

Upptäcka och hantera cybersäkerhetsincidenter

EU:s samarbetsram gör framsteg, men är endast delvis ändamålsenlig på grund av förseningar i genomförandet och begränsat informationsutbyte



Innehållsförteckning

Punkt

01–24 | **Huvudbudskap**

01–08 | Varför detta område är viktigt

09–24 | Vad vi konstaterade och rekommenderar

25–01 | **Våra iakttagelser mer i detalj**

25–75 | Även om EU:s nätverk och mekanismer för cybersäkerhet främjar samarbete och insatser minskar deras ändamålsenlighet på grund av begränsat informationsutbyte och ofullständigt genomförande

25–52 | EU-nätverken möjliggör samarbete mellan medlemsstaterna, men ett begränsat informationsutbyte minskar deras mervärde

53–62 | EU:s cybersäkerhetsreserv gör det möjligt att snabbt införa tjänster för incidenthantering

63–75 | Det europeiska varningssystemet för cybersäkerhet syftar till att förbättra förmågan att upptäcka hot, men är ännu inte i drift

76–01 | EU-finansierade projekt inom Digital syftar till att stärka cybersäkerheten, men står inför utmaningar när det gäller genomförande och rapportering

76–82 | Förseningar i inrättandet hindrade kompetensgemenskapen för cybersäkerhet från att utforma Digital i enlighet med sina behov

83–97 | EU-finansierade projekt har relevanta mål, men många stöter på operativa problem

98–01 | Prestationsramarna för de flesta EU-finansierade projekten är otillräckliga, och de cybersäkerhetsrelaterade prestationsuppgifterna för Digital är inte korrekta

Bilagor

Bilaga I – Om revisionen

Bilaga II – EU:s cybersäkerhetslandskap

Bilaga III – Utvalda cybersäkerhetsåtgärder

Bilaga IV – Revisionsrättens bedömning av EU-finansierade cybersäkerhetsprojekt

Förkortningar

Ordlista

Kommissionens svar

Svaren från Europeiska kompetenscentrumet för cybersäkerhet (ECCC).

Svar från Europeiska unionens cybersäkerhetsbyrå (Enisa)

Tidsplan

Vi som arbetat med revisionen

01

Huvudbudskap

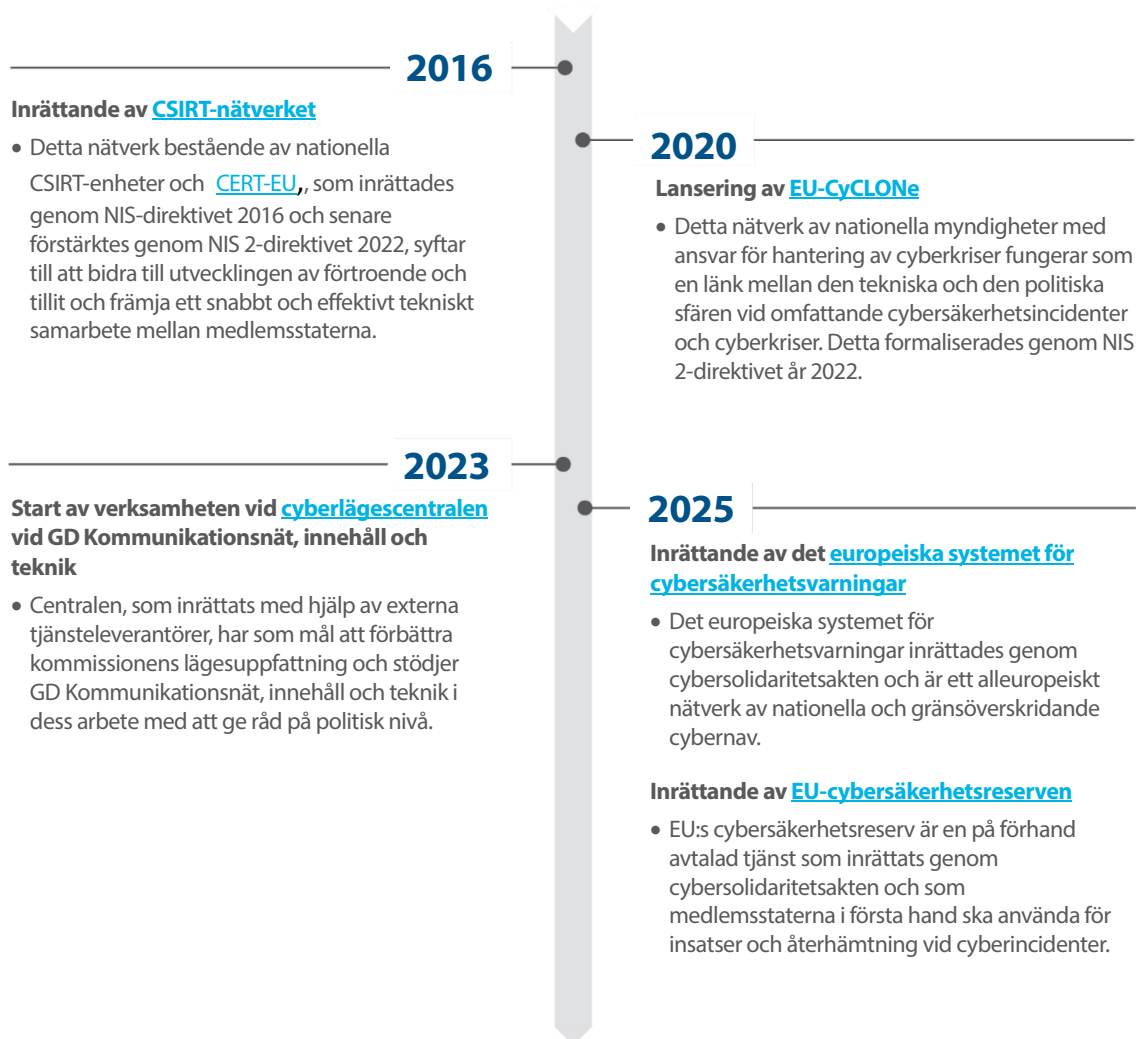
Varför detta område är viktigt

- 01** Risken för cyberattacker ökar i takt med att vår ekonomi och vår vardag blir allt mer digitaliserad. Cybersäkerhet definieras som "all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot."¹ Cybersäkerhet kräver ett helhetsperspektiv för att förebygga, upptäcka, hantera och återhämta sig från cyberhot.
- 02** EU:s cybersäkerhetslandskap omfattar ett stort antal offentliga och privata aktörer på regional och nationell nivå och EU-nivå inom den civila sektorn. Cybersäkerhet är också en viktig del av nationella säkerhets- och försvarssystem.
- 03** Medlemsstaterna har det primära ansvaret för förebyggande av, beredskap inför och hantering av cybersäkerhetsincidenter och kriser som påverkar dem. Eftersom dessa incidenter kan påverka den inre marknadens förmåga att fungera väl spelar EU också en viktig roll i händelse av en betydande incident eller kris. Under de senaste åren har EU stärkt sitt regelverk för cybersäkerhet², som är under ständig utveckling, och inrättat nätverk och mekanismer, såsom visas i **Figur 1** nedan samt i **bilaga II**.

¹ Förordning 2019/881: ([cybersäkerhetsakten](#)).

² Till exempel föreslog kommissionen en [digital omnibusförordning](#) i november 2025 och en reviderad [EU-cybersäkerhetsakt](#) i januari 2026.

Figur 1 | EU:s nätverk och mekanismer för cybersäkerhet 2016–2025



CSIRT-enheter: enheter för hantering av datasäkerhetsincidenter

GD Kommunikationsnät, innehåll och teknik: Generaldirektoratet för kommunikationsnät, innehåll och teknik.

EU-CyCLONe: Europeiska kontaktnätverket för cyberkriser

NIS-direktivet: Direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen

NIS 2-direktivet: Direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen

Källa: Revisionsrätten.

- 04** Enligt den nuvarande fleråriga budgetramen för 2021–2027 är den viktigaste finansieringskällan för cybersäkerhet [programmet för ett digitalt Europa](#) (Digital). Det har en total budget på 8,1 miljarder euro, varav 1,4 miljarder euro avsätts för att stärka cybersäkerheten.

- 05** Syftet med vår revision var att bedöma om EU:s åtgärder gör det lättare att upptäcka och hantera betydande och storskaliga cybersäkerhetsincidenter på ett ändamålsenligt sätt. Vi bedömde om detta var fallet för
- nätverk och mekanismer på EU-nivå (dvs. nätverk för enheter för hantering av it-säkerhetsincidenter (CSIRT-nätverket), Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), det europeiska systemet för cybersäkerhetsvarningar, cyberlägescentralen och EU:s cybersäkerhetsreserv),
 - åtgärder som finansieras inom ramen för Digital.
- 06** Vi räknar med att våra slutsatser kommer att bidra till att stärka EU:s cyberresiliens genom att öka ändamålsenligheten och effektiviteten hos EU:s nätverk och mekanismer samt förbättra urvals- och övervakningsprocesserna för EU-finansierade åtgärder.
- 07** Revisionen omfattar perioden 2022–2025. Den bygger på en skrivbordsgranskning och analys av relevanta handlingar, revisionsbesök i tre medlemsstater (Irland, Grekland och Italien) samt skriftliga frågeformulär och intervjuer med berörda intressenter. Mer bakgrundsinformation och närmare uppgifter om revisionens inriktning och omfattning samt revisionsmetod finns i [bilaga I](#).

Vad vi konstaterade och rekommenderar

- 08** Sammantaget drar vi slutsatsen att EU:s åtgärder endast delvis underlättar upptäckten och hanteringen av betydande och storskaliga cybersäkerhetsincidenter. En samarbetsram har stegvis införts, men arbetet mot att uppnå fullständigt upprättande pågår fortfarande. Begränsat informationsutbyte, rapportering av brister och avsevärda förseningar i genomförandet hindrar EU:s nätverk och mekanismer från att uppnå sin fulla potential. Projekten som finansieras av Digital eftersträvar relevanta mål, men står inför flera operativa utmaningar och förseningar, och det finns brister i den övergripande ramen för prestationsövervakning.
- 09** Det nuvarande systemet med EU-nätverk och mekanismer som syftar till att underlätta upptäckt och hantering av betydande cybersäkerhetsincidenter har byggts upp gradvis. År 2025 antog rådet [cyberplanen](#), där EU:s ram för hantering av cyberkriser fastställs. Vi konstaterade att cyberplanen i stor utsträckning klargör roller och ansvarsområden när det gäller EU:s hantering av cyberkriser. Trots detta har de praktiska arrangemangen för hur CSIRT-nätverket (inrättades 2016) och EU-CyCLONe (formaliserades 2023) ska samarbeta ännu inte formaliserats (punkterna [25–31](#)).

- 10** Vi har konstaterat att informationsutbytet via dessa nätverk är begränsat. Detta beror främst på förseningar i införlivandet av [direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen](#) (NIS 2-direktivet), svårigheter att avgöra om en incident har gränsöverskridande konsekvenser och nationell säkerhetslagstiftning som förhindrar informationsutbyte. Nätverkens mervärde minskar avsevärt om medlemsstaterna inte är villiga att dela med sig av aktuell och användbar information (punkterna [32–45](#)).



Rekommendation 1

Stärka informationsutbytet mellan medlemsstaterna

För att förbättra upptäckten och hanteringen av cybersäkerhetsincidenter bör kommissionen, med stöd av Europeiska unionens cybersäkerhetsbyrå (Enisa)

- a) föreslå att samarbetsgruppen för nät- och informationssäkerhet genomför en detaljerad analys av nationella säkerhetsrestriktioner som begränsar informationsutbytet och påverkar EU:s cyberresiliens, och identifiera rättsliga och tekniska lösningar för att öka informationsutbytet samtidigt som gränserna för den nationella säkerheten respekteras,
- b) utan att det påverkar beslut av medlagstiftare, i samarbete med medlemsstaterna säkerställa att den gemensamma kontaktpunkten för incidentrapportering som föreslås i den digitala omnibusförordningen kan upptäcka möjliga gränsöverskridande incidenter,
- c) arbeta på lösningar för att möjliggöra incidentanmälan i realtid till Enisa.

Måldatum för genomförande: a) och b) 2027, c) 2028

- 11** År 2022 etablerade kommissionen sin sektor ”cyberlägescentralen” för att öka sin lägesuppfattning, med målet att stödja sitt institutionella ansvar för krishantering. Centralens verksamhet är i hög grad beroende av avtal med externa tjänsteleverantörer. Vi konstaterade att det arbete som utförs av de externa tjänsteleverantörerna delvis överlappar den befintliga kapaciteten hos Europeiska unionens cybersäkerhetsbyrå (Enisa) när det gäller lägesuppfattning och hotövervakning. Vi anser att man vid inrättandet av cyberlägescentralen inte i tillräcklig utsträckning utnyttjat möjligheterna till effektivisering genom att ta vara på den information som redan fanns tillgänglig hos kommissionen och Enisa. Dessutom utgör avsaknaden av en omfattande, detaljerad framtidsplan efter att avtalet löper ut en risk för cyberlägescentralens verksamhet efter 2026 (punkterna [46–52](#)).



Rekommendation 2

Rationalisera EU:s kapacitet för lägesuppfattning på cybersäkerhetsområdet och optimera spridningen av information

För att öka effektiviteten bör kommissionen i samarbete med Enisa bedöma möjligheterna att gemensamt insamla och analysera information för lägesuppfattningen. Kommissionen bör också göra denna information och de tillhörande rapporterna om cyberhot tillgängliga för alla berörda avdelningar och byråer inom EU.

