og mere afhængige af digitale teknologier, og borgerne bliver i stadig større omfang udsat for alvorlige cyberhændelser. Den fremtidige sikkerhed afhænger bl.a. af en styrkelse af den teknologiske og industrielle evne til at beskytte EU mod cybertrusler, da både den civile infrastruktur og den militære kapacitet er afhængige af sikre digitale systemer.

(2) EU har i tidens løb regelmæssigt øget sine aktiviteter med henblik på at tackle de stadig større cybersikkerhedsudfordringer efter cybersikkerhedsstrategien fra 2013[20], der havde til formål at fremme et pålideligt, sikkert og åbent cyberøkosystem. I 2016 vedtog EU de første foranstaltninger inden for cybersikkerhed gennem Europa-Parlamentets og Rådets direktiv (EU) 2016/1148[21] om sikkerhed for net- og informationssystemer.

---

18 EUT C, s. ...

19 EUT C […] af […], s. […].

20 Fælles meddelelse til Europa-Parlamentet og Rådet: EU-strategi for cybersikkerhed: Et åbent, sikkert og beskyttet cyberspace, JOIN (2013) 1 final.

21 Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

(3) I september 2017 fremlagde Kommissionen og EU's højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik en fælles meddelelse[22] "Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU" for yderligere at styrke EU's modstandsdygtighed over for, afskrækkelse af og reaktion på cyberangreb.

(4) Stats- og regeringscheferne på det digitale topmøde i Tallinn i september 2017 opfordrede EU til at blive en "global leder inden for cybersikkerhed senest i 2025 for at sikre tillid og beskyttelse af vores borgere, forbrugere og virksomheder på nettet og for at muliggøre et frit og lovstyret internet."

(5) Væsentlige nedbrud af net- og informationssystemer kan påvirke individuelle medlemsstater og EU som helhed. Sikkerheden i net- og informationssystemer er derfor afgørende for et velfungerende indre marked. På nuværende tidspunkt er EU afhængig af ikke-europæiske udbydere af cybersikkerhed. Det er i EU's strategiske interesse at sikre, at det bevarer og udvikler afgørende kapaciteter til at sikre den teknologiske cybersikkerhed på det digitale indre marked, og navnlig for at beskytte kritiske net- og informationssystemer og tilvejebringe vigtige cybersikkerhedstjenester.

(6) Der findes omfattende ekspertise og erfaring inden for cybersikkerhedsforskning, teknologisk og industriel udvikling i EU, men forskernes og erhvervslivets indsats er fragmenteret og savner tilpasning og en fælles mission, hvilket hæmmer EU's konkurrenceevne på dette område. Denne indsats og ekspertise skal samles og anvendes i netværk på en effektiv måde for at styrke og supplere eksisterende forskning, teknologisk og industriel kapacitet på EU-plan og nationalt plan.

(7) Rådets konklusioner, der blev vedtaget i november 2017, opfordrede Kommissionen til hurtigt at forelægge en konsekvensanalyse om mulighederne for at oprette et netværk af kompetencecentre for cybersikkerhed med et europæisk forsknings- og kompetencecenter og inden midten af 2018 at foreslå det relevante retlige instrument.

(8) Kompetencecentret bør være EU's vigtigste instrument for sammenlægning af investeringer i forskning, teknologisk og industriel udvikling af cybersikkerhed og for gennemførelse af relevante projekter og initiativer sammen med kompetencenetværk for cybersikkerhed. Det bør yde cybersikkerhedsrelateret finansiel støtte fra programmerne Horisont Europa og det digitale Europa og bør i givet fald være åbent for Den Europæiske Fond for Regionaludvikling og andre programmer. Denne tilgang bør bidrage til at skabe synergier og koordinering af finansiel støtte i forbindelse med forskning, innovation, teknologisk og industriel udvikling inden for cybersikkerhed og til at undgå overlapning.

(9) I betragtning af, at målene med dette initiativ bedst kan opnås, hvis alle medlemsstater eller så mange medlemsstater som muligt deltager og som et incitament for medlemsstaterne til at deltage, bør kun medlemsstater, der bidrager finansielt til kompetencecentrets administrations- og driftsomkostninger, have stemmeret.

(10) De deltagende medlemsstaters finansielle deltagelse bør stå i rimeligt forhold til EU's finansielle bidrag til initiativet.

---

[22] Fælles meddelelse til Europa-Parlamentet og Rådet, "Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU", JOIN(2017) 450 final.

(11) Kompetencecentret bør lette og fremme koordineringen af arbejdet i kompetencenetværket for cybersikkerhed ("netværket"), der består af nationale koordinationscentre i hver medlemsstat. Nationale koordinationscentre bør modtage direkte finansiel EU-støtte, herunder tilskud uden indkaldelse af forslag, med henblik på at udføre aktiviteter i forbindelse med denne forordning.

(12) Nationale koordinationscentre bør udvælges af medlemsstaterne. Ud over den nødvendige administrative kapacitet skal centrene enten råde over eller have direkte adgang til teknologisk ekspertise i cybersikkerhed, herunder især på områder som kryptering, ikt-sikkerhedstjenester, afsløring af indtrængen, systemsikkerhed, netsikkerhed, software- og applikationssikkerhed, eller de menneskelige og samfundsmæssige aspekter af sikkerhed og privatlivets fred. De bør også have kapacitet til effektivt at inddrage og koordinere med erhvervslivet, den offentlige sektor, herunder de myndigheder, der er udpeget i henhold til Europa-Parlamentets og Rådets direktiv (EU) 2016/1148[23], og forskningsverdenen.

(13) Hvis der ydes finansiel støtte til nationale koordinationscentre for at støtte tredjeparter på nationalt niveau, skal dette videregives til relevante interessenter gennem kaskadetilskudsaftaler.

(14) Nye teknologier såsom kunstig intelligens, tingenes internet, højtydende databehandling (HPC) og kvantedatabehandling, blockchain og koncepter som sikre digitale identiteter skaber både nye udfordringer for cybersikkerhed og byder samtidig på løsninger. Vurdering og validering af eksisterende eller fremtidige ikt-systemers robusthed vil kræve test af sikkerhedsløsninger mod angreb på højtydende databehandling og kvanteteknologimaskiner. Kompetencecentret, netværket og kompetencefællesskabet for cybersikkerhed bør bidrage til at fremme og formidle de seneste cybersikkerhedsløsninger. Samtidig bør kompetencecentret og netværket være tilgængeligt for udviklere og operatører i kritiske sektorer, som f.eks. transport, energi, sundhed, finans, offentlige myndigheder, telekommunikation, fremstilling, forsvar og rumfart, med det formål at hjælpe dem med at løse deres udfordringer omkring cybersikkerhed.

(15) Kompetencecentret bør have flere vigtige funktioner. For det første bør kompetencecentret lette og bidrage til koordineringen af arbejdet i det europæiske kompetencenetværk for cybersikkerhed og fremme kompetencefællesskabet for cybersikkerhed. Centret bør fremme den teknologiske dagsorden for cybersikkerhed og lette adgangen til ekspertise i netværket og kompetencefællesskabet for cybersikkerhed. For det andet bør det gennemføre relevante dele af programmet for det digitale Europa og Horisont Europa, typisk ved at yde tilskud efter indkaldelse af forslag. For det tredje bør kompetencecentret fremme fælles investeringer fra EU, medlemsstaterne og/eller industrien.

(16) Kompetencecentret bør stimulere og støtte samarbejdet og samordningen af aktiviteterne i kompetencefællesskabet for cybersikkerhed, hvilket vil omfatte en stor, åben og forskelligartet gruppe af aktører, der er involveret i teknologi vedrørende cybersikkerhed. Dette fællesskab bør navnlig omfatte forskningsenheder, udbudsbaserede industrier, efterspørgselsbaserede industrier, samt den offentlige sektor. Kompetencefællesskabet for cybersikkerhed bør bidrage til kompetencecentrets

[23] Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

aktiviteter og arbejdsplan, og det bør også kunne trække på kompetencecentrets og netværkets aktiviteter for udvikling af fællesskaber, men bør i øvrigt ikke nyde nogen fortrinsstilling i forbindelse med indkaldelser af forslag eller udbud.

(17) For at imødekomme behovene hos industrier på både efterspørgsels- og udbudssiden bør kompetencecentrets opgave med at levere viden om og teknisk bistand vedrørende cybersikkerhed til industrier omfatte både ikt-produkter og tjenesteydelser samt alle andre industrielle og teknologiske produkter og løsninger, hvor cybersikkerhed skal forankres.

(18) Selv om kompetencecentret og netværket bør tilstræbe synergier mellem civile og forsvarsrelaterede områder for cybersikkerhed, vil projekter finansieret af Horisont Europa-programmet blive gennemført i overensstemmelse med forordning XXX [forordningen om Horisont Europa], i henhold til hvilken forsknings- og innovationsaktiviteter, der gennemføres under Horisont Europa-programmet, skal være rettet mod civile anvendelsesformål.

(19) For at sikre et struktureret og bæredygtigt samarbejde bør forholdet mellem kompetencecentret og de nationale koordinationscentre være baseret på en kontraktmæssig aftale.

(20) Der bør fastsættes passende bestemmelser, der skal garantere kompetencecentrets ansvar og gennemsigtighed.

(21) I betragtning af deres respektive ekspertise inden for cybersikkerhed bør Kommissionens Fælles Forskningscenter og Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) spille en aktiv rolle i kompetencenetværket for cybersikkerhed og det industrielle og videnskabelige rådgivende organ.

(22) Hvis de modtager et finansielt bidrag fra EU's almindelige budget, bør de nationale koordinationscentre og enheder, som er en del af kompetencenetværket for cybersikkerhed gøre opmærksom på, at de pågældende aktiviteter udføres i forbindelse med det aktuelle initiativ.

(23) EU's bidrag til kompetencecentret bør finansiere halvdelen af udgifterne til oprettelse, administration og koordinering af kompetencecentret. For at undgå dobbelt finansiering bør disse aktiviteter ikke samtidigt modtage bidrag fra andre EU-programmer.

(24) Kompetencecentrets bestyrelse, der er sammensat af medlemmer fra medlemsstaterne og Kommissionen, bør fastlægge de overordnede retningslinjer for kompetencecentrets drift og sikre, at centret udfører sine opgaver i overensstemmelse med denne forordning. Bestyrelsen bør have de nødvendige beføjelser til at fastlægge budgettet, kontrollere dets gennemførelse, vedtage passende finansielle bestemmelser, fastlægge gennemsigtige arbejdsprocedurer for beslutningsprocessen i kompetencecentret, vedtage kompetencecentrets arbejdsprogram og flerårige strategiske plan, som bør afspejle prioriteterne om at nå kompetencecentrets mål, vedtage sin egen forretningsorden, udnævne den administrerende direktør og træffe afgørelse om forlængelse af den administrerende direktørs embedsperiode og om ophævelse heraf.

(25) For at kompetencecentret kan fungere korrekt og effektivt, bør Kommissionen og medlemsstaterne sikre, at personer, der udpeges til bestyrelsen, har passende faglig ekspertise og erfaring inden for de relevante områder. Kommissionen og medlemsstaterne bør bestræbe sig på at begrænse udskiftningen af deres repræsentanter i bestyrelsen med henblik på at sikre kontinuiteten i dens arbejde.

(26) For at kompetencecentret skal fungere problemfrit, kræver det, at den administrerende direktør udnævnes på grundlag af kvalifikationer og dokumenterede administrative og ledelsesmæssige færdigheder samt kvalifikationer og erfaring, der er relevante for cybersikkerhed, og at den administrerende direktørs opgaver udføres i fuld uafhængighed.

(27) Kompetencecentret bør have et industrielt og videnskabeligt rådgivende organ, der kan sørge for en løbende dialog med den private sektor, forbrugerorganisationerne og andre relevante interessenter. Det industrielle og videnskabelige rådgivende organ bør fokusere på spørgsmål, der er relevante for interessenter, og forelægge dem for kompetencecentrets bestyrelse. Det industrielle og videnskabelige rådgivende organs sammensætning og de pålagte opgaver, f.eks. at blive hørt om arbejdsprogrammet, bør sikre tilstrækkelig repræsentation af interessenter i kompetencecentrets arbejde.

(28) Kompetencecentret bør nyde godt af det særlige sagkundskab og interessenternes brede og relevante repræsentation opbygget gennem det kontraktlige offentligt-private partnerskab om cybersikkerhed under Horisont 2020, via dets industrielle og videnskabelige rådgivende organ.

(29) Kompetencecentret bør vedtage regler for forebyggelse og håndtering af interessekonflikter. Kompetencecentret bør ligeledes følge de relevante EU-bestemmelser om aktindsigt som fastlagt i Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001[24]. Kompetencecentrets behandling af personoplysninger vil være omfattet af Europa-Parlamentets og Rådets forordning (EU) nr. XXX/2018. Kompetencecentret bør overholde de bestemmelser, der gælder for EU-institutionerne samt national lovgivning vedrørende behandling af oplysninger, herunder navnlig følsomme ikkeklassificerede oplysninger og EU-klassificerede oplysninger.

(30) EU's og medlemsstaternes finansielle interesser bør beskyttes ved hjælp af forholdsmæssige foranstaltninger under hele udgiftscyklussen, herunder ved forebyggelse, afsløring og efterforskning af uregelmæssigheder, inddrivelse af tabte, uberettiget udbetalte eller ukorrekt anvendte midler, og i givet fald anvendelse af administrative og finansielle sanktioner i overensstemmelse med Europa-Parlamentets og Rådets forordning XXX (EU, Euratom)[25] [finansforordningen].

(31) Kompetencecentret bør fungere på en åben og gennemsigtig måde og forelægge alle relevante oplysninger inden for en rimelig frist samt fremme dets aktiviteter, herunder gennem kommunikations- og formidlingsaktiviteter rettet mod offentligheden. Forretningsordenen for organerne i kompetencecentret bør gøres offentligt tilgængelige.

(32) Kommissionens interne revisor bør udøve samme beføjelser over for kompetencecentret som dem, han er tillagt over for Kommissionen.

(33) Kommissionen, kompetencecentret, Revisionsretten og Det Europæiske Kontor for Bekæmpelse af Svig bør have adgang til alle nødvendige oplysninger og lokaler med henblik på at gennemføre revisioner og undersøgelser af tilskud, kontrakter og aftaler indgået af kompetencecentret.

