EUROPEISKA
KOMMISSIONEN

Bryssel den 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum

Bidrag från Europeiska kommissionen som presenterades för ledarna vid toppmötet i Salzburg den 19-20 september 2018

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

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

I takt med att vår vardag och våra ekonomier blir alltmer beroende av digital teknik löper medborgarna också större risk att utsättas för allvarliga cyberincidenter. Vår framtida säkerhet förutsätter att vi stärker förmågan att skydda unionen mot cyberhot, eftersom både civil infrastruktur och militär kapacitet är beroende av säkra digitala system.

För att hantera de växande utmaningarna har unionen stadigt ökat sina insatser på detta område med utgångspunkt i cybersäkerhetsstrategin från 2013[1] och dess mål och principer för att främja ett tillförlitligt, säkert och öppet ekosystem för cybersäkerhet. År 2016 antog unionen de första åtgärderna på cybersäkerhetsområdet genom Europaparlamentets och rådets direktiv (EU) 2016/1148[2] om säkerhet i nätverks- och informationssystem.

Eftersom utvecklingen sker snabbt inom cybersäkerhetsområdet lade kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik i september 2017 fram ett gemensamt meddelande[3] om resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU för att ytterligare stärka unionens resiliens, avskräckning och hantering av cyberattacker. Det gemensamma meddelandet utgick från tidigare initiativ och föreslog åtgärder som att bl.a. stärka Europeiska unionens byrå för nät- och informationssäkerhet (Enisa), skapa en frivillig EU-ram för cybersäkerhetscertifiering för att öka cybersäkerheten hos den digitala världens produkter och tjänster samt en konkret plan för snabb och samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser.

I det gemensamma meddelandet framhölls att det även ligger i unionens strategiska intresse att bibehålla och vidareutveckla nödvändig teknisk kapacitet inom cybersäkerhet för att trygga sin digitala inre marknad och framför allt skydda kritiska nätverk och informationssystem samt tillhandahålla grundläggande cybersäkerhetstjänster. Unionen måste ha förmåga att själv säkra sina digitala tillgångar och kunna konkurrera på en global cybersäkerhetsmarknad.

I dag är unionen nettoimportör av cybersäkerhetsprodukter och lösningar och i stor utsträckning beroende av icke-europeiska leverantörer.[4] Den globala cybersäkerhetsmarknaden är värd 600 miljarder euro och väntas växa de kommande fem åren med i genomsnitt 17 % i fråga om omsättning, antal företag och sysselsättning. Bland de 20 länder som är marknadsledande inom cybersäkerhet är emellertid bara sex medlemsstater[5].

I unionen finns samtidigt omfattande sakkunskap och erfarenhet inom cybersäkerhet – mer än 660 organisationer från hela EU anmälde sig i samband med kommissionen kartläggning nyligen av kunskapscentrumen inom cybersäkerhet.[6] Denna sakkunskap kan, om den omsätts

---

1 GEMENSAMT MEDDELANDE TILL EUROPAPARLAMENTET OCH RÅDET: EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd JOIN(2013) 1 final).

2 Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

3 GEMENSAMT MEDDELANDE TILL EUROPAPARLAMENTET OCH RÅDET – Resiliens, avskräckning och försvar: stärkt cybersäkerhet i EU, JOIN(2017) 450 final.

4 Utkast till slutrapport om undersökningen av cybersäkerhetsmarknaden, 2018.

5 Utkast till slutrapport om undersökningen av cybersäkerhetsmarknaden, 2018.

6 Gemensamma forskningscentrets tekniska rapport: European Cybersecurity Centres of Expertise, 2018.

i säljbara produkter och lösningar, göra det möjligt för unionen att täcka hela värdekedjan när det gäller cybersäkerhet. Insatserna inom forskarsamhället och näringslivet är emellertid fragmenterade, saknar inriktning och ett gemensamt mål, vilket hämmar EU:s konkurrenskraft på detta område och dess möjligheter att säkra sina digitala tillgångar. Stödet till relevanta cybersäkerhetssektorer (t.ex. energi, rymden, försvar och transport) och deras underområden är i dag otillräckligt.[7] Dessutom tillvaratas inte synergieffekterna mellan den civila och den försvarsrelaterade cybersäkerhetssektorn fullt ut i Europa.

Etableringen av det offentlig-privata partnerskapet för cybersäkerhet (nedan kallat *cPPP*) i unionen 2016 var ett viktigt första steg mot att sammanföra forskarsamhället, näringslivet och den offentliga sektorn för att främja forskning och innovation inom cybersäkerhet och bör inom budgetramen 2014–2020 leda till bra och mer fokuserade resultat. Genom cPPP kunde näringslivspartner utlova individuella satsningar på områden som definieras i partnerskapets strategiska forsknings- och innovationsagenda.

Unionen kan emellertid göra en betydligt större satsning och behöver en effektivare mekanism för att skapa en varaktig kapacitet, slå samman insatser, kompetenser och stimulera utvecklingen av innovativa lösningar på näringslivets cybersäkerhetsutmaningar när det gäller ny teknik med flera användningsområden (t.ex. artificiell intelligens, kvantdatorer, blockkedjor och säkra digitala identiteter) samt inom kritiska sektorer (t.ex. transport, energi, hälsa, finans, offentlig förvaltning, telekommunikation, tillverkningsindustri, försvar och rymden).

I det gemensamma meddelandet beaktades möjligheten att stärka unionens kapacitet på cybersäkerhetsområdet genom ett nätverk av kompetenscentrum för cybersäkerhet med ett europeiskt kompetenscentrum för cybersäkerhet som nav. Syftet skulle vara att komplettera den befintliga kapacitetsuppbyggnad inom detta område som pågår på unionsnivå och nationellt. I det gemensamma meddelandet fastställdes att kommissionen planerade påbörja en konsekvensbedömning 2018 för att granska tillgängliga alternativ för att inrätta en sådan struktur. Som ett första steg och som underlag för framtida diskussioner inledde kommissionen en pilotfas inom ramen för Horisont 2020 för att sammanföra de nationella centrumen i ett nätverk som skapar ny drivkraft för kompetensutveckling och teknisk utveckling inom cybersäkerhet.

Vid det digitala toppmötet i Tallinn i september 2017 uppmanade stats- och regeringscheferna unionen att bli ”ledande när det gäller cybersäkerhet senast 2025 för att försäkra oss om att våra medborgare, konsumenter och företag kan ha förtroende för och åtnjuta skydd på internet och för att möjliggöra ett fritt internet som styrs av lagen”.

I de rådsslutsatser[8] som antogs i november 2017 uppmanades kommissionen att inom kort tillhandahålla en konsekvensbedömning av och senast i mitten av 2018 föreslå de relevanta rättsliga instrumenten för genomförande av initiativet.

Syftet med programmet för ett digitalt Europa, som kommissionen föreslog i juni 2018[9] , är att inom alla relevanta EU-politikområden driva på och maximera de positiva effekterna av

[7] Gemensamma forskningscentrets tekniska rapport: Outcomes of the Mapping Exercise (se bilagorna 4 och 5 för närmare information).

[8] Rådets slutsatser om det gemensamma meddelandet till Europaparlamentet och rådet: Resiliens, avskräckning och försvar: stärkt cybersäkerhet i EU, som antogs av rådet (allmänna frågor) den 20 november 2017.

[9] COM(2018) 434 Förslag till Europaparlamentets och rådets förordning om inrättande av programmet för ett digitalt Europa för perioden 2021–2027.

den digitala omvandlingen för europeiska medborgare och företag, att stärka politiken och stödja ambitionerna med en digital inre marknad. I programmet föreslås en enhetlig och övergripande metod för att säkerställa ett optimalt utnyttjande av avancerad teknik och en lämplig kombination av teknisk kapacitet och mänsklig kompetens för den digitala omvandlingen – inte bara när det gäller cybersäkerhet, utan även i fråga om smart datainfrastruktur, artificiell intelligens, avancerade färdigheter och applikationer inom näringslivet och på områden i allmänhetens intresse. Allt detta hänger ihop, är ömsesidigt förstärkande och kan, om det främjas samtidigt, nå den skala som krävs för att dataekonomin ska blomstra.[10] Även *Horisont Europa-programmet* [11] – som är EU:s nästa ramprogram för forskning och innovation – har satt upp cybersäkerhet som en av sina prioriteringar.

I detta sammanhang föreslås i förordningen att det upprättas en europeisk kompetens för cybersäkerhet med ett nätverk av nationella samordningscentrum. Denna ändamålsenliga samarbetsmodell skulle i syfte att stimulera det europeiska ekosystemet för cybersäkerhet inom näringsliv och teknik fungera på följande sätt: Kompetenscentrumet ska främja och bidra till att samordna arbetet inom nätverket och stödja kompetensgemenskapen för cybersäkerhet genom att driva agendan i cybersäkerhetsfrågor och göra det lättare att få tillgång till den sakkunskap som samlas i nätverket. För att åstadkomma detta kommer kompetenscentrumet i synnerhet att genomföra relevanta delar av programmen Ett digitalt Europa och Horisont Europa genom att bevilja bidrag och utföra offentliga upphandlingar. Mot bakgrund av de avsevärda investeringar i cybersäkerhet som gjorts i andra delar av världen och behovet av att samordna och slå samman relevanta resurser i Europa föreslås att kompetenscentrumet ska utgöra ett europeiskt partnerskap[12], och sålunda underlätta gemensamma investeringar av unionen, medlemsstaterna och/eller näringslivet. Därför föreskrivs det i förslaget att medlemsstaterna ska lämna proportionella bidrag till kompetenscentrumets och nätverkets åtgärder. Det huvudsakliga beslutande organet är styrelsen, där alla medlemsstater deltar men endast de medlemstater som deltar finansiellt har rösträtt. Röstsystemet i styrelsen följer principen om dubbel majoritet där det fordras 75 % av det finansiella bidraget och 75 % av rösterna. På grund av kommissionens ansvar för unionens budget har kommissionen 50 % av rösterna. För sitt arbete i styrelsen kommer kommissionen att när så är lämpligt utnyttja de fackkunskaper som den europeiska avdelningen för yttre åtgärder besitter. Styrelse biträds av en näringslivs- och vetenskapsnämnd för att säkerställa regelbunden dialog med den privata sektorn, konsumentorganisationer och andra berörda intressenter.

Det europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning skulle, i nära samarbete med det nätverk av nationella samordningscentrum och den kompetensgemenskap för cybersäkerhet som inrättas genom denna förordning (en stor och mångskiftande grupp aktörer som arbetar med teknikutveckling inom cybersäkerhet, t.ex. forskarorganisationer, företag på utbuds- och efterfrågesidan samt offentlig sektor), vara det genomförandeorgan som får merparten av de EU-medel som avsätts för cybersäkerhet i det föreslagna *programmet för ett digitalt Europa*och *Horisont Europa-programmet.*

---

10 Se SWD(2018) 305.

11 COM(2018) 435 Förslag till Europaparlamentets och rådets förordning om inrättande av Horisont Europa – ramprogrammet för forskning och innovation, och om dess regler för deltagande och spridning.

12 Som fastställs i COM(2018) 435 Förslag till Europaparlamentets och rådets förordning om inrättande av Horisont Europa – ramprogrammet för forskning och innovation, och om dess regler för deltagande och spridning. och som det hänvisas till i COM(2018) 434 Förslag till Europaparlamentets och rådets förordning om inrättande av programmet för ett digitalt Europa för perioden 2021–2027.

Det här breda angreppsättet skulle göra det möjligt att främja cybersäkerhet längs hela värdekedjan, från forskning till införande och ibruktagande av grundläggande teknik. Medlemsstaternas del av finansieringen bör stå i proportion till EU:s bidrag till finansieringen av detta initiativ och är en nödvändig förutsättning för att det ska bli en framgång.

Med tanke på dess särskilda sakkunskap och breda och relevanta representation av intressenter bör den europeiska organisationen för cybersäkerhet, som är kommissionens motpart i det avtalsbaserade offentlig-privata partnerskapet för cybersäkerhet inom Horisont 2020, bjudas in att medverka till centrumets och nätverkets arbete.

Det europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning bör även försöka öka synergieffekterna mellan de civila och försvarsrelaterade aspekterna av cybersäkerhet. Det bör stödja medlemsstater och andra relevanta aktörer genom att ge rådgivning, utbyta sakkunskap och underlätta samarbete vad gäller projekt och åtgärder. På medlemsstaters begäran skulle det även kunna fungera som projektledare, i synnerhet i förhållande till Europeiska försvarsfonden. Syftet med detta initiativ är att hantera följande problem:

- **Otillräckligt samarbete mellan sektorerna på utbuds- och efterfrågesidan** För europeiska företag är utmaningen att både värna sin fortsatta säkerhet och att erbjuda sina kunder säkra produkter och tjänster. Ändå kan de ofta inte säkra sina befintliga produkter, tjänster och tillgångar på lämpligt sätt eller ta fram säkra innovativa produkter och tjänster. Viktiga cybersäkerhetstillgångar är ofta alltför kostsamma att ta fram och införa för enskilda aktörer vars kärnverksamhet inte är cybersäkerhet. Kopplingarna mellan efterfråge- och utbudssidorna av cybersäkerhetsmarknaden är samtidigt inte tillräckligt väl utvecklade, vilket leder till en suboptimal tillgång till europeiska produkter och lösningar som är anpassade för olika sektorers behov, samt till en brist på förtroende mellan marknadsaktörerna.
- **Det saknas en effektiv samarbetsmekanism för medlemsstaternas kapacitetsuppbyggnad inom näringslivet.** I nuläget saknas det även en effektiv samarbetsmekanism för att medlemsstaterna tillsammans ska kunna arbeta för att bygga upp nödvändig kapacitet till stöd för innovation på cybersäkerhetsområdet inom olika sektorer och införande av europeiska cybersäkerhetslösningar som ligger i framkant. Den typen av verksamhet ryms inte inom mandatet för de nuvarande samarbetsmekanismerna för medlemsstaterna på cybersäkerhetsområdet i direktiv (EU) 2016/1148.
- **Otillräckligt samarbete inom och mellan forskarsamhället och näringslivet.** Även om EU i teorin kan täcka in hela värdekedjan inom cybersäkerhet finns det relevanta cybersäkerhetssektorer (t.ex. energi, rymden, försvar, transport) och underområden som för närvarande inte får mycket stöd från forskarsamhället eller bara av några få forskningsorganisationer (t.ex. postkvant- och kvantkryptering, förtroende och cybersäkerhet inom AI). Även om sådant samarbete naturligtvis finns handlar det mycket ofta om kortsiktiga konsultsamarbeten som inte gör det möjligt att sjösätta långsiktiga forskningsplaner som kan möta näringslivets utmaningar inom cybersäkerhet.
- **Otillräckligt samarbete mellan civila och försvarsrelaterade aktörer när det gäller forskning och innovation om cybersäkerhet.** Problemet med otillräckligt samarbete finns även mellan civila och försvarsrelaterade aktörer. För närvarande tillvaratas inte alla synergieffekter eftersom det saknas effektiva mekanismer för att dessa aktörer ska kunna samarbeta effektivt och bygga förtroende, vilket i ännu större utsträckning än på andra områden är en förutsättning för ett framgångsrikt samarbete. Förutom detta finns det

begränsad finansiell kapacitet på EU:s cybersäkerhetsmarknad, bl.a. en brist på medel för innovation.

- **Förenlighet med befintliga bestämmelser inom området**

Kompetensnätverket och det europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning ska fungera som ett ytterligare stöd vid sidan om befintliga bestämmelser och aktörer på cybersäkerhetsområdet. Det europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning ska ha ett uppdrag som kompletterar Enisas arbete men ha en annan inriktning och kräva annan kompetens. Medan Enisa ska ha en rådgivande roll när det gäller forskning och innovation inom cybersäkerhet i EU föreslås centrumet i första hand ha andra uppgifter som är avgörande för att stärka resiliensen inom EU på cybersäkerhetsområdet. Enisas uppdrag omfattar dessutom inte den typ av aktiviteter som skulle vara centrumets och nätverkets kärnuppgifter – att stimulera utveckling och användning av cybersäkerhetsteknik och att komplettera kapacitetsuppbyggnaden på detta område inom EU och nationellt.

Det europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning ska tillsammans med kompetensnätverket för cybersäkerhet även stödja forskning för att främja och påskynda standardiserings- och certifieringsprocesser, i synnerhet de som rör certifieringssystem i den mening som avses i förslaget till cybersäkerhetsakt[13][14].

Genom detta initiativ utvidgas i själva verket det offentlig-privata partnerskapet för cybersäkerhet (cPPP), som var det första EU-omfattande försöket att sammanföra cybersäkerhetssektorn, efterfrågesidan (köpare av cybersäkerhetsprodukter och lösningar, inbegripet offentlig förvaltning och kritiska sektorer som transport, hälsa, energi och finans) och forskarsamhället för att skapa en plattform för kontinuerlig dialog och förutsättningar för frivillig samfinansiering. cPPP etablerades 2016 och har lett till investeringar på upp till 1,8 miljarder euro fram till 2020. Storleken på de investeringar som är på gång i andra delar av världen (t.ex. investerade USA 19 miljarder euro i cybersäkerhet bara 2017) visar att EU måste göra mer för att nå en kritisk massa av investeringar och komma till rätta med den fragmenterade kapaciteten inom EU.

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

Det europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning ska fungera som gemensamt genomförandeorgan för flera unionsprogram till stöd för cybersäkerhet (programmet för ett digitalt Europa och Horisont Europa-programmet) och förbättra samstämmighet och synergieffekter mellan dem.

Detta initiativ kommer även att göra det möjligt att komplettera medlemsstaternas ansträngningar genom att ge utbildningspolitiska beslutsfattare lämpligt underlag för att förbättra kompetensen inom cybersäkerhet (t.ex. genom att utarbeta läroplaner om

[13] Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”), COM(2017) 477 final/3.

[14] Detta påverkar inte certifieringsmekanismerna i den allmänna dataskyddsförordningen, i vilka dataskyddsmyndigheter spelar en roll, i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (nedan kallad *allmänna dataskyddsförordningen*).

cybersäkerhet i civila och militära utbildningssystem) och få fram kvalificerad arbetskraft inom cybersäkerhet i EU – vilket är viktigt för både cybersäkerhetsföretag och andra sektorer för vilka cybersäkerhet är viktigt. När det gäller teoretisk och praktisk utbildning om it-försvar kommer detta initiativ att vara förenligt med arbetet inom plattformen för utbildning, träning och övning inom cyberförsvar, som inrättades inom Europeiska säkerhets- och försvarsakademin.