Måldatum för genomförande: 2027

- 12** Genom 2024 års [cybersolidaritetsakt](#) inrättas EU:s cybersäkerhetsreserv, vars syfte är att stödja medlemsstaterna i deras hantering av och återhämtning efter allvarliga cybersäkerhetsincidenter. Den består av utvalda tjänsteleverantörer för varje medlemsstat, som kan reagera på incidenter dygnet runt. Denna strategi bidrar till att tillgodose medlemsstaternas särskilda krav och bygga upp förtroende, men den tillgängliga budgeten är jämnt fördelad mellan dem och tar inte hänsyn till varje medlemsstats särskilda behov (punkterna [53–58](#)).
- 13** Vi anser att användningen av förhandsavtalade leverantörer gör det möjligt att snabbt införa incidenthanteringstjänster. Även om EU-cybersäkerhetsreserven främst syftar till att stödja insatser och återhämtning kan den när den inte används för incidenthantering användas för beredskap. Denna flexibla strategi kan förhindra att förbetalda tjänster förblir outnyttjade. Reserven riskerar dock att i första hand användas för beredskap snarare än för insatser, vilket strider mot dess avsedda syfte (punkterna [59–62](#)).
- 14** Det europeiska systemet för cybersäkerhetsvarningar är ett nätverk av nationella och gränsöverskridande cybernav som syftar till att förbättra upptäckten, analysen och hanteringen av cyberhot. Vi konstaterade att de två naven (ATHENA och ENSOC) vid tidpunkten för revisionen ännu inte var i drift på grund av betydande förseningar i upphandlingen av verktyg och tjänster, och att det europeiska systemet för cybersäkerhetsvarningar ännu inte var i drift (punkterna [63–71](#)).

- 15** Ett av de viktigaste målen för det europeiska systemet för cybersäkerhetsvarningar är att uppmuntra meningsfullt informationsutbyte mellan olika kluster av medlemsstater. Även om detta har potential att lösa vissa av problemen kring informationsutbytet är det en stor utmaning att integrera cybernaven i det redan komplexa cybersäkerhetslandskapet. Vi konstaterade att de samarbetsavtal, den gemensamma taxonomi och de interoperabilitetsstandarder som krävs för att det europeiska systemet för cybersäkerhetsvarningar ska fungera fullt ut ännu inte hade införts (punkterna [72–75](#)).



Rekommendation 3

Integrera det europeiska systemet för cybersäkerhetsvarningar i EU:s cybersäkerhetslandskap

Kommissionen bör, tillsammans med Enisa och medlemsstaterna, säkerställa att samarbetsavtal och interoperabilitetsstandarder finns på plats för att underlätta informationsutbyte mellan gränsöverskridande nav som ingår i det europeiska systemet för cybersäkerhetsvarningar, CSIRT-nätverket och EU-CyCLONe.

Måldatum för genomförande: 2028

- 16** År 2018 föreslog kommissionen att Europeiska kompetenscentrumet för cybersäkerhet skulle inrättas för att hantera cybersäkerhetskomponenten i Digital från och med 2021. I [förordningen om Europeiska kompetenscentrumet](#) föreslogs inrättandet av ett kompetensnätverk för cybersäkerhet bestående av företrädare för näringslivet samt den akademiska världen och forskningsorganisationer. Utvalda medlemmar från kompetensgemenskapen för cybersäkerhet skulle sedan bilda en strategisk rådgivande grupp (punkterna [76–77](#)).
- 17** Vi konstaterade att det förekom förseningar i fråga om kompetenscentrumets uppnående av finansiell autonomi samt i fråga om inrättandet av kompetensgemenskapen för cybersäkerhet och den strategiska rådgivande gruppen. Detta innebär att kompetensgemenskapen för cybersäkerhet och den strategiska rådgivande gruppen inte kunde bidra med synpunkter när det gällde att utforma arbetsprogrammen för Digital. Vi anser att detta var en förlorad möjlighet (punkterna [78–82](#)).
- 18** Vi konstaterade att alla de projekt som vi granskade hade relevanta mål som bidrar till att uppnå cybersäkerhetsmålen för Digital. Dock fanns fall där den kvalitet eller de resultat som uppnåddes inte var tillfredsställande, främst på grund av förseningar i genomförandet (punkterna [83–88](#)).

- 19** I [förordningen om programmet för ett digitalt Europa \(Digital\)](#) anges att finansiering av cybersäkerhet av säkerhetsskäl kan begränsas till entiteter som är etablerade i medlemsstater och som kontrolleras av medlemsstater eller medborgare i medlemsstater. Den centrala valideringstjänsten vid [Europeiska genomförandeorganet för forskning](#) utför denna bedömning av ägar- och kontrollförhållanden på Europeiska kompetenscentrumets vägnar (punkterna [89–92](#)).
- 20** När det gäller ekonomiskt stöd till tredje part är det projektstödmottagarna som ansvarar för bedömningen av ägar- och kontrollförhållanden, utifrån sin egen strategi och metodik. Vi har konstaterat att Europeiska kompetenscentrumet för cybersäkerhet varken validerar sin metodik eller genomför kontroller för att säkerställa att de utvalda tredje parterna ägs och kontrolleras av EU. Vi anser att det finns en betydande risk för att stödmottagarna inte har kapacitet att utföra dessa kontroller på ett korrekt sätt. Denna risk har inte hanterats på ett tillfredsställande sätt och kan leda till att känslig infrastruktur, driftsdata och säkerhetskritisk teknik utsätts för risker (punkterna [93–97](#)).



Rekommendation 4

Säkerställa en gedigen bedömning av ägar- och kontrollförhållanden för entiteter som får EU-finansiering inom ramen för programmet för ett digitalt Europa

Europeiska kompetenscentrumet för cybersäkerhet bör

- a) erhålla rimlig säkerhet om att stödmottagare som är ansvariga för att tillhandahålla finansiellt stöd till tredje parter har den administrativa och tekniska kapacitet som krävs för att utföra adekvata bedömningar av ägar- och kontrollförhållanden på grundval av befintlig metodik som är tillgänglig för stödmottagare som genomför finansiellt stöd för tredje parter, och
- b) på stickprovsbasis kontrollera om endast berättigade entiteter har erhållit EU-finansiering.

Måldatum för genomförande: a) 2026, b) 2027

- 21** Stödmottagare som förvaltar EU-finansierade projekt måste rapportera om sina framsteg och resultat till Europeiska kompetenscentrumet för cybersäkerhet, med hjälp av delmål och eftersträvar resultat. Dessa är avgörande för projektövervakningen och bör definieras på ett korrekt sätt. Vi konstaterade att nästan inget av projekten i vårt urval följde instruktionerna om hur delmål och eftersträvar resultat ska fastställas och att många av dem inte var användbara för att följa framstegen (punkterna [98–100](#)).

- 22** Vi konstaterade att många av de prestationsindikatorer som används av stödmottagarna inte är relevanta eller mätbara och att de saknar mål eller utgångsvärde. Vidare var rapporteringen om dessa indikatorer otillräcklig och kan därför inte ligga till grund för bedömningen av projektets resultat (punkterna [101–103](#)).
- 23** För att övervaka resultaten av Digital som helhet måste alla projekt rapportera om särskilda programindikatorer som ligger till grund för kommissionens årliga [programresultatförklaringar](#). Kompetenscentrumet ansvarar för att samla in och kontrollera uppgifterna om dessa indikatorer. Vi upptäckte flera brister i hur uppgifterna samlades in och i deras övergripande kvalitet. Vi har inte funnit några belegg för att kompetenscentrumet skulle ha kontrollerat riktigheten i de rapporterade uppgifterna. På grundval av våra stickprovskontroller anser vi att de rapporterade uppgifterna inte korrekt speglar de uppnådda resultaten (punkterna [104–107](#)).



Rekommendation 5

Stärka ramen för prestationsövervakning när det gäller cybersäkerhetskomponenten i programmet för ett digitalt Europa

För att möjliggöra lämplig övervakning av framsteg och resultat bör Europeiska kompetenscentrumet för cybersäkerhet göra följande:

- a) Innan bidragsavtalet undertecknas, säkerställa att alla projekt har fastställda delmål, eftersträvar resultat och prestationsindikatorer som överensstämmer med instruktionerna i ansökningsformuläret.
- b) Utforma och genomföra ett robust system för insamling, spårbarhet, verifiering och aggregering av uppgifterna för prestationsindikatorerna för cybersäkerhetskomponenten i programmet för ett digitalt Europa, för att säkerställa att indikatorerna korrekt speglar de uppnådda resultaten.

Måldatum för genomförande: 2027

Våra iakttagelser mer i detalj

Även om EU:s nätverk och mekanismer för cybersäkerhet främjar samarbete och insatser minskar deras ändamålsenlighet på grund av begränsat informationsutbyte och ofullständigt genomförande

EU-nätverken möjliggör samarbete mellan medlemsstaterna, men ett begränsat informationsutbyte minskar deras mervärde

- 24** EU:s nuvarande ram för nätverk och mekanismer som syftar till att underlätta upptäckt av och hantering av betydande cybersäkerhetsincidenter har byggts upp stegvis, med utgångspunkt i [direktivet om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen](#)³ (NIS-direktivet), som trädde i kraft i augusti 2016. Vi ger en översikt över den aktuella situationen inom EU i [bilaga II](#).

³ Direktiv (EU) 2016/1148.

EU-nätverken möjliggör samarbete mellan medlemsstaterna på teknisk och operativ nivå.

- 25** Genom NIS-direktivet inrättades [CSIRT-nätverket](#), som samlar [CERT-EU](#) (cybersäkerhetstjänsten för unionens institutioner, organ byråer) och de CSIRT-enheter som utsetts av medlemsstaterna. Detta nätverk syftar till att bygga upp förtroende och tillit mellan nationella CSIRT-enheter och främja ett snabbt och ändamålsenligt operativt samarbete mellan medlemsstaterna.
- 26** [EU-CyCLONe](#) bildades 2020 som ett informellt samarbetsnätverk för nationella myndigheter med ansvar för hantering av cyberkriser. Den fungerar som en länk mellan den tekniska nivå inom vilket CSIRT-nätverket verkar och den politiska nivån för Europeiska unionens råd och dess arrangemang för [integrerad politisk krishantering](#). När NIS 2-direktivet trädde i kraft 2023 fastställdes roll och tydligt uppdrag för EU-CyCLONe.
- 27** Vi har undersökt om dessa nätverks roller och ansvarsområden på EU-nivå är tydligt definierade och om de underlättar samarbetet mellan medlemsstaterna.
- 28** [Enisa](#) fungerar som sekretariat för CSIRT-nätverket och EU-CyCLONe och tillhandahåller resurser, sakkunskap, infrastruktur och it-verktyg som krävs för samarbete och säker kommunikation för informationsutbyte. I sin enkät om intressenternas nöjdhet⁴ från början av 2025 fick Enisa goda poäng för sitt arbete som sekretariat för dessa nätverk. Denna positiva återkoppling bekräftades också under våra granskningsbesök, där nationella cybersäkerhetsmyndigheter uttryckte sin uppskattning.
- 29** År 2025 antog rådet [cyberplanen](#), som fastställer roller och ansvarsområden för de viktigaste aktörerna (däribland CSIRT-nätverket och EU-CyCLONe) samt de mekanismer som ska tillämpas vid omfattande cybersäkerhetsincidenter eller cyberkriser. Vi har konstaterat att cyberplanen i stor utsträckning klargör roller och ansvarsområden när det gäller EU:s hantering av cyberkriser och tar hänsyn till de förändringar som skett sedan den första versionen av planen från 2017. I planen definieras tre nivåer av samarbete: tekniskt, operativt och politiskt. Den beskriver de nya nätverk och strukturer som inrättats sedan 2017 – såsom EU-CyCLONe, EU:s snabbinsatsteam för hybridhot och det europeiska systemet för cybersäkerhetsvarningar – och tar upp hur cyberkrishantering bör integreras i EU:s bredare ram för krishantering.