---

[24] Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 af 30. maj 2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter (EFT L 145 af 31.5.2001, s. 43).

[25] [Tilføj titel og EUT-reference]

(34) Da målene for denne forordning, nemlig at fastholde og udvikle EU's teknologiske og industrielle kapacitet på cybersikkerhedsområdet, øge konkurrenceevnen i EU's cybersikkerhedsindustri og gøre cybersikkerhed til en konkurrencefordel for EU's øvrige industrier, ikke i tilstrækkelig grad kan opfyldes af medlemsstaterne på grund af den omstændighed, at de nuværende, begrænsede ressourcer er spredt, samt på grund af omfanget af den nødvendige investering, men bedre kan gennemføres på EU-plan for at undgå unødig overlapning af disse bestræbelser og bidrage til at opnå kritisk masse af investeringer og sikre, at de offentlige midler udnyttes bedst muligt, kan EU derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke ud over, hvad der er nødvendigt for at nå dette mål —

VEDTAGET DENNE FORORDNING:

KAPITEL I

GENERELLE BESTEMMELSER OG PRINCIPPER FOR KOMPETENCECENTRET OG NETVÆRKET

Artikel 1

Genstand

1. Ved denne forordning oprettes det europæiske industri-, teknologi- og forskningskompetencecenter ("kompetencecentret") samt netværket af nationale koordinationscentre, og der fastsættes regler for udpegelsen af nationale koordinationscentre samt for oprettelsen af kompetencenetværket for cybersikkerhed.
2. Kompetencecentret skal bidrage til gennemførelsen af cybersikkerhedsdelen i programmet for det digitale Europa oprettet ved forordning nr. XXX og navnlig aktionerne i tilknytning til artikel 6 i forordning (EU) nr. XXX [programmet for det digitale Europa] samt i Horisont Europa-programmet oprettet ved forordning XXX og navnlig afsnit 2.2.6 i søjle II i bilag I. i afgørelse nr. XXX om særprogrammet til gennemførelse af Horisont Europa - rammeprogrammet for forskning og innovation [ref. nummer i særprogrammet].
3. Kompetencecentrets hovedsæde placeres i [Bruxelles, Belgien.]
4. Kompetencecentret har status som juridisk person. Det skal i alle medlemsstater nyde den mest vidtgående rets- og handleevne, der kan tilkomme juridiske personer i henhold til lovgivningen i denne medlemsstat. Det kan i særdeleshed erhverve eller afhænde fast ejendom og løsøre og optræde som part i retssager.

Artikel 2

Definitioner

I denne forordning forstås ved:

(1) "cybersikkerhed": beskyttelse af net- og informationssystemer, deres brugere og andre personer mod cybertrusler

(2) "cybersikkerhedsprodukter og -løsninger": ikt-produkter, -tjenester eller -processer med det specifikke formål at beskytte net- og informationssystemer, deres brugere og berørte personer mod cybertrusler

(3) "offentlig myndighed": en statslig eller anden offentlig forvaltning, herunder offentlige rådgivende organer, på nationalt, regionalt eller lokalt niveau eller enhver fysisk eller juridisk person, der udøver offentlige administrative funktioner i henhold til national ret, herunder konkrete opgaver

(4) "deltagende medlemsstat": en medlemsstat, som frivilligt bidrager finansielt til kompetencecentrets administrations- og driftsomkostninger.

Artikel 3

Centrets og netværkets mission

1. Kompetencecentret og netværket skal bistå EU med at:

   (a) bevare og udvikle de teknologiske og industrielle kapaciteter vedrørende cybersikkerhed, der er nødvendige for at sikre det digitale indre marked

   (b) øge EU's cybersikkerhedsindustris konkurrenceevne og gøre cybersikkerhed til en konkurrencemæssig fordel for andre industrier i EU.

2. Kompetencecentret skal, hvor det er relevant, udføre sine opgaver i samarbejde med netværket af nationale koordinationscentre og et kompetencefællesskab for cybersikkerhed.

Artikel 4

Centrets mål og opgaver

Kompetencecentret har følgende mål og opgaver i forbindelse hermed:

1. at fremme og koordinere arbejdet i de nationale koordinationscentres netværk ("netværket") som omhandlet i artikel 6, og i kompetencefællesskabet for cybersikkerhed som omhandlet i artikel 8

2. at bidrage til gennemførelsen af cybersikkerhedsdelen i programmet for det digitale Europa oprettet ved forordning nr. XXX[26] og navnlig aktionerne i tilknytning til artikel 6 i forordning (EU) nr. XXX [programmet for det digitale Europa] samt i Horisont Europa-programmet oprettet ved forordning nr. XXX[27] og navnlig afsnit 2.2.6 i søjle II i bilag I. i afgørelse nr. XXX om særprogrammet til gennemførelse af Horisont Europa — rammeprogrammet for forskning og innovation [ref. nummer i særprogrammet] og andre EU-programmer, når det er fastsat i EU-retsakter]

3. at forbedre de cybersikkerhedskapaciteter, den viden og den infrastruktur, der står til rådighed for virksomheder, den offentlige sektor og forskningsverdenen, ved at udføre følgende opgaver:

   (a) under henvisning til de nyeste industri- og forskningsinfrastrukturer for cybersikkerhed og tjenester i tilknytning hertil at erhverve, opgradere, drive og stille sådanne infrastrukturer og tjenester i forbindelse hermed til

[26] [indsæt fuldstændig titel og EUT-henvisning]
[27] [indsæt fuldstændig titel og EUT-henvisning]

rådighed for en bred vifte af brugere i hele EU fra erhvervslivet, herunder SMV'er, den offentlige sektor og forsknings- og videnskabskredse

(b) under henvisning til de nyeste industri- og forskningsinfrastrukturer for cybersikkerhed og tjenester i tilknytning hertil at yde støtte til andre enheder, herunder finansielt, at erhverve, opgradere, drive og stille sådanne infrastrukturer og tjenester i forbindelse hermed til rådighed for en bred vifte af brugere i hele EU fra erhvervslivet, herunder SMV'er, den offentlige sektor og forsknings- og videnskabskredse

(c) at levere viden om og teknisk bistand vedrørende cybersikkerhed til erhvervslivet og offentlige myndigheder, især ved at støtte initiativer, der tager sigte på at lette adgangen til den ekspertise, der er til rådighed inden for netværket og kompetencenetværket for cybersikkerhed

4. at bidrage til udbredelse af avancerede cybersikkerhedsprodukter og -løsninger i hele økonomien ved at udføre følgende opgaver:

(a) stimulere forskning i og udvikling af cybersikkerhed og offentlige myndigheders og brugerindustriers udnyttelse af EU's cybersikkerhedsprodukter og -løsninger

(b) hjælpe de offentlige myndigheder, industrier på efterspørgselssiden og andre brugere med at indføre og integrere de seneste cybersikkerhedsløsninger

(c) støtte især offentlige myndigheder med tilrettelæggelsen af deres offentlige indkøb eller gennemførelse af deres køb af avancerede cybersikkerhedsprodukter og -løsninger på offentlige myndigheders vegne

(d) yde finansiel støtte og teknisk bistand til nystartede cybersikkerhedsvirksomheder og SMV'er med henblik på at komme i kontakt med potentielle markeder og tiltrække investeringer

5. at forbedre forståelsen af internetsikkerhed og bidrage til at indhente kvalifikationsunderskuddet i EU vedrørende cybersikkerhed ved at udføre følgende opgaver:

(a) støtte videreudviklingen af færdigheder inden for cybersikkerhed sammen med relevante EU-agenturer og -organer, herunder ENISA, hvor det er relevant

6. at bidrage til at styrke forskning i og udvikling i EU af cybersikkerhed ved at:

(a) yde finansiel støtte til indsatser for forskning i cybersikkerhed på grundlag af en fælles, løbende evalueret og forbedret flerårig strategisk, industriel, teknologisk og forskningsmæssig dagsorden

(b) støtte omfattende forsknings- og demonstrationsprojekter i teknologiske kompetencer inden for næstegenerationscybersikkerhed i samarbejde med industrien og netværket

(c) støtte forskning og innovation med henblik på standardisering inden for cybersikkerhedsteknologi

7. at styrke samarbejdet mellem civilbeskyttelses- og forsvarsområdet med hensyn til anvendelse af teknologier med dobbelt anvendelsesformål inden for cybersikkerhed ved at udføre følgende opgaver:

   (a) støtte medlemsstater og aktører på industri- og forskningsområdet med hensyn til forskning, udvikling og udbredelse

   (b) bidrage til samarbejdet mellem medlemsstater ved at støtte uddannelse og øvelser

   (c) samle interessenter med det formål at skabe synergier mellem forskning og markeder for cybersikkerhed inden for civilbeskyttelse og forsvar

8. at styrke synergierne mellem civilbeskyttelses- og forsvarsdimensionerne af cybersikkerhed i forbindelse med Den Europæiske Forsvarsfond ved udførelsen af følgende opgaver:

   (a) yde rådgivning og udveksle ekspertise og fremme samarbejde mellem relevante interessenter

   (b) forvalte multinationale cyberforsvarsprojekter, når medlemsstaterne anmoder herom, og således fungere som projektleder i henhold til forordning XXX [forordningen om oprettelse af Den Europæiske Forsvarsfond].

Artikel 5

Investering i og brug af infrastrukturer, kapaciteter, produkter eller løsninger

1. Hvis kompetencecentret finansierer infrastrukturer, kapaciteter, produkter eller løsninger i henhold til artikel 4, stk. 3, og stk. 4 i form af et tilskud eller en præmie, kan kompetencecentrets arbejdsplan navnlig indeholde følgende oplysninger:

   (a) regler for driften af en infrastruktur eller kapacitet, og hvor det er relevant også overdragelse af driften til en værtsenhed på grundlag af kriterier, som kompetencecentret fastlægger

   (b) regler for adgang til og brug af en infrastruktur eller kapacitet.

2. Kompetencecentret kan være ansvarligt for den overordnede gennemførelse af relevante fælles indkøb, herunder prækommercielle indkøb på vegne af netværkets medlemmer, medlemmer af kompetencefællesskabet for cybersikkerhed, eller andre tredjeparter, der repræsenterer brugere af cybersikkerhedsprodukter og -løsninger. Med henblik herpå kan kompetencecentret bistås af et eller flere nationale koordinationscentre eller medlemmer af kompetencenetværket for cybersikkerhed.

Artikel 6

Udpegelse af nationale koordinationscentre

1. Senest den [dato] skal hver medlemsstat udpege den enhed, der skal fungere som det nationale koordinationscenter i forbindelse med denne forordning og give Kommissionen meddelelse herom.

2. På grundlag af en vurdering af, om virksomheden opfylder kriterierne i stk. 4, træffer Kommissionen en afgørelse inden for 6 måneder fra den udnævnelse, som medlemsstaten har fremsendt om akkreditering af enheden som et nationalt

koordinationscenter eller afvisning af udnævnelsen. Listen over nationale koordinationscentre offentliggøres af Kommissionen.

3. Medlemsstaterne kan til enhver tid indstille en ny enhed som det nationale koordinationscenter med henblik på denne forordning. Stk. 1 og 2 finder anvendelse på udpegelsen af en ny enhed.

4. Det udpegede nationale koordinationscenter skal kunne støtte kompetencecentret og netværket med at opfylde deres mission, der er fastsat i denne forordnings artikel 3. De skal råde over eller have direkte adgang til teknologisk ekspertise inden for cybersikkerhed og være i stand til effektivt at inddrage og koordinere med erhvervslivet, den offentlige sektor og forskningsverdenen.

5. Forholdet mellem kompetencecentret og de nationale koordinationscentre skal være baseret på en kontraktmæssig aftale indgået mellem kompetencecentret og hvert af de nationale koordinationscentre. Aftalen skal fastsætte regler for forholdet og fordelingen af opgaver mellem kompetencecentret og hvert nationalt koordinationscenter.

6. De nationale koordinationscentres netværk består af alle de nationale koordinationscentre, som er udpeget af medlemsstaterne.

Artikel 7

De nationale koordinationscentres opgaver

1. De nationale koordinationscentre skal have følgende opgaver:

   (a) støtte kompetencecentret med at opfylde dets mål og navnlig at koordinere kompetencecentret for cybersikkerhed

   (b) lette industriens og andre aktørers deltagelse på medlemsstatsniveau i grænseoverskridende projekter

   (c) bidrage, sammen med kompetencecentret, til at identificere og møde sektorspecifikke industrielle udfordringer vedrørende cybersikkerhed

   (d) fungere som kontaktpunkt på nationalt plan for cybersikkerhed og kompetencenetværk for cybersikkerhed og kompetencecentret

   (e) tilstræbe at skabe synergivirkninger med relevante aktiviteter på nationalt og regionalt plan

   (f) gennemføre specifikke aktioner, som kompetencecentret har ydet tilskud til, herunder ved ydelse af finansiel støtte til tredjeparter i overensstemmelse med artikel 204 i forordning XXX [ny finansforordning] på de betingelser, der er fastsat i de pågældende tilskudsaftaler.

   (g) fremme og formidle relevante resultater af arbejdet i netværket, kompetencefællesskabet for cybersikkerhed og kompetencecentret på nationalt eller regionalt niveau

   (h) vurdere anmodninger fra enheder, der er etableret i samme medlemsstat som koordinationscentret, om at blive en del af kompetencefællesskabet for cybersikkerhed.

2. Med henblik på litra f) kan finansiel støtte til tredjeparter ydes i en af de former, der er omhandlet i artikel 125 forordning XXX [ny finansforordning], herunder i form af engangsbeløb.

3. Nationale koordinationscentre kan modtage et tilskud fra EU i overensstemmelse med artikel 195, litra d), i forordning XXX [ny finansforordning] i forbindelse med udførelsen af de opgaver, der er fastsat i denne artikel.

4. De nationale koordinationscentre skal, hvor det er relevant, samarbejde via netværket med henblik på gennemførelsen af opgaver, der er omhandlet i litra a), b), c), e) og g) i stk. 1.

Artikel 8

Kompetencefællesskabet for cybersikkerhed

1. Kompetencefællesskabet for cybersikkerhed skal bidrage til kompetencecentrets opgaver som fastsat i artikel 3 og styrke og formidle cybersikkerhedsekspertise i hele EU.