Detta initiativ kommer att komplettera och stödja arbetet i de digitala innovationsknutpunkterna inom ramen för programmet för det digitala Europa. Digitala innovationsknutpunkter är ideella organisationer som hjälper företag – särskilt nystartade företag, små och medelstora företag samt medelstora börsbolag – att bli mer konkurrenskraftiga genom att förbättra sina affärs-/produktionsprocesser och produkter och tjänster med hjälp av smarta innovationer som är möjliga tack vare digital teknik. Digitala innovationsknutpunkter erbjuder affärsorienterade innovationstjänster som marknadsinformation, finansieringsrådgivning, relevanta test- och försöksmöjligheter, utbildning och kunskapsutveckling för att nya produkter och tjänster ska kunna lanseras på marknaden eller för att införa bättre produktionsprocesser. En del digitala innovationsknutpunkter, som besitter särskild sakkunskap inom cybersäkerhet, kan delta direkt i den kompetensgemenskap för cybersäkerhet som etableras genom detta initiativ. I de flesta fall skulle emellertid digitala innovationsknutpunkter utan någon särskild cybersäkerhetsprofil hjälpa sina medlemmar att få tillgång till den expertis, kunskap och kapacitet inom cybersäkerhet som finns i kompetenscentrumet för cybersäkerhet genom att ha ett nära samarbete med nätverket av nationella samordningscentrum och det europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning. Digitala innovationsknutpunkter skulle även främja införande av innovativa cybersäkerhetsprodukter och lösningar som tillgodoser företagens och andra slutanvändares behov. Sektorsspecifika digitala innovationsknutpunkter skulle sist men inte minst kunna dela med sig av sina kunskaper om sektorernas verkliga behov till nätverket och centrumet så att forsknings- och innovationsagendan svarar mot företagens behov.

Synergieffekter med EIT:s (Europeiska institutet för innovation och teknik) relevanta kunskaps- och innovationsgrupper, särskilt EIT Digital, ska eftersträvas.

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

• Rättslig grund

Kompetenscentrumet bör med hänsyn till sin karaktär och sina särskilda mål etableras på två rättsliga grunder. På grundval av artikel 187 i EUF-fördraget kan kompetenscentrumet genom att inrätta de strukturer som behövs för att effektivt genomföra unionens program för forskning, teknisk utveckling och demonstration uppnå synergieffekter och samla resurser för att investera i den kapacitet som behövs på medlemsstatsnivå och utveckla europeiska gemensamma tillgångar (t.ex. genom att gemensamt köpa in nödvändig infrastruktur för tester och försök inom cybersäkerhet). Sådana åtgärder kan antas enligt artikel 188 första stycket. Artikel 188 första stycket räcker emellertid inte som rättslig grund om andra aktiviteter än forskning och utveckling ska bedrivas för att uppnå kompetenscentrumets mål enligt denna förordning, dvs. att stödja marknadens upptag av cybersäkerhetsprodukter och lösningar, hjälpa den europeiska cybersäkerhetssektorn att bli mer konkurrenskraftig och öka sin marknadsandel samt att tillföra ett mervärde till de nationella ansträngningarna att komma till rätta med bristen på kvalificerad arbetskraft inom cybersäkerhet. För att uppnå dessa mål är

det därför nödvändigt att lägga till artikel 173.3 som en rättslig grund, eftersom den gör det möjligt för unionen att vidta åtgärder för att stödja industrins konkurrenskraft.

- **Motivering av förslaget med hänsyn till subsidiaritets- och proportionalitetsprinciperna**

Cybersäkerhet är en fråga av gemensamt intresse för unionen, vilket bekräftades i de ovannämnda rådsslutsatserna. Ett tydligt exempel är omfattningen av gränsöverskridande incidenter som *WannaCry* och *NonPetya*. EU måste med tanke på de tekniska cybersäkerhetsutmaningarnas karaktär och omfattning, liksom den otillräckliga samordningen av ansträngningar inom och mellan näringsliv, offentlig sektor och forskarsamhället, ge ytterligare stöd till samordningsansträngningar för att både uppnå en kritisk massa resurser och säkerställa en bättre kunskaps- och tillgångshantering. Detta är nödvändigt med tanke på de resurser som krävs för viss forskning, utveckling och användning av cybersäkerhetsteknik, vikten av tvärdisciplinär tillgång till cybersäkerhetskunskaper inom olika discipliner (som ofta bara delvis är tillgängliga på nationell nivå), de globala industriella värdekedjorna och globala konkurrenters verksamhet på olika marknader.

Detta kräver resurser och sakkunskap av en omfattning som knappast kan uppnås av enskilda medlemsstater. Ett Europatäckande nätverk för kvantkommunikation kan t.ex. kräva EU-investeringar på omkring 900 miljoner euro, beroende på vilka investeringar medlemsstaterna gör (för att vara kompatibla med/komplettera dessa) och i vilken utsträckning tekniken gör det möjligt att återanvända befintlig infrastruktur. Initiativet är vara avgörande för att slå samman finansiella resurser och möjliggöra denna typ av investeringar i unionen.

Målen med detta initiativ kan inte uppnås fullt ut av medlemsstaterna själva. Som framgår ovan kan de lättare uppnås på EU-nivå genom att insatser slås samman och inte överlappar varandra, så att det blir möjligt att uppnå en kritisk massa av investeringar och säkerställa att offentliga medel används på bästa möjliga sätt. I enlighet med proportionalitetsprincipen går denna förordning samtidigt inte utöver vad som är nödvändigt för att uppnå detta mål. Insatser på EU-nivå är därför motiverat av subsidiaritets- och proportionalitetsskäl.

Denna rättsakt medför inga nya regelstadgade skyldigheter för företag. Företag, framför allt små och medelstora företag, kan sannolikt sänka sina kostnader för att ta fram innovativa cybersäkra produkter eftersom initiativet gör det möjligt att slå samman resurser för att investera i nödvändig kapacitet på medlemsstatsnivå eller utveckla europeiska gemensamma tillgångar (t.ex. genom att gemensamt köpa in nödvändiga tester och försök inom cybersäkerhet). Dessa tillgångar kan användas av industrier och små och medelstora företag inom olika sektorer för att cybersäkra produkter och göra cybersäkerhet till en konkurrensfördel.

- **Val av instrument**

Genom den föreslagna rättsakten inrättas ett organ som ska genomföra cybersäkerhetsåtgärder inom ramen för programmet för ett digitalt Europa och Horisont Europa-programmet. Den beskriver dess mandat, uppdrag och styrningsstruktur. Inrättandet av ett sådant unionsorgan förutsätter antagande av en förordning.

3. SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

Förslaget om att inrätta ett kompetensnätverk för cybersäkerhet med ett Europeiskt kompetenscentrum för cybersäkerhet inom näringsliv, teknik och forskning är ett nytt

initiativ. Det är en fortsättning och utvidgning av det avtalsbaserade offentlig-privata partnerskapet för cybersäkerhet som skapades 2016.

- **Samråd med berörda parter**

Cybersäkerhet är en bred och sektorsövergripande fråga. Kommissionen använde olika samrådsmetoder för att säkerställa att allmänintresset i unionen – och inte ett fåtal intressentgruppers särintressen – verkligen beaktades i detta initiativ. Denna metod säkerställer transparens och ansvarighet i kommissionens arbete. Även om inget öppet offentligt samråd genomfördes specifikt för detta initiativ med tanke på målgruppen (näringsliv, forskarsamhället och medlemsstaterna) hade temat redan tagits upp i flera andra öppna offentliga samråd:

- Ett allmänt öppet offentligt samråd som genomfördes 2018 om investeringar, forskning och innovation, små och medelstora företag och den inre marknaden.
- Ett tolvveckors offentligt samråd online inleddes 2017 för att få in allmänhetens synpunkter (omkring 90 respondenter) om utvärderingen och översynen av Enisa.
- Ett tolvveckors offentligt samråd online genomfördes 2016 i samband med det avtalsbaserade offentlig-privata partnerskapet för cybersäkerhet (omkring 240 respondenter).

Kommissionen organiserade även riktade samråd om detta initiativ, bland annat workshoppar, möten och riktade begäranden om synpunkter (från Enisa och Europeiska försvarsbyrån). Samrådsperioden sträckte sig över sex månader, från november 2017 till mars 2018. Kommissionen gjorde även en kartläggning av kunskapscentrum som gjorde det möjligt att samla in svar från 665 sådana centrum om deras kunskap, aktiviteter, arbetsområden och internationella samarbete. Enkäten inleddes i januari och svar som inkom före den 8 mars 2018 beaktades i analysrapporten.

Intressenter från näringsliv och forskarsamhället ansåg att kompetenscentrumet och nätverket kan tillföra ett mervärde till de pågående ansträngningarna på nationell nivå genom att skapa ett Europatäckande ekosystem för cybersäkerhet som möjliggör ökat samarbete mellan forskarsamhället och näringslivet. De ansåg också att EU och medlemsstaterna måste ha en proaktiv, mer långsiktig och strategisk cybersäkerhetspolitik som inte bara är inriktad på forskning och innovation. Intressenterna framförde att det är viktigt med tillgång till test- och försöksmöjligheter och med en högre ambitionsnivå när det gäller att åtgärda bristen på kvalificerad arbetskraft inom cybersäkerhet, t.ex. genom storskaliga europeiska projekt som lockar de största begåvningarna. Allt detta sågs även som nödvändigt för att unionen ska bli världsledande inom cybersäkerhet.

I samband med de samråd som har genomförts sedan september[15] förra året och de särskilda rådsslutsatserna[16] har medlemsstaterna välkomnat planen att inrätta ett kompetensnätverk för cybersäkerhet för att stimulera utveckling och användning av cybersäkerhetsteknik. De har framhållit att det är viktigt att vara inkluderande i förhållande till alla medlemsstater och deras nuvarande spjutspets- och kompetenscenter och att lägga särskild vikt vid komplementaritet. När det närmare bestämt gäller det framtida kompetenscentrumet underströk medlemsstaterna vikten av dess samordnande roll när det gäller att stödja nätverket. Framför allt i fråga om

[15] T.ex. rundabordskonferensen med höga företrädare från medlemsstater, vice ordförande Andrus Ansip och kommissionsledamot Mariya Gabriel den 5 december 2017.

[16] Rådet (allmänna frågor): Rådets slutsatser om det gemensamma meddelandet till Europaparlamentet och rådet: Resiliens, avskräckning och försvar: stärkt cybersäkerhet i EU (20 november 2017)

nationella aktiviteter och behov inom cyberförsvar visade den kartläggning av medlemsstaternas cyberförsvarsbehov som gjordes av europeiska avdelningen för yttre åtgärder i maj 2018 att majoriteten av medlemsstaterna ser EU-mervärdet i teoretisk och praktisk utbildning inom cybersäkerhet och i stödet till näringslivet genom forskning och utveckling.[17] Initiativet skulle genomföras tillsammans med medlemsstaterna eller aktörer som stöds av dessa. Samarbete mellan näringsliv, forskarsamhället och/eller offentlig sektor skulle sammanföra och stärka befintliga aktörer och ansträngningar i stället för att skapa nya. Medlemsstaterna skulle även delta i utformningen av särskilda åtgärder inriktade på offentlig sektor som en direkt användare av cybersäkerhetsteknik och kompetens.

- **Konsekvensbedömning**

En konsekvensbedömning av detta initiativ överlämnades den 11 april 2017 till nämnden för lagstiftningskontroll, som lämnade ett positivt yttrande med reservationer. Konsekvensbedömningen reviderades senare mot bakgrund av nämndens kommentarer. Nämndens yttrande och en bifogad förklaring om hur nämndens kommentarer beaktades offentliggörs tillsammans med detta förslag.

Flera alternativ, både lagstiftning och andra åtgärder, har övervägts i konsekvensbedömningen. En fördjupad bedömning gjordes av följande alternativ:

- Referensscenario – samarbetsbaserat alternativ – fortsättning på den nuvarande strategin att bygga upp industriell och teknisk cybersäkerhetskapacitet i EU genom stöd till forskning och innovation och närliggande samarbetsmekanismer i nionde ramprogrammet.
- Alternativ 1: Kompetensnätverk för cybersäkerhet med ett europeiskt kompetenscentrum för cybersäkerhet inom näringsliv, teknik och forskning, som ska ha det dubbla uppdraget att genomföra åtgärder både till stöd för industriell teknik och inom forskning och innovation.
- Alternativ 2: Kompetensnätverk med ett europeiskt forsknings- och kompetenscentrum för cybersäkerhet som är inriktat på forskning och innovation.

De alternativ som förkastades i ett tidigt skede var 1) att inte vidta några åtgärder alls, 2) att enbart etablera ett kompetensnätverk för cybersäkerhet, 3) att även inrätta en centraliserad struktur, och 4) att använda ett befintligt organ (Enisa – Europeiska unionens byrå för nät- och informationssäkerhet, REA (Genomförandeorganet för forskning) eller Inea (Genomförandeorganet för innovation och nätverk).

Slutsatsen av analysen var att alternativ 1 var bäst för att uppnå initiativets mål och samtidigt uppnådde optimala ekonomiska, sociala och miljörelaterade effekter samt skyddade unionens intressen. Huvudargumenten för detta alternativ var bland annat möjligheten att skapa en verklig cybersäkerhetspolitik som inte bara stöder forskning och utveckling utan även marknadens upptag, flexibilitet att använda olika samarbetsmodeller med nätverket av kompetenscentrum för att optimera utnyttjandet av befintliga kunskaper och resurser, och möjligheter att strukturera samarbetet och gemensamma åtaganden av offentliga och privata intressenter inom alla relevanta sektorer, inklusive försvaret. Alternativ 1 möjliggör sist men inte minst ökade synergieffekter och kan fungera som en genomförandemekanism för två olika finansieringsströmmar för cybersäkerhet inom ramen för nästa fleråriga budgetram (Ett digitalt Europa och Horisont Europa).

[17] EEAS, mars 2018

- **Grundläggande rättigheter**

Initiativet kommer att göra det möjligt för offentliga myndigheter och industrier i medlemsstaterna att mer effektivt förhindra och reagera på cyberhot genom att erbjuda och utrusta sig med säkrare produkter och lösningar. Detta är särskilt relevant för att skydda tillgången till grundläggande tjänster (inom t.ex. transport, hälsa, banktjänster och finansiella tjänster).

Om Europeiska unionen får ökad kapacitet att själv säkra sina produkter och tjänster blir det dessutom lättare för medborgare att utöva sina demokratiska rättigheter (genom att t.ex. bättre skydda deras informationsrelaterade rättigheter enligt stadgan om de grundläggande rättigheterna, i synnerhet rätten till skydd av personuppgifter och privatlivet) och därmed stärka deras förtroende för det digitala samhället och ekonomin.

4. BUDGETKONSEKVENSER

Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning ska, i samarbete med kompetensnätverket för cybersäkerhet, vara det huvudsakliga organet för genomförande av EU:s ekonomiska stöd till cybersäkerhet inom programmen Ett digitalt Europa och Horisont Europa.

Budgetkonsekvenserna av genomförandet av programmet för ett digitalt Europa beskrivs närmare i den finansieringsöversikt som är bifogad detta förslag. Bidraget från finansieringsramen för klustret Inkluderande och säkra samhällen i pelare II ”Globala utmaningar och industriell konkurrenskraft” av Horisont Europa (finansieringsram på totalt 2 800 000 000euro) som avses i artikel 21.1 b ska föreslås av kommissionen under lagstiftningsprocessen och under alla omständigheter innan en politisk överenskommelse har ingåtts. Förslaget kommer att grundas på resultatet av den strategiska planeringsprocess som fastställs i artikel 6.6 i förordning XXX [ramprogrammet om Horisont Europa].

5. ÖVRIGA INSLAG

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

En uttrycklig utvärderingsklausul om att kommissionen ska göra en oberoende utvärdering förutses i detta förslag (artikel 38). Kommissionen kommer därefter att avlägga rapport till Europaparlamentet och rådet om sin utvärdering, som vid behov åtföljs av ett förslag om översyn, för att mäta rättsaktens inverkan och mervärde. Kommissionens ”bättre lagstiftning”-metod för utvärderingar kommer att användas.

Den verkställande direktören bör som fastställs i artikel 17 i detta förslag vartannat år överlämna en utvärdering till styrelsen av den verksamhet som har bedrivits av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket. Den verkställande direktören bör även utarbeta en handlingsplan för uppföljning av de slutsatser som dragits av efterhandsutvärderingarna samt rapportera om framstegen till kommissionen vartannat år. Styrelsen bör som fastställs i artikel 16 i detta förslag ansvara för att övervaka att slutsatserna följs upp på ett tillfredsställande sätt.

Påstådda missförhållanden i kompetenscentrumets verksamhet kan komma att undersökas av Europeiska ombudsmannen i enlighet med artikel 228 i fördraget.

2018/0328 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum

Bidrag från Europeiska kommissionen som presenterades för ledarna vid toppmötet i Salzburg den 19-20 september 2018

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 173.3 och artikel 188 första stycket,

med beaktande av Europeiska kommissionens förslag,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[18],

med beaktande av Regionkommitténs yttrande[19],

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) I takt med att vår vardag och våra ekonomier blir alltmer beroende av digital teknik löper medborgarna också större risk att utsättas för allvarliga cyberincidenter. Vår framtida säkerhet förutsätter bland annat att vi stärker teknikens och näringslivets förmåga att skydda unionen mot cyberhot, eftersom både civil infrastruktur och militär kapacitet är beroende av säkra digitala system.

(2) Sedan cybersäkerhetsstrategin[20] infördes 2013 i syfte att främja ett tillförlitligt, säkert och öppet cyberekosystem har unionen stadigt ökat sina insatser för att hantera utmaningarna inom cybersäkerhet. År 2016 antog unionen de första åtgärderna på cybersäkerhetsområdet genom Europaparlamentets och rådets direktiv (EU) 2016/1148[21] om säkerhet i nätverks- och informationssystem.

---

18 EUT C […], […], s. […].

19 EUT C […], […], s. […].

20 Gemensamt meddelande till Europaparlamentet och rådet: EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd JOIN(2013) 1 final).