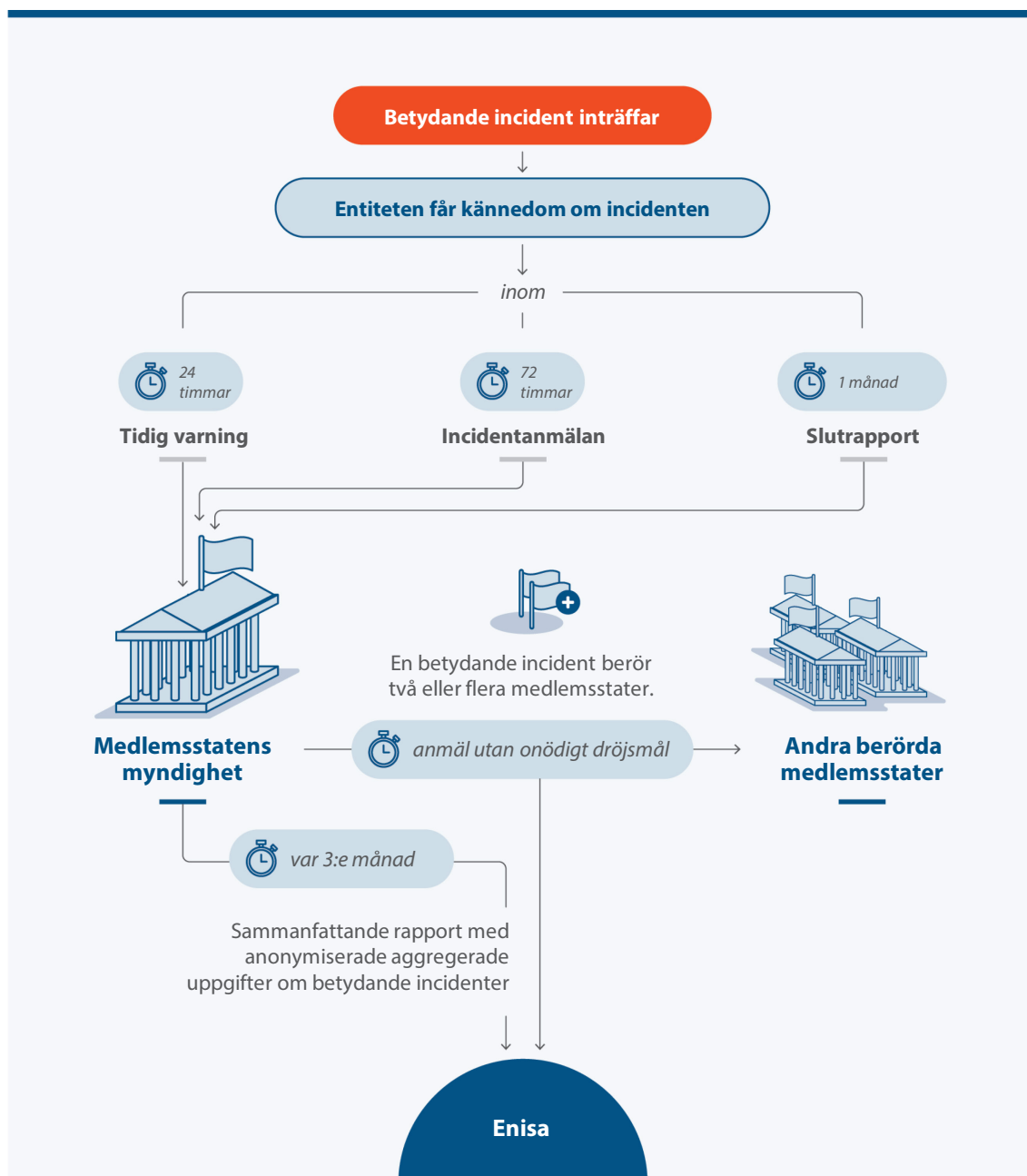
⁴ Enisas [konsoliderade årliga verksamhetsrapport för 2024](#), s. 33 och s. 36.

- 30** Trots att CSIRT-nätverket inrättades officiellt 2016 och EU-CyCLONe 2023 har de två nätverken ännu inte fastställt några formella rutiner för hur de ska samarbeta. De har inte heller enats om vilka kriterier som ska gälla för att CSIRT-nätverket ska kunna meddela EU-CyCLONe att en konstaterad cybersäkerhetsincident utgör en potentiell eller pågående cybersäkerhetsincident i stor skala. De två nätverken måste också enas om en gemensam klassificering av incidenternas allvarlighetsgrad och nyckelbegrepp – såsom ”hot”, ”fientlig aktör”, ”incident” eller ”påverkan” – vilket är nödvändigt för att möjliggöra automatiserat informationsutbyte. För närvarande råder det tolkningsutrymme i fråga om när en incident ska betraktas som betydande eller storskalig. Bristen på en gemensam klassificeringsmodell togs upp av cybersäkerhetsmyndigheterna i alla tre medlemsstater som vi besökte.

Begränsning av informationsutbyte och rapportering minskar avsevärt dessa nätverks mervärde.

- 31** Geografiska gränser hindrar inte att cybersäkerhetsincidenter och cyberattacker inträffar och sprider sig. Informationsutbyte mellan medlemsstaterna, till exempel rörande de taktiker och tekniker som hotaktörer använder sig av, samt om digitala tecken på att ett nätverk eller informationssystem har utsatts för intrång (”angreppsindikatorer”), kan i hög grad bidra till ökad cybersäkerhet.
- 32** Vi konstaterade att informationsutbytet var begränsat, vilket avsevärt minskade mervärdet av dessa nätverk. De begränsningar vi har konstaterat gäller främst förseningar i införlivandet av NIS 2-direktivet, svårigheter att avgöra om en incident har gränsöverskridande påverkan, nationell säkerhetslagstiftning som begränsar informationsutbytet samt bristande förtroende. Genom NIS 2-direktivet införs flera rapporteringskrav för entiteter som omfattas av det direktivet och för medlemsstaternas myndigheter, såsom visas i [figur 2](#).

Figur 2 | Tidsram för rapportering av incidenter enligt direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela EU (NIS 2)



Källa: Revisionsrätten, på grundval av uppgifter från Enisa.

- 33** Medlemsstaterna hade fram till oktober 2024 på sig att [införliva NIS 2-direktivet](#) i sin nationella lagstiftning, men endast två höll tidsfristen. Förseningar i införlivandet har en betydande påverkan på informationsutbytet eftersom de enheter som omfattas av NIS 2-direktivet under tiden inte har någon rättslig skyldighet att rapportera incidenter. Kommissionen uppskattade⁵ att 15 500 enheter omfattades av NIS-direktivet, medan över 110 000 enheter omfattas av NIS 2-direktivet. Till exempel hade den offentliga förvaltningen – den sektor som enligt Enisas [hotbilsrapport](#) från 2025 var mest utsatt i EU – ingen skyldighet att rapportera incidenter inom ramen för NIS-direktivet.
- 34** Rapporteringen av incidentuppgifter till Enisa var tredje månad (dvs. långt efter att en incident kan ha ägt rum) begränsar dess mervärde. Dessa uppgifter används främst för statistiska ändamål och för att redovisa historiska trender, inte för att förbättra upptäckt och hantering. Enisa tillhandahåller ett [webbaserat verktyg](#) som medlemsstaterna kan använda för att lämna in sina rapporter. Rapporteringsmallen innehåller en minimiuppsättning uppgifter som måste tillhandahållas, såsom typen av incident och den berörda sektorn. Enisa föreslår dessutom att medlemsstaterna tillhandahåller ytterligare information för att möjliggöra en mer ingående analys av uppgifterna, till exempel genom att koppla incidenter till specifika sårbarheter. Det är dock inte alla medlemsstater som väljer att lämna dessa uppgifter, vilket avsevärt försämrar de insamlade uppgifternas kvalitet och mervärde.
- 35** Enisa uppgav i sin [rapport från 2024 om cybersäkerhetssituationen i EU](#) att incidenterna sannolikt är underrapporterade, eftersom antalet rapporterade incidenter verkade vara lågt. Under åren 2018–2021 rapporterade medlemsstaterna mellan 100 och 500 incidenter varje år till Enisa. Antalet har ökat gradvis och uppgick år 2024 till 1 276⁶.

⁵ Europeiska kommissionen, 2020 års [konsekvensbedömningsrapport](#).

⁶ Uppgifter från [CIRAS](#) för 2024.

- 36** I sin [hotbilsrapport](#) för 2025, som omfattar perioden juni 2024–juni 2025, identifierade Enisa cirka 4 800 cyberincidenter⁷ via underrättelseinhämtning genom öppna källor såsom nyhetsartiklar. Alla dessa incidenter skulle inte ha varit rapporteringspliktiga enligt NIS 2-direktivet, eftersom Enisa vid insamlingen av uppgifter täcker ett bredare spektrum av incidenter. Omvänt rapporteras många betydande incidenter inte i underrättelseinhämtning genom öppna källor. Eftersom de uppgifter som rapporteras av medlemsstaterna är anonymiserade kan Enisa inte koppla de incidenter som byrån identifierar till dem som rapporteras av medlemsstaterna. Det är därför inte möjligt att exakt fastställa omfattningen av underrapporteringen, men vi anser att skillnaden mellan antalet incidenter som rapporteras av medlemsstaterna och antalet incidenter i hotbilsrapporten visar att inte alla betydande incidenter rapporteras.
- 37** En annan indikation på underrapportering är antalet anmälningar till andra berörda medlemsstater och Enisa om betydande gränsöverskridande incidenter. Ett liknande krav fanns i NIS-direktivet, men ansågs vara ineffektivt eftersom kommissionen under 2020 konstaterade⁸ att anmälningar sällan skickades in trots skyldigheten. Kommissionen ansåg att underlåtenheten att anmäla berodde på bristen på tydliga villkor för informationsutbyte och avsaknaden av gemensamma mål som uppmuntrar till utbyte.
- 38** Skyldigheten att informera andra medlemsstater är avgörande för att förhindra att incidenter sprider sig – underlåtenhet att göra detta påverkar EU:s cybersäkerhet negativt. Under 2025 rapporterades endast 14 betydande gränsöverskridande incidenter av sju medlemsstater. Medlemsstaterna lämnade in två incidentrapporter under 2024, ingen under 2023 och tre under 2022 med möjlig gränsöverskridande inverkan. Detta visar att rapporteringen av betydande gränsöverskridande incidenter är mycket liten och inte speglar den verkliga omfattningen av sådana attacker. För att sätta detta i perspektiv identifierade Enisa 322 incidenter som specifikt riktar sig mot två eller flera medlemsländer i sin [hotbilsrapport från 2024](#). Collins Aerospace-incidenten (se [ruta 1](#)) är ett exempel på att medlemsstater inte rapporterar en incident trots att den har en betydande gränsöverskridande inverkan.

⁷ Enisas [hotbilsrapport för 2025](#).

⁸ Europeiska kommissionen, 2020 års [konsekvensbedömningsrapport](#).

Ruta 1

Cybersäkerhetsincident störde flygplatsverksamhet

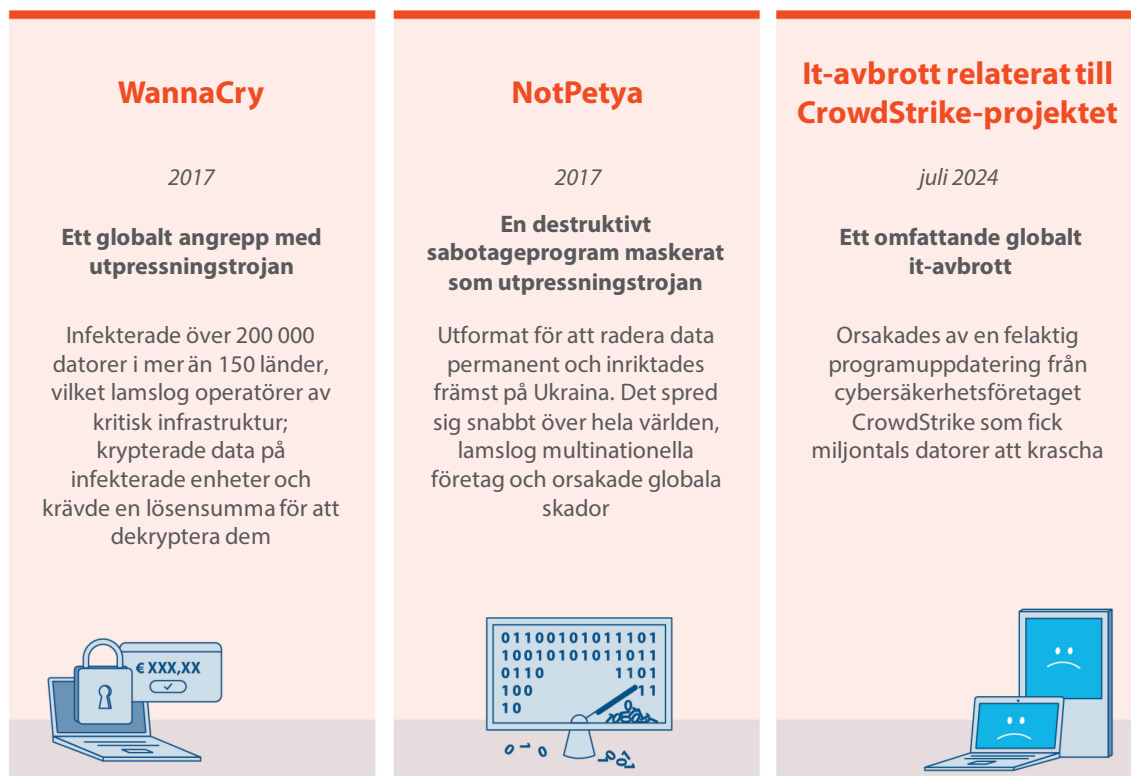
I september 2025 drabbades Collins Aerospace, en ledande teknikleverantör till flygindustrin, av en omfattande attack med en utpressningstrojan riktad mot företagets programvara för passagerarhantering. Attacken tvingade stora europeiska flygplatser att övergå till manuell drift, vilket ledde till omfattande flygförseningar och inställda flyg. Störningarna var allvarligast på Heathrow-flygplatsen i London, flygplatsen i Bryssel, Brandenburg-flygplatsen i Berlin och flygplatsen i Dublin.

Enligt NIS 2-direktivet betraktas en incident som "betydande" om den bland annat orsakar allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för den berörda entiteten. Ingen medlemsstat betraktade dock incidenten som vare sig betydande eller som storskalig och gränsöverskridande. Därför underrättade ingen av de berörda medlemsstaterna formellt Enisa eller andra medlemsstater om incidenten. CSIRT-nätverket informerade inte EU-CyCLONE, som därför inte bidrog till den samordnade hanteringen av incidenten.

Källa: Revisionsrättens analys bygger på intervjuer med Enisa.