2. Kompetencefællesskabet for cybersikkerhed skal bestå af industrielle, akademiske og almennyttige forskningsorganisationer og sammenslutninger samt offentlige organer og andre enheder, der beskæftiger sig med operationelle og tekniske spørgsmål. Det skal samle de vigtigste aktører med hensyn til teknologisk og industriel kapacitet for cybersikkerhed i EU. Det omfatter nationale koordinationscentre samt EU-institutioner og -organer med relevant ekspertise.

3. Kun enheder, der er etableret i EU, kan blive akkrediteret som medlemmer af kompetencecentret for cybersikkerhed. De skal påvise, at de har ekspertise inden for cybersikkerhed på mindst et af følgende områder:

   (a) forskning

   (b) industriel udvikling

   (c) uddannelse

4. Kompetencecentret skal akkreditere enheder etableret i henhold til national lovgivning som medlemmer af kompetencefællesskabet for cybersikkerhed efter en vurdering foretaget af det nationale koordinationscenter i den medlemsstat, hvor enheden er etableret, af, hvorvidt den pågældende enhed opfylder kriterierne i stk. 3. En akkreditering skal ikke være tidsbegrænset, men kan til enhver tid tilbagekaldes af kompetencecentret, hvis det eller de relevante nationale koordinationscentre mener, at enheden ikke opfylder kriterierne i stk. 3, eller den falder ind under de relevante bestemmelser i artikel 136 i forordning XXX [ny finansforordning].

5. Kompetencecentret akkrediterer relevante organer, agenturer og kontorer i EU som medlemmer af kompetencefællesskabet for cybersikkerhed efter en vurdering af, om denne enhed opfylder kriterierne i stk. 3. En akkreditering skal ikke være tidsbegrænset, men kan til enhver tid tilbagekaldes af kompetencecentret, hvis det mener, at enheden ikke opfylder kriterierne i stk. 3, eller den er omfattet af de relevante bestemmelser i artikel 136 i forordning XXX [ny finansforordning].

6. Kommissionens repræsentanter kan deltage i fællesskabets arbejde.

Artikel 9

Medlemmerne af kompetencecentret for cybersikkerhed og deres opgaver

Medlemmerne af kompetencefællesskabet for cybersikkerhed skal:

(1) støtte kompetencecentret i at udføre de opgaver og nå de mål, der er fastsat i artikel 3 og 4, og med henblik herpå arbejde tæt sammen med kompetencecentret og de relevante nationale koordinationscentre

(2) deltage i aktiviteter, der fremmes af kompetencecentret og nationale koordinationscentre

(3) i givet fald deltage i arbejdsgrupper nedsat af bestyrelsen for kompetencecentret med det formål at udføre særlige aktiviteter som fastsat af kompetencecentrets arbejdsplan

(4) i givet fald støtte kompetencecentret og de nationale koordinationscentre med at fremme specifikke projekter

(5) fremme og formidle relevante resultater af de aktiviteter og projekter, der gennemføres i fællesskabet.

Artikel 10

Kompetencecentrets samarbejde med EU's institutioner, organer, kontorer og agenturer

1. Kompetencecentret samarbejder med EU's relevante institutioner, organer, kontorer og agenturer, herunder Den Europæiske Unions Agentur for Net- og Informationssikkerhed, IT-Beredskabsenheden (CERT-EU), Tjenesten for EU's Optræden Udadtil, Det Fælles Forskningscenter under Kommissionen, Forvaltningsorganet for Forskning, Forvaltningsorganet for Innovation og Netværk, Det Europæiske Center for Bekæmpelse af Cyberkriminalitet hos Europol samt Det Europæiske Forsvarsagentur.

2. Dette samarbejde finder sted inden for rammerne af samarbejdsordninger. Disse ordninger skal forelægges Kommissionen til forhåndsgodkendelse.

KAPITEL II

KOMPETENCECENTRETS OPBYGNING

Artikel 11

Medlemskab og struktur

1. Medlemmerne af kompetencecentret er EU, repræsenteret ved Kommissionen, samt medlemsstaterne.

2. Kompetencecentrets struktur omfatter:

(a) en bestyrelse, der varetager de i artikel 13 omhandlede opgaver

(b) en administrerende direktør, der varetager de i artikel 16 omhandlede opgaver

(c) et industrielt og videnskabeligt rådgivende organ, der varetager de i artikel 20 omhandlede funktioner.

AFDELING I

BESTYRELSEN

Artikel 12

Bestyrelsens sammensætning

1. Bestyrelsen består af en repræsentant for hver medlemsstat samt fem repræsentanter for Kommissionen, på vegne af EU.
2. Hvert medlem af bestyrelsen har en suppleant, der repræsenterer dem i deres fravær.
3. Medlemmerne af bestyrelsen og deres suppleanter udpeges på grundlag af deres viden inden for teknologi samt relevante ledelsesmæssige, administrative og budgetmæssige færdigheder. Kommissionen og medlemsstaterne bestræber sig på at begrænse udskiftningen af deres repræsentanter i bestyrelsen med henblik på at sikre kontinuitet i bestyrelsens arbejde. Kommissionen og medlemsstaterne tilstræber at opnå en ligelig repræsentation af mænd og kvinder i bestyrelsen.
4. Medlemmer af bestyrelsen og deres suppleanter udnævnes for en fireårig periode, der kan fornys.
5. Medlemmerne af bestyrelsen handler i kompetencecentrets interesse, idet de fremmer centrets mål og mission, identitet, autonomi og sammenhæng på uafhængig og gennemsigtig vis.
6. Kommissionen kan indbyde observatører, herunder repræsentanter fra de relevante EU-organer, -kontorer og -agenturer, til at deltage i bestyrelsens møder, hvis det er relevant.
7. Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) skal være permanent observatør i bestyrelsen.

Artikel 13

Bestyrelsens opgaver

1. Bestyrelsen har det overordnede ansvar for den strategiske orientering og driften af kompetencecentret og fører tilsyn med gennemførelsen af dets aktiviteter.
2. Bestyrelsen vedtager sin forretningsorden, som omfatter specifikke procedurer til at afdække og undgå interessekonflikter og sikre fortrolig behandling af følsomme oplysninger.
3. Bestyrelsen skal træffe de nødvendige strategiske beslutninger, navnlig om at:
   (a) vedtage en flerårig strategiplan, med en redegørelse for kompetencecentrets vigtigste prioriterede områder og planlagte initiativer, herunder et skøn over finansieringsbehovet og -kilderne
   (b) vedtage kompetencecentrets arbejdsplan, årsregnskab og resultatopgørelse samt den årlige aktivitetsrapport på grundlag af et forslag fra den administrerende direktør
   (c) vedtage de finansielle bestemmelser for kompetencecentret i overensstemmelse med [finansforordningens artikel 70]
   (d) vedtage en procedure for udnævnelse af den administrerende direktør
   (e) vedtage kriterierne og procedurerne for vurdering og akkreditering af de enheder, som er medlemmer af kompetencefællesskabet for cybersikkerhed

(f) udnævne, afskedige, forlænge ansættelsesperioden for og udstikke retningslinjerne for den administrerende direktør og overvåge dennes resultater samt at udnævne regnskabsføreren

(g) vedtage kompetencecentrets årlige budget, herunder stillingsfortegnelsen med angivelse af antallet af midlertidige stillinger i hver ansættelsesgruppe og lønklasse samt antallet af kontraktansatte og udstationerede nationale eksperter udtrykt i fuldtidsækvivalenter

(h) vedtage regler vedrørende interessekonflikter

(i) nedsætte arbejdsgrupper med medlemmer af kompetencefællesskabet for cybersikkerhed

(j) udpege medlemmer til det industrielle og videnskabelige rådgivende organ

(k) oprette en intern revisionsfunktion i overensstemmelse med Kommissionens delegerede forordning (EU) nr. 1271/2013[28]

(l) promovere kompetencecentret på verdensplan med henblik på at øge dets tiltrækningskraft og gøre det til et organ i verdensklasse, der repræsenterer ekspertise inden for cybersikkerhed

(m) fastlægge kompetencecentrets kommunikationspolitik efter anbefaling fra den administrerende direktør

(n) være ansvarlig for at overvåge den passende opfølgning af konklusionerne af efterfølgende evalueringer

(o) i givet fald fastlægge gennemførelsesbestemmelser for personalevedtægten og ansættelsesvilkårene i henhold til artikel 31, stk. 3

(p) i givet fald fastsætte bestemmelser for udstationering af nationale eksperter til kompetencecentret og for anvendelsen af praktikanter i overensstemmelse med artikel 32, stk. 2

(q) vedtage sikkerhedsregler for kompetencecentret

(r) vedtage en strategi til bekæmpelse af svig, som står i forhold til risikoen for svig under hensyntagen til en cost-benefit-analyse af de foranstaltninger, der skal gennemføres

(s) indføre metoden for beregning af det finansielle bidrag fra medlemsstaterne

(t) påtage sig ansvaret for enhver opgave, der ikke specifikt tildeles et bestemt organ i kompetencecentret bestyrelsen kan overdrage disse opgaver til en hvilken som helst person i kompetencecentret

Artikel 14

Formanden og møder i bestyrelsen

1. Bestyrelsen vælger en formand og en næstformand blandt sine medlemmer med stemmeret for en periode på to år. Formandens og næstformandens mandat kan forlænges én gang, efter en afgørelse truffet af bestyrelsen. Hvis deres medlemskab

[28] Kommissionens delegerede forordning (EU) nr. 1271/2013 af 30. september 2013 om rammefinansforordningen for de organer, der er omhandlet i artikel 208 i Europa-Parlamentets og Rådets forordning (EU, Euratom) nr. 966/2012 (EUT L 328 af 7.12.2013, s. 42).

af bestyrelsen ophører på et tidspunkt under mandatperioden, udløber deres mandatperiode dog automatisk den samme dato. Næstformanden træder uden videre i stedet for formanden, hvis denne er forhindret i at udøve sit hverv. Formanden deltager i afstemningen.

2. Bestyrelsen afholder ordinært møde mindst tre gange om året. Den kan afholde ekstraordinære møder på opfordring fra Kommissionen eller på anmodning af en tredjedel af alle dens medlemmer, på anmodning af formanden eller på anmodning af den administrerende direktør i forbindelse med udførelsen af dennes opgaver.

3. Den administrerende direktør deltager i drøftelserne, medmindre bestyrelsen beslutter noget andet, men har ikke stemmeret. Bestyrelsen kan fra sag til sag indbyde andre personer til at deltage i sine møder som observatører.

4. Medlemmer af det industrielle og videnskabelige rådgivende organ kan efter invitation fra formanden deltage i bestyrelsens møder uden stemmeret.

5. Medlemmerne af bestyrelsen og deres suppleanter kan, medmindre andet er fastsat i dens forretningsorden, bistås af rådgivere eller eksperter.

6. Kompetencecentret varetager sekretariatsopgaverne for bestyrelsen.

Artikel 15

Bestyrelsens afstemningsregler

1. EU har 50 % af stemmerettighederne. EU's stemmerettigheder er udelelige.

2. Hver deltagende medlemsstat skal have én stemme.

3. Bestyrelsen træffer sine beslutninger med et flertal på mindst 75 % af alle stemmer, herunder fraværende medlemmers stemmer, der mindst repræsenterer 75 % af det samlede finansielle bidrag til kompetencecentret. Det finansielle bidrag vil blive beregnet på grundlag af de anslåede udgifter, som er foreslået af de medlemsstater, der er omhandlet i artikel 17, stk. 2, og baseret på rapporten om værdien af bidragene fra de deltagende medlemsstater, der er omhandlet i artikel 22, stk. 5.

4. Kun repræsentanterne for Kommissionen og de deltagende medlemsstaters repræsentanter har stemmeret.

5. Formanden deltager i afstemningen.

AFSNIT II

DEN ADMINISTRERENDE DIREKTØR

Artikel 16

Udnævnelse, afskedigelse eller forlængelse af tjenesteperioden for den administrerende direktør

1. Direktøren er en person med ekspertise og et godt omdømme inden for de områder, kompetencecentret opererer på.

2. Den administrerende direktør ansættes i en stilling som midlertidigt ansat ved kompetencecentret i henhold til artikel 2, litra a), i ansættelsesvilkårene for de øvrige ansatte.

3. Den administrerende direktør udnævnes af bestyrelsen ud fra en liste over kandidater, som Kommissionen foreslår, på baggrund af en åben og gennemsigtig udvælgelsesprocedure.

4. Med henblik på indgåelsen af kontrakten med den administrerende direktør repræsenteres kompetencecentret af formanden for bestyrelsen.

5. Den administrerende direktør udnævnes for fire år. Ved udgangen af denne periode foretager Kommissionen en vurdering, der tager evalueringen af den administrerende direktørs resultater og kompetencecentrets fremtidige opgaver og udfordringer op til overvejelse.

6. Bestyrelsen kan på forslag fra Kommissionen, der tager udgangspunkt i den i stk. 5 omhandlede vurdering, forlænge den administrerende direktørs mandatperiode med højst fire år.

7. En administrerende direktør, hvis mandatperiode er blevet forlænget, kan ikke deltage i endnu en udvælgelsesprocedure til samme stilling.

8. Den administrerende direktør kan kun afskediges ved en afgørelse truffet af bestyrelsen efter forslag fra Kommissionen.

Artikel 17

Den administrerende direktørs opgaver

1. Den administrerende direktør er ansvarlig for driften og den daglige ledelse af kompetencecentret og skal være dets retlige repræsentant. Den administrerende direktør er ansvarlig over for bestyrelsen og udfører sine opgaver i fuld uafhængighed inden for rammerne af de beføjelser, denne har fået overdraget.