21 Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

(3) I september 2017 lade kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik fram ett gemensamt meddelande[22] om resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU för att ytterligare stärka unionens resiliens, avskräckning och hantering av cyberattacker.

(4) Vid det digitala toppmötet i Tallinn i september 2017 uppmanade stats- och regeringscheferna unionen att bli ”ledande när det gäller cybersäkerhet senast 2025 för att försäkra oss om att våra medborgare, konsumenter och företag kan ha förtroende för och åtnjuta skydd på internet och för att möjliggöra ett fritt internet som styrs av lagen”.

(5) Allvarliga störningar i nätverks- och informationssystem kan både drabba enskilda medlemsstater och unionen som helhet. Det är därför helt nödvändigt för en väl fungerande inre marknad att nätverks- och informationssystem är säkra. Unionen är för närvarande beroende av icke-europeiska leverantörer av cybersäkerhetslösningar. Det ligger emellertid i unionens strategiska intresse att bibehålla och vidareutveckla nödvändig teknisk kapacitet inom cybersäkerhet för att trygga sin digitala inre marknad och framför allt skydda kritiska nätverk och informationssystem samt tillhandahålla grundläggande cybersäkerhetstjänster.

(6) Det finns omfattande sakkunskap och erfarenhet inom unionen när det gäller cybersäkerhetsforskning, cybersäkerhetsteknik och industriell utveckling av cybersäkerhetslösningar, men insatserna inom forskarsamhället och näringslivet är fragmenterade, saknar inriktning och ett gemensamt mål, vilket hämmar konkurrenskraften på detta område. Insatser och sakkunskap måste slås ihop, sammanföras i nätverk och användas på ett effektivt sätt för att förstärka och komplettera befintlig kapacitet inom forskning, teknik och näringsliv på EU-nivå och nationellt.

(7) I de rådsslutsatser som antogs i november 2017 uppmanades kommissionen att inom kort tillhandahålla en konsekvensbedömning av och senast i mitten av 2018 föreslå de relevanta rättsliga instrumenten för att skapa ett nätverk av kompetenscentrum för cybersäkerhet och ett europeiskt forsknings- och kompetenscentrum för cybersäkerhet.

(8) Kompetenscentrumet bör vara unionens huvudorgan för sammanslagning av investeringar i cybersäkerhetsforskning, cybersäkerhetsteknik och industriell utveckling av cybersäkerhetslösningar och genomförande av relevanta projekt och initiativ tillsammans med kompetensnätverket för cybersäkerhet. Det bör ge finansiellt stöd till cybersäkerhet från programmen Horisont Europa och Ett digitalt Europa och i lämpliga fall vara öppet för Europeiska regionala utvecklingsfonden och andra program. Detta bör skapa synergieffekter och samordna det ekonomiska stödet till forskning, innovation, teknik och industriell utveckling inom cybersäkerhet och därmed undvika överlappningar.

(9) Med tanke på att målen med detta initiativ bäst uppnås om alla eller så många medlemsstater som möjligt deltar, och som ett incitament för medlemsstaterna att delta, bör bara medlemsstater som bidrar till finansieringen av kompetenscentrumets administrativa och operativa kostnader ha rösträtt.

(10) De deltagande medlemsstaternas del av finansieringen bör stå i proportion till unionens bidrag till finansieringen av detta initiativ.

---

[22] Gemensamt meddelande till Europaparlamentet och rådet – Resiliens, avskräckning och försvar: stärkt cybersäkerhet i EU, JOIN(2017) 450 final.

(11) Kompetenscentrumet bör främja och bidra till att samordna arbetet inom kompetensnätverket för cybersäkerhet (nedan kallat *nätverket*), vilket ska utgöras av nationella samordningscentrum i varje medlemsstat. Nationella samordningscentrum bör få direkt finansiellt stöd från unionen, däribland bidrag som beviljas utan någon föregående förslagsinfordran, för att bedriva verksamhet som omfattas av denna förordning.

(12) Nationella samordningscentrum bör utses av medlemsstaterna. Förutom nödvändig administrativ kapacitet bör samordningscentrumen själva besitta eller ha direkt tillgång till teknisk sakkunskap inom cybersäkerhet, framför allt när det gäller kryptografi, IKT-säkerhetstjänster, intrångsdetektering, systemsäkerhet, nätverkssäkerhet, programvaru- och applikationssäkerhet samt säkerhets- och integritetsaspekter för enskilda och samhället. De bör även ha kapacitet att effektivt samverka och samordna med näringsliv, offentlig sektor, inklusive de myndigheter som utses i enlighet med Europaparlamentets och rådets direktiv (EU) 2016/1148[23], och forskarsamhället.

(13) Om finansiellt stöd ges till nationella samordningscentrum för att stödja tredje parter på nationell nivå ska det vidarebefordras till relevanta intressenter genom kaskadavtal.

(14) Ny teknik som artificiell intelligens, sakernas internet, högpresterande datorsystem, kvantdatorer, blockkedjor och säkra digitala identiteter leder till nya utmaningar när det gäller cybersäkerhet men erbjuder samtidigt lösningar. För att bedöma och validera befintliga och framtida IKT-systems resiliens krävs tester av säkerhetslösningar mot attacker mot högpresterande datorsystem och kvantmaskiner. Kompetenscentrumet, nätverket och kompetensgemenskapen för cybersäkerhet bör driva på och sprida de senaste cybersäkerhetslösningarna. Kompetenscentrumet och nätverket bör samtidigt stå till tjänst för produktutvecklare och aktörer inom kritiska sektorer som transport, energi, hälsa, finans, offentlig förvaltning, telekommunikation, tillverkningsindustri, försvar och rymden och hjälpa dem att hantera sina utmaningar inom cybersäkerhet.

(15) Kompetenscentrumet bör ha flera viktiga funktioner. För det första bör det främja och bidra till att samordna arbetet inom det europeiska kompetensnätverket för cybersäkerhet och stödja kompetensgemenskapen för cybersäkerhet. Centrumet bör driva agendan i cybersäkerhetsfrågor och göra det lättare att få tillgång till den sakkunskap som samlas i nätverket och kompetensgemenskapen för cybersäkerhet. För det andra bör kompetenscentrumet genomföra relevanta delar av programmen Ett digitalt Europa och Horisont Europa genom att bevilja bidrag, normalt efter en förslagsinfordran. För det tredje bör kompetenscentrumet främja gemensamma investeringar av unionen, medlemsstaterna och/eller näringslivet.

(16) Kompetenscentrumet bör stimulera och stödja samarbete och samordning av insatserna inom kompetensgemenskapen för cybersäkerhet, som ska vara en stor och öppen grupp bestående av många olika aktörer som arbetar med cybersäkerhetsteknik. Kompetensgemenskapen bör i synnerhet omfatta forskningsorganisationer, företag på utbudssidan, företag på efterfrågesidan och offentlig sektor. Kompetensgemenskapen för cybersäkerhet bör lämna synpunkter på kompetenscentrumets insatser och arbetsprogram och även få ta del av kompetenscentrumets och nätverkets

[23] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

gemenskapsbyggande verksamhet, men i övrigt inte ha någon förmånsställning i förslags- eller anbudsinfordringar.

(17) För att svara mot företagens behov på både utbuds- och efterfrågesidan bör kompetenscentrumets uppdrag att erbjuda näringslivet kunskap och tekniskt stöd inom cybersäkerhet gälla både IKT-produkter och IKT-tjänster samt alla andra industriella och tekniska produkter och lösningar i vilka cybersäkerhet är en integrerad del.

(18) Även om kompetenscentrumet och nätverket bör eftersträva synergieffekter mellan cybersäkerhet på det civila och det försvarsrelaterade området ska projekt som finansieras genom Horisont Europa-programmet genomföras i enlighet med förordning XXX [Horisont Europa-förordningen], i vilken det fastställs att forsknings- och innovationsverksamhet som utförs inom ramen för Horisont Europa ska fokusera på civila tillämpningar.

(19) För att säkerställa ett strukturerat och hållbart samarbete bör förhållandet mellan kompetenscentrumet och de nationella samordningscentrumen regleras genom ett avtal.

(20) Lämpliga bestämmelser bör införas som garanterar kompetenscentrumets ansvar och transparens.

(21) Med tanke på deras respektive sakkunskap inom cybersäkerhet bör kommissionens gemensamma forskningscentrum och Europeiska byrån för nät- och informationssäkerhet (Enisa) spela en aktiv roll i kompetensgemenskapen för cybersäkerhet och i den rådgivande näringslivs- och vetenskapsnämnden.

(22) Nationella samordningscentrum och aktörer som ingår i kompetensgemenskapen för cybersäkerhet bör, om de får finansiella bidrag från unionens allmänna budget, offentliggöra att de relevanta aktiviteterna genomförs inom ramen för detta initiativ.

(23) Unionens bidrag till kompetenscentrumet bör finansiera hälften av kostnaderna för centrumets etablering samt administrations- och samordningsverksamhet. För att undvika dubbelfinansiering bör dessa aktiviteter inte samtidigt få bidrag från andra unionsprogram.

(24) Kompetenscentrumets styrelse, bestående av företrädare för medlemsstaterna och kommissionen, bör fastställa den allmänna inriktningen för kompetenscentrumets verksamhet och säkerställa att det fullgör sitt uppdrag i enlighet med denna förordning. Styrelsen bör få nödvändiga befogenheter att fastställa budgeten och kontrollera dess genomförande, anta lämpliga finansiella regler, fastställa klara och tydliga förfaranden för kompetenscentrumets beslutsfattande, anta kompetenscentrumets arbetsprogram och fleråriga strategiska plan som återspeglar prioriteringarna vid fullgörandet av kompetenscentrumets mål och uppgifter, anta sin egen arbetsordning, utse en verkställande direktör och besluta om förlängning respektive avslutande av dennes förordnande.

(25) För att kompetenscentrumet ska fungera väl och effektivt bör kommissionen och medlemsstaterna säkerställa att personer som utses till styrelseledamöter har lämplig yrkesmässig sakkunskap och erfarenhet inom verksamhetsområdena. För att skapa kontinuitet i styrelsens arbete bör medlemsstaterna och kommissionen även eftersträva att begränsa omsättningen av deras respektive företrädare.

(26) För att kompetenscentrumet ska fungera väl krävs att den verkställande direktören utses på grundval av sina meriter, sin dokumenterade kompetens inom förvaltning och

ledarskap samt sina kvalifikationer och erfarenheter inom cybersäkerhet, och den verkställande direktören bör vara helt oberoende i fullgörandet av sitt uppdrag.

(27) Kompetenscentrumet bör ha en näringslivs- och vetenskapsnämnd som rådgivande organ för att säkerställa regelbunden dialog med den privata sektorn, konsumentorganisationer och andra berörda intressenter. Den rådgivande näringslivs- och vetenskapsnämnden bör inrikta sig på frågor som är relevanta för intressenter och göra kompetenscentrumets styrelse uppmärksam på dem. Den rådgivande näringslivs- och vetenskapsnämndens sammansättning och de uppgifter som den tilldelas, t.ex. att rådfrågas om arbetsprogrammet, bör säkerställa att intressenter ges en tillräcklig representation i kompetenscentrumets verksamhet.

(28) Kompetenscentrumet bör genom sin rådgivande näringslivs- och vetenskapsnämnd få ta del av den särskilda sakkunskap och den breda och relevanta representation av intressenter som etableras genom det offentlig-privata partnerskapet om cybersäkerhet under Horisont 2020-programmets löptid.

(29) Kompetenscentrumet bör ha regler för att förebygga och hantera intressekonflikter. Kompetenscentrumet bör vidare tillämpa relevanta unionsbestämmelser om allmänhetens tillgång till handlingar enligt Europaparlamentets och rådets förordning (EG) nr 1049/2001[24]. Kompetenscentrumets behandling av personuppgifter ska omfattas av Europaparlamentets och rådets förordning (EU) nr XXX/2018. Kompetenscentrumet bör följa de bestämmelser som är tillämpliga på unionens institutioner och den nationella lagstiftning som rör hantering av information, i synnerhet känsliga icke-säkerhetsskyddsklassificerade uppgifter och säkerhetsskyddsklassificerade EU-uppgifter.

(30) Unionens ekonomiska intressen bör under hela utgiftscykeln skyddas genom proportionella åtgärder, inbegripet åtgärder för att förebygga, spåra och utreda oriktigheter, återkräva medel som förlorats, utbetalats på felaktiga grunder eller använts felaktigt och, när så är tillämpligt, tillämpa administrativa och ekonomiska i enlighet med Europaparlamentets och rådets förordning (EU, Euratom) nr XXX[25] [nedan kallad *budgetförordningen*].

(31) Kompetenscentrumet bör bedriva sin verksamhet på ett öppet och transparent sätt, utan dröjsmål tillhandahålla all relevant information och synliggöra sin verksamhet genom bland annat informations- och upplysningsinsatser riktade till allmänheten. Arbetsordningen för kompetenscentrumets organ bör vara offentlig.

(32) Kommissionens internrevisor bör utöva samma befogenheter över kompetenscentrumet som över kommissionen.

(33) Kommissionen, kompetenscentrumet, revisionsrätten och Europeiska byrån för bedrägeribekämpning bör få tillgång till all information och alla lokaler som de behöver för att genomföra revisioner och utredningar avseende bidrag, avtal och överenskommelser som ingåtts av kompetenscentrumet.

(34) Unionen kan vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen, eftersom målen med denna förordning, nämligen att bibehålla och vidareutveckla unionens tekniska och industriella kapacitet inom cybersäkerhet,

---

[24] Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (EGT L 145, 31.5.2001, s. 43).

[25] [infoga titel och EUT-hänvisning]

stärka konkurrenskraften hos unionens cybersäkerhetssektor och göra cybersäkerhet till en konkurrensfördel för andra sektorer inom unionen, på grund av att de befintliga, begränsade resurserna är utspridda och att det krävs omfattande investeringar, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna, utan, för att undvika onödiga överlappningar mellan olika ansträngningar, för att uppnå en kritisk massa av investeringar och för att säkerställa att offentliga medel används på bästa möjliga sätt, lättare kan uppnås på unionsnivå. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER OCH PRINCIPER FÖR KOMPETENSCENTRUMET OCH NÄTVERKET

Artikel 1

Syfte

1. Genom denna förordning upprättas Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning (nedan kallat kompetenscentrumet) och nätverket av nationella samordningscentrum, och det fastställs regler för utnämningen av nationella samordningscentrum och för upprättandet av kompetensgemenskapen för cybersäkerhet.

2. Kompetenscentrumet ska bidra till genomförandet av cybersäkerhetsdelen av det program för ett digitalt Europa som inrättades genom förordning (EU) [...] och i synnerhet åtgärder som har anknytning till artikel 6 i förordning (EU) nr XXX [programmet för ett digitalt Europa] och av det Horisont Europa-program som inrättades genom förordning nr XXX och i synnerhet avsnitt 2.2.6 i pelare II i bilaga I till beslut nr XXX om inrättandet av det särskilda programmet för genomförande av Horisont Europa – ramprogrammet för forskning och innovation [ref.nr till det specifika programmet].

3. Kompetenscentrumet ska ha sitt säte i Bryssel i Belgien.

4. Kompetenscentrumet ska vara en juridisk person. Det ska i varje medlemsstat ha den mest vittgående rättskapacitet som tillerkänns juridiska personer enligt den nationella lagstiftningen. Det ska särskilt kunna förvärva och avyttra fast och lös egendom samt föra talan inför domstolar och andra myndigheter.

Artikel 2

Definitioner

I denna förordning gäller följande definitioner: cybersäkerhet:

(1) att skydda nät- och informationssystem, deras användare och andra personer mot cyberhot. cybersäkerhetsprodukter och cybersäkerhetslösningar:

(2) IKT-produkter, IKT-tjänster och IKT-processer som är specifikt utformade för att skydda nät- och informationssystem, deras användare och andra personer mot cyberhot. offentlig myndighet:

(3) statlig eller annan offentlig förvaltning, inbegripet offentliga rådgivande organ, på nationell, regional eller lokal nivå, eller fysisk eller juridisk person som har offentliga förvaltningsuppgifter enligt nationell lag, inklusive särskilda uppdrag.

(4) deltagande medlemsstat: medlemsstat som frivilligt bidrar ekonomiskt till kompetenscentrumets administrativa kostnader och driftskostnader.

Artikel 3

Centrumets och nätverkets uppdrag

1. Kompetenscentrumet och nätverket ska hjälpa unionen att

   (a) behålla och utveckla den tekniska och industriella kapacitet inom cybersäkerhet som krävs för att säkra unionens digitala inre marknad,

   (b) göra unionens cybersäkerhetssektor mer konkurrenskraftig och göra cybersäkerhet till en konkurrensfördel inom unionens övriga sektorer.

2. Kompetenscentrumet ska i lämpliga fall utföra sina uppgifter i samarbete med nätverket av nationella samordningscentrum och en kompetensgemenskap för cybersäkerhet.

Artikel 4

Kompetenscentrumets mål och uppgifter

Kompetenscentrumet ska ha följande mål och därmed sammanhängande uppgifter:

1. Underlätta och hjälpa till att samordna arbetet inom det nätverk av nationella samordningscentrum (nedan kallat *nätverket*) som avses i artikel 6 och kompetensgemenskapen som avses i artikel 8.

2. Bidra till genomförandet av cybersäkerhetsdelen av det program för ett digitalt Europa som inrättades genom förordning (EU) XXX[26] och i synnerhet åtgärder som har anknytning till artikel 6 i förordning (EU) nr XXX [programmet för ett digitalt Europa] och av det Horisont Europa-program som inrättades genom förordning nr XXX[27] och i synnerhet avsnitt 2.2.6 i pelare II i bilaga I till beslut nr XXX om inrättandet av det särskilda programmet för genomförande av Horisont Europa – ramprogrammet för forskning och innovation [ref.nr till det specifika programmet].

3. Stärka cybersäkerhetskapaciteten, cybersäkerhetskunskapen och cybersäkerhetsinfrastrukturen till förfogande för näringslivet, den offentliga sektorn och forskarsamhället, genom att utföra följande uppgifter:

   (a) När det gäller den senaste cybersäkerhetsinfrastrukturen för näringsliv och forskning och därmed sammanhängande tjänster, förvärva, uppgradera, ta i drift och göra sådan infrastruktur och därmed sammahängande tjänster tillgängliga för ett brett spektrum av användare i hela unionen från näringslivet, inklusive små och medelstora företag, offentlig sektor och forskarsamhället.