- 39** En annan orsak till att antalet rapporterade gränsöverskridande incidenter är begränsat är att det är upp till myndigheterna i varje medlemsstat att avgöra om en rapporterad incident har gränsöverskridande påverkan och att identifiera de övriga berörda medlemsstaterna. På grundval av den information som de har tillgång till kan det hända att den rapporterande entiteten eller medlemsstatens myndighet inte är medveten om att vissa attacker är gränsöverskridande. För närvarande finns det ingen EU-omfattande plattform som tar emot incidentrapporter i realtid från alla medlemsstater och som kan koppla samman information om sektorer eller angreppsindikatorer för att upptäcka gränsöverskridande incidenter. Det finns därför en betydande risk för att vissa gränsöverskridande incidenter inte identifieras och rapporteras.
- 40** Ingen cybersäkerhetsincident har betraktats som "storskalig" av någon medlemsstat sedan 2016. I princip omfattas alla incidenter som i betydande grad påverkar minst två medlemsstater av denna definition. Även cybersäkerhetsincidenter som har orsakat globala avbrott och betydande skador, såsom de som visas i [figur 3](#), har dock inte ansetts vara storskaliga. Till följd av detta har eskaleringsförfarandet mellan EU och EU-CyCLONE aldrig aktiverats fullt ut på grund av en storskalig cybersäkerhetsincident.

Figur 3 | Exempel på betydande cybersäkerhetsincidenter



Källa: Revisionsrätten, hämtat från [Cloudflare](#), [Enisa](#), [Europol](#), [Wired](#), [IBM](#) och [CrowdStrike](#).

- 41** Utöver den rapporteringsskyldighet som ålagts organisationer och medlemsstater har CSIRT-nätverket inrättats för att underlätta informationsutbytet. Förtroendet mellan medlemsstaterna är centralt för CSIRT-nätverket, där information delas på frivillig basis. Nätverkets mervärde minskar avsevärt om medlemsstaterna inte är villiga att i rätt tid dela användbar information.
- 42** Informationsutbytet på EU-nivå begränsas av varje medlemsstats nationella säkerhetslagstiftning. Om en medlemsstat bedömer att information om cyberattacker mot en kritisk entitet är säkerhetsskyddsklassificerad, eller att rapportering om en specifik incident skulle vara till skada för dess nationella säkerhet, är den inte skyldig att dela med sig av informationen. Under våra besök i medlemsstaterna framhöll företrädare för CSIRT-nätverket och EU-CyCLONe att informationsutbytet endast kan ske inom ramen för den nationella säkerhetslagstiftningen. Någon analys av medlemsstaternas nationella rättsliga ramar och deras inverkan på informationsutbytet har inte genomförts på EU-nivå.

- 43** År 2016 bestod CSIRT-nätverket av 28 nationella CSIRT-enheter, med två företrädare per medlemsstat. Bristen på informationsutbyte har varit ett återkommande problem, och i [kommissionens utvärdering](#) av NIS-direktivet konstaterades att "[m]edlemsstaterna delar inte systematiskt information med varandra", vilket särskilt påverkar cybersäkerhetsåtgärdernas ändamålsenlighet och graden av gemensam situationsmedvetenhet på EU-nivå. Inom ramen för NIS 2-direktivet har många medlemsstater inrättat sektorsspecifika CSIRT-enheter utöver sina nationella CSIRT-enheter, vilket har lett till att nätverket har vuxit avsevärt. Vid tidpunkten för granskningen bestod nätverket av 42 CSIRT-enheter och över 700 enskilda deltagare. Detta gör det ännu svårare att bygga upp förtroende, eftersom det är svårt att upprätthålla nära kontakter mellan alla medlemmar.
- 44** CSIRT-nätverket är medvetet om problemet med informationsutbytet och överväger olika åtgärder för att stärka förtroendet inom ett växande nätverk. Skapandet av mindre kluster av medlemsstater som bildar gränsöverskridande nav, vilket beskrivs i punkterna [63–75](#), är ett alternativ till ett EU-omfattande nätverk som kan bidra till att hantera denna utmaning.

Cyberlägescentralens avtalade tjänster överlappar delvis befintlig kapacitet och dess framtida funktion är oklar

- 45** I enlighet med NIS 2-direktivet och i fall där en potentiell eller pågående storskalig cybersäkerhetsincident har eller sannolikt kommer att ha en betydande inverkan, blir kommissionen medlem i EU-CyCLONe⁹. Denna nya roll, i kombination med utvecklingen av hotbilden, ledde till att kommissionen inrättade en arbetsgrupp för cybersamordning inom GD Kommunikationsnät, innehåll och teknik år 2022. I denna arbetsgrupp ingår en cyberlägescentral som ska hjälpa kommissionen att öka sin lägesuppfattning med målet att stödja dess institutionella ansvar för krishantering. Den ska även hjälpa GD Connect att ge råd på politisk nivå.
- 46** För att inrätta cybersäkerhetscentralen stöds kommissionen i stor utsträckning av externa tjänsteleverantörer med vilka [avtal ingicks](#) i december 2022 för nästan 18 miljoner euro under fyra år. Vi har granskat centralens inrättande, dess output samt kommissionens planer för dess framtida verksamhet.

⁹ Artikel 16.2 i [NIS 2-direktivet](#).

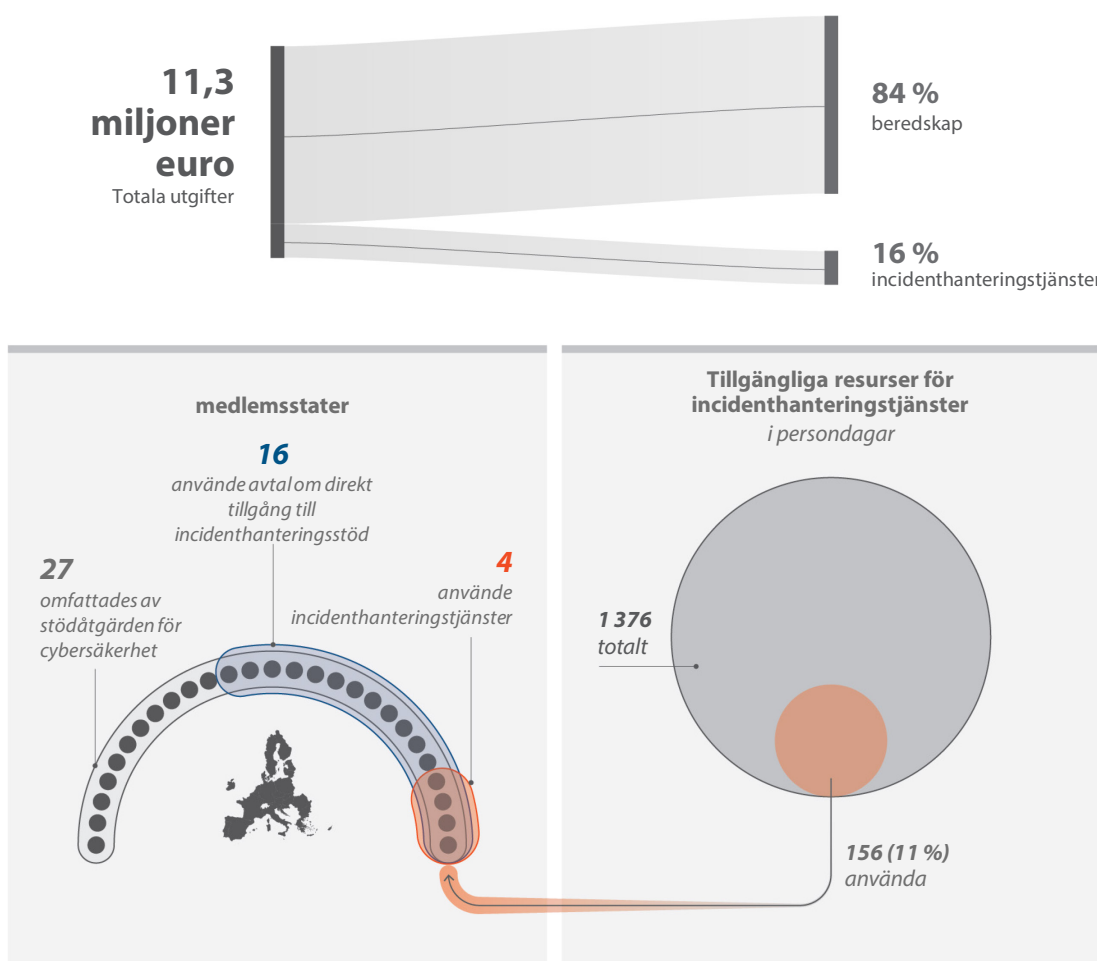
- 47** Som en del av de tjänster som tillhandahålls har entreprenörerna inrättat en resultattavla baserad på kommersiella underrättelseflöden om cyberhot för att lägga fram och dela information om hot. De tar även fram olika underrättelserapporter om cyberhot, däribland dagliga och veckovisa rapporter samt tematiska rapporter om länder eller ekonomiska sektorer. Den fysiska cyberlägescentralen, som består av ett rum utrustat med arbetsstationer som är fjärranslutna till den resultattavla som förvaltas av entreprenörerna, har inrättats i en av kommissionens byggnader. Vid tidpunkten för revisionen omfattade cyberlägescentralen ett litet antal anställda från kommissionen och fick stöd av många analytiker från entreprenörerna samt experter från Enisa.
- 48** Vi konstaterade att arbete som utförs av de externa tjänsteleverantörerna för cyberlägescentralen delvis överlappar med Enisas befintliga kapacitet. Enisa har permanent kapacitet för lägesuppfattning och hotövervakning. Byrån offentliggör regelbundet rapporter om cyberhot, däribland snabbrapporter om specifika incidenter samt veckorapporter som ger en översikt över hotbilden. Rapporterna bygger på underrättelser från öppna källor och liknar dem som tagits fram av entreprenörerna. Dessutom tar Enisa fram eller bidrar till översiktsrapporter på hög nivå riktade till beslutsfattare i krislägen, vilket också kan jämföras med det material som cyberlägescentralen tar fram.
- 49** Vidare bygger de uppgifter som cyberlägescentralen använder för att ta fram dessa rapporter på kommersiella informationsflöden om cyberhot och liknar de uppgifter som används av andra avdelningar inom kommissionen, såsom generaldirektoratet för digitala tjänster och CERT-EU. Vi anser att man vid inrättandet av cyberlägescentralen inte i tillräcklig utsträckning utnyttjat möjligheterna till rationalisering genom att använda redan tillgänglig information från kommissionen och Enisa.
- 50** Avtalet löper ut i december 2026, varefter entreprenörerna inte längre kommer att tillhandahålla tjänsterna för cyberlägescentralen. Dessa tjänster, som utgör större delen av centralen, omfattar tillhandahållande av de uppgifter som finns tillgängliga på resultattavlan och framtagning av hotrapporter. Resultattavlan kommer att överlämnas till kommissionen, men förlorar sitt mervärde om den inte kontinuerligt uppdateras med underrättelser om cyberhot.
- 51** Vid tidpunkten för revisionen hade kommissionen inga planer när det gäller stöd av externa tjänsteleverantörer för driften av cyberlägescentralen efter det att avtalet löpt ut. Vi anser att avsaknaden av en omfattande, detaljerad framtidsplan efter att avtalet löper ut utgör en risk för cyberlägescentralens verksamhet efter 2026.

EU:s cybersäkerhetsreserv gör det möjligt att snabbt införa tjänster för incidenthantering

- 52** Under 2022, direkt efter Rysslands militära angrepp mot Ukraina och med tanke på att storskaliga cyberattacker blivit vanligare, tillhandahöll kommissionen Enisa 15 miljoner euro i exceptionell finansiering för att testa [stödgärden för cybersäkerhet](#), som lanserades 2023. Under 2023 tillhandahöll kommissionen ytterligare finansiering (cirka 20 miljoner euro) för att förlänga programmet till slutet av 2026.
- 53** Kommissionen föreslog också [cybersolidaritetsakten](#), som antogs i december 2024, för att förbereda sig för storskaliga cybersäkerhetsincidenter. Genom akten inrättas en EU-cybersäkerhetsreserv som omfattar incidenthanteringstjänster från betrodda leverantörer. Verksamheten inleddes gradvis under 2025, med en budget på 36 miljoner euro för perioden 2025–2027.
- 54** Vi har granskat hur programmet för stödgärden för cybersäkerhet är organiserat, eftersom det utgör grunden för EU:s cybersäkerhetsreserv. Vi har också undersökt om de lärdomar som dragits sedan 2022 har beaktats vid utformningen av EU:s cybersäkerhetsreserv.
- 55** Enisa utformade stödgärden för cybersäkerhet som en mekanism för att tillhandahålla tjänster till stöd för medlemsstaternas beredskap och insatser vid storskaliga cybersäkerhetsincidenter eller cyberkriser. Alla tjänster har på förhand kontrakterats av Enisa, vilket innebär att tjänsteleverantörerna kan börja arbeta så snart medlemsstaterna kräver det. Detta beror också på Enisas organisation, som säkerställer att det alltid finns en tjänsteman i beredskap dygnet runt för att hantera medlemsstaternas begäranden.
- 56** Enisa valde att fördela den tillgängliga budgeten lika mellan medlemsstaterna. I praktiken inledde byrån ett öppet anbudsförfarande som var uppdelat i 27 delar, en för varje medlemsstat, för att välja ut upp till tre privata säkerhetsleverantörer som skulle tillhandahålla tjänster fram till slutet av 2026. Dessutom valde Enisa ut vissa leverantörer inom ramen för en alleuropeisk del för att tillhandahålla tjänster till stödberättigade länder utanför EU samt till EU:s institutioner, organ och byråer, eller för att stödja insatser vid gränsöverskridande incidenter.
- 57** Detta tillvägagångssätt gjorde det möjligt för Enisa att ta hänsyn till särskilda nationella krav, däribland språkkrav, nationella säkerhetsgodkännanden eller etablerad närvaro i medlemsstaterna. Eftersom leverantörerna inte valdes ut för att kunna tillhandahålla tjänster i hela EU är dock en stor nackdel med denna strategi att om en medlemsstat inte utnyttjar de förhandsavtalade tjänsterna, kan budgeterade medel för sådana tjänster för en specifik medlemsstat inte användas för att bistå en annan medlemsstat.