2. Den administrerende direktør skal navnlig varetage følgende opgaver i fuld uafhængighed:

   (a) gennemføre afgørelser vedtaget af bestyrelsen

   (b) støtte bestyrelsen i dens arbejde og sørge for sekretariatsbistand i forbindelse med dens møder samt forsyne den med alle de oplysninger, der er nødvendige for udførelsen af dens opgaver

   (c) efter samråd med bestyrelsen og Kommissionen udarbejde og med henblik på vedtagelse forelægge bestyrelsen udkastet til den flerårige strategiplan og kompetencecentrets årlige arbejdsprogram, herunder omfanget af indkaldelser af forslag, indkaldelser af interessetilkendegivelser og indkaldelser af bud, der er nødvendige for at gennemføre arbejdsplanen og de tilhørende anslåede udgifter på forslag af medlemsstaterne og Kommissionen

   (d) udarbejde og med henblik på vedtagelse forelægge bestyrelsen udkastet til det årlige budget, herunder stillingsfortegnelsen med angivelse af antallet af midlertidige stillinger i hver funktionsgruppe og lønklasse samt antallet af kontraktansatte og udstationerede nationale eksperter udtrykt i fuldtidsækvivalenter

   (e) gennemføre arbejdsprogrammet og aflægge rapport til bestyrelsen herom

   (f) udarbejde et udkast til den årlige aktivitetsrapport om kompetencecentret, herunder oplysninger om de tilsvarende udgifter

(g) sikre gennemførelsen af effektive overvågnings- og evalueringsprocedurer knyttet til udøvelsen af kompetencecentret

(h) udarbejde en handlingsplan, der følger op på konklusionerne på efterfølgende evalueringer, og aflægge en statusrapport til Kommissionen hvert andet år

(i) forberede, forhandle og indgå aftaler med de nationale koordinationscentre

(j) være ansvarlig for administrative, finansielle og personalemæssige spørgsmål, herunder gennemførelsen af kompetencecentrets budget, under hensyntagen til rådgivning fra den interne revisionsfunktion, inden for rammerne af bestyrelsens delegation af beføjelser

(k) godkende og forvalte iværksættelsen af indkaldelser af forslag i henhold til arbejdsplanen og forvalte støtteaftalerne og -afgørelserne

(l) godkende fortegnelsen over aktioner, der er udvalgt til at modtage støtte på grundlag af en prioriteringsliste udarbejdet af en jury bestående af uafhængige eksperter

(m) godkende og forvalte iværksættelsen af indkaldelser af bud i overensstemmelse med arbejdsplanen og forvalte aftalerne

(n) godkende de bud, der er udvalgt til at modtage støtte

(o) indsende udkastet til årsregnskab og balance til den interne revisionsfunktion, og efterfølgende til bestyrelsen

(p) sikre, at der foretages risikovurdering og risikostyring

(q) underskrive individuelle støtteaftaler og afgørelser og kontrakter

(r) underskrive indkøbsaftaler

(s) udarbejde en handlingsplan som opfølgning på konklusionerne i interne eller eksterne auditrapporter samt undersøgelser fra Det Europæiske Kontor for Bekæmpelse af Svig (OLAF) og aflægge statusrapport to gange om året til Kommissionen og regelmæssigt til bestyrelsen

(t) udarbejde udkast til finansielle bestemmelser for kompetencecentret

(u) etablere og opretholde et velfungerende og effektivt internt kontrolsystem og indberette alle betydelige ændringer heraf til bestyrelsen

(v) sikre effektiv kommunikation med EU's institutioner

(w) træffe enhver anden foranstaltning, der er nødvendig for at vurdere kompetencecentrets fremskridt mod sin mission og mål som fastsat i artikel 3 og 4 i denne forordning;

(x) varetage alle andre opgaver, der er tildelt eller delegeret til denne af bestyrelsen.

AFSNIT III

DET INDUSTRIELLE OG VIDENSKABELIGE RÅDGIVENDE ORGAN

Artikel 18

Sammensætningen af det industrielle og videnskabelige rådgivende organ

1. Det industrielle og videnskabelige rådgivende organ består af højst 16 medlemmer. Medlemmerne udnævnes af bestyrelsen blandt repræsentanterne for enhederne i kompetencefællesskabet for cybersikkerhed.

2. Medlemmer af det industrielle og videnskabelige rådgivende organ skal have erfaring med hensyn til cybersikkerhed, industriel udvikling, liberale tjenesteydelser eller anvendelsen heraf. Kravene til en sådan ekspertise skal præciseres yderligere af bestyrelsen.

3. Procedurerne for udnævnelse af medlemmerne af bestyrelsen og det rådgivende organs drift skal specificeres i kompetencecentrets forretningsorden og offentliggøres.

4. Mandatperioden for medlemmerne af det industrielle og videnskabelige rådgivende organ er tre år, der kan fornys.

5. Repræsentanter for Kommissionen og Det Europæiske Agentur for Net- og Informationssikkerhed kan deltage i og støtte arbejdet i det industrielle og videnskabelige rådgivende organ.

Artikel 19

Den industrielle og videnskabelige rådgivende organs funktion

1. Det industrielle og videnskabelige rådgivende organ mødes mindst to gange om året.

2. Det industrielle og videnskabelige rådgivende organ kan rådgive bestyrelsen om nedsættelsen af arbejdsgrupper om særlige forhold af relevans for kompetencecentrets arbejde, om nødvendigt med overordnede koordinering forestået af et eller flere medlemmer af det industrielle og videnskabelige rådgivende organ.

3. Det industrielle og videnskabelige rådgivende organ vælger en formand.

4. Det industrielle og videnskabelige rådgivende organ fastsætter selv sin forretningsorden, herunder udnævnelsen af repræsentanter, der repræsenterer det rådgivende organ, hvor det er relevant, og varigheden af deres udnævnelse.

Artikel 20

Det industrielle og videnskabelige rådgivende organs opgaver

Det industrielle og videnskabelige rådgivende organ rådgiver kompetencecentret med hensyn til udførelsen af dets aktiviteter og skal:

(1) give den administrerende direktør og bestyrelsen strategisk rådgivning og input til udarbejdelsen af arbejdsplanen og flerårige strategiske plan inden for de tidsfrister, der er fastlagt af bestyrelsen

(2) afholde offentlige høringer, som er åbne for alle offentlige og private berørte parter med interesser inden for cybersikkerhed for at indsamle bidrag til den i stk. 1 anførte strategiske rådgivning

(3) fremme og indsamle feedback om kompetencecentrets arbejdsprogram og flerårige strategiske plan.

KAPITEL III

FINANSIELLE BESTEMMELSER

Artikel 21

EU's finansielle bidrag

1. EU's bidrag til kompetencecentret til dækning af administrationsomkostninger og driftsomkostninger omfatter følgende:

   (a) 1 981 668 000 EUR fra programmet for det digitale Europa, herunder op til 23 746 000 EUR til administrationsomkostninger

   (b) et beløb fra Horisont Europa-programmet, herunder administrationsomkostninger, fastsættes under hensyntagen til den strategiske planlægningsproces, der skal gennemføres i henhold til artikel 6, stk. 6, i forordning XXX [Horisont Europa-forordningen].

2. EU's maksimale bidrag betales over bevillingerne i EU's almindelige budget, der er afsat til [Digital Europa] og til særprogrammet til gennemførelse Horisont Europa, oprettet ved afgørelse XXX.

3. Kompetencecentret gennemfører cybersikkerhedstiltag i [programmet for det digitale Europa] og [Horisont Europa-programmet] i overensstemmelse med litra c), nr. iv), i artikel 62, i forordning (EU, Euratom) XXX[29] [finansforordningen].

4. EU's finansielle bidrag må ikke omfatte de opgaver, der er omhandlet i artikel 4, stk. 8, litra b)

Artikel 22

De deltagende medlemsstaters bidrag

1. De deltagende medlemsstater yder et samlet bidrag til kompetencecentrets driftsomkostninger og administrationsomkostninger af mindst samme størrelsesorden som de i artikel 21, stk. 1, i denne forordning anførte.

2. Med henblik på at vurdere de bidrag, der er nævnt i stk. 1 og i litra b), nr. ii), i artikel 23, stk. 3, fastlægges omkostningerne i overensstemmelse med de berørte medlemsstaters sædvanlige praksis for omkostningsberegning, de regnskabsstandarder, som gælder i den pågældende medlemsstat, og de relevante internationale regnskabsstandarder og International Financial Reporting Standards. Omkostningerne attesteres af en uafhængig ekstern revisor, som udpeges af den pågældende medlemsstat. Værdiansættelsesmetoden kan kontrolleres af kompetencecentret, hvis der er usikkerhedsmomenter vedrørende attesteringen.

3. Såfremt en deltagende medlemsstat undlader at overholde sine forpligtelser vedrørende sit finansielle bidrag, meddeler den administrerende direktør dette skriftligt og fastsætter en rimelig frist, inden for hvilken misligholdelsen skal bringes til ophør. Såfremt situationen ikke afhjælpes inden fristens udløb, indkalder den administrerende direktør til et bestyrelsesmøde med henblik på at beslutte, om det misligholdende medlem skal fratages sin stemmeret, eller hvorvidt der skal træffes andre foranstaltninger, indtil medlemmet overholder sine forpligtelser. Det misligholdende medlems stemmerettigheder suspenderes, indtil misligholdelsen er afhjulpet.

4. Kommissionen kan indstille, forholdsmæssigt nedsætte eller suspendere, EU's finansielle bidrag til kompetencecentret, såfremt de deltagende medlemsstater ikke

[29] [indsæt fuldstændig titel og EUT-henvisning]

bidrager, kun bidrager delvist eller bidrager for sent med de bidrag, der er omhandlet i stk. 1.

5. De deltagende medlemsstater meddeler senest den 31. januar hvert år bestyrelsen værdien af de bidrag, der er nævnt i stk. 1, som er ydet i hvert af de foregående regnskabsår.

Artikel 23

Kompetencecentrets omkostninger og indtægter

1. Kompetencecentret finansieres i fællesskab af EU og medlemsstaterne via finansielle bidrag, der betales i rater, og bidrag bestående af omkostninger, som de nationale koordinationscentre og støttemodtagere afholder i forbindelse med gennemførelsen af aktioner, som ikke refunderes af kompetencecentret.

2. Kompetencecentrets administrationsomkostninger må ikke overstige [beløb] EUR og dækkes gennem finansielle bidrag, som på årsbasis fordeles ligeligt mellem EU og de deltagende medlemsstater. Hvis en del af bidraget til administrationsomkostninger ikke anvendes, kan det stilles til rådighed til dækning af kompetencecentrets driftsomkostninger.

3. Kompetencecentrets driftsomkostninger dækkes over følgende bidrag:

   (a) EU's finansielle bidrag

   (b) bidrag fra de deltagende medlemsstater i form af:

      i) finansielle bidrag og

      ii) i givet fald bidrag i naturalier fra de deltagende medlemsstater til nationale koordinationscentres og støttemodtageres omkostninger i forbindelse med gennemførelsen af indirekte aktioner, med fradrag af bidraget fra kompetencecentret og alle andre EU-bidrag til disse omkostninger.

4. Kompetencecentrets ressourcer, der er indført i dets budget, består af følgende bidrag:

   (a) de deltagende medlemsstaters finansielle bidrag til administrationsomkostningerne

   (b) de deltagende medlemsstaters finansielle bidrag til driftsomkostningerne

   (c) eventuelle indtægter genereret af kompetencecentret

   (d) eventuelle andre finansielle bidrag, ressourcer og indtægter.

5. Eventuelle renter af de bidrag, der betales til kompetencecentret af de deltagende medlemsstater, betragtes som tilhørende kompetencecentret

6. Alle kompetencecentrets indtægter og dets aktiviteter bidrager til at nå de mål, der er fastsat i artikel 4.

7. Kompetencecentret ejer alle aktiver, som det genererer, eller som overføres til det med det formål at opfylde dets målsætninger.

8. Undtagen når kompetencecentret likvideres, udbetales eventuelle overskud i indtægterne i forhold til udgifterne ikke til de deltagende medlemmer af kompetencecentret.

Artikel 24

Finansielle forpligtelser

Kompetencecentrets finansielle forpligtelser må ikke overstige værdien af de finansielle ressourcer, der er til rådighed, eller som medlemmerne har afsat til dets budget.

Artikel 25

Regnskabsår

Regnskabsåret løber fra den 1. januar til den 31. december.

Artikel 26

Opstilling af budgettet

1. Hvert år udarbejder den administrerende direktør et udkast til overslag over kompetencecentrets indtægter og udgifter for det følgende regnskabsår og forelægger det for bestyrelsen, ledsaget af et udkast til stillingsfortegnelse. Der skal være balance mellem indtægter og udgifter. Kompetencecentrets udgifter omfatter udgifter til personale, administration, infrastruktur og drift. Administrative udgifter skal holdes på et minimum.
2. Hvert år udarbejder bestyrelsen på grundlag af udkastet til overslag over indtægter og udgifter, der er omhandlet i stk. 1, et overslag over indtægter og udgifter for kompetencecentret for det følgende regnskabsår.
3. Bestyrelsen fremsender senest den 31. januar hvert år det i stk. 2 nævnte overslag, der skal være en del af udkastet til det samlede programmeringsdokument, til Kommissionen.
4. På grundlag af dette overslag opfører Kommissionen i forslaget til EU's budget de overslag, den skønner nødvendige for stillingsfortegnelsen, og de tilskud, der skal ydes over det almindelige budget, som den forelægger Europa-Parlamentet og Rådet i overensstemmelse med artikel 313 og 314 i TEUF.
5. Europa-Parlamentet og Rådet godkender bevillingerne til bidraget til kompetencecentret.
6. Europa-Parlamentet og Rådet vedtager kompetencecentrets stillingsfortegnelse.
7. Bestyrelsen vedtager centrets budget, sammen med arbejdsplanen. Det bliver endeligt efter den endelige vedtagelse af EU's almindelige budget. Om nødvendigt afpasser bestyrelsen kompetencecentrets budget og arbejdsprogram i overensstemmelse med EU's almindelige budget.

Artikel 27

Præsentation af kompetencecentrets regnskaber og decharge

Præsentation af kompetencecentrets foreløbige og endelige regnskaber og decharge skal følge reglerne og tidsplanen i finansforordningen og i dens finansielle bestemmelser, der vedtages i overensstemmelse med artikel 29.

Artikel 28

Operationel og finansiel rapportering

1. Den administrerende direktør rapporterer årligt til bestyrelsen om varetagelsen af vedkommendes opgaver i overensstemmelse med kompetencecentrets finansielle bestemmelser.

2. Senest to måneder efter hvert regnskabsårs afslutning forelægger den administrerende direktør med henblik på godkendelse bestyrelsen en årlig aktivitetsrapport om de fremskridt, som kompetencecentret har gjort i det foregående kalenderår, navnlig med hensyn til arbejdsplanen for det pågældende år. Denne rapport skal bl.a. omfatte oplysninger om følgende:

   (a) operationelle aktioner, der gennemføres, og de tilhørende udgifter

   (b) de indsendte forslag til aktioner fordelt efter deltagertype, herunder SMV'er, og efter medlemsstat

   (c) de aktioner, der er udvalgt til at modtage støtte, fordelt på deltagertype, herunder SMV'er, og efter medlemsstat og angivelse af kompetencecentrets bidrag til de enkelte deltagere og aktioner

   (d) fremskridt mod opfyldelsen af målsætningerne i artikel 4 og forslag til yderligere nødvendigt arbejde med henblik på at nå disse mål.