   (b) När det gäller avancerad industri- och forskningsinfrastruktur inom cybersäkerhet och därmed sammanhängande tjänster, ge stöd till andra

[26] [Ange fullständig titel och EUT-hänvisning].
[27] [Ange fullständig titel och EUT-hänvisning].

aktörer, inklusive ekonomiskt stöd, för att införskaffa, uppdatera, ta i drift och göra sådan infrastruktur och därmed sammahängande tjänster tillgänglig för ett brett spektrum av användare i hela unionen från näringslivet, inklusive de små och medelstora företagen, den offentliga sektorn och forsknings- och vetenskapsvärlden.

(c) Tillhandahålla kunskap och tekniskt stöd inom cybersäkerhet till företag och offentliga myndigheter, särskilt genom att stödja åtgärder avsedda att underlätta tillgången till den sakkunskap som finns i nätverket och i kompetensgemenskapen.

4. Bidra till brett införande av avancerade produkter och lösningar inom cybersäkerhet i hela ekonomin, genom att utföra följande uppgifter:

(a) Stimulera forskning och utveckling inom cybersäkerhet och offentliga myndigheters och användarindustriers användning av unionens cybersäkerhetsprodukter och cybersäkerhetslösningar.

(b) Hjälpa offentliga myndigheter, företag på efterfrågesidan och andra användare att anta och integrera de senaste cybersäkerhetslösningarna.

(c) Hjälpa i synnerhet offentliga myndigheter att anordna offentliga upphandlingar eller handla upp avancerade cybersäkerhetsprodukter och cybersäkerhetslösningar på offentliga myndigheters vägnar.

(d) Ge ekonomiskt stöd och tekniskt bistånd till nystartade och små och medelstora cybersäkerhetsföretag att få tillträde till potentiella marknader och locka till sig investeringar.

5. Förbättra kunskaperna om cybersäkerhet och bidra till att minska bristen på kvalificerad arbetskraft inom cybersäkerhet i unionen genom att utföra följande uppgifter:

(a) Ge stöd till ytterligare kompetensutveckling inom cybersäkerhet, när så är lämpligt tillsammans med de relevanta EU-byråerna och EU-organen, bl.a. Enisa.

6. Bidra till ökad forskning och utveckling inom cybersäkerhet i unionen genom att

(a) ge ekonomiskt stöd till forskning om cybersäkerhet på grundval av en gemensam och förbättrad flerårig strategisk agenda för näringsliv, teknik och forskning som utvärderas fortlöpande,

(b) stödja storskaliga forsknings- och demonstrationsprojekt kring nästa generation cybersäkerhetsteknik i samarbete med näringslivet och nätverket,

(c) stödja forskning och innovation för standardisering av cybersäkerhetsteknik.

7. Stärka samarbetet mellan civila och försvarsrelaterade sektorer när det gäller teknikens och tillämpningarnas dubbla användningsområden inom cybersäkerhet genom att utföra följande uppgifter:

(a) Ge medlemsstater och intressenter från näringslivet och forskarsamhället stöd vad gäller forskning, utveckling och ibruktagande.

(b) Bidra till samarbetet mellan medlemsstater genom att stödja utbildning, fortbildning och övningar.

(c) Sammanföra intressenter för att skapa synergieffekter mellan den civila och den försvarsrelaterade sektorns forskning och marknader på cybersäkerhetsområdet.

8. Stärka synergieffekterna mellan cybersäkerhet på det civila respektive det försvarsrelaterade området rörande Europeiska försvarsfonden genom att utföra följande uppgifter:

(a) Tillhandahålla rådgivning, utbyta sakkunskap och underlätta samarbete bland de relevanta intressenterna.

(b) Driva multinationella cybersäkerhetsprojekt, på medlemsstaternas begäran, och därmed agera projektledare i den mening som avses i förordning XXX [förordningen om upprättande av Europeiska försvarsfonden].

Artikel 5

Investering i och utnyttjande av infrastruktur, kapacitet, produkter eller lösningar

1. När kompetenscentrumet tillhandahåller finansiering för infrastruktur, kapacitet, produkter eller lösningar i enlighet med artikel 4.3 och 4.4 i form av bidrag eller pris, får följande anges i kompetenscentrumets arbetsplan:

(a) Regler för driften av infrastruktur eller kapacitet, inbegripet, i tillämpliga fall, anförtro åt en aktör att sköta driften utifrån kriterier som ska fastställas av kompetenscentrumet.

(b) Regler för tillgång till och användande av en infrastruktur eller kapacitet.

2. Kompetenscentrumet får ha ansvar för det övergripande genomförandet av relevanta gemensamma upphandlingsåtgärder, bl.a. förkommersiell upphandling, som företrädare för nätverksmedlemmarna, medlemmarna i kompetensgemenskapen eller tredje part som företräder användarna av cybersäkerhetsprodukter och cybersäkerhetslösningar. För detta ändamål får kompetenscentrumet bistås av ett eller flera nationella samordningscentrum eller medlemmar i kompetensgemenskapen.

Artikel 6

Utnämning av nationella samordningscentrum

1. Senast [datum] ska varje medlemsstat utnämna den aktör som ska vara nationellt samordningscentrum i enlighet med denna förordning och anmäla detta till kommissionen.

2. På grundval av en bedömning av om den aktören uppfyller de kriterier som fastställs i punkt 4 ska kommissionen utfärda ett beslut inom sex månader från den dag utnämningen anmäldes av medlemsstaten om ackreditering av den aktören som nationellt samordningscentrum eller om avslag av utnämningen. Förteckningen över nationella samordningscentrum ska offentliggöras av kommissionen.

3. Medlemsstaterna får när som helst utnämna en ny aktör till nationellt samordningscentrum i enlighet med denna förordning. Punkterna 1 och 2 ska gälla vid utnämningen av varje ny aktör.

4. Det utnämnda nationella samordningscentrumet ska kunna ge stöd åt kompetenscentrumet och nätverket i fullgörandet av deras uppdrag enligt artikel 3 i denna förordning. De ska äga eller ges direkt tillgång till teknisk sakkunskap om cybersäkerhet och vara i stånd att föra en dialog med och samordna arbetet med näringslivet, den offentliga sektorn och forskarsamhället.

5. Förhållandet mellan kompetenscentrumet och de nationella samordningscentrumen ska bygga på ett avtal som tecknas mellan kompetenscentrumet och vart och ett av de nationella samordningscentrumen. I avtalet ska fastställas bestämmelser om förhållandet och fördelningen av uppgifter mellan kompetenscentrumet och vart och ett av de nationella samordningscentrumen.

6. Nätverket av nationella samordningscentrum ska bestå av alla de nationella samordningscentrum som utnämnts av medlemsstaterna.

Artikel 7

De nationella samordningscentrumens uppgifter

1. De nationella samordningscentrumen ska ha följande uppgifter:

   (a) Hjälpa kompetenscentrumet att uppfylla sina mål och i synnerhet samordna kompetensgemenskapen.

   (b) Göra det lättare för näringslivet och andra aktörer på medlemsstatsnivå att delta i gränsöverskridande projekt.

   (c) Tillsammans med kompetenscentrumet bidra till att kartlägga och hantera sektorspecifika cybersäkerhetsutmaningar för näringslivet.

   (d) Fungera som kontaktpunkt på nationell nivå för kompetensgemenskapen och kompetenscentrumet.

   (e) Sträva efter att uppnå synergieffekter med relevanta aktiviteter på nationell och regional nivå.

   (f) Genomföra särskilda åtgärder för vilka kompetenscentrumet beviljat bidrag, t.ex. genom att tillhandahålla ekonomiskt stöd till tredje parter i enlighet med artikel 204 i förordning XXX [nya budgetförordningen] enligt de villkor som anges i de berörda bidragsavtalen.

   (g) Främja och sprida relevanta resultat av det arbete som bedrivs inom nätverket, kompetensgemenskapen och kompetenscentrumet på nationell och regional nivå.

   (h) Bedöma begäranden från aktörer som är etablerade i samma medlemsstat som samordningscentrumet om att få ingå i kompetensgemenskapen för cybersäkerhet.

2. I enlighet med punkt f får det ekonomiska stödet till tredje parter tillhandahållas i någon av de former som anges i artikel 125 i förordning XXX [nya budgetförordningen], bland annat i form av klumpsummor.

3. De nationella samordningscentrumen får ta emot bidrag från unionen i enlighet med artikel 195 d i förordning XXX [nya budgetförordningen] i samband med utförandet av de uppgifter som fastställs i denna artikel.

4. De nationella samordningscentrumen ska, när så är lämpligt, samarbeta via nätverket för att genomföra de uppgifter som avses i punkterna a, b, c, e och g i punkt 1.

Artikel 8

Kompetensgemenskapen för cybersäkerhet

1. Kompetensgemenskapen för cybersäkerhet ska bidra till kompetenscentrumets uppdrag i enlighet med vad som anges i artikel 3 och öka och sprida sakkunskap om cybersäkerhet i hela unionen.

2. Kompetensgemenskapen för cybersäkerhet ska bestå av näringslivet, den akademiska världen, icke vinstdrivande forskningsorganisationer, samt organisationer och offentliga och andra aktörer som arbetar med driftsfrågor och tekniska frågor. Den ska föra samman de viktigaste intressenterna inom teknisk och industriell kapacitet på cybersäkerhetsområdet i unionen. Den ska engagera de nationella samordningscentrumen och de unionsinstitutioner och unionsorgan som har relevant sakkunskap.

3. Endast aktörer som är etablerade inom unionen får ackrediteras som medlemmar i kompetensgemenskapen för cybersäkerhet. De ska kunna visa att de har sakkunskap inom cybersäkerhet på minst ett av områdena

   (a) forskning,

   (b) industriell utveckling,

   (c) utbildning och fortbildning.

4. Kompetenscentrumet ska ackreditera aktörer som etablerats i enlighet med nationell lag som medlemmar i kompetensgemenskapen för cybersäkerhet efter det att det nationella samordningscentrumet i den medlemsstat där den aktören är etablerad gjort en bedömning av om den uppfyller kriterierna i punkt 3. En ackreditering ska inte vara tidsbegränsad men får när som helst återkallas av kompetenscentrumet om kompetenscentrumet eller det relevanta nationella samordningscentrumet anser att den aktören inte uppfyller kriterierna i punkt 3 eller inte omfattas av de relevanta bestämmelserna i artikel 136 i förordning XXX [nya budgetförordningen].

5. Kompetenscentrumet ska ackreditera relevanta unionsinstitutioner, unionsorgan och unionsbyråer som medlemmar i kompetensgemenskapen för cyberssäkerhet efter att ha gjort en bedömning av om de uppfyller kriterierna i punkt 3. En ackreditering ska inte vara tidsbegränsad men kan när som helst återkallas av kompetenscentrumet om det anser att den aktören inte uppfyller kriterierna i punkt 3 eller inte omfattas av de relevanta bestämmelserna i artikel 136 i förordning XXX [nya budgetförordningen].

6. Kommissionens företrädare får delta i kompetensgemenskapens arbete.

Artikel 9

Kompetensgemenskapen för cybersäkerhet: medlemmarnas uppgifter

Medlemmarna i kompetensgemenskapen för cybersäkerhet ska

   (1) hjälpa kompetenscentrumet att fullgöra det uppdrag och uppnå de mål som fastställs i artiklarna 3 och 4 och för detta ändamål föra ett nära samarbete med kompetenscentrumet och de relevanta nationella samordningscentrumen,

   (2) delta i den verksamhet som främjas av kompetenscentrumet och de nationella samordningscentrumen,

(3) i relevanta fall, delta i de arbetsgrupper som inrättas av kompetenscentrumets styrelse för att utföra särskilda uppgifter i enlighet med kompetenscentrumets arbetsplan,

(4) i relevanta fall stödja kompetenscentrumet och de nationella samordningscentrumen i främjandet av specifika projekt,

(5) främja och sprida relevanta resultat av de uppgifter och projekt som genomförts inom kompetensgemenskapen.

Artikel 10

Kompetenscentrumets samarbete med unionens institutioner, organ, kontor och byråer

1. Kompetenscentrumet ska samarbeta med unionens relevanta institutioner, organ, kontor och byråer, bl.a. Europeiska unionens byrå för nät- och informationssäkerhet (Enisa), incidenthanteringsorganisationen för EU:s institutioner och byråer (CERT-EU), den europeiska avdelningen för yttre åtgärder, kommissionens gemensamma forskningscentrum, genomförandeorganet för forskning (Rea), genomförandeorganet för innovation och nätverk (Inea), Europeiska it-brottscentrumet vid Europol och Europeiska försvarsbyrån (EDA).
2. Samarbetet ska ske inom ramen för samarbetsavtal. Sådana avtal ska föreläggas kommissionen för förhandsgodkännande.

KAPITEL II

KOMPETENSCENTRUMETS ORGANISATION

Artikel 11

Medlemmar och struktur

1. Medlemmar i kompetenscentrumet ska vara unionen, företrädd av kommissionen, och medlemsstaterna.
2. Kompetenscentrumets struktur ska omfatta följande:

(a) En styrelse, som ska ha de uppgifter som anges i artikel 13.

(b) En verkställande direktör, som ska ha de uppgifter som anges i artikel 16.

(c) En rådgivande näringslivs- och vetenskapsnämnd, som ska utföra de uppgifter som anges i artikel 20,

AVSNITT I

STYRELSEN

Artikel 12

Styrelsens sammansättning

1. Styrelsen ska bestå av en företrädare för varje medlemsstat och fem företrädare från kommissionen som ska representera unionen.
2. Varje ledamot av styrelsen ska ha en suppleant som företräder ledamoten i hans eller hennes frånvaro.

3. Styrelseledamöterna och deras suppleanter ska utses mot bakgrund av deras kunskaper inom teknik, och relevanta kunskaper i fråga om ledarskap, administration och budget. Kommissionen och medlemsstaterna ska bemöda sig om att begränsa omsättningen av sina företrädare i styrelsen för att säkerställa kontinuitet i styrelsens arbete. Kommissionen och medlemsstaterna ska ha som mål att uppnå en jämn könsfördelning i styrelsen.

4. Mandatperioden för styrelsens ledamöter och deras suppleanter ska vara fyra år. Mandatperioden får förlängas.

5. Styrelseledamöterna ska handla i kompetenscentrumets intresse och främja dess mål, uppdrag, identitet, självständighet och enhetlighet på ett oberoende och transparent sätt.

6. Kommissionen får vid behov bjuda in observatörer, inklusive företrädare för unionens berörda byråer och organ, att delta i styrelsens sammanträden.

7. Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) ska vara ständig observatör i styrelsen.

Artikel 13

Styrelsens uppgifter

1. Styrelsen ska ha det övergripande ansvaret för kompetenscentrumets strategiska inriktning och drift och ska övervaka genomförandet av dess verksamhet.

2. Styrelsen ska själv anta sin arbetsordning. Den ska omfatta särskilda förfaranden för att fastställa och undvika intressekonflikter och säkerställa konfidentialiteten för känslig information.

3. Styrelsen ska fatta nödvändiga strategiska beslut, och särskilt

   (a) anta en flerårig strategisk plan som ska innehålla med en redogörelse för kompetenscentrumets huvudsakliga prioriteringar och planerade initiativ, inklusive en uppskattning av finansieringsbehov och finansieringskällor,

   (b) anta kompetenscentrumets arbetsplan, årsredovisning och balansräkning samt årliga verksamhetsrapport på grundval av ett förslag från verkställande direktören,

   (c) anta kompetenscentrumets särskilda finansiella regler i enlighet med [artikel 70 i budgetförordningen],

   (d) anta ett förfarande för utnämning av den verkställande direktören,

   (e) anta kriterier och förfaranden för att bedöma och ackreditera aktörer som medlemmar i kompetensgemenskapen för cybersäkerhet,

   (f) utse, entlediga, förlänga mandatperioden för och ge vägledning till den verkställande direktören, övervaka dennes resultat samt utse räkenskapsföraren,

   (g) anta kompetenscentrumets årliga budget, inbegripet motsvarande tjänsteförteckning med uppgifter om antalet tillfälliga tjänster per tjänstegrupp och grad, antalet kontraktsanställda och utlånade nationella experter uttryckt i heltidsekvivalenter,

   (h) anta regler för intressekonflikter,

(i) inrätta arbetsgrupper med medlemmar i kompetensgemenskapen för cybersäkerhet,

(j) utse medlemmarna i den rådgivande näringslivs- och vetenskapsnämnden,

(k) inrätta en intern revisionsfunktion i enlighet med kommissionens delegerade förordning (EU) nr 1271/2013[28],

(l) sprida information om kompetenscentrumets verksamhet internationellt för att öka dess attraktionskraft och göra det till ett spjutspetsorgan i världsklass inom cybersäkerhet,

(m) fastställa kompetenscentrumets kommunikationspolicy på rekommendation av den verkställande direktören,

(n) ansvara för att övervaka att det sker en lämplig uppföljning av slutsatser som dragits av efterhandsutvärderingar,

(o) vid behov fastställa genomförandebestämmelser för tjänsteföreskrifterna och anställningsvillkoren i enlighet med artikel 13.3,

(p) vid behov fastställa bestämmelser om utlåning av nationella experter till kompetenscentrumet och om användning av praktikanter i enlighet med artikel 32.2,

(q) anta säkerhetsregler för kompetenscentrumet,

(r) anta en bedrägeribekämpningsstrategi som står i proportion till bedrägeririskerna med beaktande av en kostnads–nyttoanalys av de åtgärder som ska genomföras,

(s) anta en metod för beräkning av det finansiella bidraget från medlemsstaterna,

(t) ansvara för alla uppgifter som inte uttryckligen tilldelats ett särskilt organ inom kompetenscentrumet; den får delegera dessa till något av kompetenscentrumets organ.

Artikel 14

Styrelseordförande och styrelsens sammanträden

1. Styrelsen ska välja en ordförande och en vice ordförande bland sina röstberättigade ledamöter för en period av två år. Ordförandens och vice ordförandens mandat får efter beslut av styrelsen förlängas en gång. Om deras styrelseuppdrag emellertid upphör någon gång under deras mandatperiod, upphör deras mandatperiod automatiskt vid denna tidpunkt. Vice ordföranden ska träda i ordförandens ställe om ordföranden inte kan fullgöra sitt uppdrag. Ordföranden ska delta i omröstningen.