58 För stödåtgärden för cybersäkerhet kan medlemsländerna välja mellan beredskaps- eller insatstjänster, eller en kombination av båda. Medlemsstaterna valde i första hand att använda de tillgängliga medlen för att förbättra sin beredskap (84 % av utgifterna 2023). Medlemsstater som valde att satsa på ett avtal om direkt tillgång till incidenthanteringsstöd (dvs. ett i förväg fastställt avtal med en leverantör som säkerställer att medlemsstaten kan få tillgång till leverantörens tjänster när det krävs snabba insatser vid cyberincidenter) använde det sparsamt, såsom visas i [figur 4](#). I de tre medlemsstater som besöktes uttryckte myndigheterna sin uppskattning för Enisas genomförande av stödåtgärden för cybersäkerhet.

Figur 4 | Enisas stödåtgärd för cybersäkerhet fram till 2023



Källa: Revisionsrätten, på grundval av uppgifter från Enisa.

- 59** För perioden 2024–2026 har endast nio medlemsstater ansökt om ett avtal om direkt tillgång till incidenthanteringsstöd. Våra intervjuer med Enisa och myndigheter i tre medlemsstater har bekräftat att det finns en stark preferens för beredskapsverksamhet.
- 60** Även om EU-cybersäkerhetsreserven främst syftar till att stödja insatser och återhämtning vid större cybersäkerhetsincidenter kan tjänster som på förhand ställts till förfogande från EU-cybersäkerhetsreserven och som inte används för incidenthantering omvandlas till beredskapstjänster. Denna flexibla lösning kan förhindra att förbetalda tjänster förblir outnyttjade.
- 61** Vi anser att den modell som valts för EU-cybersäkerhetsreserven bygger på lärdomarna från programmet för stödåtgärden för cybersäkerhet. Uppgifterna om användningen av programmet för stödåtgärder för cybersäkerhet tyder dock på att EU:s cybersäkerhetsreserv främst kan komma att användas för beredskap och inte för insatser, vilket strider mot det syfte som anges i cybersolidaritetsakten.

Det europeiska varningssystemet för cybersäkerhet syftar till att förbättra förmågan att upptäcka hot, men är ännu inte i drift

- 62** Ett av de viktigaste målen för det europeiska systemet för cybersäkerhetsvarningar är att uppmuntra till meningsfullt informationsutbyte för att förbättra upptäckt, analys och hantering av cyberhot. Deltagandet i varningssystemet är frivilligt, men de medlemsstater som väljer att ansluta sig till ett gränsöverskridande cybernav måste åta sig att dela relevant information med de andra medlemmarna. Genom att samarbeta i kluster i en betrodd och säker miljö kan medlemsstaterna undvika vissa av de problem med informationsutbyte som anges i punkterna [32–45](#).
- 63** Vid tidpunkten för revisionen hade 13 medlemsstater valt att ansluta sig till det europeiska varningssystemet för cybersäkerhet, vilket innebar att två gränsöverskridande nav inrättades: ATHENA och ENSOC. Ett tredje gränsöverskridande cybernav, NBCC, hade tilldelats finansiering för sitt inrättande 2026, vilket innebar att totalt 20 länder (18 medlemsstater samt Island och Norge) blev medlemmar,¹⁰ vilket framgår av [figur 5](#).

¹⁰ Associerade länder utanför EU i enlighet med artikel 10.1 a i förordning (EU) 2021/694.

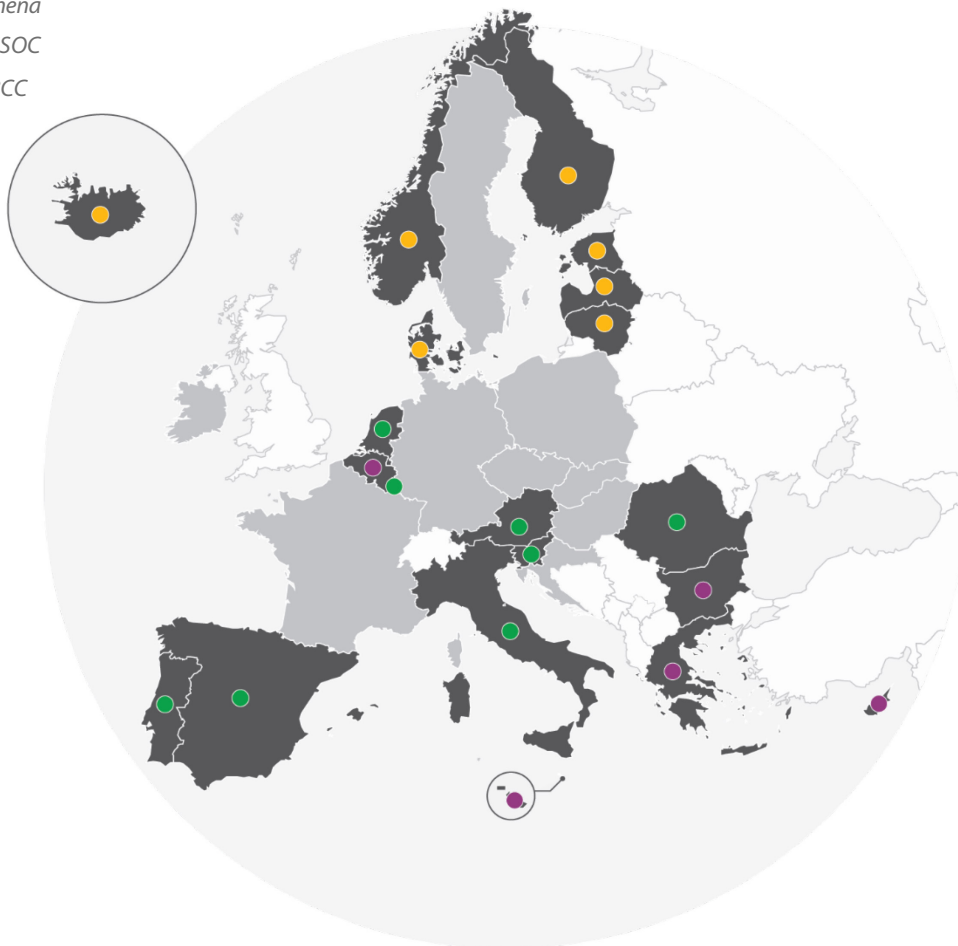
Figur 5 | Länder i det europeiska systemet för cybersäkerhetsvarningar

■ Länder i det europeiska systemet för cybersäkerhetsvarningar

● Athena

● ENSOC

● NBCC



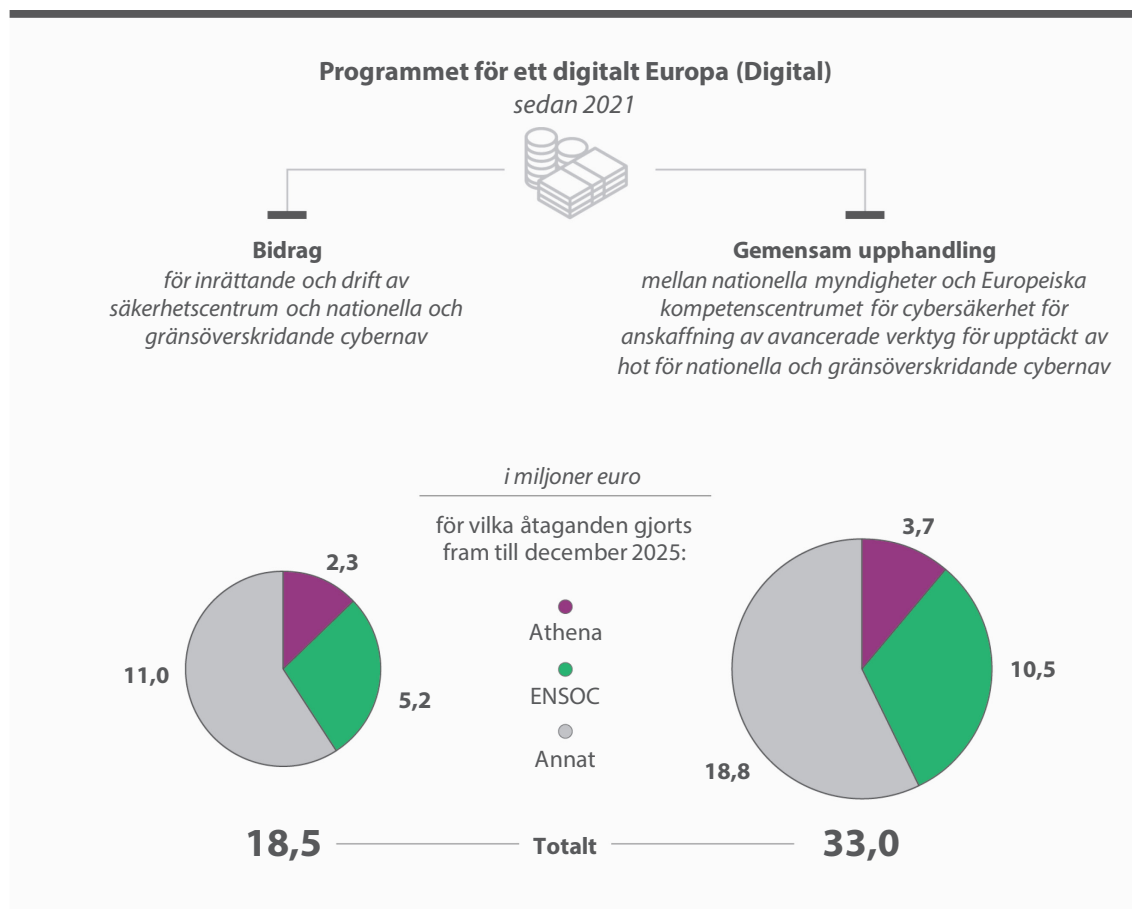
Källa: Revisionsrätten.

- 64** Vi bedömde hur de två första gränsöverskridande cybernaven har inrättats samt deras framsteg mot målen för det europeiska systemet för cybersäkerhetsvarningar. Vi undersökte också hur inrättandet av gränsöverskridande cybernav passar in i det bredare cybersäkerhetslandskapet och samverkar med befintliga nätverk och strukturer.

På grund av betydande förseningar i upphandlingen har ännu inte några konkreta resultat uppnåtts

- 65** Finansiering för att stödja inrättandet av nationella och gränsöverskridande cybernav har funnits tillgänglig genom Digital sedan 2021. Finansieringen sker genom ett komplext förfarande med två parallella spår: traditionella bidrag för att stödja inrättandet och driften av naven samt gemensam upphandling för att köpa in avancerade verktyg för upptäckt av hot, vilket framgår av [figur 6](#). Efter en ansökningsomgång i november 2022 inledde ATHENA och ENSOC sitt arbete i januari 2024.

Figur 6 | Finansiering från programmet för ett digitalt Europa till cybernav



Källa: Revisionsrätten, på grundval av uppgifter från Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning.

- 66** De selektiva upphandlingsförfarandena i två faser¹¹ anordnades av medlemmarna i ATHENA och ENSOC samt av GD Kommunikationsnät, innehåll och teknik (första fasen) och det nyligen inrättade europeiska kompetenscentrumet för cybersäkerhet (andra fasen). Tvåfasmetoden syftar till att begränsa spridningen av känslig information genom att endast de sökande som valts ut i den första fasen får tillgång till de detaljerade tekniska specifikationerna.
- 67** Den första fasen inleddes i maj 2024 för ENSOC och i juli 2024 för ATHENA. Intresserade företag hade en månad på sig att ansöka. De antagna sökandena fick dock besked först i april 2025, nästan ett år efter det att förfarandet inleddes.

¹¹ Anbudsinfordran för ENSOC och anbudsinfordran för ATHENA.

- 68** Dessutom kunde varken upphandlingsförfarandena för ENSOC eller för ATHENA gå vidare till den andra fasen vid den tidpunkten, eftersom navets medlemmar och Europeiska kompetenscentrumet för cybersäkerhet inte kunde förse de utvalda företagen med de tekniska specifikationer som krävdes för att de skulle kunna lämna in ett anbud, eftersom de fortfarande arbetade med att slutföra dem.
- 69** Den andra fasen av upphandlingsförfarandet inleddes först i augusti 2025 för vissa delar av ENSOC och planerades till början av 2026 för ATHENA. Vid tidpunkten för revisionen, 18 månader efter det att upphandlingsförfarandet inleddes, hade inget avtal undertecknats för någon av delarna. Vi anser att bristen på tillräcklig förberedelse och upphandlingsförfarandenas komplexitet förhindrade att de kunde slutföras i tid.
- 70** Vi konstaterade därför att de gränsöverskridande naven inte är på rätt väg för att uppnå sina mål. Utan verktyg för att upptäcka hot och dela information står deras verksamhet i på paus, och det europeiska systemet för cybersäkerhetsvarningar är ännu inte i drift, vilket fördröjer den ändamålsenliga utvecklingen av avancerade resurser för att upptäcka och förebygga cyberhot och cyberincidenter. Tilläggsavtal har undertecknats för att förlänga bidragsavtalets giltighetstid, i syfte att ta hänsyn till de förseningar som hittills uppstått i upphandlingsförfarandena (15 månader för ATHENA och 18 månader för ENSOC).