3. Når bestyrelsen har godkendt den årlige aktivitetsrapport, gøres den offentligt tilgængelig.

Artikel 29

Finansielle regler

Kompetencecentret vedtager særlige finansielle regler i overensstemmelse med artikel 70 i forordning XXX [ny finansforordning].

Artikel 30

Beskyttelse af finansielle interesser

1. Kompetencecentret træffer passende foranstaltninger for at sikre, at når foranstaltninger finansieret i henhold til denne forordning gennemføres, er EU's økonomiske interesser beskyttet ved at anvende forebyggende foranstaltninger mod svig, korruption og enhver anden ulovlig aktivitet, gennem effektiv kontrol og, hvis der konstateres uregelmæssigheder, gennem inddrivelse af uretmæssigt udbetalte beløb, og i givet fald ved hjælp af effektive, forholdsmæssige og afskrækkende administrative sanktioner.

2. Kompetencecentret giver Kommissionens personale og andre personer med tilladelse fra Kommissionen samt Revisionsretten adgang til sine lokaler og til al information, herunder i elektronisk form, som er nødvendig for at gennemføre revisionerne.

3. Det Europæiske Kontor for Bekæmpelse af Svig (OLAF) kan udføre undersøgelser, herunder kontrol og inspektion på stedet, i overensstemmelse med bestemmelserne og procedurerne i Rådets forordning (Euratom, EF) nr. 2185/96[30] og Europa-

[30] Rådets forordning (Euratom, EF) nr. 2185/96 af 11. november 1996 om Kommissionens kontrol og inspektion på stedet med henblik på beskyttelse af De Europæiske Fællesskabers finansielle interesser mod svig og andre uregelmæssigheder (EFT L 292 af 15.11.1996, s. 2).

Parlamentets og Rådets forordning (EU, Euratom) nr. 883/2013[31] med henblik på at fastslå, om der foreligger svig, korruption eller andre ulovlige aktiviteter, der påvirker EU's finansielle interesser i forbindelse med en tilskudsaftale eller en kontrakt, der direkte eller indirekte er finansieret i overensstemmelse med denne forordning.

4. Med forbehold af stk. 1, 2 og 3 i denne artikel, indeholder kontrakter og aftaler om tilskud som følge af gennemførelsen af denne forordning bestemmelser, der udtrykkeligt bemyndiger Kommissionen, kompetencecentret, Revisionsretten og OLAF til at gennemføre sådanne revisioner og undersøgelser i overensstemmelse med deres respektive beføjelser. Hvis gennemførelsen af en aktion uddelegeres eller videredelegeres, helt eller delvis, eller hvis den kræver indgåelse af en kontrakt om offentligt indkøb eller finansiel støtte til tredjemand, indeholder kontrakten eller tilskudsaftalen kontrahentens eller tilskudsmodtagerens forpligtelse til at kræve, at alle involverede tredjeparter udtrykkelig accepterer Kommissionens, kompetencecentrets, Revisionsrettens og OLAF's beføjelser.

KAPITEL IV

KOMPETENCECENTRETS ANSATTE

Artikel 31

Personale

1. Vedtægten for tjenestemænd og ansættelsesvilkårene for de øvrige ansatte i Den Europæiske Union som fastlagt i Rådets forordning (EØF, Euratom, EKSF) nr. 259/68[32] ("personalevedtægten" og "ansættelsesvilkårene") og de regler, der i fællesskab er vedtaget af Den Europæiske Unions institutioner med henblik på anvendelsen af vedtægten og ansættelsesvilkårene, finder anvendelse på kompetencecentrets ansatte.

2. Bestyrelsen udøver med hensyn til kompetencecentrets ansatte de beføjelser, som vedtægten tillægger ansættelsesmyndigheden, og de beføjelser, som ansættelsesvilkårene tillægger den myndighed, der er beføjet til at indgå ansættelseskontrakter ("ansættelsesmyndighedsbeføjelser").

3. I overensstemmelse med artikel 110 i personalevedtægten vedtager bestyrelsen i medfør af artikel 2, stk. 1, i personalevedtægten og artikel 6 i ansættelsesvilkårene en beslutning, der tillægger den administrerende direktør de relevante ansættelsesmyndighedsbeføjelser og opstiller betingelserne for at suspendere denne delegation. Den administrerende direktør har bemyndigelse til at uddelegere disse beføjelser.

---

31 Europa-Parlamentets og Rådets forordning (EU, Euratom) nr. 883/2013 af 11. september 2013 om undersøgelser, der foretages af Det Europæiske Kontor for Bekæmpelse af Svig (OLAF) og om ophævelse af Europa-Parlamentets og Rådets forordning (EF) nr. 1073/1999 og Rådets forordning (Euratom) nr. 1074/1999 (EUT L 248 af 18.9.2013, s. 1).

32 Rådets forordning (EØF, Euratom, EKSF) nr. 259/68 af 29. februar 1968 om vedtægten for tjenestemænd i De europæiske Fællesskaber og om ansættelsesvilkårene for de øvrige ansatte i disse Fællesskaber samt om særlige midlertidige foranstaltninger for tjenestemænd i Kommissionen (EFT L 56 af 4.3.1968, s. 1).

4. Under helt særlige omstændigheder kan bestyrelsen ved afgørelse midlertidigt suspendere de ansættelsesmyndighedsbeføjelser, der er uddelegeret til den administrerende direktør, og enhver efterfølgende uddelegering af sidstnævnte. I sådanne tilfælde udøver bestyrelsen selv ansættelsesmyndighedsbeføjelserne eller uddelegerer dem til et af sine medlemmer eller til en medarbejder i kompetencecentret, der ikke er den administrerende direktør.

5. Bestyrelsen vedtager gennemførelsesbestemmelser til personalevedtægten og ansættelsesvilkårene i overensstemmelse med personalevedtægtens artikel 110.

6. Personaleressourcerne fastlægges i stillingsfortegnelsen for kompetencecentret, med angivelse af antallet af midlertidige stillinger i hver stillingsgruppe og lønklasse samt antallet af kontraktansatte udtrykt i fuldtidsækvivalenter i tråd med dets årlige budget.

7. Kompetencecentrets personale består af midlertidigt ansatte og kontraktansatte.

8. Alle personaleomkostninger afholdes af kompetencecentret.

Artikel 32

Udstationerede nationale eksperter og andet personale

1. Kompetencecentret kan gøre brug af udstationerede nationale eksperter eller andre medarbejdere, der ikke er ansat af kompetencecentret.

2. Bestyrelsen vedtager efter aftale med Kommissionen en beslutning om fastlæggelse af bestemmelser om udstationering af nationale eksperter til kompetencecentret.

Artikel 33

Privilegier og immuniteter

Protokol nr. 7 vedrørende Den Europæiske Unions privilegier og immuniteter, der er knyttet som bilag til traktaten om Den Europæiske Union og til traktaten om Den Europæiske Unions funktionsmåde, finder anvendelse på kompetencecentret og dets personale.

KAPITEL V

FÆLLES BESTEMMELSER

Artikel 34

Sikkerhedsregler

1. Artikel 12, stk. 7, i forordning (EU) nr. XXX [programmet for det digitale Europa] finder anvendelse på deltagelse i alle aktioner, som finansieres af kompetencecentret.

2. Følgende særlige sikkerhedsregler finder anvendelse på aktioner, der finansieres af Horisont Europa-programmet:

   (a) med henblik på artikel 34, stk. 1 [Ejerskab og beskyttelse] i forordning (EU) nr. XXX [Horisont Europa], når dette er fastsat i arbejdsplanen, kan udstedelse af ikke-eksklusive licenser begrænses til tredjeparter, der er etableret eller anses for at være etableret i medlemsstater og kontrolleret af medlemsstaterne og/eller statsborgere i medlemsstaterne

(b) med henblik på artikel 36, stk. 4, litra b) (Overførsel og licensudstedelse] i forordning (EU) nr. XXX [Horisont Europe], skal overdragelse eller licens til en juridisk enhed, der er etableret i et associeret land eller etableret i EU, men kontrolleret fra tredjelande, også være grund til at modsætte sig overdragelse af ejendomsretten til resultaterne, eller overdragelse af en eksklusivlicens vedrørende resultater

(c) i henhold til artikel 37, stk. 3, litra a) [Adgangsret] i forordning (EU) nr. XXX [Horisont Europe], når dette er fastsat i arbejdsplanen, kan indrømmelse af adgang til resultater og baggrundsviden begrænses til en juridisk enhed, der er etableret eller anses for at være etableret i medlemsstater og kontrolleret af medlemsstaterne og/eller statsborgere i medlemsstaterne.

Artikel 35

Gennemsigtighed

1. Kompetencecentret gennemfører sine aktiviteter med en høj grad af åbenhed.

2. Kompetencecentret sikrer, at offentligheden og eventuelle interesserede parter får passende, objektive, pålidelige og let tilgængelige oplysninger, navnlig med hensyn til resultaterne af dets arbejde. Det offentliggør også interesseerklæringer afgivet i overensstemmelse med artikel 41.

3. Bestyrelsen kan efter forslag fra den administrerende direktør tillade interesserede parter at følge gennemførelsen af nogle af kompetencecentrets aktiviteter.

4. Kompetencecentret fastsætter i sin forretningsorden de nærmere bestemmelser for gennemførelse af gennemsigtighedsregler, der er omhandlet i stk. 1 og 2. For aktioner finansieret fra Horisont Europa vil det tage behørigt hensyn til bestemmelserne i bilag III i Horisont Europa-forordningen.

Artikel 36

Sikkerhedsregler for beskyttelse af klassificerede oplysninger og ikkeklassificerede følsomme oplysninger

1. Uden at dette berører artikel 35, må kompetencecentret ikke til tredjeparter videregive oplysninger, som det behandler eller modtager, og for hvilke der foreligger en begrundet begæring om hel eller delvis fortrolig behandling.

2. Medlemmerne af bestyrelsen, den administrerende direktør, medlemmerne af det industrielle og videnskabelige rådgivende organ, eksterne eksperter, der deltager i ad hoc-arbejdsgrupper, samt medlemmer af centrets personale, skal overholde fortrolighedskravene i artikel 339 i traktaten om Den Europæiske Unions funktionsmåde, selv efter at deres hverv er ophørt.

3. Kompetencecentrets bestyrelse vedtager kompetencecentrets sikkerhedsregler, efter Kommissionens godkendelse, på grundlag af de principper og regler, der er fastsat i Kommissionens sikkerhedsforskrifter til beskyttelse af EU-klassificerede oplysninger (EUCI) og følsomme ikkeklassificerede oplysninger, herunder bl.a. bestemmelserne

vedrørende behandling og opbevaring af sådanne oplysninger som fastsat i Kommissionens afgørelse (EU, Euratom) 2015/443[33] og 2015/444[34].

4. Kompetencecentret kan træffe alle nødvendige foranstaltninger for at lette udvekslingen af oplysninger, der er relevante for dets opgaver, med Kommissionen og medlemsstaterne og i givet fald de relevante EU-agenturer og -organer. Administrative ordninger, der er indgået med henblik herpå til udveksling af EU's klassificerede informationer eller, i mangel af en sådan ordning, ekstraordinær ad hoc-videregivelse af EU's klassificerede informationer skal forhåndsgodkendes af Kommissionen.

Artikel 37

Aktindsigt

1. Forordning (EF) nr. 1049/2001 finder anvendelse på dokumenter, der opbevares af kompetencecentret.

2. Bestyrelsen vedtager ordninger for gennemførelse af forordning (EF) nr. 1049/2001 senest seks måneder efter oprettelsen af kompetencecentret.

3. Afgørelser truffet af kompetencecentret i henhold til artikel 8 i forordning (EF) nr. 1049/2001 kan gøres til genstand for en klage til ombudsmanden i henhold til artikel 228 i traktaten om Den Europæiske Unions funktionsmåde eller indbringes for Den Europæiske Unions Domstol i henhold til artikel 263 i traktaten om Den Europæiske Unions funktionsmåde.

Artikel 38

Overvågning, evaluering og revision

1. Kompetencecentret sikrer, at dets aktiviteter, herunder de aktiviteter, der forvaltes gennem de nationale koordinationscentre og netværk, underkastes løbende og systematisk overvågning og regelmæssig evaluering. Kompetencecentret sikrer, at data for overvågning af programmets gennemførelse og resultater indsamles effektivt og rettidigt, og at der skal pålægges modtagere af EU-midler og medlemsstaterne proportionalitet i rapporteringskravene. Resultaterne af evalueringen offentliggøres.

2. Når der foreligger tilstrækkelige oplysninger om gennemførelsen af denne forordning, og senest tre og et halvt år efter indledningen af gennemførelsen af denne forordning, foretager Kommissionen en foreløbig evaluering af kompetencecentret. Kommissionen udarbejder en rapport om denne evaluering og forelægger senest den 31. December 2024 denne rapport for Europa-Parlamentet og Rådet. Kompetencecentret og medlemsstaterne sender Kommissionen de oplysninger, der er nødvendige for udarbejdelsen af denne rapport.

3. Den i stk. 2 omhandlede evaluering skal omfatte en vurdering af de resultater, der er opnået gennem kompetencecentret, under hensyntagen til dets mål, mandat og opgaver. Såfremt Kommissionen finder, at en videreførelse af kompetencecentret er

[33] Kommissionens afgørelse (EU, Euratom) 2015/443 af 13. marts 2015 om sikkerhedsbeskyttelse i Kommissionen (EUT L 72 af 17.3.2015, s. 41).

[34] Kommissionens afgørelse (EU, Euratom) 2015/444 af 13. marts 2015 om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer (EUT L 72 af 17.3.2015, s. 53).

berettiget i forhold til de tildelte målsætninger, mandat og opgaver, kan den foreslå, at varigheden af kompetencecentrets mandat i henhold til artikel 46 forlænges.

4. På baggrund af konklusioner fra den foreløbige evaluering som omhandlet i stk. 2 kan Kommissionen handle i overensstemmelse med [artikel 22, stk. 5,] eller træffe andre passende foranstaltninger.