2. Styrelsen ska hålla ordinarie sammanträden minst tre gånger per år. Den får hålla extraordinarie sammanträden på begäran av kommissionen, en tredjedel av ledamöterna, ordföranden eller den verkställande direktören vid fullgörandet av hans eller hennes uppgifter.

[28] Kommissionens delegerade förordning (EU) nr 1271/2013 av den 30 september 2013 med rambudgetförordning för de organ som avses i artikel 208 i Europaparlamentets och rådets förordning (EU, Euratom) nr 966/2012 (EUT L 328, 7.12.2013, s. 42.)

3. Den verkställande direktören ska delta i diskussionerna, såvida inte styrelsen beslutar något annat, men ska inte ha någon rösträtt. Styrelsen får bjuda in andra personer att närvara vid dess sammanträden som observatörer i enskilda fall.

4. Ledamöterna i den rådgivande näringslivs- och vetenskapsnämnden får på ordförandens inbjudan delta i styrelsens sammanträden utan rösträtt.

5. Om inte annat följer av styrelsens arbetsordning får styrelseledamöterna och deras suppleanter bistås av rådgivare eller experter vid sammanträdena.

6. Kompetenscentrumet ska tillhandahålla sekretariatet för styrelsen.

Artikel 15

Omröstningsregler för styrelsen

1. Unionen ska ha 50 % av rösterna. Unionens rösträttigheter ska vara odelbara.

2. Varje deltagande medlemsstat ska ha en röst.

3. Styrelsen ska fatta beslut med en majoritet av minst 75 % av alla röster, inbegripet rösterna från de medlemmar som är frånvarande, vilka står för minst 75 % av det totala ekonomiska bidraget till kompetenscenstrumet. Det ekonomiska bidraget ska beräknas utifrån de utgiftsberäkningar från medlemsstaterna som avses i artikel 17.2 c, och utifrån den rapport om storleken på de deltagande medlemsstaternas bidrag som avses i artikel 22.5.

4. Endast kommissionens företrädare och de deltagande medlemsstaternas företrädare ska ha rösträtt.

5. Ordföranden ska delta i omröstningen.

AVSNITT II

VERKSTÄLLANDE DIREKTÖR

Artikel 16

Utnämning och entledigande av samt förlängning av mandatperioden för den verkställande direktören

1. Den verkställande direktören ska vara en person med sakkunskap och gott anseende på de områden där kompetenscentrumet är verksamt.

2. Den verkställande direktören ska vara tillfälligt anställd vid kompetenscentrumet i enlighet med artikel 2 a i anställningsvillkoren för övriga anställda.

3. Den verkställande direktören ska utnämnas av styrelsen utifrån en förteckning över kandidater som föreslås av kommissionen på grundval av ett öppet och transparent urvalsförfarande.

4. I det avtal som sluts med den verkställande direktören ska kompetenscentrumet företrädas av styrelsens ordförande.

5. Den verkställande direktörens mandatperiod ska vara fyra år. I slutet av denna period ska kommissionen genomföra en utvärdering som beaktar den verkställande direktörens arbetsinsats och kompetenscentrumets framtida uppgifter och utmaningar.

6. Styrelsen får på ett förslag från kommissionen som beaktar den utvärdering som avses i punkt 5 förlänga den verkställande direktörens mandatperiod en gång med högst fyra år.

7. En verkställande direktör vars mandat förlängs får inte delta i något ytterligare uttagningsförfarande för samma befattning.

8. Den verkställande direktören ska avsättas endast efter ett styrelsebeslut på förslag av kommissionen.

Artikel 17

Den verkställande direktörens uppgifter

1. Den verkställande direktören ska ansvara för verksamheten och den dagliga ledningen av kompetenscentrumet och vara dess rättsliga företrädare. Den verkställande direktören ska vara ansvarig inför styrelsen och i sin tjänsteutövning vara fullständigt oberoende inom ramen för sina befogenheter.

2. Den verkställande direktören ska i synnerhet utföra följande uppgifter på ett oberoende sätt:

   (a) Genomföra de beslut som antas av styrelsen.

   (b) Stödja styrelsen i dess arbete, tillhandahålla sekretariatshjälp för deras sammanträden och förse dem med all information som krävs för att de ska kunna fullgöra sina uppgifter.

   (c) Efter samråd med styrelsen och kommissionen, utarbeta och för godkännande överlämna till styrelsen ett utkast till kompetenscentrumets fleråriga strategiska plan och ett utkast till årlig arbetsplan som visar omfattningen av de ansökningsomgångar, intresseanmälningar och anbudsinfordringar som krävs för att genomföra arbetsplanen och motsvarande utgiftsberäkningar enligt förslagen från medlemsstaterna och kommissionen.

   (d) För antagande av styrelsen utarbeta och lämna in ett förslag till årlig budget, inbegripet tillhörande tjänsteförteckning med uppgift om antalet tillfälliga tjänster i varje lönegrad och tjänstegrupp och antalet kontraktsanställda och utlånade nationella experter, uttryckt i heltidsekvivalenter.

   (e) Genomföra arbetsplanen och rapportera till styrelsen om detta.

   (f) Utarbeta ett utkast till årsrapport om verksamheten inom kompetenscentrumet, inbegripet uppgifter om tillhörande utgifter.

   (g) Säkra genomförandet av effektiva övervaknings- och utvärderingsförfaranden när det gäller kompetenscentrumets verksamhet.

   (h) Utarbeta en handlingsplan för uppföljning av slutsatserna från efterhandsutvärderingarna samt rapportera vartannat år till kommissionen om de framsteg som gjorts.

   (i) Förbereda, förhandla om och ingå avtal med de nationella samordningscentrumen.

   (j) Inom ramen för styrelsens delegering ansvara för administrativa och ekonomiska frågor och personalfrågor, inklusive genomförandet av kompetenscentrumets budget, varvid vederbörlig hänsyn ska tas till internrevisionsfunktionens råd.

(k) Godkänna och hantera lansering av ansökningsomgångar i enlighet med arbetsplanen och administrera bidragsavtal och bidragsbeslut.

(l) Godkänna förteckningen över aktiviteter som valts ut för finansiering baserat på den rangordnade lista som tagits fram av en grupp oberoende experter.

(m) Godkänna och hantera lanseringen av anbudsinfordringar i enlighet med arbetsplanen och administrera kontrakten.

(n) Godkänna förteckningen över anbud som valts ut för finansiering.

(o) Lämna förslag till kompetenscentrumets årsredovisning och balansräkning till internrevisionen och därefter till styrelsen.

(p) Säkerställa att riskbedömning och riskhantering görs.

(q) Underteckna enskilda bidragsöverenskommelser, bidragsbeslut och kontrakt.

(r) Underteckna upphandlingskontrakt.

(s) Utarbeta en handlingsplan för uppföljning av slutsatserna från interna eller externa revisionsrapporter, liksom utredningar utförda av Europeiska byrån för bedrägeribekämpning (Olaf), samt rapportera om läget två gånger om året till kommissionen och regelbundet till styrelsen.

(t) Utarbetande av ett utkast till finansiella regler som ska tillämpas på kompetenscentrumet.

(u) Fastställa ett ändamålsenligt och effektivt internt kontrollsystem, säkerställa dess funktionssätt och rapportera alla betydande ändringar av det till styrelsen.

(v) Se till att det finns en effektiv kommunikation med unionsinstitutionerna.

(w) Vidta eventuella ytterligare åtgärder som krävs för att bedöma hur kompetenscentrumet uppfyller sina mål enligt artiklarna 3 och 4 i denna förordning.

(x) Utföra alla övriga uppgifter som styrelsen tilldelat eller delegerat till den verkställande direktören.

AVSNITT II

RÅDGIVANDE NÄRINGSLIVS- OCH VETENSKAPSNÄMND

Artikel 18

Den rådgivande näringslivs- och vetenskapsnämndens sammansättning

1. Den rådgivande industri- och vetenskapsnämnden ska ha högst 16 ledamöter. Ledamöterna ska utses av styrelsen bland företrädarna för aktörerna i kompetensgemenskapen för cybersäkerhet.

2. Ledamöterna i den rådgivande näringslivs- och vetenskapsnämnden ska ha sakkunskap om antingen forskning, industriell utveckling eller professionella tjänster när det gäller cybersäkerhet eller om ibruktagande. Kraven på sådan sakkunskap ska fastställas närmare av styrelsen.

3. Förfarandena för styrelsens utnämning av den rådgivande nämndens ledamöter och för dess arbete ska anges i kompetenscentrumets arbetsordning och offentliggöras.

4. Mandatperioden för den rådgivande näringslivs- och vetenskapsnämndens ledamöter ska vara tre år. Mandatperioden får förlängas.

5. Företrädare för kommissionens och för Europeiska byrån för nät- och informationssäkerhet får delta i och stödja den rådgivande näringslivs- och vetenskapsnämndens arbete.

Artikel 19

Den rådgivande näringslivs- och vetenskapsnämndens arbetsformer

1. Den rådgivande näringslivs- och vetenskapsnämnden ska sammanträda minst två gånger per år.
2. Den rådgivande näringslivs- och vetenskapsnämnden får ge råd till styrelsen om inrättandet av arbetsgrupper för särskilda frågor av relevans för arbetet i kompetenscentrumet vilka vid behov ska samordnas av en eller flera ledamöter i den rådgivande näringslivs- och vetenskapsnämnden.
3. Den rådgivande näringslivs- och vetenskapsnämnden ska välja sin ordförande.
4. Den rådgivande näringslivs- och vetenskapsnämnden ska anta sin arbetsordning och även utse de personer som i relevanta fall ska företräda den rådgivande nämnden samt fastställa längden på deras mandatperiod.

Artikel 20

Den rådgivande näringslivs- och vetenskapsnämndens uppgifter

Den rådgivande näringslivs- och vetenskapsnämnden ska ge kompetenscentrumet råd med avseende på genomförandet av dess verksamhet samt

(1) ge den verkställande direktören och styrelsen strategiska råd och lämna synpunkter inför utarbetandet av arbetsprogrammet och den fleråriga strategiska planen inom de tidsfrister som styrelsen fastställt,

(2) anordna offentliga samråd som är öppna för alla offentliga och privata intressenter för vilka cybersäkerhet är viktigt för att samla in underlag för de strategiska råd som avses i punkt 1, och

(3) främja och samla in synpunkter på kompetenscentrumets arbetsprogram och fleråriga strategiska plan.

KAPITEL III

FINANSIELLA BESTÄMMELSER

Artikel 21

Unionens ekonomiska bidrag

1. Unionens bidrag till kompetenscentrumet för att täcka de administrativa kostnaderna och driftkostnaderna ska omfatta följande:

(a) 1 981 668 000 EUR från programmet för ett digitalt Europa, inklusive upp till 23 746 000 EUR för administrativa kostnader.

(b) Ett belopp från Horisont Europa-programmet, inklusive för administrativa kostnader, som ska fastställas med beaktande av den strategiska planeringsprocess som ska genomföras i enlighet med artikel 6.6 i förordning XXX [Horisont Europa-förordningen].

2. Maximalt bidrag från unionen ska betalas från de anslag i unionens allmänna budget som anslagits för [programmet för ett digitalt Europa] och för det särskilda programmet för genomförande av Horisont Europa, som inrättades genom beslut XXX.

3. Kompetenscentrumet ska genomföra cybersäkerhetsåtgärder inom ramen för [programmet för ett digitalt Europa] och [Horisont Europa-programmet] i enlighet med artikel 62 c iv i förordning (EU, Euratom) nr XXX[29] [budgetförordningen].

4. Unionens finansiella bidrag ska inte omfatta de uppgifter som anges i artikel 4.8 b.

Artikel 22

Bidrag från de deltagande medlemsstaterna

1. De deltagande medlemsstaterna ska lämna ett totalt bidrag till kompetenscentrumets driftskostnader och administrativa kostnader som uppgår till minst samma belopp som anges i artikel 21.1 i denna förordning.

2. Vid bedömningen av de bidrag som avses i punkt 1 och i punkt 3 b ii i artikel 23 ska kostnaderna fastställas i enlighet med sedvanliga kostnadsredovisningsmetoder i den berörda medlemsstaten, tillämpliga redovisningsstandarder i medlemsstaten och tillämpliga internationella redovisningsstandarder och IFRS-standarder. Kostnaderna ska styrkas av en oberoende extern revisor som utsetts av den berörda medlemsstaten. Värderingsmetoden kan kontrolleras av kompetenscentrumet, om bestyrkandet skulle ge upphov till någon osäkerhet.

3. Om en deltagande medlemsstat inte fullgör sina åtaganden i fråga om det finansiella bidraget ska den verkställande direktören dokumentera detta skriftligen och fastställa en rimlig tidsfrist inom vilken detta ska rättas till. Om situationen inte rättas till inom tidsfristen ska den verkställande direktören sammankalla ett möte med styrelsen för att besluta om den berörda medlemsstatens medlemskap ska sägas upp eller om det ska vidtas några andra åtgärder tills medlemsstaten har fullgjort sina skyldigheter. Den försumliga medlemsstatens rösträtt ska upphävas till dess att den har fullgjort sina åtaganden.

4. Kommissionen får avsluta, minska proportionerligt eller tillfälligt dra in unionens ekonomiska bidrag till kompetenscentrumet, om de deltagande medlemsstaterna inte bidrar, endast delvis bidrar eller bidrar för sent när det gäller de bidrag som avses i punkt 1.

5. Senast den 31 januari varje år ska den deltagande medlemsstaten rapportera till styrelsen om värdet på de bidrag enligt punkt 1 som de lämnat under varje föregående budgetår.

Artikel 23

Kompetenscentrumets kostnader och resurser

1. Kompetenscentrumet ska finansieras gemensamt av unionen och medlemsstaterna genom finansiella bidrag som betalas ut i delbetalningar och bidrag bestående av de nationella samordningscentrumens och betalningsmottagarnas utgifter för genomförandeåtgärder som inte ersätts av kompetenscentrumet.

[29] [Ange fullständig titel och EUT-hänvisning].

2. De administrativa kostnaderna för kompetenscentrumet får inte överstiga [belopp] euro och ska täckas genom finansiella bidrag som ska fördelas jämnt på årsbasis mellan unionen och de deltagande medlemsstaterna. Om en del av bidraget för administrativa kostnader inte används, får det göras tillgängligt för att täcka kompetenscentrumets driftskostnader.

3. Kompetenscentrumets driftskostnader ska täckas genom

   (a) unionens finansiella bidrag,

   (b) bidrag från de deltagande medlemsstaterna i form av

      (i) finansiella bidrag, och

      ii) när så är lämpligt, naturabidrag från de deltagande medlemsstaterna som omfattar de nationella samordningscentrumens och stödmottagarnas utgifter för genomförandet av indirekta åtgärder med avdrag för bidragen från kompetenscentrumet och alla andra unionsbidrag till dessa kostnader.

4. De medel som tas upp i kompetenscentrumets budget ska bestå av följande bidrag:

   (a) De deltagande medlemsstaternas finansiella bidrag till de administrativa kostnaderna.

   (b) De deltagande medlemsstaternas finansiella bidrag till driftskostnaderna.

   (c) Kompetenscentrumets eventuella egna inkomster.

   (d) Andra finansiella bidrag, medel och inkomster.

5. Alla räntor på de bidrag som betalas till kompetenscentrumet av de deltagande medlemsstaterna ska betraktas som kompetenscentrumets inkomster.

6. Komptenscentrumets samtliga resurser och dess åtgärder ska syfta till att uppnå de mål som anges i artikel 4.

7. Kompetenscentrumet ska äga alla tillgångar som det genererat eller som överförts till det för att uppfylla målen.

8. Med undantag för om kompetenscentrumet avvecklas ska ett eventuellt överskott inte betalas ut till de deltagande medlemmarna i kompetenscentrumet.

Artikel 24

Finansiella åtaganden

Kompetenscentrumets finansiella åtaganden får inte överstiga beloppet för de ekonomiska resurser som finns tillgängliga eller som medlemmarna ska betala till dess budget.

Artikel 25

Räkenskapsår

Räkenskapsåret ska inledas den 1 januari och avslutas den 31 december.

Artikel 26

Upprättandet av budgeten

1. Varje år ska den verkställande direktören upprätta en preliminär beräkning av kompetenscentrumets inkomster och utgifter för följande räkenskapsår och överlämna denna till styrelsen tillsammans med ett utkast till tjänsteförteckning. Inkomster och utgifter ska vara i balans. Kompetenscentrumets utgifter ska omfatta utgifter för personal, administration, infrastruktur och drift. Administrativa utgifter ska hållas så låga som möjligt.

2. Varje år ska styrelsen, på grundval av den preliminära beräkning av inkomster och utgifter som avses i punkt 1 lägga fram en beräkning av kompetenscentrumets inkomster och utgifter för det därpå följande räkenskapsåret.

3. Styrelsen ska senast den 31 januari varje år till kommissionen överlämna den beräkning som avses i punkt 2, vilken ska utgöra en del av utkastet till det samlade programdokumentet.

4. På grundval av den beräkningen ska kommissionen ta upp de medel som den anser vara nödvändiga för tjänsteförteckningen och storleken på det anslag som ska belasta den allmänna budgeten i förslaget till unionens budget, som den ska förelägga Europaparlamentet och rådet i enlighet med artiklarna 313 och 314 i EUF-fördraget.

5. Europaparlamentet och rådet ska bevilja anslagen för bidraget till kompetenscentrumet.

6. Europaparlamentet och rådet ska anta kompetenscentrumets tjänsteförteckning.

7. Styrelsen ska anta kompetenscentrumets budget tillsammans med arbetsprogrammet. Den blir slutlig när unionens allmänna budget slutgiltigt har antagits. Styrelsen ska vid behov anpassa kompetenscentrumets budget och arbetsprogrammet till unionens allmänna budget.

Artikel 27

Kompetenscentrumets räkenskaper och beviljande av ansvarsfrihet

Kompetenscentrumets preliminära och slutliga redovisning och beviljandet av ansvarsfrihet ska följa bestämmelserna och tidsplanen i budgetförordningen och i dess finansiella regler som antagits i enlighet med artikel 29.

Artikel 28

Operativ och finansiell rapportering

1. Den verkställande direktören ska varje år rapportera till styrelsen om utförandet av sina uppgifter i enlighet med de finansiella reglerna för kompetenscentrumet.