Gränsöverskridande cybernav skapar ytterligare kommunikationskanaler som ökar komplexiteten ännu mer

- 71** En av de viktigaste uppgifterna för de gränsöverskridande cybernaven är att dela relevant information för att förbättra upptäckten och hanteringen av hot. Detta innebär information om cyberhot, sårbarheter, angreppsindikatorer och fientliga aktörer. De gränsöverskridande cybernavens uppgifter överlappar delvis de uppgifter som utförs av de nationella CSIRT-enheterna och CSIRT-nätverket, särskilt när det gäller informationsutbyte om cyberhot och sårbarheter. Det finns ingen tydlig gräns mellan de olika rollerna för gränsöverskridande cybernav och CSIRT-enheter. Enligt cyberplanen från 2025 (punkt **30**) är de gränsöverskridande cybernaven avsedda att fungera både på teknisk nivå (såsom de nationella CSIRT-enheterna och CSIRT-nätverket) och operativ nivå (såsom EU-CyCLONE).

- 72** Enligt cybersolidaritetsakten ska de gränsöverskridande cybernaven ingå samarbetsavtal med varandra för att underlätta informationsutbyte. Enisa bör ha utfärdat riktlinjer för interoperabilitet mellan gränsöverskridande cybernav senast i februari 2026, såsom föreskrivs i cybersolidaritetsakten. Under tiden beviljade kompetenscentrumet för cybersäkerhet i december 2025 ett bidrag till ett konsortium (som bland annat bestod av vissa medlemmar i ENSOC och ATHENA) för att utforma en teknisk ram för interoperabilitet mellan gränsöverskridande cybernav. Riktlinjerna och ramen kommer dock inte att vara färdiga förrän de gränsöverskridande cybernaven har tagits i drift. Som vi påpekade i vårt yttrande från 2023 om förslaget till cybersolidaritetsakt¹² finns det en risk för att det, om man inte snabbt når en överenskommelse, utvecklas system som inte är kompatibla med varandra, vilket leder till ökade kostnader.
- 73** Gränsöverskridande cybernav måste också utan onödigt dröjsmål utbyta relevant information om storskaliga cybersäkerhetsincidenter med EU-CyCLONE och CSIRT-nätverket. På medlemsstatsnivå skapar inrättandet av nationella cybernav och deltagandet i gränsöverskridande cybernav ytterligare nivåer av kommunikation. Samordningen med stater utanför EU¹³, som inte ingår i CSIRT-nätverket eller EU-CyCLONE, ökar också komplexiteten.
- 74** Tydliga samarbetsavtal är nödvändiga för att man ska kunna enas om en gemensam taxonomi och om hur information ska utbytas och för att säkerställa interoperabilitet. Lärdomarna från CSIRT-nätverket visar att detta är en stor utmaning. Vi konstaterade att det vid tidpunkten för revisionen inte hade ingåtts några överenskommelser om rutiner för samarbete och informationsutbyte. Vi anser att inrättandet av nationella och gränsöverskridande cybernav skulle kunna främja ett effektivare informationsutbyte. Det kommer dock att bli en utmaning att integrera de gränsöverskridande naven i det redan komplexa cybersäkerhetslandskapet, och detta kräver ytterligare kommunikationskanaler och samarbetsarrangemang.

¹² Yttrande 02/2023 över förslaget till Europaparlamentets och rådets förordning om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter, punkt 26.

¹³ Island och Norge.

EU-finansierade projekt inom Digital syftar till att stärka cybersäkerheten, men står inför utmaningar när det gäller genomförande och rapportering

Förseningar i inrättandet hindrade kompetensgemenskapen för cybersäkerhet från att utforma Digital i enlighet med sina behov

- 75** För att hantera cybersäkerhetskompontenten i Digital föreslog kommissionen 2018 att Europeiska kompetenscentrumet för cybersäkerhet skulle inrättas. Enligt förordningen om Europeiska kompetenscentrumet för cybersäkerhet skulle kompetenscentrumet få stöd av ett nätverk av 29 nationella samordningscentrum, en för varje medlemsstat samt Island och Norge. Det uppmanades också till att upprätta kompetensgemenskapen för cybersäkerhet (gemenskapen), som skulle bestå av företrädare näringslivet, akademiska organisationer och forskningsorganisationer samt andra relevanta organisationer i det civila samhället.
- 76** Upp till 20 medlemmar från gemenskapen skulle utses till den strategiska rådgivande gruppen, som är en av de tre komponenterna i strukturen för kompetenscentrumet för cybersäkerhet. En av den strategiska rådgivande gruppens viktigaste uppgifter är att anordna offentliga samråd som ska ligga till grund för dagordningen för kompetenscentrumet för cybersäkerhet och arbetsprogrammen för Digital.
- 77** Vi har bedömt om Digital och dess arbetsprogram har antagits på grundval av en gedigen behovsanalys samt hur centrumet, nätverket av nationella samordningscentrum, gemenskapen och den strategiska rådgivande gruppen har kunnat bidra till arbetsprogrammen. I praktiken har centrumet, nätverket av nationella samordningscentrum, gemenskapen och den strategiska rådgivande gruppen inrättats gradvis under flera år (se [figur 7](#)).



- 78** Eftersom Europeiska kompetenscentrumet för cybersäkerhet inte blev verksamt fullt ut förrän i september 2024 antog kommissionen, på kompetenscentrumets vägnar, arbetsprogrammen för perioderna 2021–2022 och 2023–2024. Gemenskapen kunde inte bidra till de två arbetsprogram som antogs av kommissionen.
- 79** Samtidigt började medlemsstaterna inrätta sina nationella samordningscentrum, som fungerar som kontaktpunkter på nationell nivå för gemenskapen. Deras inrättande och verksamhet har samfinansierats av Digital, med över 90 miljoner euro i EU-finansiering som hade beviljats vid tidpunkten för revisionen, inklusive cirka 44 miljoner euro som kommer att fördelas ytterligare genom ekonomiskt stöd till tredje parter. Ytterligare 38 miljoner euro har avsatts i budgeten fram till 2027 för att stödja nationella samordningscentrum.
- 80** Vi konstaterade att gemenskapen i december 2025, fyra år efter att kompetenscentrumet och nätverket av nationella samordningscentrum inrättats, ännu inte hade bildats och att den strategiska rådgivande gruppen ännu inte hade utsetts. Den 14 mars 2025 antog kompetenscentrumet Digital's senaste arbetsprogram för cybersäkerhet, som omfattar perioden 2025–2027. Kompetenscentrumet utarbetade och antog sitt arbetsprogram efter omfattande samråd med medlemsstaterna och nätverket av nationella samordningscentrum, men kunde inte få synpunkter och råd från gemenskapen eller den vetenskapliga rådgivande gruppen. Detta strider mot bestämmelserna i inrättandeförordningen och vi anser att detta är en förlorad möjlighet.
- 81** Digital löper ut 2027, och om dess mandat inte förlängs förväntas kompetenscentrumet avvecklas under 2029. Därför kan stödet från nätverket av nationella samordningscentrum, gemenskapen och den strategiska rådgivande gruppen, när den väl har inrättats, endast vara relevant under en kort period.

EU-finansierade projekt har relevanta mål, men många stöter på operativa problem

82 Vi valde ut elva projekt som var relevanta för upptäckt och hantering av cybersäkerhetsincidenter och som finansierades inom ramen för Digital under perioden 2022–2025 (se [figur 5](#) i [bilagorna I och III](#)). Vi bedömde om

- projekten hade mål som överensstämde med de förväntade utfallen som angavs i ansökningsomgångarna och med målen för Digital som helhet,
- projekten hittills har uppnått output och resultat som planerats,
- projektens output har levererats i tid.

Vi presenterar resultatet av denna bedömning i [bilaga IV](#).

Vissa projekt visar tidiga resultat, men många står inför operativa utmaningar och drabbas av förseningar

83 Vi konstaterade att alla projekt har mål som bidrar till att uppnå cybersäkerhetsmålen för Digital¹⁴ och att de uppfyller de flesta målen i ansökningsomgångarna¹⁵.

84 Av de elva projekten i vårt urval befann sig två i ett tidigt genomförandestadium, och vi kunde därför inte dra några slutsatser om deras resultat. Av de återstående bedömde vi fyra som tillfredsställande när det gäller uppnåendet av output och resultat som planerats. Vi ansåg att två projekt uppvisade vissa brister och bedömde tre som otillfredsställande (se [bilaga IV](#)).

85 Digital har som uttryckligt mål att höja cybersäkerhetsnivån hos små och medelstora företag (SMF). I det avseendet erbjuder flera projekt konkreta lösningar för små och medelstora företag (se [ruta 2](#)).

¹⁴ Artikel 6 i [förordning \(EU\) 2021/694](#) om inrättande av programmet för ett digitalt Europa.

¹⁵ Ansökningsomgångar: [Uppbyggnad av kapacitet hos säkerhetscentrum, utbyggnad av nätverket av nationella samordningscentrum med medlemsstaterna, beredskapsstöd och ömsesidigt bistånd samt nya tillämpningar av AI och annan möjliggörande teknik för säkerhetscentrum.](#)

Ruta 2

Exempel på projekt som ger konkreta resultat för små och medelstora företag

Projektet **GR-SME-SOC** (projekt 6 i **bilaga III**) syftar till att tillhandahålla cybersäkerhetsverktyg och cybersäkerhetstjänster till små och medelstora företag i Grekland genom att inrätta ett säkerhetscentrum som är anpassat till deras behov. Projektet inleddes i januari 2024 och genomförs av ett konsortium bestående av fem grekiska organisationer. Planen är att kostnadsfritt erbjuda cybersäkerhetstjänster till 120 små och medelstora företag under ett år, varefter tjänsterna kommer att bli kommersiellt tillgängliga. Projektet erbjuder avancerade tjänster för små och medelstora företag såsom realtidsövervakning, AI-driven hotspårning och smidig incidenthantering.

Genom projektet **NCC-IE** (projekt 3 i **bilaga III**) tillhandahöll projektsamordnaren omkring 1,8 miljoner euro i bidrag till över 50 irländska små och medelstora företag för att förbättra deras cybersäkerhet. Bidragssystemet riktade sig till företag med mellan 2 och cirka 200 anställda, däribland familjeföretag, nystartade företag och globala exportörer inom olika sektorer. Bidragen var avsedda enbart för företag som tidigare genomgått en cybersäkerhetsgranskning som genomförts av statliga organet Enterprise Ireland. Bidraget täckte 80 % av kostnaderna (upp till 60 000 euro) för att genomföra rekommendationerna från granskningen.

Källa: Revisionsrätten.

- 86** Många projekt i vårt urval har svårt att hålla tidsfristerna eller står inför operativa utmaningar (se **bilaga IV**). Vi konstaterade att fyra projekt är kraftigt försenade. Detta omfattar ENSOC och ATHENA, i enlighet med vad som beskrivs i punkterna **66–71**. Vi ger andra exempel i **ruta 3**.

Ruta 3

Exempel på projekt som står inför operativa utmaningar och drabbas av förseningar

I Irland är den lokala förvaltningsmyndigheten den enda mottagaren av bidraget för projektet **ILG-SOC** (projekt 8 i **bilaga III**). Projektets mål är att inrätta ett centralt säkerhetscentrum för 31 lokala myndigheter som ska använda avancerade verktyg för att upptäcka och hantera hot. Projektet inleddes i oktober 2023 och löper över tre år. Halvtidsöversynen ledde till att alla eftersträlvade resultat runderkändes. Projektet omfattar flera upphandlingsförfaranden som har misslyckats eller försenats. Projektets löptid kommer att förlängas (utan ytterligare finansiering), vilket kan ge projektet tillräckligt med tid för att avslutas på ett framgångsrikt sätt.

I Grekland syftar projektet **EL-SOC** (projekt 5 i **bilaga III**) till att inrätta ett konsoliderat säkerhetscentrum på nationell nivå, som ska samla information från sektorsspecifika säkerhetscentrum. Detta ska ge en heltäckande översikt över cybersäkerhetsläget i realtid. Projektet pågår från januari 2024 till december 2026. Den planerade upphandlingen av maskinvara och tjänster försenades på grund av problem med att färdigställa och offentliggöra de tekniska specifikationerna för anbudsinfordran. Som orsaker till förseningen nämnde projektsamordnaren även problem med att säkra nationell medfinansiering samt bristen på personal inom upphandlingsområdet.

Källa: Revisionsrätten.

- 87** Två andra projekt i vårt urval är måttligt försenade. Tre projekt har levererat sin output i tid. Slutligen befinner sig två projekt i ett tidigt genomförandestadium och vi kan därför inte dra någon slutsats.