5. Overvågning, evaluering, udfasning og fornyelse af bidraget fra Horisont Europa skal følge bestemmelserne i artikel 8, 45 og 47 og bilag III i Horisont Europa-forordningen og vedtagne gennemførelsesbestemmelser.

6. Overvågning, rapportering og evaluering af bidraget fra det digitale Europa skal følge bestemmelserne i artikel 24 og 25 i programmet for det digitale Europa.

7. I tilfælde af afvikling af kompetencecentret foretager Kommissionen en endelig evaluering af kompetencecentret inden for seks måneder efter kompetencecentrets afvikling, dog senest to år efter udløsningen af afviklingsproceduren som omhandlet i denne forordnings artikel 46. Resultaterne af denne endelige evaluering forelægges for Europa-Parlamentet og Rådet.

Artikel 39

Kompetencecentrets ansvar

1. Kompetencecentrets ansvar i kontraktforhold reguleres efter den lovgivning, der finder anvendelse på den pågældende aftale, afgørelse eller kontrakt.

2. Hvad angår ansvar uden for kontraktforhold, erstatter kompetencecentret i overensstemmelse med de almindelige retsgrundsætninger, der er fælles for medlemsstaternes retssystemer, skader forvoldt af dets ansatte under udøvelsen af deres hverv.

3. Kompetencecentrets betalinger som følge af et erstatningsansvar som omhandlet i stk. 1 og 2 samt omkostninger og udgifter i denne forbindelse anses for kompetencecentrets udgifter og afholdes af dets midler.

4. Kompetencecentret er eneansvarligt for at opfylde sine forpligtelser.

Artikel 40

Den Europæiske Unions Domstols kompetence og lovvalg

1. Den Europæiske Unions Domstol har kompetence:

   (1) i henhold til eventuelle voldgiftsbestemmelser i aftaler, beslutninger eller kontrakter indgået af kompetencecentret

   (2) i tvister vedrørende erstatning for skader forårsaget af personale af kompetencecentret under udøvelsen af deres hverv

   (3) ved enhver tvist mellem kompetencecentret og dets personale inden for de grænser og på de betingelser, der er fastsat i vedtægten.

2. Med hensyn til anliggender, som ikke er omfattet af denne forordning eller andre EU-retsakter, finder lovgivningen i den medlemsstat anvendelse, hvor kompetencecentrets hjemsted er beliggende

Artikel 41

Medlemmernes ansvar og forsikring

1. Medlemmernes økonomiske ansvar for kompetencecentrets gæld er begrænset til det bidrag, de allerede har ydet til de administrative omkostninger.
2. Kompetencecentret skal tegne en passende forsikring.

Artikel 42

Interessekonflikter

Kompetencecentrets bestyrelse vedtager bestemmelser om forebyggelse og håndtering af interessekonflikter i forhold til dets medlemmer, organer og personale. Disse regler skal indeholde bestemmelser, som har til hensigt at undgå interessekonflikter hos repræsentanterne for de medlemmer, der sidder i bestyrelsen og det videnskabelige og industrielle rådgivende organ i overensstemmelse med forordning XXX [ny finansforordning].

Artikel 43

Beskyttelse af personoplysninger

1. Kompetencecentrets behandling af personoplysninger sker i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. XXX/2018.
2. Bestyrelsen vedtager gennemførelsesbestemmelser, som omhandlet i artikel xx, stk. 3, i forordning (EU) nr. xxx/2018. Bestyrelsen kan vedtage supplerende foranstaltninger, der er nødvendige for kompetencecentrets anvendelse af forordning (EU) nr. xxx/2018.

Artikel 44

Støtte fra værtsmedlemsstaten

Der kan indgås en administrativ aftale mellem kompetencecentret og medlemsstaten [Belgien], hvor det har hjemsted, angående privilegier og immuniteter og anden støtte, som denne medlemsstat skal yde kompetencecentret.

KAPITEL VII

AFSLUTTENDE BESTEMMELSER

Artikel 45

Indledende foranstaltninger

1. Kommissionen har ansvaret for oprettelsen og den indledende drift af kompetencecentret, indtil det har operativ kapacitet til at gennemføre sit eget budget. Kommissionen gennemfører i overensstemmelse med EU-retten alle nødvendige foranstaltninger i samarbejde med kompetencecentrets kompetente organer.
2. Med henblik på stk. 1 kan Kommissionen, indtil den administrerende direktør tiltræder sin stilling efter at være blevet udnævnt af bestyrelsen i overensstemmelse

med artikel 16, udpege en midlertidig administrerende direktør og udføre de opgaver, som er overdraget den administrerende direktør, der kan bistås af et begrænset antal tjenestemænd fra Kommissionen. Kommissionen kan udpege et begrænset antal af sine tjenestemænd midlertidigt.

3. Den midlertidige administrerende direktør kan anvise alle betalinger, som er omfattet af bevillingerne i kompetencecentrets årlige budget, når bestyrelsen har godkendt dem, og kan indgå kontrakter, beslutninger og aftaler, herunder ansættelseskontrakter efter vedtagelsen af kompetencecentrets stillingsfortegnelse.

4. Den midlertidige administrerende direktør skal efter aftale med den administrerende direktør for kompetencecentret og med forbehold for bestyrelsens godkendelse, fastsætte den dato, hvor kompetencecentret har kapacitet til at gennemføre sit eget budget. Fra og med denne dato afholder Kommissionen sig fra at indgå forpligtelser og foretage betalinger for kompetencecentrets aktiviteter.

Artikel 46

Varighed

1. Kompetencecentret oprettes for perioden fra den 1. januar 2021 til den 31. december 2029.

2. Ved udløbet af denne frist udløses afviklingsproceduren, medmindre andet besluttes ved en revision af denne forordning. Afviklingsproceduren udløses automatisk, hvis EU eller alle deltagende medlemsstater trækker sig fra kompetencecentret.

3. Til at forestå afviklingen af kompetencecentret udpeger bestyrelsen en eller flere likvidatorer, som handler i overensstemmelse med bestyrelsens afgørelser.

4. Når kompetencecentret afvikles, skal dets aktiver anvendes til at dække dets forpligtelser og udgifterne til afviklingen. Et eventuelt overskud fordeles mellem EU og de deltagende medlemsstater i forhold til deres finansielle bidrag til kompetencecentret. Et eventuelt overskud, der tilfalder EU, tilbageføres til EU's budget.

Artikel 47

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 alle medlemsstater.

Udfærdiget i Bruxelles, 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) inden for ABM/ABB-strukturen

1,3. Forslagets/initiativets art

1,4. Mål

1,5. Forslagets/initiativets begrundelse

1,6. Varighed og finansielle virkninger

1,7. Påtænkt(e) forvaltningsmetode(r)

2. FORVALTNINGSFORANSTALTNINGER

2,1. Bestemmelser om overvågning og rapportering

2,2. Forvaltnings- og kontrolsystem

2,3. Foranstaltninger til forebyggelse af svig og uregelmæssigheder

3. FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

3,1. Berørt(e) udgiftspost(er) på budgettet og udgiftsområde(r) i den flerårige finansielle ramme

3,2. Anslåede virkninger for udgifterne

3.2.1. Sammenfatning af udgifternes anslåede virkninger

3.2.2. Anslåede virkninger for aktionsbevillingerne

3.2.3. Anslåede virkninger for administrationsbevillingerne

3.2.4. Forenelighed med indeværende flerårige finansielle ramme

3.2.5. Tredjeparters bidrag

3,3. Anslåede virkninger for indtægterne

FINANSIERINGSOVERSIGT

1. FORSLAGETS/INITIATIVETS RAMME

1,1. Forslagets/initiativets betegnelse

Forordning om oprettelse af det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed

1,2. Berørt(e) politikområde(r) inden for ABM/ABB-strukturen[35]

Forskning og innovation

Europæiske Strategiske Investeringer

1,3. Forslagets/initiativets art

☒Forslaget/initiativet drejer sig om **en ny foranstaltning**

☐ Forslaget/initiativet vedrører en **ny foranstaltning som opfølgning på et pilotprojekt/en forberedende foranstaltning**[36]

☐ Forslaget/initiativet vedrører **en forlængelse af en eksisterende foranstaltning**

☐ Forslaget/initiativet vedrører **omlægning af en foranstaltning til en ny foranstaltning**

1,4. Mål

1.4.1. Kommissionens flerårige strategiske mål for forslaget/initiativet

1. Et forbundet digitalt indre marked

2. Nyt skub i beskæftigelse, vækst og investeringer

1.4.2. Berørt(e) specifikt/specifikke mål

Specifikke mål

1.3 Den digitale økonomi kan udvikle sit fulde potentiale, som bygger på initiativer, der muliggør fuld vækst i digitale teknologier og datateknologierne.

2.1 Europa fastholder sin førerposition i verden inden for den digitale økonomi, hvor europæiske virksomheder kan vokse globalt og trække på stærke digitale iværksætteraktiviteter og nystartede virksomheder, og hvor industrien og offentlige tjenester behersker den digitale omstilling.

2,2. Europas forskning finder investeringsmuligheder for potentielle teknologiske gennembrud og flagskibsinitiativer, navnlig Horisont 2020-programmet og ved hjælp af private/offentligt partnerskaber.

[35] ABM: aktivitetsbaseret ledelse ABB: aktivitetsbaseret budgetlægning.

[36] Jf. artikel 54, stk. 2, litra a) eller litra b), i finansforordningen.

1.4.3. Forventede resultater og virkninger

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

Kompetencecentret vil sammen med netværket og kompetencefællesskabet søge at nå følgende mål:

(1) bidrage til gennemførelsen af cybersikkerhedsdelen i programmet for det digitale Europa oprettet ved forordning nr. XXX og navnlig foranstaltningerne i tilknytning til artikel 6 i forordning (EU) nr. XXX [programmet for det digitale Europa] og Horisont Europa-programmet oprettet ved forordning nr. XXX og navnlig punkt 2.2.6 i bilag I til afgørelse nr. XXX om oprettelse af særprogrammet til gennemførelse af Horisont Europa - rammeprogrammet for forskning og innovation, og af andre EU-programmer, når det er fastsat i EU-retsakter]

(2) forbedre cybersikkerhedskapaciteter, viden og infrastruktur til rådighed for virksomheder, den offentlige sektor og forskningsverdenen

(3) bidrage til bred anvendelse af de seneste cybersikkerhedsprodukter og -løsninger i hele økonomien

(4) skabe større forståelse af internetsikkerhed og bidrage til at indhente kvalifikationsunderskuddet i EU vedrørende cybersikkerhed

(5) bidrage til at styrke forskning i og udvikling af cybersikkerhed i EU

(6) styrke samarbejdet mellem civile og forsvarsrelaterede områder med hensyn til anvendelse af teknologier med dobbelt anvendelsesformål

(7) styrke synergier mellem den civile og forsvarsmæssige dimension af cybersikkerhed

(8) hjælpe med at koordinere og lette arbejdet for de nationale koordinationscentres netværk ("netværket") som omhandlet i artikel 10, og kompetencefællesskabet for cybersikkerhed, der er omhandlet i artikel 12.

1.4.4. Resultat- og effektindikatorer

Angiv indikatorerne for overvågning af forslagets/initiativets gennemførelse.

· Antal infrastrukturer/redskaber vedrørende cybersikkerhed, der indkøbes i fællesskab.

· Adgang til test- og eksperimenttid for europæiske forskere og industri i hele netværket og centret. Når faciliteterne allerede findes, et øget antal timer til rådighed for disse fællesskaber i forhold til det antal, der er til rådighed.

· Stigning i antallet af betjente brugerfællesskaber og antal forskere, der får adgang til de europæiske cybersikkerhedsfaciliteter, sammenlignet med antallet af dem, der må søge sådanne ressourcer uden for Europa.

· Europæiske leverandørers konkurrenceevne begynder at stige målt i global markedsandel (en markedsandel på 25 % inden 2027) og i andelen af europæiske FoU-resultater, der anvendes af industrien.

· Bidrag til næstegenerations cybersikkerhedsteknologier målt i forhold til copyright, patenter, videnskabelige publikationer og kommercielle produkter.

· Antal læseplaner vedrørende færdigheder inden for cybersikkerhed evalueres og tilpasses, antal faglige certificeringsprogrammer for cybersikkerhed vurderes

· Antal uddannede videnskabsfolk, studerende, brugere (industrielle og offentlige forvaltninger).

1,5. Forslagets/initiativets begrundelse

1.5.1. Behov, der skal dækkes på kort eller lang sigt

At skabe kritisk masse af investeringer i teknologiske og industriel udvikling for cybersikkerhed og at fjerne fragmenteringen af kapaciteter spredt ud over hele EU.

1.5.2. Merværdi som følge af EU-foranstaltningen

Cybersikkerhed er et anliggende af fælles interesse i EU, som bekræftet af ovennævnte konklusioner fra Rådet. Omfanget og den grænseoverskridende karakter af hændelser såsom WannaCry eller NonPetya er et glimrende eksempel på dette. Arten og omfanget af de teknologiske udfordringer, samt utilstrækkelig koordinering af indsatsen inden for og på tværs af erhvervslivet, den offentlige sektor og forskningsverden kræver, at EU yderligere støtter koordineringsindsatser for både at samle kritisk masse af ressourcer og sikre bedre viden og forvaltning af aktiver. Dette er påkrævet på grund af de ressourcemæssige krav vedrørende visse kapaciteter for forskning i, udvikling og udbredelse af cybersikkerhed behovet for at give adgang til tværfaglig cybersikkerhedsknowhow på tværs af forskellige fagområder (ofte kun delvist tilgængelige på nationalt plan) den globale karakter af industrielle værdikæder samt aktiviteten hos globale konkurrenter, der arbejder på tværs af markederne.

Dette kræver ressourcer og ekspertise i et omfang, der næppe kan modsvares af en individuel foranstaltning i nogen medlemsstat. Eksempelvis kan et paneuropæisk kvantekommunikationsnetværk kræve investeringer i størrelsesordenen 900 mio. EUR, afhængigt af investeringer fra medlemsstaterne (sammenhængende/suppleret), og i hvilket omfang teknologi giver mulighed for genbrug af eksisterende infrastruktur.