2. Inom två månader efter räkenskapsårets slut ska den verkställande direktören överlämna en årlig verksamhetsrapport om kompetenscentrumets resultat under det föregående kalenderåret, särskilt i förhållande till arbetsplanen för det året, till styrelsen för godkännande. Denna rapport ska bland annat innehålla information om följande:

   (a) Operativa åtgärder som vidtagits och motsvarande utgifter.

   (b) Åtgärder som föreslagits fördelat på typ av deltagare, däribland små och medelstora företag, och medlemsstat.

(c) De åtgärder som valts ut för finansiering fördelat på typ av deltagare, däribland små och medelstora företag, och medlemsstat samt med uppgift om kompetenscentrumets bidrag till enskilda deltagare och åtgärder.

(d) Framsteg mot ett uppnående av målen i artikel 4 och förslag till fortsatt nödvändigt arbete för att nå dessa mål.

3. Efter styrelsens godkännande ska den årliga verksamhetsrapporten offentliggöras.

Artikel 29

Finansiella regler

Kompetenscentrumet ska anta sina särskilda finansiella regler i enlighet med artikel 70 i förordning XXX [nya budgetförordningen].

Artikel 30

Skydd av ekonomiska intressen

1. Kompetenscentrumet ska säkerställa att unionens ekonomiska intressen skyddas vid genomförandet av insatser som finansieras enligt denna förordning genom förebyggande åtgärder mot bedrägeri, korruption och annan olaglig verksamhet, genom effektiva kontroller och, om oriktigheter upptäcks, genom återkrav av felaktigt utbetalda belopp samt vid behov genom effektiva, proportionella och avskräckande administrativa och ekonomiska sanktioner.

2. Kompetenscentrumet ska ge kommissionens personal och andra personer som har auktoriserats av kommissionen, samt revisionsrätten, tillträde till sina områden och lokaler och till all den information som behövs för att utföra kontrollerna, även information i elektroniskt format.

3. Europeiska byrån för bedrägeribekämpning (Olaf) får utföra utredningar, till exempel kontroller på plats och inspektioner, i enlighet med de bestämmelser och förfaranden som fastställs i rådets förordning (Euratom, EG) nr 2185/96[30] och Europaparlamentets och rådets förordning (EU, Euratom) nr 833/2013[31], i syfte att fastställa om det har förekommit bedrägeri, korruption eller annan olaglig verksamhet som påverkar unionens ekonomiska intressen i samband med ett bidragsavtal eller ett kontrakt som direkt eller indirekt har finansierats i enlighet med denna förordning.

4. Utan att det påverkar tillämpningen av punkterna 1, 2 och 3 i denna artikel ska kontrakt och bidragsavtal som följer av genomförandet av detta beslut innehålla bestämmelser som uttryckligen ger kommissionen, kompetenscentrumet, revisionsrätten och Olaf behörighet att utföra sådana kontroller och utredningar, i enlighet med deras respektive befogenheter. Om genomförandet av en åtgärd helt eller delvis kontrakteras ut eller vidaredelegeras, eller om det krävs att ett offentligt

[30] Rådets förordning (Euratom, EG) nr 2185/96 av den 11 november 1996 om de kontroller och inspektioner på platsen som kommissionen utför för att skydda Europeiska gemenskapernas finansiella intressen mot bedrägerier och andra oegentligheter (EGT L 292, 15.11.1996, s. 2).

[31] Europaparlamentets och rådets förordning (EU, Euratom) nr 883/2013 av den 11 september 2013 om utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf) och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1073/1999 och rådets förordning (Euratom) nr 1074/1999 (EUT L 248, 18.9.2013, s. 1).

kontrakt eller ekonomiskt stöd tilldelas en tredje part, ska kontraktet eller bidragsavtalet innehålla en skyldighet för entreprenören eller stödmottagaren kräva att alla inblandade tredje parter uttryckligen godkänner dessa befogenheter för kommissionen, kompetenscentrumet, revisionsrätten och Olaf.

KAPITEL IV

KOMPETENSCENTRUMETS PERSONAL

Artikel 31

Personal

1. Tjänsteföreskrifterna för tjänstemän och anställningsvillkoren för övriga anställda i Europeiska unionen, som fastställs i rådets förordning (EEG, Euratom, EKSG) nr 259/68[32] (nedan kallade *tjänsteföreskrifterna och anställningsvillkoren*), och de bestämmelser som antagits gemensamt av unionens institutioner för tillämpningen av tjänsteföreskrifterna och anställningsvillkoren ska gälla för kompetenscentrumets personal.

2. I förhållande till kompetenscentrumets personal ska styrelsen utöva de befogenheter som genom tjänsteföreskrifterna tilldelas tillsättningsmyndigheten och de befogenheter som genom anställningsvillkoren tilldelas den myndighet som är behörig att ingå avtal (nedan kallade *tillsättningsmyndighetsbefogenheter*).

3. Styrelsen ska i enlighet med artikel 110 i tjänsteföreskrifterna anta ett beslut grundat på artikel 2.1 i tjänsteföreskrifterna och artikel 6 i anställningsvillkoren om delegering av relevanta befogenheter som tillsättningsmyndighet till den verkställande direktören och om fastställande av på vilka villkor den delegeringen får dras in. Den verkställande direktören får vidaredelegera dessa befogenheter.

4. Om exceptionella omständigheter kräver det får styrelsen genom ett beslut tillfälligt dra in delegeringen av befogenheterna som tillsättningsmyndighet till den verkställande direktören samt eventuell vidaredelegering som denne gjort. I sådant fall ska styrelsen själv utöva befogenheterna som tillsättningsmyndighet eller delegera dem till en av sina medlemmar eller till en annan anställd i kompetenscentrumet än den verkställande direktören.

5. Styrelsen ska i enlighet med artikel 110 i tjänsteföreskrifterna anta genomförandebestämmelser för tjänsteföreskrifterna och för anställningsvillkoren.

6. Personalstyrkan ska fastställas i en tjänsteförteckning för kompetenscentrumet som anger antalet tillfälliga tjänster per tjänstegrupp och lönegrad och antalet kontraktsanställda uttryckt i heltidsekvivalenter i enlighet med kompetenscentrumets årsbudget.

7. Kompetenscentrumets personal ska utgöras av tillfälligt anställda och kontraktsanställda.

8. Alla personalkostnader ska bäras av kompetenscentrumet.

---

[32] Rådets förordning (EEG, Euratom, EKSG) nr 259/68 av den 29 februari 1968 om fastställande av tjänsteföreskrifter för tjänstemännen i Europeiska gemenskaperna och anställningsvillkor för övriga anställda i dessa gemenskaper samt om införande av särskilda tillfälliga åtgärder beträffande kommissionens tjänstemän (EGT L 56, 4.3.1968, s. 1).

Artikel 32

Utlånade nationella experter och annan personal

1. Kompetenscentrumet får använda sig av utlånade nationella experter och annan personal som inte är anställd av kompetenscentrumet.

2. Styrelsen ska, efter överenskommelse med kommissionen, anta ett beslut om regler för utlåning av nationella experter till kompetenscentrumet.

Artikel 33

Immunitet och privilegier

Kompetenscentrumet och dess personal ska omfattas av protokoll nr 7 om Europeiska unionens immunitet och privilegier, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt.

KAPITEL V
GEMENSAMMA BESTÄMMELSER

Artikel 34

Säkerhetsbestämmelser

1. Artikel 12.7 i förordning (EU) nr XXX [programmet för ett digitalt Europa] ska tillämpas på deltagandet i alla åtgärder som finansieras av kompetenscentrumet.

2. Följande särskilda säkerhetsregler ska tillämpas på åtgärder som finansieras genom Horisont Europa.

   (a) I enlighet med artikel 34.1 [Äganderätt och skydd] i förordning (EU) nr XXX [Horisont Europa] får när så föreskrivs i arbetsprogrammet beviljandet av icke-exklusiva licenser begränsas till tredjeparter som är etablerade i eller anses vara etablerade i en medlemsstat eller som kontrolleras av en medlemsstat och/eller medborgare i en medlemsstat.

   (b) I enlighet med artikel 36.4 b [Överlåtelse och licensiering] i förordning (EU) nr XXX [Horisont Europa] ska överlåtelse eller licensiering till en aktör som är etablerad i ett associerat tredjeland eller etablerad i unionen men kontrolleras från ett tredjeland, också utgöra skäl att invända mot överlåtelser av äganderätten till resultat, eller till beviljande av en exklusiv licens för resultat.

   (c) I enlighet med artikel 37.3 a [Åtkomsträtt] i förordning (EU) nr XXX [Horisont Europa] får när så föreskrivs i arbetsprogrammet beviljandet av åtkomst till resultat och bakgrundsinformation begränsas till en aktör som är etablerad i eller anses vara etablerad i en medlemsstat eller som kontrolleras av en medlemsstat och/eller medborgare i en medlemsstat.

Artikel 35

Öppenhet

1. Kompetenscentrumet ska utföra sitt arbete med en hög grad av transparens.

2. Kompetenscentrumet ska säkerställa att allmänheten och alla berörda parter får lämplig, saklig, tillförlitlig och lättillgänglig information, framför allt om resultaten

av dess arbete. Den ska också offentliggöra de intresseförklaringar som avges i enlighet med artikel 41.

3. Styrelsen får på den verkställande direktörens förslag ge andra berörda parter tillstånd att observera delar av kompetenscentrumets verksamhet.

4. Kompetenscentrumet ska i sin arbetsordning fastställa hur de transparensregler som avses i punkterna 1 och 2 ska tillämpas praktiskt. För åtgärder som finansieras genom Horisont Europa ska vederbörlig hänsyn i detta sammanhang tas till bestämmelserna i bilaga III till Horisont Europa-förordningen.

Artikel 36

Säkerhetsbestämmelser om skydd av säkerhetsskyddsklassificerade uppgifter och känsliga uppgifter som inte är säkerhetsskyddsklassificerade

1. Utan att detta påverkar artikel 35 ska kompetenscentrumet inte för tredje part röja uppgifter som det behandlar eller mottar, om det i en motiverad ansökan har begärts att uppgifterna helt eller delvis ska behandlas konfidentiellt.

2. Ledamöterna i styrelsen, den verkställande direktören, medlemmarna i den rådgivande näringslivs- och vetenskapsnämnden, de externa experter som deltar i olika tillfälliga arbetsgrupper och kompetenscentrumets personal ska omfattas av tystnadsplikt enligt artikel 339 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), även efter det att deras uppdrag upphört.

3. Kompetenscentrumets styrelse ska efter godkännande av kommissionen anta kompetenscentrumets säkerhetsbestämmelser, grundade på säkerhetsprinciperna i kommissionens säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter och känsliga icke-säkerhetsskyddsklassificerade uppgifter, i enlighet med kommissionens beslut (EU, Euratom) 2015/443[33] och 2015/444[34].

4. Kompetenscentrumet får vidta de åtgärder som krävs för att göra det lättare att utbyta information som är relevant för dess arbetsuppgifter med kommissionen och medlemsstaterna, och vid behov med relevanta unionsbyråer. Varje administrativt arrangemang för detta ändamål om utbyte av säkerhetsskyddsklassificerade EU-uppgifter, eller i frånvaro av sådana arrangemang, ad hoc-utlämning av säkerhetsskyddsklassificerade EU-uppgifter i undantagsfall, ska ske med kommissionens förhandsgodkännande.

Artikel 37

Tillgång till handlingar

1. Förordning (EG) nr 1049/2001 ska tillämpas på de handlingar som finns hos kompetenscentrumet.

2. Styrelsen ska vidta åtgärder för att genomföra förordning (EG) nr 1049/2001 inom sex månader efter det att kompetenscentrumet inrättats.

---

33 Kommissionens beslut (EU, Euratom) 2015/443 av den 13 mars 2015 om säkerhet inom kommissionen (EUT L 72, 17.3.2015, s. 41).

34 Kommissionens beslut (EU, Euratom) 2015/444 av den 13 mars 2015 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (EUT L 72, 17.3.2015, s. 53).

3. Beslut som fattas av kompetenscentrumet i enlighet med artikel 8 i förordning (EG) nr 1049/2001 får bli föremål för ett klagomål till ombudsmannen enligt artikel 228 i fördraget om Europeiska unionens funktionssätt eller väckande av talan vid Europeiska unionens domstol i enlighet med artikel 263 i fördraget om Europeiska unionens funktionssätt.

Artikel 38

Övervakning, utvärdering och översyn

1. Kompetenscentrumet ska säkerställa att dess verksamhet, inklusive den som förvaltas genom de nationella samordningscentrumen och nätverket, ska vara föremål för löpande övervakning och regelbundna utvärderingar. Kompetenscentrumet ska säkerställa att uppgifter för övervakning av programmets genomförande och resultat samlas in effektivt och utan onödigt dröjsmål och proportionella rapporteringskrav ska ställas på mottagarna av unionens medel och medlemsstaterna. Resultaten av utvärderingen ska offentliggöras.

2. Kommissionen ska göra en interimsutvärdering av kompetenscentrumet när det finns tillräckligt med information om genomförandet av denna förordning, dock senast tre och ett halvt år efter det att programmet började genomföras. Kommissionen ska upprätta en rapport om den utvärderingen och överlämna denna till Europaparlamentet och rådet senast den 31 december 2024. Kompetenscentrumet och medlemsstaterna ska förse kommissionen med den information som är nödvändig för att upprätta rapporten.

3. Den utvärdering som avses i punkt 2 ska omfatta en bedömning av de resultat som uppnåtts av kompetenscentrumet, med beaktande av dess mål, mandat och uppgifter. Om kommissionen anser att det är motiverat att kompetenscentrumet fortsätter sin verksamhet med tanke på dess uppsatta mål, mandat och uppgifter får den föreslå en förlängning av det mandat för kompetenscentrumet som anges i artikel 46.

4. Med utgångspunkt i slutsatserna från den deltidsutvärdering som avses i punkt 2 får kommissionen agera i enlighet med [artikel 22.5] eller vidta andra lämpliga åtgärder.

5. Övervakning, utvärdering, avveckling och förnyande av bidragen från Horisont Europa kommer att ske enligt bestämmelserna i artiklarna 8, 45 och 47 samt bilaga III i Horisont Europa-förordningen och de överenskomna genomförandeformerna.

6. Övervakning, utvärdering, avveckling och förnyande av bidragen från ett digitalt Europa kommer att ske enligt bestämmelserna i artiklarna 24 och 25 i programmet för ett digitalt Europa.

7. Om kompetenscentrumet avvecklas ska kommissionen göra en slutlig utvärdering av kompetenscentrumet inom sex månader från det att det har avvecklats, dock senast inom två år efter det att det avvecklingsförfarande som avses i artikel 46 i denna förordning har inletts. Resultatet av den slutliga utvärderingen ska läggas fram för Europaparlamentet och rådet.

Artikel 39

Kompetenscentrumets ansvar

1. Kompetenscentrumets avtalsenliga ansvar ska regleras av den lagstiftning som är tillämplig på överenskommelsen, beslutet eller avtalet i fråga.

2. Vad beträffar utomobligatoriskt ansvar ska kompetenscentrumet ersätta skada som orsakats av dess personal under tjänsteutövningen i enlighet med de allmänna principer som är gemensamma för medlemsstaternas rättsordningar.

3. Kompetenscentrumets utbetalningar till följd av det skadeståndsansvar som avses i punkterna 1 och 2 samt kostnader och utgifter i samband med detta ska räknas som utgifter för kompetenscentrumet och täckas med dess medel.

4. Kompetenscentrumet ska ensamt vara ansvarigt för fullgörandet av sina skyldigheter.

Artikel 40

Europeiska unionens domstols behörighet och tillämplig lagstiftning

1. Europeiska unionens domstol ska vara behörig

   (1) i enlighet med eventuella skiljedomsklausuler i överenskommelser eller avtal som ingås eller i beslut som fattas av kompetenscentrumet,

   (2) vid tvister om ersättning för skada som vållats av kompetenscentrumets personal under deras tjänsteutövning, och

   (3) vid tvister mellan kompetenscentrumet och dess tjänstemän, inom de gränser och på de villkor som anges i tjänsteföreskrifterna.

2. Lagstiftningen i den stat där kompetenscentrumet har sitt säte ska tillämpas i alla frågor som inte omfattas av denna förordning eller av några andra unionsrättsakter.

Artikel 41

Medlemmarnas ansvar och försäkring

1. Medlemmarnas ekonomiska ansvar för kompetenscentrumets skulder ska vara begränsat till deras redan inbetalade bidrag till de administrativa kostnaderna.

2. Kompetenscentrumet ska teckna och ha lämpliga försäkringar.

Artikel 42

Intressekonflikter

Kompetenscentrumets styrelse ska anta bestämmelser för att förebygga och hantera intressekonflikter som uppstår i fråga om kompetenscentrumets medlemmar, organ och anställda. Dessa bestämmelser ska omfatta bestämmelser om undvikande av intressekonflikter bland företrädarna för de medlemmar som ingår i styrelsen och den rådgivande näringslivs- och vetenskapsnämnden i enlighet med förordning XXX [nya budgetförordningen].

Artikel 43

Skydd av personuppgifter

1. Kompetenscentrumet ska behandla personuppgifter i enlighet med Europaparlamentets och rådets förordning (EG) nr 45/2018.

2. Styrelsen ska anta de genomförandebestämmelser som avses i artikel 24.8 i förordning (EG) nr XXX/2018. Styrelsen får anta ytterligare åtgärder som behövs för kompetenscentrumets tillämpning av förordning (EG) nr XXX/2018.

Artikel 44

Stöd från värdmedlemsstaten

Kompetenscentrumet och den medlemsstat [Belgien] där det har sitt säte får ingå en administrativ överenskommelse om immunitet och privilegier och annat stöd från den medlemsstaten till kompetenscentrumet.