Säkerhetsbegränsningar har lett till operativa utmaningar, och det finns betydande risker när kontroller utförs av stödmottagare

- 88** I förordningen om programmet för ett digitalt Europa (Digital) anges att finansiering av cybersäkerhet av säkerhetsskäl kan begränsas till entiteter som är etablerade i EU och som kontrolleras av medlemsstater eller EU-medborgare. Syftet med denna begränsning är att minska risken för inblandning eller påverkan från stater utanför EU och förhindra att känslig säkerhetsinformation delas med myndigheter utanför EU.
- 89** EU:s ägande- och kontrollskyldighet gäller inte bara för bidragsmottagare utan även för deras underleverantörer och alla mottagare av ekonomiskt stöd till tredje parter. Med undantag för den senare kategorin (se punkterna [93–97](#)) gör den centrala valideringstjänsten vid [Europeiska genomförandeorganet för forskning](#) bedömningen. Det slutliga beslutet om rätten att delta i begränsade ansökningsomgångar fattas dock fortfarande av den beviljande myndigheten, dvs. GD Kommunikationsnät, innehåll och teknik eller Europeiska kompetenscentrumet för cybersäkerhet.
- 90** Under vårt revisionsarbete nämnde stödmottagarna upprepade gånger de praktiska utmaningar som bedömningar av ägar- och kontrollförhållandena innebär. Att bedöma EU:s ägar- och kontrollförhållanden kan vara en komplex och utdragen process. Det kräver en analys av varje organisations fullständiga ägarstruktur och kontrollkedja, inklusive alla ägarnivåer ända fram till de slutliga ägarna. Den centrala valideringstjänsten kräver att varje entitet lämnar in omfattande [dokumentation](#) som styrker dess ägarstruktur och särskilda rättigheter, bolagsstyrning samt eventuella kommersiella, finansiella eller andra kopplingar som medför kontroll.
- 91** I tre EU-finansierade projekt i vårt urval uteslöts minst en av ett konsortiums stödmottagare i efterhand, eftersom man bedömde att denne ägdes eller kontrollerades av aktörer utanför EU. Att vissa konsortiemedlemmar uteslutits visar att begreppet alla deltagare i Digital inte fullt ut förstår vad som avses med EU:s ägar- och kontrollförhållanden. På grundval av uppgifter från den centrala valideringstjänsten har totalt 7 % av alla sökande eller underleverantörer på området för cybersäkerhet inom ramen för Digital underkänts i bedömningen under perioden 2022–2025. Icke stödberättigade deltagares inlämning av ansökningar till en ansökningsomgång orsakar förseningar, såsom visas i [ruta 4](#).

Ruta 4

Exempel på ett fall där stödmottagare uteslöts efter att ha underkänts i säkerhetskontroller

Två av konsortiemedlemmarna i projektet **NG-SOC** (projekt 7 i, *[bilaga III](#)*) underkändes i bedömningen av ägar- och kontrollförhållanden. Resultatet tillkännagavs cirka en månad innan tidsfristen för undertecknande av bidragsavtalet löpte ut.

Projektsamordnaren var tvungen att gå med på att ta över det arbete som hade tilldelats de två uteslutna medlemmarna, eftersom det inte fanns tid att hitta en ny partner. En av de uteslutna medlemmarna var verksam inom just den sektor där den utvecklade lösningen skulle testas. En betydande del av projektet, som handlade om att testa lösningarna i praktiken, kunde därför inte genomföras som planerat. Denna situation åtgärdades senare genom att bidragsavtalet ändrades så att det även omfattade nya medlemmar.

Källa: Revisionsrätten.

- 92** Två av de projekt som vi granskade (NCC-IE och CYberSynchrony) ger ekonomiskt stöd till tredje parter. Denna finansieringsmekanism gör det möjligt för stödmottagare att använda en del av bidragsfinansieringen för att finansiera andra entiteter genom öppna ansökningsomgångar. Ekonomiskt stöd till tredje parter kan underlätta tillgången till EU-finansiering. I detta fall är det stödmottagarna som bär det fulla ansvaret för att genomföra bedömningarna av ägar- och kontrollförhållanden, och den centrala valideringstjänsten är inte inblandad.
- 93** År 2021 publicerade kommissionen en allmän offentlig vägledning för sökande för begränsade ansökningsomgångar, vilken uppdaterades 2026. Även om ekonomiskt stöd till tredje parter har funnits sedan 2021 för ansökningsomgångar inom ramen för Digital har varken kommissionen eller Europeiska kompetenscentrumet för cybersäkerhet tillhandahållit stödmottagarna någon detaljerad metod för hur de ska utföra bedömningar av ägar- och kontrollförhållanden vid bedömningen av de tredje parter till vilka de ger ekonomiskt stöd. I juli 2025 offentliggjorde Europeiska kompetenscentrumet för cybersäkerhet icke-obligatorisk vägledning som förser nätverket av nationella samordningscentrum med en strukturerad metod för hantering av bedömningar av ägar- och kontrollförhållanden. Vägledningsdokumentet innehåller allmänna principer och åtgärder som kan vidtas. I vägledningen anges dock inte hur kontrollerna ska genomföras, vilket innebär att stödmottagarna själva ansvarar för att utforma sin egen metod.

- 94** Vi har konstaterat att Europeiska kompetenscentrumet för cybersäkerhet varken granskar den metod som stödmottagarna tillämpar eller genomför stickprovskontroller för att säkerställa att metoden är tillräckligt tillförlitlig och att de utvalda mottagarna av ekonomiskt stöd verkligen ägs och kontrolleras av EU.
- 95** I vår [årsrapport för 2024](#) konstaterade vi att de stödmottagare som av kommissionen anförtrotts förvaltningen av ekonomiskt stöd till tredje parter (på forskningsområdet) inte var skyldiga att visa att deras kontroller för att säkerställa EU-utgifternas korrekthet var ändamålsenliga. På samma sätt har kompetenscentrumet inte gjort någon bedömning av mottagarnas administrativa och tekniska kapacitet för att hantera bedömningarna av ägar- och kontrollförhållanden på ett korrekt sätt. Såsom beskrivs i punkt [91](#) kan denna bedömning vara komplex och utförs på EU-nivå av en särskild avdelning med specialiserad sakkunskap.
- 96** I detta sammanhang anser vi att det finns en betydande risk för att stödmottagarna, som ansvarar för att genomföra bedömningarna av ägar- och kontrollförhållanden, inte har tillräcklig kapacitet för att utföra dem på ett korrekt sätt. Med tanke på vilken typ av verksamhet som finansieras kan denna brist innebära att känslig infrastruktur, operativa uppgifter och säkerhetskritisk teknik utsätts för risker.

Prestationsramarna för de flesta EU-finansierade projekten är otillräckliga, och de cybersäkerhetsrelaterade prestationsuppgifterna för Digital är inte korrekta

Prestationsramarna för de flesta EU-finansierade projekten är otillräckliga

- 97** Stödmottagare som förvaltar EU-finansierade projekt måste rapportera om sina framsteg och resultat till Europeiska kompetenscentrumet för cybersäkerhet med hjälp av delmål, eftersträvar resultat och indikatorer, såsom visas i [figur 8](#). Vi har bedömt om de delmål och resultat som fastställts för varje projekt på ett tillfredsställande sätt möjliggör projektövervakning. Vi har också granskat om deras prestationsindikatorer är relevanta och mätbara samt om de har ett utgångsvärde och ett mål.

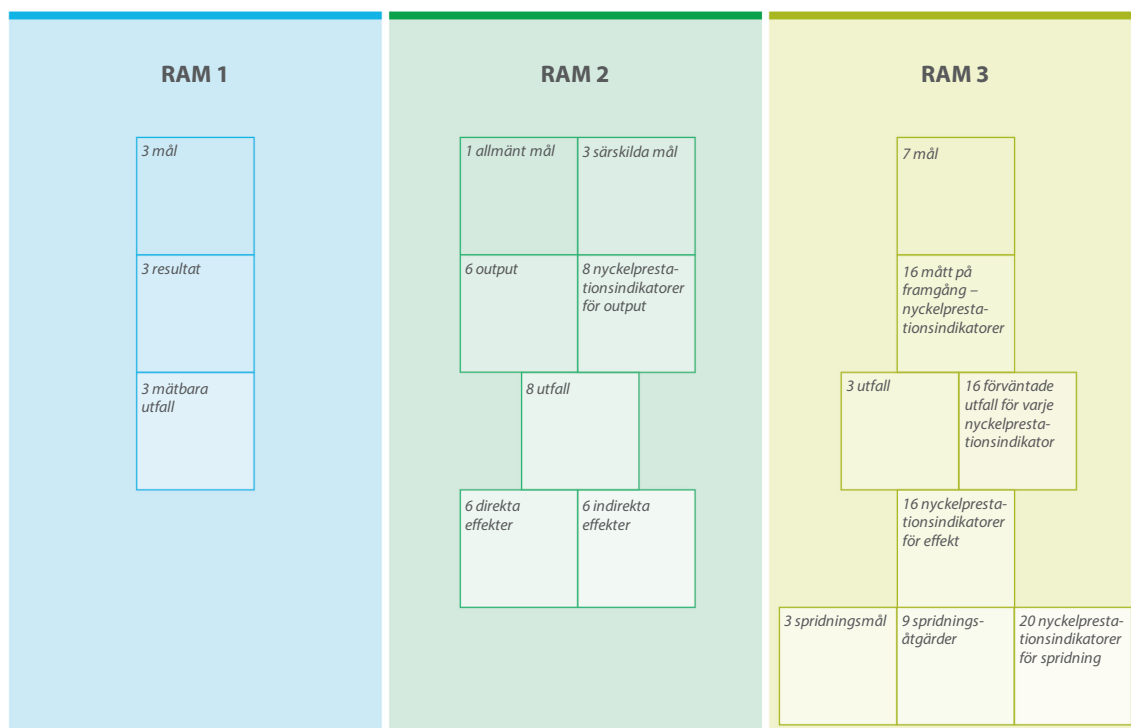
Figur 8 | Delmål, resultat och prestationsindikatorer i Digital-projekt

			
	Delmål	Eftersträvar resultat	Prestationsindikatorer
Vad de är	kontrollpunkter under hela projektet vilka underlättar kartläggningen av framstegen	projektoutput som inlämnas för att visa framsteg	används för att mäta resultat
Hur man fastställer dem	endast kopplade till större output (i begränsat antal)	endast större output (högst 10–15 per projekt)	specifika, mätbara, uppnåbara, relevanta och tidsbundna
Exempel	"Lansering av plattformens pilotfas"	"Handbok för plattformsanvändare"	"Minskning av incidenthanteringstiden med 30 %"
	En strukturerad metod som ingår i det webbaserade bidragsförvaltningssystemet		Ostrukturerad metod

Källa: Revisionsrätten, på grundval av [formuläret för bidragsansökan](#).

- 98** I sitt projektförslag måste stödmottagarna fastställa en rad delmål och eftersträvade resultat enligt en strukturerad metod som anges i instruktionerna till de sökande. Alla delmål och eftersträvade resultat förtecknas i onlinesystemet för bidragsförvaltning för att underlätta uppföljningen av dem. Europeiska kompetenscentrumet för cybersäkerhet granskar vanligtvis varje projekt två gånger: en gång halvvägs in i projektet och en gång efter att det har slutförts. Under dessa granskningar kontrollerar externa experter att delmål och eftersträvade resultat har uppnåtts, och Europeiska kompetenscentrumet för cybersäkerhet godkänner dem. Milstolpar och delmål är därför avgörande för projektövervakningen och bör fastställas på ett korrekt sätt.
- 99** Vi konstaterade att nästan inget av projekten i vårt urval följde instruktionerna om antalet delmål och eftersträvade resultat: antalet delmål per projekt varierar mellan 8 och 39, medan antalet eftersträvade resultat varierar mellan 8 och 45. Många av delmålen och de eftersträvade resultaten följer inte riktlinjerna för hur de ska utformas och är därför inte användbara för att följa upp framstegen (till exempel "möte för att inleda utarbetandet av en ansökningsomgång för forskningsbidrag" eller "protokoll från formellt projektmöte"). För tre projekt hade utvärderingskommittén fastställt dessa problem redan innan bidragsavtalet undertecknades. I två fall föreslog stödmottagarna endast mindre ändringar (t.ex. avseende förfallodatum) utan att ta itu med de centrala frågorna, medan den tredje inte gjorde några ändringar alls. För sex andra projekt i vårt urval visar vår analys att delmålen eller de eftersträvade resultaten inte överensstämmer med instruktionerna och inte alltid är tillräckliga. Vi anser att det blir svårt att följa upp framstegen om de eftersträvade resultaten eller delmålen är dåligt definierade eller om det finns för många av dem.
- 100** Till skillnad från delmål och resultat följer prestationsindikatorerna inte någon strukturerad metod och sammanställs inte i en tabell i bidragsförvaltningssystemet, utan återfinns i stället i olika delar av ansökan. Denna metod har lett till att stödmottagarna har lagt fram ett stort antal förslag till prestationsramar. Vissa har endast fastställt projektmål kopplade till prestationsindikatorer, medan andra har utarbetat betydligt mer komplexa prestationsramar. Vi ger några exempel i [figur 9](#) nedan.

Figur 9 | Exempel på de olika prestationsramarna som utformats för projekten



Källa: Revisionsrätten.

101 Vår analys visar att många av de prestationsindikatorer som används i projekten varken är relevanta eller mätbara, och att de saknar mål eller utgångsvärde (se [ruta 5](#)). Dessutom har man i sju projekt definierat 20 eller fler indikatorer, varav 52 för ett projekt. Vi presenterar resultatet av denna bedömning i [bilaga IV](#).