1.5.3. Erfaringer fra lignende tidligere foranstaltninger

Den foreløbige evaluering af Horisont 2020 bekræftede bl.a. den fortsatte relevans af EU-støtte til FoU og de samfundsmæssige udfordringer (heriblandt "Sikre samfund", hvorfra FoU inden for cybersikkerhed støttes). Samtidig bekræfter evalueringen, at en styrkelse af industrielt lederskab vedbliver at udgøre en udfordring, og at der fortsat eksisterer et innovationsunderskud, hvor EU sakker agterud med hensyn til banebrydende, markedsskabende innovation.

Midtvejsevalueringen af Connecting Europe-faciliteten (CEF) synes at bekræfte merværdien af EU's indsats ud over FoU, selv om cybersikkerhed under CEF havde et noget andet fokus (på operationel sikkerhed) og interventionslogik. Samtidig gav de fleste af modtagerne af cybersikkerhedstilskud under CEF - fællesskabet af nationale CSIRT — udtryk for et ønske om et skræddersyet støtteprogram under den næste FFR.

Oprettelsen af det offentlig-private partnerskab i 2016 (OPP) vedrørende cybersikkerhed i EU var et godt første skridt mod at samle fællesskaber inden for forskning, industri og den offentlige sektor om at fremme forskning og innovation inden for cybersikkerhed, og bør inden for den finansielle ramme for 2014-2020 give gode, mere målrettede resultater inden for forskning og innovation. OPP gjorde det muligt for industrielle partnere at give tilsagn om deres respektive udgifter på de

områder, der er fastlagt i partnerskabets strategiske forsknings- og innovationsdagsorden.

1.5.4. Kompatibilitet med andre relevante instrumenter og eventuel synergivirkning

Kompetencenetværket for cybersikkerhed og det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed vil fungere som en supplerende støtte til eksisterende politikbestemmelser og aktører på cybersikkerhedsområdet. Mandatet for det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed vil være et supplement til ENISA's indsats, men har et forskelligt fokus og kræver et andet sæt af færdigheder. ENISA spiller en rolle i forbindelse med rådgivning om cybersikkerhed for forskning og innovation i EU, men dets foreslåede mandat fokuserer først og fremmest på andre opgaver af afgørende betydning for styrkelse af modstandsdygtighed over for cybersikkerhed i EU. Centret bør stimulere udviklingen og anvendelsen af teknologi inden for cybersikkerhed og supplere kapacitetsopbygningsbestræbelserne på dette område på EU-plan og på nationalt plan.

Det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed vil sammen med kompetencenetværket for cybersikkerhed også arbejde hen imod at støtte forskning for at lette og fremskynde standardiserings- og certificeringsprocesser, navnlig dem, der vedrører cybersikkerhedscertificeringsordninger i den i cybersikkerhedslovgivningen anførte betydning.

Det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed vil fungere som fælles gennemførelsesmekanisme for to europæiske programmer til støtte for cybersikkerhed (programmet for det digitale Europe, Horisont Europa-programmet) og øge sammenhængen og samspillet mellem dem.

Dette initiativ giver mulighed for at supplere medlemsstaternes indsats ved at tilvejebringe relevant input til politikere på uddannelsesområdet med henblik på at forbedre uddannelse inden for cybersikkerhed (f.eks. ved at udvikle cybersikkerhedsundervisningsplaner i civile og militære uddannelsessystemer, men også input til grundlæggende uddannelse inden for cybersikkerhed). Det ville også gøre det muligt at støtte tilpasning og løbende vurdering af de professionelle cybersikkerhedscertificeringsprogrammer - alle nødvendige aktiviteter for at bidrage til at nedbryde kvalifikationskløften og lette industriers og andre fællesskabers adgang til cybersikkerhedsspecialister. Tilpasning af uddannelse og færdigheder vil bidrage til at udvikle en kvalificeret arbejdsstyrke inden for cybersikkerhed i EU - et centralt aktiv for cybersikkerhedsvirksomheder samt andre industrier, der er involveret i cybersikkerhed.

1,6. Varighed og finansielle virkninger

☒ Forslag/initiativ af **begrænset varighed**

– ☒ Forslag/initiativ gældende fra 1.1.2021 til 31.12.2029

– ☒ Finansielle virkninger fra 2021 til 2027 for forpligtelsesbevillinger og fra 2021 til 2031 for betalingsbevillinger.

☐ Forslag/initiativ af **ubegrænset varighed**

– Iværksættelse med en indkøringsperiode fra ÅÅÅÅ til ÅÅÅÅ,

– derefter gennemførelse i fuldt omfang.

1,7. Påtænkt(e) forvaltningsmetode(r)[37]

☐ **Direkte forvaltning** ved Kommissionen

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

– ☐ ved gennemførelsesorganer

☐ **Delt forvaltning** sammen med medlemsstaterne

☒

Indirekte forvaltning ved at overlade budgetgennemførelsesopgaver til:

– ☐ tredjelande eller organer, som tredjelande har udpeget

– ☐ internationale organisationer og deres organer (angives nærmere)

– ☐EIB og Den Europæiske Investeringsfond

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

– ☐ offentligretlige organer

– ☐ privatretlige organer, der har fået overdraget samfundsopgaver, forudsat at de stiller tilstrækkelige finansielle garantier

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

– ☐ 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 udpeget i den relevante basisretsakt

– *Hvis der angives mere end én forvaltningsmetode, angives de nærmere enkeltheder i afsnittet "Bemærkninger".*

[37] Forklaringer vedrørende forvaltningsmetoder og henvisninger til finansforordningen findes på webstedet BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. FORVALTNINGSFORANSTALTNINGER

2,1. Bestemmelser om overvågning og rapportering

Angiv hyppighed og betingelser.

Artikel 28 indeholder nærmere bestemmelser om overvågning og rapportering.

2,2. Forvaltnings- og kontrolsystem

2.2.1. Konstaterede risici

For at afbøde risiciene i forbindelse med driften af kompetencecentret efter dets oprettelse og forsinkelser vil Kommissionen støtte kompetencecentret i denne fase for at sikre hurtig ansættelse af nøglepersonale og oprettelse af et effektivt internt kontrolsystem og effektive procedurer.

2.2.2. Oplysninger om det indførte interne kontrolsystem

Den administrerende direktør er ansvarlig for driften og den daglige ledelse af kompetencecentret og skal være dets retlige repræsentant. Direktøren er ansvarlig over for bestyrelsen og aflægger løbende rapport til denne om udviklingen af kompetencecentrets aktiviteter. Bestyrelsen har det overordnede ansvar for den strategiske orientering og driften af kompetencecentret og fører tilsyn med gennemførelsen af dets aktiviteter. De finansielle bestemmelser for kompetencecentret vedtages af bestyrelsen efter høring af Kommissionen. De må ikke afvige fra forordning (EU) nr. 1271/2013, medmindre dette er strengt nødvendigt for kompetencecentrets drift, og Kommissionen på forhånd har givet sit samtykke. Kommissionens interne revisor udøver samme beføjelser over kompetencecentret som dem, han er tillagt over for Kommissionen. Revisionsretten har beføjelse til gennem bilagskontrol og kontrol på stedet at kontrollere alle tilskudsmodtagere, kontrahenter og underkontrahenter, som har modtaget EU-midler fra kompetencecentret.

2.2.3. Anslåede omkostninger og fordele ved kontrollen samt forventet fejlrisiko

Omkostninger og fordele ved kontrollen Kontrolomkostningerne til det europæiske industri-, teknologi-, og forskningskompetencecenter for cybersikkerhed er fordelt mellem udgifter til Kommissionens tilsyn og udgifter til operationel kontrol i gennemførelsesorganerne. Omkostningerne ved kontrollen i kompetencecentret anslås at udgøre ca. 1,19 % af betalingsbevillingerne til operationel kontrol, der gennemføres i kompetencecentret. Udgifterne til Kommissionens tilsyn anslås til 1,20 % af betalingsbevillingerne til operationel kontrol, der gennemføres i kompetencecentret. Ud fra den antagelse, at aktiviteterne ville blive fuldt forvaltet af Kommissionen uden støtte fra gennemførelsesorganet, ville omkostningerne til kontrol være væsentligt højere og kunne udgøre ca. 7,7 % af betalingsbevillingerne. Den planlagte kontrol tager sigte på at sikre Kommissionens smidige og effektive tilsyn med gennemførelsesorganerne og at sikre den nødvendige grad af sikkerhed i Kommissionen. Der er følgende fordele ved kontrollen:

- undgåelse af valg af svagere eller mangelfulde forslag

- optimering af planlægning og anvendelse af EU-midler for at bevare EU-merværdi

- sikring af kvaliteten af tilskudsaftalerne, undgåelse af fejl i identifikationen af juridiske enheder, sikring af beregningen af EU-bidrag og sikkerhed for korrekt drift af tilskud

- påvisning af ikke-støtteberettigede omkostninger i betalingsfasen

- påvisning af fejl, som har indvirkning på lovligheden og den formelle rigtighed for operationerne på revisionsniveau.

Anslået fejlniveau

Målet er at opretholde restfejlfrekvensen under 2 %-tærsklen for hele programmet, mens kontrolbyrden begrænses for støttemodtagerne for at opnå den rette balance mellem lovligheden og den formelle rigtighed af mål med andre mål såsom programmets tiltrækningskraft, især for SMV'er og udgifterne til kontrol.

2,3. Foranstaltninger til forebyggelse af svig og uregelmæssigheder

Angiv eksisterende eller påtænkte forebyggelses- og beskyttelsesforanstaltninger.

OLAF kan udføre undersøgelser, herunder kontrol og inspektion på stedet, i overensstemmelse med de bestemmelser og procedurer, der er fastlagt i Europa-Parlamentets og Rådets forordning nr. 883/2013 og Rådets forordning (Euratom, EF) nr. 2185/96 af 11. november 1996 om Kommissionens kontrol og inspektion på stedet med henblik på beskyttelse af EU's finansielle interesser mod svig og andre uregelmæssigheder for at beskytte Unionens finansielle interesser mod svig og andre uregelmæssigheder med henblik på at klarlægge, om der er begået svig, bestikkelse eller andre ulovlige aktiviteter, der påvirker EU's finansielle interesser i forbindelse med et tilskud eller en kontrakt, der er finansieret af kompetencecentret.

Aftaler, afgørelser og kontrakter, der følger af gennemførelsen af denne forordning, indeholder bestemmelser, som udtrykkeligt bemyndiger Kommissionen, kompetencecentret, Revisionsretten og OLAF til at udføre revisioner og undersøgelser i henhold til deres respektive kompetencer.

Kompetencecentret sikrer, at dets medlemmers finansielle interesser er tilstrækkeligt beskyttet ved at udføre eller foranledige egnede interne og eksterne kontroller.

Kompetencecentret tiltræder den interinstitutionelle aftale af 25. maj 1999 mellem Europa-Parlamentet, Rådet for Den Europæiske Union og Kommissionen for De Europæiske Fællesskaber om de interne undersøgelser, der foretages af Det Europæiske Kontor for Bekæmpelse af Svig (OLAF). Kompetencecentret træffer de fornødne foranstaltninger for at lette OLAF's arbejde med interne undersøgelser.

Kompetencecentret vedtager en strategi til bekæmpelse af svig, baseret på en risikoanalyse af svig og cost-/benefitovervejelser. Det skal beskytte EU's finansielle interesser ved at anvende forholdsregler til forebyggelse af svig, korruption og enhver anden ulovlig aktivitet, gennem effektiv kontrol og, hvis der konstateres uregelmæssigheder, gennem inddrivelse af uretmæssigt udbetalte beløb og i givet fald ved hjælp af effektive, forholdsmæssige og afskrækkende administrative og finansielle sanktioner.

3. FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

3,1. Udgiftsområde(r) i den flerårige finansielle ramme og foreslået(ede) ny(e) udgiftspost(er) på budgettet

- Nye budgetposter, som der er søgt om

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 [38]	fra EFTA-lande[39]	Fra kandidatlande[40]	fra tredjelande	I henhold til finansforordningens artikel [21, stk. 2, litra b)]
Udgiftsområde 1: Det indre marked, innovation og det digitale område	01 02 XX XX Horisont Europa Industri-, teknologi- og forskningskompetencecentret for cybersikkerhed - støtteudgifter 01 02 XX XX Horisont Europa Industri-, teknologi- og forskningskompetencecentret for cybersikkerhed 02 06 01 XX Programmet for det digitale Europa Industri-, teknologi- og forskningskompetencecentret — støtteudgifter 02 06 01 XX Programmet for det digitale Europa Industri-, teknologi- og forskningskompetencecentret	Opdelte	JA	JA (hvis angivet i det årlige arbejdsprogram)	JA (begrænset til en del af programmet)	NEJ

- Bidragene til disse budgetposter forventes at komme fra:

i mio. EUR (tre decimaler)

[38] OB = opdelte bevillinger/IOB = ikke-opdelte bevillinger.
[39] EFTA: Den Europæiske Frihandelssammenslutning.
[40] Kandidatlande og, efter omstændighederne, potentielle kandidatlande på Vestbalkan.

Budgetpost	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	**I alt**
01 01 01 01 Udgifter til tjenestemænd, midlertidigt ansatte — Horisont Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 02 Eksternt personale, der gennemfører forskningsprogrammer — Horisont Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 03 Andre administrationsudgifter til forskning — Horisont Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 02 02 Globale udfordringer og industriel konkurrenceevne	pm	pm	pm	pm	pm	pm	pm	**pm**
02 01 04 Administrativ støtte — Det digitale Europa	1,238	3,030	3,743	3,818	3,894	3,972	4,051	**23,746**
02 06 01 Cybersikkerhed — Det digitale Europa	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Udgifter i alt	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

Bidraget fra finansieringsrammen for klyngen "Rummeligt og sikkert samfund" i søjle II "Globale udfordringer og industriel konkurrenceevne" i Horisont Europa (samlet rammebeløb 2 800 000 000 EUR) omhandlet i artikel 21, stk. 1, litra b), vil blive foreslået af Kommissionen i løbet af lovgivningsprocessen, og under alle omstændigheder før der er opnået politisk enighed. Forslaget vil være baseret på resultaterne af den strategiske planlægningsproces som defineret i artikel 6, stk. 6, i forordning XXX [rammeprogrammet Horisont Europa].

Ovennævnte beløb omfatter ikke medlemsstaternes bidrag til kompetencecentrets driftsomkostninger og administrationsomkostninger svarende til EU's finansielle bidrag.