KAPITEL VII

SLUTBESTÄMMELSER

Artikel 45

Inledande åtgärder

1. Kommissionen ska ansvara för bildandet av kompetenscentrumet och dess inledande verksamhet till dess att det har operativ förmåga att genomföra sin egen budget. Kommissionen ska, i enlighet med unionsrätten, vidta alla nödvändiga åtgärder med bidrag från behöriga organ inom kompetenscentrumet.
2. I enlighet med punkt 1 får kommissionen till dess att den verkställande direktören tillträder sin tjänst, efter att ha utnämnts av styrelsen i enlighet med artikel 16, utse en tillförordnad verkställande direktör för att fullgöra de plikter som åligger den verkställande direktören, och denne får biträdas av ett begränsat antal tjänstemän från kommissionen. Kommissionen får utse ett begränsat antal tjänstemän på tillfällig basis.
3. Den tillförordnade verkställande direktören får godkänna alla betalningar som omfattas av de bemyndiganden som anges i den årliga budgeten för kompetenscentrumet, när de godkänts av styrelsen, och får ingå överenskommelser, anta beslut och ingå avtal, inbegripet anställningsavtal, när tjänsteförteckningen för kompetenscentrumet har antagits.
4. Den tillförordnade verkställande direktören ska, i samförstånd med den verkställande direktören för kompetenscentrumet, och med förbehåll för styrelsens godkännande, fastställa det datum då kompetenscentrumet ska ha förmåga att genomföra sin egen budget. Från och med det datumet ska kommissionen avstå från att göra åtaganden och utbetalningar för kompetenscentrumets verksamhet.

Artikel 46

Varaktighet

1. Kompetenscentrumet ska inrättas för perioden från och med den 1 januari 2021 till och med den 31 december 2029.

2. I slutet av denna period ska avvecklingsförfarandet inledas, såvida inte annat beslutas vid översynen av denna förordning. Avvecklingsförfarandet ska inledas automatiskt om unionen eller alla deltagande medlemsstaterna drar sig ur kompetenscentrumet.

3. För genomförande av kompetenscentrumets avveckling ska styrelsen utse en eller flera förvaltare, som ska följa styrelsens beslut.

4. När kompetenscentrumet avvecklas ska dess tillgångar användas för att täcka dess skulder samt utgifterna i samband med avvecklingen. Ett eventuellt överskott ska fördelas mellan unionen och de deltagande medlemsstaterna i förhållande till deras finansiella bidrag till kompetenscentrumet. Eventuellt överskott som tilldelas unionen ska återföras till unionens budget.

Artikel 47

Ikraftträdande

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

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

Utfärdad i Bryssel den

På Europaparlaments vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets titel

1.2. Berörda politikområden i den verksamhetsbaserade förvaltningen och budgeteringen

1.3. Typ av förslag eller initiativ

1.4. Mål

1.5. Grunder för förslaget eller initiativet

1.6. Varaktighet och budgetkonsekvenser

1.7. Planerad metod för genomförandet

2. FÖRVALTNING

2.1. Regler om uppföljning och rapportering

2.2. Förvaltnings- och kontrollsystem

2.3. Åtgärder för att förebygga bedrägeri och oriktigheter

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

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

3.2. Beräknad inverkan på utgifterna

3.2.1. Sammanfattning av den beräknade inverkan på utgifterna

3.2.2. Beräknad inverkan på driftsanslagen

3.2.3. Beräknad inverkan på anslag av administrativ natur

3.2.4. Förenlighet med den gällande fleråriga budgetramen

3.2.5. Bidrag från tredje part

3.3. Beräknad inverkan på inkomsterna

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets titel

Förordning om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning

1.2. Berörda politikområden i den verksamhetsbaserade förvaltningen och budgeteringen[35]

Forskning och innovation

Forskning och innovation

1.3. Typ av förslag eller initiativ

☒Typ av förslag eller initiativ: **Ny åtgärd**

☐ Förslaget/initiativet gäller en **ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd**[36]

☐ Förslaget/initiativet gäller en **befintlig åtgärd vars genomförande förlängs i tiden**

☐ Förslaget/initiativet gäller **en åtgärd som omformas till en ny åtgärd**

1.4. Mål

1.4.1. Fleråriga strategiska mål för kommissionen som förslaget eller initiativet är avsett att bidra till

1. En sammankopplad digital inre marknad

2. En ny satsning på sysselsättning, tillväxt och investeringar

1.4.2. Specifikt/specifika mål som berörs

Särskilda mål

1.3 Den digitala ekonomin kan infria hela sin potential om den stöds genom initiativ som möjliggör full utveckling av digital teknik och datateknik.

2.1 Europa behåller sin position som världsledande inom den digitala ekonomin och europeiska företag kan växa globalt med hjälp av ett starkt digitalt entreprenörskap och framgångsrika nyföretag, samtidigt som industri och myndigheter har kontroll över den digitala omvandlingen. 2,2.

2.2. Europeisk forskning får möjlighet att investera i potentiellt banbrytande teknik och flaggskeppsteknik, framför allt genom Horisont 2020/Horisont Europa-programmet och genom offentlig-privata partnerskap.

35 ABM: verksamhetsbaserad förvaltning; ABB: verksamhetsbaserad budgetering.

36 I den mening som avses i artikel 54.2 a och b i budgetförordningen.

1.4.3. Verkan eller resultat som förväntas

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

Kompetenscentrumet ska tillsammans med nätverket och kompetensgemenskapen eftersträva följande mål:

(1) Bidra till genomförandet av cybersäkerhetsdelen av programmet för ett digitalt Europa som inrättades genom förordning (EU) XXX och i synnerhet åtgärder med anknytning till artikel 6 i förordning (EU) nr XXX [programmet för ett digitalt Europa] och i Horisont Europa-programmet som inrättades genom förordning nr XXX och i synnerhet avsnitt 2.2.6 i bilaga I till beslut nr XXX om inrättandet av det särskilda programmet för genomförande av Horisont Europa – ramprogrammet för forskning och innovation och i andra EU-program om detta föreskrivs i unionens rättsakter.

(2) Stärka cybersäkerhetskapaciteten, cybersäkerhetskunskapen och cybersäkerhetsinfrastrukturen till förmån för näringsliv, offentlig sektor och forskarsamhället.

(3) Bidra till införande på bred basis i hela ekonomin av de senaste produkterna och lösningarna inom cybersäkerhet.

(4) Öka kunskaperna om cybersäkerhet och bidra till att minska bristen på kvalificerad arbetskraft inom cybersäkerhet i unionen.

(5) Bidra till att stärka forskning och utveckling inom cybersäkerhet i unionen.

(6) Stärka samarbetet mellan den civila och den försvarsrelaterade sektorn när det gäller teknikens och tillämpningarnas dubbla användningsområden.

(7) Öka synergieffekterna mellan de civila och försvarsrelaterade aspekterna av cybersäkerhet.

(8) Underlätta och hjälpa till att samordna arbetet inom det nätverk av nationella samordningscentrum (nedan kallat *nätverket*) som avses i artikel 10 och den cybersäkerhetsgemenskap som avses i artikel 12.

1.4.4. Indikatorer för bedömning av resultat eller verkan

Ange vilka indikatorer som ska användas för att följa upp hur förslaget eller initiativet genomförs.

· Antal infrastrukturer/verktyg för cybersäkerhet som köps in gemensamt.

· Test- och försöksmöjligheter för europeiska forskare och industrier inom nätverket och centrumet. Om anläggningar redan finns, fler tillgängliga timmar för dessa grupper jämfört med i dag.

· Antal användargrupper som får hjälp och antal forskare som får tillgång till europeiska cybersäkerhetsanläggningar ökar jämfört med de antal som tvingas söka sådana resurser utanför Europa.

· De europeiska leverantörernas konkurrenskraft börjar öka, mätt genom den globala marknadsandelen (mål om en marknadsandel på 25 % 2027) och andelen europeiska FoU-resultat som används av näringslivet.

· Bidrag till ny cybersäkerhetsteknik, mätt genom upphovsrätt, patent, vetenskapliga publikationer och kommersiella produkter.

· Antal läroplaner för cybersäkerhetskompetens som bedömts och anpassats, antal program för professionell certifiering av cybersäkerhet.

· Antal forskare, studenter och användare (näringslivet och offentliga förvaltningar) som utbildats.

1.5. Grunder för förslaget eller initiativet

1.5.1. Behov som ska tillgodoses på kort eller lång sikt

Uppnå en kritisk massa av investeringar i teknisk och industriell utveckling inom cybersäkerhet och att komma till rätta med den utspridda kapaciteten i EU i dag.

1.5.2. Mervärdet av en åtgärd på unionsnivå

Cybersäkerhet är en fråga av gemensamt intresse för unionen, vilket bekräftades i de ovannämnda rådsslutsatserna. Ett tydligt exempel är omfattningen av gränsöverskridande incidenter som WannaCry och NonPetya. EU måste med tanke på de tekniska cybersäkerhetsutmaningarnas karaktär och omfattning, liksom den otillräckliga samordningen av ansträngningar inom och mellan näringsliv, offentlig sektor och forskarsamhället, ge ytterligare stöd till samordningsansträngningar för att både uppnå en kritisk massa resurser och säkerställa en bättre kunskaps- och tillgångshantering. Detta är nödvändigt med tanke på de resurser som krävs för viss forskning, utveckling och användning av cybersäkerhetsteknik, vikten av tvärdisciplinär tillgång till cybersäkerhetskunskaper inom olika discipliner (som ofta bara delvis är tillgängliga på nationell nivå), de globala industriella värdekedjorna och globala konkurrenters verksamhet på olika marknader.

Detta kräver resurser och sakkunskap av en omfattning som knappast kan uppnås av enskilda medlemsstater. Ett Europatäckande nätverk för kvantkommunikation kan t.ex. kräva EU-investeringar på omkring 900 miljoner euro, beroende på medlemsstaternas investeringar (för att vara kompatibla med/komplettera dessa) och i vilken utsträckning tekniken gör det möjligt att återanvända befintlig infrastruktur.

1.5.3. Erfarenheter från tidigare liknande åtgärder

Interimsutvärderingen av bl.a. Horisont 2020 bekräftade att EU:s stöd till FoU och samhällsutmaningar (t.ex. Säkra samhällen, som stöder FoU inom cybersäkerhet) är fortsatt relevant. Utvärderingen bekräftar samtidigt att stärkt industriellt ledarskap fortfarande är en stor utmaning och att innovationsgapet kvarstår, eftersom EU ligger efter när det gäller banbrytande innovation som skapar nya marknader.

Halvtidsutvärderingen av fonden för ett sammanlänkat Europa tycks bekräfta mervärdet av EU-insatser på andra områden än FoU, även om fonden hade en något annan infallsvinkel på cybersäkerhet (på operativ säkerhet) och insatserna motiverades på andra grunder. Majoriteten av mottagarna av cybersäkerhetsbidrag från fonden för ett sammanlänkat Europa – de nationella CSIRT-enheterna – uttryckte en önskan om ett särskilt stödprogram under den kommande fleråriga budgetramen.

Etableringen av ett offentligt-privat partnerskap om cybersäkerhet (nedan kallat *cPPP*) i unionen 2016 var ett viktigt första steg mot att sammanföra forskarsamhället, näringslivet och den offentliga sektorn för att främja forskning och innovation inom cybersäkerhet och bör inom budgetramen 2014–2020 leda till bra och mer fokuserade resultat inom forskning och innovation. Genom cPPP kunde

näringslivspartner utlova individuella satsningar på områden som definieras i partnerskapets strategiska forsknings- och innovationsagenda.

1.5.4. Förenlighet med andra lämpliga instrument och eventuella synergieffekter

Kompetensnätverket och det europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning ska fungera som ett ytterligare stöd vid sidan om befintliga bestämmelser och aktörer på cybersäkerhetsområdet. Det europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning ska ha ett uppdrag som kompletterar Enisas arbete men ha en annan inriktning och kräva annan kompetens. Medan Enisa har en rådgivande roll när det gäller forskning och innovation inom cybersäkerhet i EU ska centrumets föreslagna uppdrag i första hand inriktas på andra uppgifter som är avgörande för att stärka resiliensen inom EU på cybersäkerhetsområdet. Centrumet bör stimulera utveckling och användning av cybersäkerhetsteknik och komplettera insatserna för att bygga upp kapaciteten inom detta område på EU-nivå och nationell nivå.

Det europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning ska tillsammans med kompetensnätverket för cybersäkerhet även stödja forskning för att främja och påskynda standardiserings- och certifieringsprocesser, i synnerhet de som rör certifieringssystem i den mening som avses i cybersäkerhetsakten.

Det europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning ska fungera som gemensamt genomförandeorgan för två EU-program till stöd för cybersäkerhet (programmet för ett digitalt Europa och Horisont Europa-programmet) och förbättra samstämmighet och synergieffekter mellan dem.

Detta initiativ gör det möjligt att komplettera medlemsstaternas ansträngningar genom att ge utbildningspolitiska beslutsfattare lämpligt underlag för att förbättra kompetensen inom cybersäkerhet (t.ex. genom att utarbeta läroplaner om cybersäkerhet i civila och militära utbildningssystem, men även för grundutbildning i cybersäkerhet). Det skulle även göra det möjligt att anpassa och fortlöpande bedöma program för professionell certifiering av cybersäkerhet – vilket behövs för att åtgärda bristen på kvalificerad arbetskraft inom cybersäkerhet och göra det lättare för näringsliv och andra sektorer att få tillgång till specialister på cybersäkerhet. Anpassning av utbildning och kompetens kommer att bidra till att få fram kvalificerad arbetskraft inom cybersäkerhet i EU – vilket är avgörande för både cybersäkerhetsföretag och andra sektorer för vilka cybersäkerhet är viktigt.

1.6. Varaktighet och budgetkonsekvenser

☒ Förslag eller initiativ som pågår under **begränsad tid**

– ☒ Förslaget eller initiativet ska gälla från den 1.1.2021 till den 31.12.2029.

– ☒ Budgetkonsekvenser från och med 2021 till och med 2027 för åtagandebemyndiganden och från och med 2021 till och med 2031 för betalningsbemyndiganden.

☐ Förslag eller initiativ som pågår under **obegränsad tid**

– Efter en inledande period ÅÅÅÅ–ÅÅÅÅ,

– beräknas genomförandetakten nå en stabil nivå.

1.7. Planerad metod för genomförandet[37]

☐ **Direkt förvaltning** som sköts av kommissionen

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

– ☐ av genomförandeorgan

☐ **Delad förvaltning** med medlemsstaterna

☒

Indirekt förvaltning genom att uppgifter som ingår i budgetgenomförandet anförtros

– ☐ tredjeländer eller organ som de har utsett

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

– ☐EIB och Europeiska investeringsfonden

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

– ☐ offentligrättsliga organ

– ☐ privaträttsliga organ som anförtrotts uppgifter som faller inom offentlig förvaltning och som lämnat tillräckliga ekonomiska garantier

– ☐ organ som omfattas av privaträtten i en medlemsstat, som anförtrotts genomförandet av ett offentlig-privat partnerskap och som lämnat tillräckliga ekonomiska garantier

– ☐ personer som anförtrotts ansvaret för genomförandet av särskilda åtgärder inom Gusp som följer av avdelning V i fördraget om Europeiska unionen och som anges i den relevanta grundläggande rättsakten

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

[37] Närmare förklaringar av de olika metoderna för genomförande med hänvisningar till respektive bestämmelser i budgetförordningen återfinns på BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. FÖRVALTNING

2.1. Regler om uppföljning och rapportering

Ange intervall och andra villkor för sådana åtgärder:

Artikel 28 innehåller närmare bestämmelser om övervakning och rapportering.

2.2. Förvaltnings- och kontrollsystem

2.2.1. Risker som identifierats:

För att minska risker i samband med kompetenscentrumets uppbyggnad eller till följd av förseningar kommer kommissionen att ge stöd under denna fas för att säkerställa en snabb rekrytering av nyckelpersonal och inrättande av ett effektivt internt kontrollsystem och goda rutiner.

2.2.2. Uppgifter om det interna kontrollsystemet:

Den verkställande direktören ska ansvara för verksamheten och den dagliga ledningen av kompetenscentrumet och vara dess rättsliga företrädare. Direktören ska vara ansvarig inför styrelsen och löpande rapportera till den om hur kompetenscentrumets verksamhet utvecklas.

Styrelsen ska ha det övergripande ansvaret för kompetenscentrumets strategiska inriktning och verksamhet och övervaka genomförandet av dess aktiviteter.

Finansiella regler för kompetenscentrumet ska antas av styrelsen efter samråd med kommissionen. De får inte avvika från förordning (EU) nr 1271/2013 såvida det inte är helt nödvändigt för kompetenscentrumets verksamhet och kommissionen på förhand har godkänt detta.

Kommissionens internrevisor ska utöva samma befogenheter över kompetenscentrumet som över kommissionen. Revisionsrätten ska ha befogenhet att utföra revision, på grundval av handlingar och kontroller på plats, hos alla stödmottagare, uppdragstagare och underleverantörer som fått unionsmedel från kompetenscentrumet.

2.2.3. Beräknade kostnader för och fördelar med kontroller – bedömning av förväntad risk för fel

Kostnaden för och nyttan med kontroller

Kostnaderna för kontroll av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning utgörs dels av kostnader för övervakning på kommissionsnivå, dels av kostnader för operativa kontroller hos genomförandeorganet.

Kostnaderna för kontroller hos kompetenscentrumet beräknas utgöra omkring 1,19 % av betalningsbemyndigandena för kompetenscentrumets verksamhet.

Kostnaderna för övervakning på kommissionsnivå beräknas utgöra 1,20 % av betalningsbemyndigandena för kompetenscentrumets verksamhet.

Om kommissionen skulle ha hand om alla aktiviteter utan stöd från genomförandeorganet skulle kontrollkostnaderna bli väsentligt högre och kunna utgöra omkring 7,7 % av betalningsbemyndigandena.

Kontrollerna ska syfta till att säkerställa att kommissionens övervakning över genomförandeenheterna fungerar smidigt och är ändamålsenlig och till att säkerställa den nödvändiga graden av säkerhet på kommissionsnivå.

Nyttan med kontrollerna är följande:

- Man undviker att satsa på dåligt underbyggda eller bristfälliga förslag.
- Man optimerar planeringen och användningen av EU-medel, vilket säkrar EU-mervärdet.
- Man säkerställer kvaliteten på bidragsavtalen, undviker misstag i identifieringen av aktörer, säkerställer en korrekt beräkning av EU-anslagen och vidtar de åtgärder som är nödvändiga för att bidragen ska fungera på rätt sätt.
- Ej stödberättigande kostnader upptäcks i utbetalningsskedet.
- Fel som påverkar verksamhetens laglighet och korrekthet upptäcks i revisionsskedet.

Uppskattad felnivå

Syftet är att hålla den kvarstående felfrekvensen under tröskeln på 2 % för hela programmet och samtidigt minska kontrollbördan för stödmottagarna för att uppnå rätt balans mellan målet avseende laglighet och korrekthet och övriga mål, såsom programmets attraktionskraft för i synnerhet små och medelstora företag och kostnaden för kontrollerna.