3,2. Anslåede virkninger for udgifterne

3.2.1. Sammenfatning af udgifternes anslåede virkninger

i mio. EUR (tre decimaler)

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

			2021[41]	2022	2023	2024	2025	2026	2027	*Efter 2027*	I ALT
Afsnit 1 (personaleudgifter)	Forpligtelser = Betalinger	(1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Afsnit 2 (Infrastruktur og driftsudgifter)	Forpligtelser = Betalinger	(2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Afsnit 3 (driftsudgifter)	Forpligtelser	(3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		**1 957,922**
	Betalinger	(4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1 061,715	**1 957,922**
Bevillinger finansieret over bevillingsrammen for programmerne I ALT[42]	Forpligtelser	=1+2+3	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**		**1 981,668**
	Betalinger	=1+2+4	**22,459**	**105,795**	**153,954**	**171,154**	**160,369**	**154,096**	**152,126**	**1 061,715**	**1 981,668**

41 Personalebevillingerne tegnede sig kun for et halvt år i 2021

42 De samlede bevillinger, der er fastsat, vedrører alene EU's finansielle ressourcer til cybersikkerhed under programmet for det digitale Europa. Bidraget fra finansieringsrammen for klyngen "Rummeligt og sikkert samfund" i søjle II "Globale udfordringer og industriel konkurrenceevne" i Horisont Europa (samlet rammebeløb 2 800 000 000 EUR) omhandlet i artikel 5, stk. 1, litra b), vil blive foreslået af Kommissionen i løbet af lovgivningsprocessen, og under alle omstændigheder før der er opnået politisk enighed. Forslaget vil være baseret på resultaterne af den strategiske planlægningsproces som defineret i artikel 6, stk. 6, i forordning XXX [rammeprogrammet Horisont Europa].

Udgiftsområde i den flerårige finansielle ramme	7	"Administration"

i mio. EUR (tre decimaler)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Efter 2027***	**I ALT**
Menneskelige ressourcer		3,090	3,233	3,233	3,233	3,233	3,233	3,805		**23,060**
Andre administrationsudgifter		0,105	0,100	0,104	0,141	0,147	0,153	0,159		**0,909**
Bevillinger I ALT under UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme	(Forpligtelser i alt = betalinger i alt)	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**		**23,969**

i mio. EUR (tre decimaler)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Efter 2027***	**I ALT**
Bevillinger I ALT på tværs af UDGIFTSOMRÅDER i den flerårige finansielle ramme	Forpligtelser	**289,325**	**328,607**	**334,657**	**255,574**	**260,569**	**265,572**	**271,332**		**2 005,637**
	Betalinger	**25,654**	**109,128**	**157,291**	**174,528**	**163,749**	**157,482**	**156,090**	**1 [2]061,715**	**2 005,637**

3.2.2. 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	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**I ALT**
UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme								
Menneskelige ressourcer	3,090	3,233	3,233	3,233	3,233	3,233	3,805	**23,060**
Andre administrationsudgifter	0,105	0,100	0,104	0,141	0,147	0,153	0,159	**0,909**
Subtotal UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**	**23,969**
Uden for UDGIFTSOMRÅDE 7[43] i den flerårige finansielle ramme								
Menneskelige ressourcer								
Andre administrationsudgifter	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Subtotal Uden for UDSGIFTSOMRÅDE 7 i den flerårige finansielle ramme	**1,238**	**3,030**	**3,743**	**3,818**	**3,894**	**3,972**	**4,051**	**23,746**
I ALT	**4,433**	**6,363**	**7,079**	**7,192**	**7,274**	**7,358**	**8,016**	**47,715**

Bevillingerne til menneskelige ressourcer og andre administrationsudgifter vil blive dækket ved hjælp af de af generaldirektoratets bevillinger, som allerede er afsat til forvaltning af aktionen, og/eller interne rokader i GD'et, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige GD i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

Ovennævnte nødvendige bevillinger til menneskelige ressourcer og andre administrationsudgifter uden for udgiftsområde 7 svarer til det beløb, der dækkes af EU's finansielle bidrag fra programmet for det digitale Europa.

Bevillingerne til menneskelige ressourcer og andre administrationsudgifter uden for udgiftsområde 7 forhøjes med det beløb, der dækkes af EU's finansieringsbidrag fra Horisont Europa-programmet, når bidraget fra den finansielle støtte til klyngen "Rummelige og sikre samfund" søjle II "Globale udfordringer og industriens konkurrenceevne" i Horisont Europa (samlet

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

rammebeløb 2 800 000 000 EUR) omhandlet i artikel 21, stk. 1, litra b), vil blive foreslået af Kommissionen i løbet af lovgivningsprocessen, og under alle omstændigheder før der er opnået politisk enighed.

Ovenstående beløb af de nødvendige bevillinger til menneskelige ressourcer og andre administrationsudgifter uden for udgiftsområde 7 omfatter ikke medlemsstaternes bidrag til kompetencecentrets administrationsomkostninger svarende til EU's finansielle bidrag.

3.2.2.1. Kommissionens anslåede 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 fuldtidsækvivalenter

År		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Stillinger i stillingsfortegnelsen (tjenestemænd og midlertidigt ansatte)								
I hovedsædet og Kommissionens repræsentationskontorer		20	21	21	21	21	21	22
Delegationer								
Forskning								
• Eksternt personale (i fuldtidsækvivalenter: FTÆ) — KA, LA, UNE, V og JED [44] Udgiftsområde 7								
Finansieret fra UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme	- i hovedsædet	3	3	3	3	3	3	3
	- i delegationer							
Finansieret over bevillingsrammen for programmet [45]	- i hovedsædet							
	- i delegationer							
Forskning								
Andet (specificeres)								
I ALT		**23**	**23**	**24**	**24**	**24**	**25**	**25**

Personalebehovet vil blive dækket ved hjælp af det personale, som generaldirektoratet allerede har afsat til aktionen, og/eller 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	Koordinering, overvågning og styring af de opgaver, som det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed har fået overdraget, herunder støtte og koordineringsaktiviteter. Politikudvikling og koordinering inden for cybersikkerhed i forhold til de opgaver, som det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed har fået overdraget, f.eks. med hensyn til fastsættelse af prioriteter for forskning og industripolitik, samarbejde mellem medlemsstaterne og de økonomiske operatører, sammenhæng med den fremtidige EU-ramme for cybersikkerhedscertificering, arbejde vedrørende ansvar og rettidig omhu, eller koordinering med politikker om HPC, kunstig intelligens, og digitale færdigheder. .
Eksternt personale	Koordinering, overvågning og styring af de opgaver, som det europæiske industri-,

[44] KA = kontraktansatte LA = lokalt ansatte UNE = udstationerede nationale eksperter INT = vikar JED = junioreksperter ved delegationerne

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

	teknologi- og forskningskompetencecenter for cybersikkerhed har fået overdraget, herunder støtte og koordineringsaktiviteter. Politikudvikling og koordinering inden for cybersikkerhed i forhold til de opgaver, som det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed har fået overdraget, f.eks. med hensyn til fastsættelse af prioriteter for forskning og industripolitik, samarbejde mellem medlemsstaterne og de økonomiske operatører, sammenhæng med den fremtidige EU-ramme for cybersikkerhedscertificering, arbejde vedrørende ansvar og rettidig omhu, eller koordinering med politikker om HPC, kunstig intelligens, og digitale færdigheder. .

3.2.2.2. Anslået behov for menneskelige ressourcer i industri-, teknologi- og forskningskompetencecentret for cybersikkerhed

	2021	2022	2023	2024	2025	2026	2027
Kommissionens tjenestemænd							
Heraf AD							
Heraf AST							
Heraf AST-SC							
Midlertidigt ansatte							
Heraf AD	10	11	13	13	13	13	13
Heraf AST							
Heraf AST-SC							
Kontraktansatte	26	32	39	39	39	39	39
UNE'er	1	1	1	1	1	1	1
I alt	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Opgavebeskrivelse:

Tjenestemænd og midlertidigt ansatte	Operationel gennemførelse af de opgaver, der overdrages til det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed i medfør af denne forordnings artikel 4, herunder støtte og koordineringsaktiviteter.
Eksternt personale	Operationel gennemførelse af de opgaver, der overdrages til det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed i medfør af denne forordnings artikel 4, herunder støtte og koordineringsaktiviteter.

Det ovenfor anslåede behov for menneskelige ressourcer i industri-, teknologi- og forskningskompetencecentret for cybersikkerhed svarer til de skønnede behov for at gennemføre EU's finansielle bidrag under det digitale Europa.

Det ovenfor anslåede behov for menneskelige ressourcer i industri-, teknologi- og forskningskompetencecentret for cybersikkerhed forhøjes med de anslåede behov for at gennemføre EU's finansielle bidrag under Horisont Europa, når bidraget fra den finansielle støtte til klyngen "Rummelige og sikre samfund" søjle II "Globale udfordringer og industriens konkurrenceevne" i Horisont Europa (samlet rammebeløb 2 800 000 000 EUR) omhandlet i artikel 21, stk. 1, litra b), vil blive foreslået af Kommissionen i løbet af lovgivningsprocessen, og under alle omstændigheder før der er opnået politisk enighed.

3.2.2.3. Stillingsfortegnelsen for industri-, teknologi- og forskningskompetencecentret

Ansættelsesgruppe og lønklasse	2021	2022	2023	2024	2025	2025	2025
AD 16							

AD 15							
AD 14	1	1	1	1	1	1	1
AD 13							
AD 12							
AD 11							
AD 10							
AD 9	5	5	6	6	6	6	6
AD 8	1	1	1	1	1	1	1
AD 7	1	2	3	3	3	3	3
AD 6	1	1	1	1	1	1	1
AD 5	1	1	1	1	1	1	1
AD i alt	10	11	13	13	13	13	13
AST 11							
AST 10							
AST 9							
AST 8							
AST 7							
AST 6							
AST 5							
AST 4							
AST 3							
AST 2							
AST 1							
AST i alt							
AST/SC 6							
AST/SC 5							
AST/SC 4							
AST/SC 3							

AST/SC 2							
AST/SC 1							
AST/SC i alt							
I ALT	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4. Anslåede virkninger for medarbejderne (yderligere) — eksternt personale i industri-, teknologi- og forskningskompetencecentret for cybersikkerhed

Kontraktansatte	2021	2022	2023	2024	2025	2026	2027
Ansættelsesgruppe IV	20	22	29	29	29	29	29
Ansættelsesgruppe III	2	4	4	4	4	4	4
Ansættelsesgruppe II	4	6	6	6	6	6	6
Ansættelsesgruppe I							
I alt	**26**	**32**	**39**	**39**	**39**	**39**	**39**

For at sikre fastfrysningen af det samlede antal stillinger opført i stillingsfortegnelsen vil det yderligere personale i industri-, teknologi- og forskningskompetencecentret for cybersikkerhed delvis blive udlignet af reduktionen i antallet af tjenestemænd og eksternt personale (dvs. den aktuelle stillingsfortegnelse og eksternt personale) i Kommissionens relevante tjenestegrene.

Antallet af medarbejdere i industri-, teknologi- og forskningskompetencecentret for cybersikkerhed i punkt 3.2.2.2-4 vil blive kompenseret som følger[46]:

I ALT	2021	2022	2023	2024	2025	2026	2027
Kommissionens tjenestemænd	5	5	6	6	6	6	6
Midlertidigt ansatte							
Kontraktansatte	14	17	20	20	20	20	20
UNE'er							
Samlede FTÆ'er	19	22	26	26	26	26	26
Antal beskæftigede	19	22	26	26	26	26	26

[46] Med forbehold af det endelige budget, hvis gennemførelse vil blive uddelegeret til kompetencecentret

Kompensation af de menneskelige ressourcer i industri-, teknologi- og forskningskompetencecentret for cybersikkerhed vil stå i forhold til andelen af EU's finansielle bidrag, dvs. 50 %.

Ovennævnte kompensation vedrører de anslåede behov for menneskelige ressourcer i industri-, teknologi- og forskningskompetencecentret for cybersikkerhed for gennemførelsen af EU's finansielle bidrag fra programmet for det digitale Europa.

Ovennævnte kompensation forhøjes med de anslåede behov for at gennemføre EU's finansielle bidrag fra Horisont Europa, når bidraget fra finansieringsrammen i klyngen "Rummelige og sikre samfund" søjle II "Globale udfordringer og industriens konkurrenceevne" i Horisont Europa (samlet rammebeløb 2 800 000 000 EUR) omhandlet i artikel 21, stk. 1, litra b), vil blive foreslået af Kommissionen i løbet af lovgivningsprocessen, og under alle omstændigheder før der er opnået politisk enighed.

3.2.3. Tredjeparters bidrag

Forslaget/initiativet:

– ☐ indeholder ikke bestemmelser om samfinansiering med tredjeparter

– ☒ indeholder bestemmelser om samfinansiering med tredjeparter[47] anslået nedenfor:

Bevillinger i mio. EUR (tre decimaler)

År	2021	2022	2023	2024	2025	2026	2027	I ALT
Medlemsstater - bidrag til personaleudgifter	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Medlemsstater — bidrag til infrastruktur og driftsudgifter	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Medlemsstater — bidrag til driftsudgifter	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Samfinansierede bevillinger I ALT	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

Ovennævnte tredjepartsbidrag vedrører kun samfinansiering svarende til EU's finansielle ressourcer til cybersikkerhed under programmet for det digitale Europa. Ovennævnte tredjepartsbidrag vil blive øget, når det finansielle bidrag fra klyngen "Rummelige og sikre samfund" søjle II "Globale udfordringer og industriens konkurrenceevne" i Horisont Europa (samlet rammebeløb 2 800 000 000 EUR) omhandlet i artikel 21, stk. 1, litra b), vil blive foreslået af Kommissionen i løbet af lovgivningsprocessen, og under alle omstændigheder før der er opnået politisk enighed. Forslaget vil være baseret på resultaterne af den strategiske planlægningsproces som defineret i artikel 6, stk. 6, i forordning XXX [rammeprogrammet Horisont Europa].

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, hvis indtægterne er formålsbestemt til udgiftsposter ☐

i mio. EUR (tre decimaler)

Indtægtspost på budgettet:	Forslagets/initiativets virkninger[48]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Artikel …….							

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

[47] Anslået bidrag i naturalier fra medlemsstaterne

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

Andre bemærkninger (f.eks. metode/formel, der anvendes til beregning af virkningen på indtægterne eller andre oplysninger).