2.3. Åtgärder för att förebygga bedrägeri och oriktigheter

Beskriv förebyggande åtgärder (befintliga eller planerade)

Olaf får göra utredningar, inbegripet kontroller på plats och inspektioner – i enlighet med bestämmelserna och förfarandena i Europaparlamentets och rådets förordning (EU, Euratom) nr 883/2013 och rådets förordning (Euratom, EG) nr 2185/9640 av den 11 november 1996 om de kontroller och inspektioner på platsen som kommissionen utför för att skydda unionens finansiella intressen mot bedrägerier och andra oriktigheter – i syfte att fastställa om det har förekommit bedrägeri, korruption eller annan olaglig verksamhet som påverkar unionens ekonomiska intressen i samband med bidrag eller kontrakt som finansierats av kompetenscentrumet.

Avtal, beslut och kontrakt som följer av genomförandet av denna förordning ska innehålla bestämmelser som uttryckligen ger kommissionen, kompetenscentrumet, revisionsrätten och Olaf rätt att utföra sådana revisioner och utredningar inom ramen för sina respektive befogenheter.

Kompetenscentrumet ska säkerställa att dess medlemmars ekonomiska intressen skyddas på ett adekvat sätt genom att utföra lämpliga interna och externa kontroller, eller se till att sådana kontroller utförs.

Kompetenscentrumet ska ansluta sig till det interinstitutionella avtalet av den 25 maj 1999 mellan Europaparlamentet, Europeiska unionens råd och Europeiska gemenskapernas kommission om interna utredningar som utförs av Europeiska byrån

för bedrägeribekämpning (Olaf). Kompetenscentrumet ska anta de bestämmelser som behövs för att underlätta interna utredningar som genomförs av Olaf.

Kompetenscentrumet ska anta en strategi mot bedrägerier som ska grundas på en analys av bedrägeririsken och kostnads-nyttohänsyn. Centrumet ska skydda unionens finansiella intressen genom förebyggande åtgärder mot bedrägeri, korruption och annan olaglig verksamhet, genom effektiva kontroller och, om oriktigheter upptäcks, genom återkrav av felaktigt utbetalda belopp samt vid behov genom effektiva, proportionella och avskräckande administrativa och ekonomiska sanktioner.

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Rubrik i den fleråriga budgetramen och föreslagna nya budgetrubriker i den årliga budgetens utgiftsdel

- Nya budgetrubriker som föreslås

  Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd

Rubrik i den fleråriga budgetramen	Budgetrubrik	Typ av anslag	Bidrag			
	Nummer	Diff./Icke-diff.[38]	från Eftaländer[39]	från kandidatländer[40]	från tredjeländer	i den mening som avses i artikel [21.2 b] i budgetförordningen
Rubrik 1: Inre marknaden, innovation och den digitala sektorn	01 02 XX XX Horisont Europa Kompetenscentrum för cybersäkerhet inom näringsliv, teknik och forskning – stödutgifter 01 02 XX XX Horisont Europa Kompetenscentrum för cybersäkerhet inom näringsliv, teknik och forskning 02 06 01 XX Ett digitalt Europa Kompetenscentrum för cybersäkerhet inom näringsliv, teknik och forskning – stödutgifter 02 06 01 XX Ett digitalt Europa Kompetenscentrum för cybersäkerhet inom näringsliv, teknik och forskning	Diff.	JA	JA (om angivet i det årliga arbetsprogrammet)	JA (begränsat till vissa delar av programmet)	NEJ

- Bidragen till dessa budgetrubriker väntas komma från:

[38] Diff. = differentierade anslag / Non-diff. = icke-differentierade anslag.
[39] Efta: Europeiska frihandelssammanslutningen.
[40] Kandidatländer och i förekommande fall potentiella kandidatländer i västra Balkan.

Miljoner euro (avrundat till tre decimaler)

Budgetrubrik	År 2021	År 2022	År 2023	År 2024	År 2025	År 2026	År 2027	**Totalt**
01 01 01 01 Utgifter för tjänstemän och tillfälligt anställda – Horisont Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 02 Extern personal som genomför forskningsprogram – Horisont Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 03 Övriga administrativa utgifter för forskning – Horisont Europa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 02 02 Globala utmaningar och industriell konkurrenskraft	pm	pm	pm	pm	pm	pm	pm	**pm**
02 01 04 Administrativt stöd – program för ett digitalt Europa	1,238	3,030	3,743	3,818	3,894	3,972	4,051	**23,746**
02 06 01 Cybersäkerhet – program för ett digitalt Europa	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Utgifter totalt	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

Bidraget från finansieringsramen för klustret Inkluderande och säkra samhällen i pelare II ”Globala utmaningar och industriell konkurrenskraft” av Horisont Europa (finansieringsram på totalt 2 800 000 000euro) som avses i artikel 21.1 b ska föreslås av kommissionen under lagstiftningsprocessen och under alla omständigheter innan en politisk överenskommelse har ingåtts. Förslaget kommer att grundas på resultatet av den strategiska planeringsprocess som fastställs i artikel 6.6 i förordning XXX [ramprogrammet om Horisont Europa].

Beloppen ovan omfattar inte medlemsstaternas bidrag till kompetenscentrumets operativa och administrativa kostnader, vilket ska stå i proportion till unionens ekonomiska bidrag.

3.2. Beräknad inverkan på utgifterna

3.2.1. Sammanfattning av den beräknade inverkan på utgifterna

Miljoner euro (avrundat till tre decimaler)

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

			2021[41]	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Efter 2027***	**TOTALT**
Avdelning 1 (Personalutgifter)	Åtaganden = Betalningar	(1)	0 619	1 515	1 871	1 909	1 947	1 986	2 026		**11 873**
Avdelning 2 (Infrastruktur och driftsutgifter)	Åtaganden = Betalningar	(2)	0 619	1 515	1 871	1 909	1 947	1 986	2 026		**11 873**
Avdelning 3 (Driftsutgifter)	Åtaganden	(3)	284,892	322,244	327,578	248,382	253,295	258,214	263 ,316		**1 957,922**
	Betalningar	(4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1 061,715	**1 957,922**
TOTALA anslag för programmets finansieringsram[42]	Åtaganden	=1+2+3	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**		**1 981,668**
	Betalningar	=1+2+4	**22,459**	**105,795**	**153,954**	**171,154**	**160,369**	**154,096**	**152,126**	**1 061,715**	**1 981,668**

41 Personalanslag anges bara för ett halvår 2021

42 De totala anslag som anges avser bara EU-resurser som avsatts för cybersäkerhet inom Ett digitalt Europa. Bidraget från finansieringsramen för klustret Inkluderande och säkra samhällen i pelare II ”Globala utmaningar och industriell konkurrenskraft” av Horisont Europa (finansieringsram på totalt 2 800 000 000 euro) som avses i artikel 25.1 b ska föreslås av kommissionen under lagstiftningsprocessen och under alla omständigheter innan en politisk överenskommelse har ingåtts. Förslaget kommer att grundas på resultatet av den strategiska planeringsprocess som fastställs i artikel 6.6 i förordning XXX [ramprogrammet om Horisont Europa].

Rubrik i den fleråriga budgetramen	7	”Administrativa utgifter”

Miljoner euro (avrundat till tre decimaler)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Efter 2027***	**TOTALT**
Personalresurser		3,090	3,233	3,233	3,233	3,233	3,233	3,805		**23,060**
Övriga administrativa utgifter		0,105	0,100	0,104	0,141	0,147	0,153	0,159		**0,909**
TOTALA anslag för RUBRIK 7 i den fleråriga budgetramen	(summa åtaganden = summa betalningar)	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**		**23,969**

Miljoner euro (avrundat till tre decimaler)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Efter 2027***	**TOTALT**
TOTALA anslag samtliga RUBRIKER i den fleråriga budgetramen	Åtaganden	**289,325**	**328,607**	**334,657**	**255,574**	**260,569**	**265,572**	**271,332**		**2 005,637**
	Betalningar	**25,654**	**109,128**	**157,291**	**174,528**	**163,749**	**157,482**	**156,090**	**1² 061,715**	**2 005,637**

3.2.2. Sammanfattning av den beräknade inverkan på anslag av administrativ natur

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

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

Miljoner euro (avrundat till tre decimaler)

År	2021	2022	2023	2024	2025	2026	2027	TOTALT
RUBRIK 7 i den fleråriga budgetramen								
Personalresurser	3,090	3,233	3,233	3,233	3,233	3,233	3,805	**23,060**
Övriga administrativa utgifter	0,105	0,100	0,104	0,141	0,147	0,153	0,159	**0,909**
Delsumma RUBRIK 7 i den fleråriga budgetramen	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**	**23,969**
Utanför RUBRIK 7[43] i den fleråriga budgetramen								
Personalresurser								
Övriga utgifter av administrativ natur	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Delsumma utanför RUBRIK 7 i den fleråriga budgetramen	**1,238**	**3,030**	**3,743**	**3,818**	**3,894**	**3,972**	**4,051**	**23,746**
TOTALT	**4,433**	**6,363**	**7,079**	**7,192**	**7,274**	**7,358**	**8,016**	**47,715**

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

Ovannämnda anslag för personal och andra utgifter av administrativ karaktär utanför rubrik 7 motsvarar de belopp som täcks genom unionens ekonomiska bidrag från programmet för ett digitalt Europa.

De anslag som krävs för personal och andra utgifter av administrativa karaktär utanför rubrik 7 kommer att höjas med de belopp som täcks genom unionens ekonomiska bidrag från Horisont Europa-programmet så snart bidraget från finansieringsramen för klustret Inkluderande och säkra samhällen i pelare II ”Globala utmaningar och industriell konkurrenskraft” av Horisont Europa (finansieringsram på totalt 2 800 000 euro) som avses i artikel 21.1 b föreslås av kommissionen under lagstiftningsprocessen och under alla omständigheter innan en politisk överenskommelse har ingåtts.

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

Ovannämnda anslag för personal och andra utgifter av administrativ karaktär utanför rubrik 7 omfattar inte medlemsstaternas bidrag till kompetenscentrumets administrativa kostnader, vilket ska stå i proportion till unionens ekonomiska bidrag.

3.2.2.1. Beräknat personalbehov hos kommissionen

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

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

Beräkningarna ska anges i heltidsekvivalenter

År		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)								
Vid huvudkontoret eller vid kommissionens kontor i medlemsstaterna		20	21	21	21	21	21	22
Vid delegationer								
För forskning								
• Extern personal (i heltidsekvivalenter: FTE) – AC, AL, END, INT och JPD [44]								
Rubrik 7								
Som finansieras genom RUBRIK 7 i den fleråriga budgetramen	- vid huvudkontoret	3	3	3	3	3	3	3
	- vid delegationer							
Som finansieras genom finansieringsramen för programmet [45]	- vid huvudkontoret							
	- vid delegationer							
För forskning								
Annan (ange)								
TOTALT		**23**	**23**	**24**	**24**	**24**	**25**	**25**

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

Beskrivning av arbetsuppgifter:

Tjänstemän och tillfälligt anställda	Samordning, övervakning och styrning av de uppgifter som tilldelats Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning, inbegripet kostnader för stöd och samordning. Utveckling och samordning av policy inom cybersäkerhet när det gäller de uppgifter som har tilldelats Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning, t.ex. fastställande av prioriteringar för forsknings- och näringslivspolitik, allmänt samarbete mellan medlemsstater och ekonomiska aktörer, överensstämmelse med EU:s framtida ram för cybersäkerhetscertifiering, arbete med ansvar och omsorgsplikt eller samordning med policy när det gäller högpresterande datorer, artificiell intelligens och digital kompetens. . .
Extern personal	Samordning, övervakning och styrning av de uppgifter som tilldelats Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning, inbegripet kostnader för stöd och samordning. Utveckling och samordning av policy inom cybersäkerhet när det gäller de uppgifter som har tilldelats Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik

[44] AC= kontraktsanställda; AL = lokalanställda; END = nationella experter; INT = personal från bemanningsföretag; JPD= unga experter som tjänstgör vid delegationerna.

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

	och forskning, t.ex. fastställande av prioriteringar för forsknings- och näringslivspolitik, allmänt samarbete mellan medlemsstater och ekonomiska aktörer, överensstämmelse med EU:s framtida ram för cybersäkerhetscertifiering, arbete med ansvar och omsorgsplikt eller samordning med policy när det gäller högpresterande datorer, artificiell intelligens och digital kompetens. . .

3.2.2.2. Beräknade personalbehov på kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning

	2021	2022	2023	2024	2025	2026	2027
Handläggare vid kommissionen							
Varav AD-tjänster							
Varav AST-tjänster							
Varav AST-SC-tjänster							
Tillfälligt anställda							
Varav AD-tjänster	10	11	13	13	13	13	13
Varav AST-tjänster							
Varav AST-SC-tjänster							
Kontraktsanställda	26	32	39	39	39	39	39
Nationella experter	1	1	1	1	1	1	1
Totalt	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Beskrivning av arbetsuppgifter:

Tjänstemän och tillfälligt anställda	Operativt utförande av de uppgifter som tilldelats Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning enligt artikel 4 i denna förordning, inbegripet kostnader för stöd och samordning.
Extern personal	Operativt utförande av de uppgifter som tilldelats Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning enligt artikel 4 i denna förordning, inbegripet kostnader för stöd och samordning.

Ovannämnda beräknade personalbehov för kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning motsvarar de beräknade behoven för att genomföra unionens finansiella bidrag inom ramen för Ett digitalt Europa.

Ovannämnda beräknade personalbehov för kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning ska höjas med de beräknade behoven för att genomföra unionens finansiella bidrag inom ramen för Horisont Europa, så snart bidraget från finansieringsramen för klustret Inkluderande och säkra samhällen i pelare II ”Globala utmaningar och industriell konkurrenskraft” av Horisont Europa (finansieringsram på totalt 2 800 000 000 euro) som avses i artikel 21.1 b föreslås av kommissionen under lagstiftningsprocessen och under alla omständigheter innan en politisk överenskommelse ingås.

3.2.2.3. Plan för inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning

Tjänstegrupper och grader	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 totalt	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 Totalt							
AST/forskning (SC) 6							
AST/forskning (SC) 5							
AST/forskning (SC) 4							
AST/forskning (SC) 3							
AST/forskning (SC) 2							
AST/forskning (SC) 1							

AST/SC Totalt							
TOTALT	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4. Beräknad effekt på (extra) personal – extern personal för kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning

Kontraktsanställda	2021	2022	2023	2024	2025	2026	2027
Tjänstegrupp IV	20	22	29	29	29	29	29
Tjänstegrupp III	2	4	4	4	4	4	4
Tjänstegrupp II	4	6	6	6	6	6	6
Tjänstegrupp I							
Totalt	**26**	**32**	**39**	**39**	**39**	**39**	**39**

För att utjämna personaleffekterna kommer den extra personalen på kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning delvis att uppvägas av färre handläggare och extern personal (dvs. den nuvarande tjänsteförteckningen och externa personalen) på relevanta avdelningar inom kommissionen.
Ersättning till personalen på kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning i punkterna 3.2.2.2–4 ska utgå enligt följande[46]:

TOTALT	2021	2022	2023	2024	2025	2026	2027
Handläggare vid kommissionen	5	5	6	6	6	6	6
Tillfälligt anställda							
Kontraktsanställda	14	17	20	20	20	20	20
Nationella experter							
Heltidsekvivalenter, totalt	19	22	26	26	26	26	26
Personalstyrka	19	22	26	26	26	26	26

Ersättningen till personal på kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning ska motsvara den andel som utgörs av unionens finansiella bidrag, dvs. 50 %.

Ovannämnda ersättning avser beräknade personalbehov för kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning för att genomföra unionens finansiella bidrag inom ramen för Ett digitalt Europa.

[46] Med förbehåll för den slutliga budget vars genomförande ska delegeras till kompetenscentrumet

Ovannämnda ersättning ska höjas med de beräknade behoven för att genomföra unionens finansiella bidrag inom ramen för Horisont Europa, så snart bidraget från finansieringsramen för klustret Inkluderande och säkra samhällen i pelare II ”Globala utmaningar och industriell konkurrenskraft” av Horisont Europa (finansieringsram på totalt 2 800 000 000 euro) som avses i artikel 21.1 b föreslås av kommissionen under lagstiftningsprocessen och under alla omständigheter innan en politisk överenskommelse ingås.

3.2.3. Bidrag från tredje part

Förslaget/initiativet:

– ☐ innehåller inga bestämmelser om samfinansiering från tredje parter

– ☒ innehåller bestämmelser om samfinansiering från tredje parter[47] enligt följande uppskattning:

Anslag i miljoner euro (avrundat till tre decimaler)

År	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**TOTALT**
Medlemsstater – bidrag till personalutgifter	0,619	1 ,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Medlemsstater – bidrag till infrastruktur och driftsutgifter	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Medlemsstater – bidrag till operativa utgifter	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
TOTALA anslag som tillförs genom samfinansiering	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

Ovannämnda bidrag från tredje part gäller endast samfinansiering motsvarande de EU-medel som är avsatta för cybersäkerhet i Ett digitalt Europa. Ovannämnda bidrag från tredje part ska höjas så snart bidraget från klustret Inkluderande och säkra samhällen i pelare II ”Globala utmaningar och industriell konkurrenskraft” av Horisont Europa (finansieringsram på totalt 2 800 000 euro) som avses i artikel 21.1 b föreslås av kommissionen under lagstiftningsprocessen och under alla omständigheter innan en politisk överenskommelse har ingåtts. Förslaget kommer att grundas på resultatet av den strategiska planeringsprocess som fastställs i artikel 6.6 i förordning XXX [ramprogrammet om Horisont Europa].

3.3. Beräknad inverkan på inkomsterna

– ☒ Förslaget/initiativet påverkar inte budgetens inkomstsida.

– ☐ Förslaget/initiativet påverkar inkomsterna på följande sätt:

☐ Påverkan på egna medel

☐ Påverkan på andra inkomster

ange om inkomsterna har avsatts för utgiftsposter ☐

Miljoner euro (avrundat till tre decimaler)

Budgetrubrik i den årliga budgetens inkomstdel:	Förslagets/initiativets inverkan på inkomsterna[48]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Artikel …….							

[47] Beräknat bidrag in natura från medlemsstater

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

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

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