Ruta 5

Exempel på otillräckliga prestationsindikatorer

Ej mätbart:

- "Angreppsindikatorn och andra tillhandahållna tjänster stärker de små och medelstora företagens cybersäkerhetskapacitet"
- "Tillhandahållande av verktyg och metoder för incidenthantering möjliggör integration med kommunikationskanalerna för EU-CyCLONe"

Inget utgångsvärde eller mål anges:

- "En förbättring med minst 20 % av personalens beredskap"
- "En minskning med minst 20 % av den arbetsinsats som krävs för att anpassa sig till och följa relevanta EU-initiativ för cybersäkerhet"

Ej prestationsrelaterat:

- "Slutrapport om projektet i slutet av finansieringsfasen"
- "Antal deltagare som kommer att delta i alla utbildningstillfällen"

Källa: Revisionsrätten, baserat på projektdokumentation.

102 Sammantaget anser vi att det stora antalet olika prestationsramar, den bristfälliga utformningen av indikatorerna och det alltför stora antalet indikatorer väsentligt försvårar prestationsövervakningen. Det är därför inte möjligt att bedöma projektets prestationer på ett korrekt sätt. Detta kompliceras ytterligare av att rapporteringsmallen inte innehåller något särskilt avsnitt om prestationsindikatorerna för projekten, vilket har lett till att de flesta projekten i vårt urval inte rapporterat om dessa.

Prestationsuppgifterna för cybersäkerhetskomponenten av Digital är inte korrekta

- 103** För att övervaka resultaten av Digital innehåller förordningen programindikatorer som alla projekt måste rapportera om, såsom beskrivs i [ruta 6](#).

Ruta 6

Digitala cybersäkerhetsindikatorer

- 1.a Antal cybersäkerhetsinfrastrukturer eller cybersäkerhetsverktyg eller båda som upphandlas gemensamt, inbegripet i samband med det europeiska systemet för cybersäkerhetsvarningar.
- 1.b Antal cybersäkerhetsinfrastrukturer eller cybersäkerhetsverktyg eller båda som införs.
2. Antal användare och användargrupper som får tillgång till europeiska cybersäkerhetssystem.
3. Antal åtgärder som stöder beredskap för och hantering av cybersäkerhetsincidenter inom ramen för cybernödmekanismen.

Källa: Bilaga II till [förordning \(EU\) 2021/694 om inrättande av programmet för ett digitalt Europa](#); övervaknings- och utvärderingsramen för programmet för ett digitalt Europa ([SWD\(2024\) 37](#)).

- 104** Vi undersökte om projekten i vårt urval hade rapporterat om dessa indikatorer och granskade hur Europeiska kompetenscentrumet för cybersäkerhet samlar in och kontrollerar dessa uppgifter.
- 105** Alla projekt uppmanas att rapportera om indikatorerna för programmet för ett digitalt Europa före halvtidsöversynen och den slutliga översynen i bidragsförvaltningssystemet. Vi konstaterade att av de sju projekt som vid tidpunkten för vår granskning hade nått halvvägs i sin tidsplan och som därför borde ha rapporterat om dessa indikatorer, var det endast tre som hade gjort detta. Av dessa tre hade två inte lämnat korrekta uppgifter: den ena hade rapporterat om fel indikator, medan den andra hade angett målvärden i stället för uppnådda resultat.

106 Varje år rapporterar kommissionen om dessa indikatorer i sina [resultatförklaringar för programmet](#). Detta gör det möjligt för berörda parter att bedöma om programmet uppfyller sina mål. Enligt resultatrapporterna för programmet 2024 ligger Digitala indikatorer för cybersäkerhet i linje med målen. Europeiska kompetenscentrumet för cybersäkerhet har förklarat för oss att man använde en rad enkäter som skickades ut till projektstödmottagarna för att sammanställa dessa indikatorer, i stället för att basera dem på bidragsförvaltningssystemet. Vi har granskat de uppdelade uppgifterna från Europeiska kompetenscentrumet för cybersäkerhet och funnit ett flertal brister i hur uppgifterna samlats in och i deras övergripande kvalitet. Vi har konstaterat att de insamlade uppgifterna inte stämmer överens med de värden som anges i resultatförklaringen för programmet, varför det är oklart hur de rapporterade värdena har beräknats. Vi har inte funnit några belegg för att Europeiska kompetenscentrumet för cybersäkerhet har kontrollerat riktigheten i de rapporterade uppgifterna. Utifrån våra kontroller av projekten i vårt urval, där de flesta uppgifterna saknas eller är felaktiga, anser vi att de rapporterade uppgifterna inte på ett korrekt sätt speglar de uppnådda resultaten.

Denna rapport antogs av revisionsrättens avdelning III, med ledamoten George-Marius Hyzler som ordförande, vid dess sammanträde i Luxemburg den 16 juni 2026.

För revisionsrätten

Tony Murphy
Ordförande

Bilagor

Bilaga I – Om revisionen

- 01** cybersäkerhet: "all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra personer som berörs av cyberhot"¹. cyberhot: "en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare av dessa system och andra personer"². Cybersäkerhet kräver ett helhetsperspektiv som består av en rad sammanlänkade verksamheter för att förebygga, upptäcka, hantera och återhämta sig från cyberhot, vilket illustreras i *figur 1* nedan.

¹ Förordning (EU) 2019/881 (cybersäkerhetsakten).

² Artikel 2 i cybersäkerhetsakten.

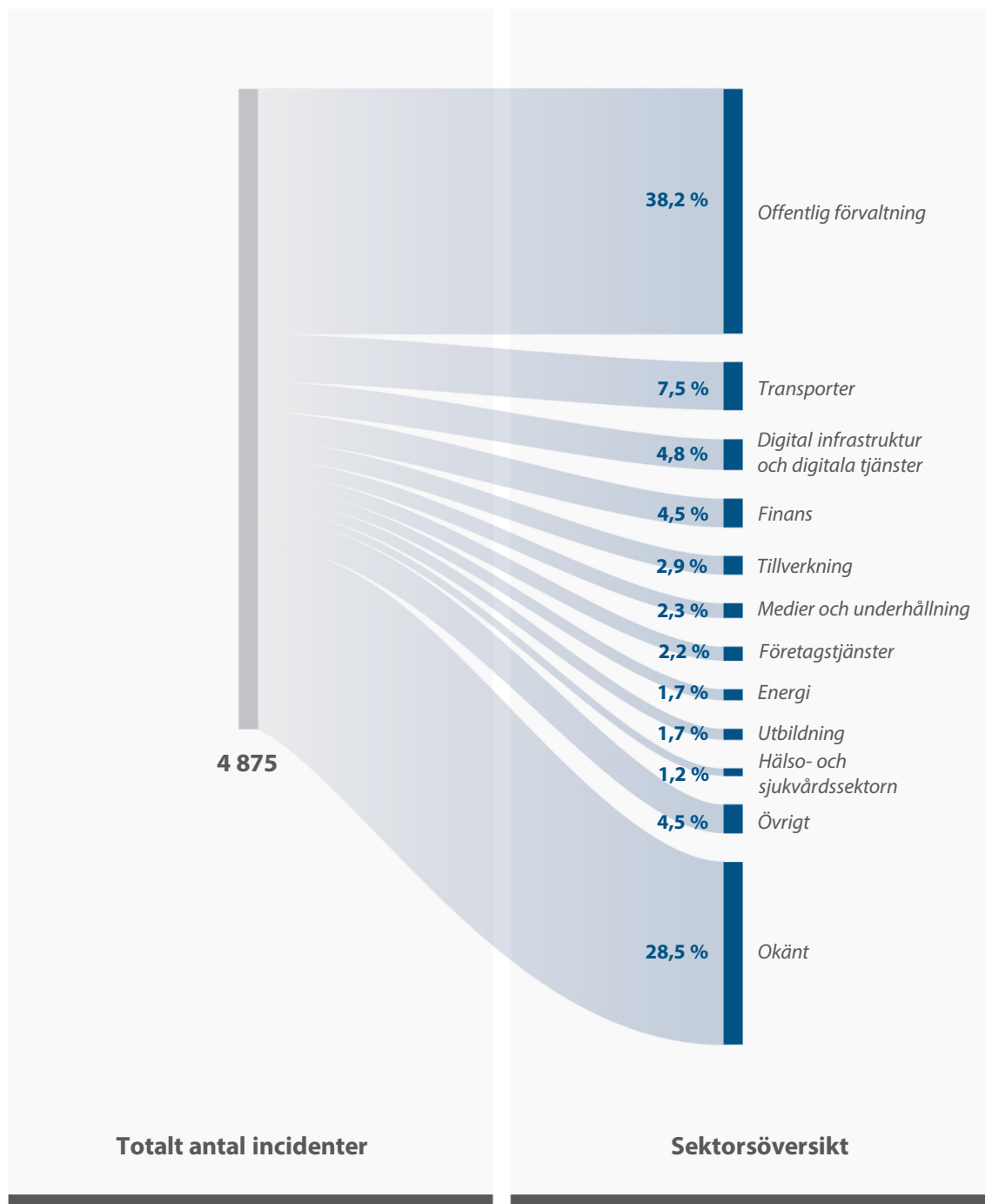
Figur 1 | Exempel på verksamheter som rör cybersäkerhet

Förebyggande 	Minska risken för cybersäkerhetsincidenter och minimera deras potentiella effekter <i>Exempel: antivirusprogram, brandväggar, kryptering, tvåfaktorsautentisering, hantering av programvaruuppdateringar, utbildning i säkerhetsmedvetenhet för personal</i>
Upptäckt 	Upptäckt av skadlig verksamhet <i>Exempel: nätverksövervakning, lägesuppfattning</i>
Insatser 	Hantering och minskning av effekterna av en cybersäkerhetsincident genom att begränsa hotet och förhindra ytterligare skador <i>Exempel: undanröjande av hot, inneslutning med hjälp av isolerade servrar, avaktivering av angripna konton och återställning av lösenord</i>
Återhämtning 	Återställande av berörda system, data och tjänster till en säker och driftsduglig nivå <i>Exempel: återinstallation av operativsystem på berörda servrar, återställande av data från säkerhetskopior, dragande av lärdomar, uppdatering av policyer</i>

Källa: Revisionsrätten, på grundval av skäl 78 i direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå (NIS 2-direktivet).

02 Europeiska unionens cybersäkerhetsbyrå (Enisa) anser att hotnivån när det gäller cybersäkerhet är betydande, men noterar samtidigt att hotbilden när det gäller cybersäkerhet har blivit och fortsätter att vara betydligt mer komplex³. Dessa hot understryker den avgörande betydelsen av cybersäkerhet i allt mer digitala ekonomier och samhällen. I sin [hotbildsrapport](#) för 2025 identifierade Enisa utpressningstrojaner som det mest kritiska hotet i EU. [Figur 2](#) visar de utsatta sektorerna.

³ Enisas [rapport om cybersäkerhetssituationen i unionen för 2024](#).

Figur 2 | Sektorer som drabbas av cyberattacker

Källa: Revisionsrätten, baserat på uppgifter från [Enisa](#).

Betydande och storskaliga cybersäkerhetsincidenter

03 Cybersäkerhetsincidenter, som omfattar cyberhot och oavsiktliga händelser (såsom dem som nämns i [figur 3](#) och punkt [41](#)), ”kan hindra tillhandahållandet av offentliga tjänster [och] utövandet av ekonomisk verksamhet, ... leda till betydande ekonomiska förluster, undergräva användarnas förtroende, orsaka stora skador på unionens ekonomier och demokratiska system och till och med få hälsomässiga eller livshotande konsekvenser.”⁴ En cybersäkerhetsincident anses vara⁵

- **betydande** om den har orsakat eller skulle kunna orsaka allvarliga störningar i tjänsterna eller ekonomiska förluster för den berörda entiteten eller påverka andra fysiska eller juridiska personer genom att orsaka betydande materiell eller immateriell skada,
- **storskalig** om den har orsakat störningar som är så omfattande att en medlemsstat inte kan hantera dem eller som har en betydande påverkan på minst två medlemsstater.

04 En omfattande cybersäkerhetsincident kan trappas upp till en fullt utvecklad **EU-cyberkris** om den hindrar den inre marknaden från att fungera korrekt eller allvarligt hotar den allmänna tryggheten och säkerheten för entiteter eller medborgare i flera medlemsstater eller i unionen som helhet⁶.

⁴ Skäl 2 i förordning (EU) 2025/38 ([cybersolidaritetsakten](#)).

⁵ Artiklarna 6 och 23 i NIS 2-direktivet, som närmare specificeras i [kommissionens genomförandeförordning \(EU\) 2024/2690](#) för ett antal leverantörer inom sektorn för digital infrastruktur.

⁶ Skäl 69 till [NIS 2 -direktivet](#).

EUs: politiska ram

- 05** EU:s cyberekosystem är komplext och mångfasetterat och omfattar ett stort antal inrikespolitiska områden såsom rättsliga och inrikes frågor, den digitala inre marknaden och forskningspolitik⁷. Inom utrikespolitiken är cybersäkerhet viktigt för diplomatin och spelar en allt viktigare roll i EU:s framväxande försvarspolitik⁸.
- 06** Under de senaste åren har EU stärkt sitt regelverk för cybersäkerhet. *Figur 3* nedan visar de viktigaste lagstiftnings- och policyinstrumenten på EU-nivå. I enlighet med revisionens inriktning och omfattning samt revisionsmetod (se punkterna *13–15*) har vi inriktat oss på instrument som rör upptäckt och hantering av betydande och storskaliga cybersäkerhetsincidenter.

⁷ Revisionsrättens briefingdokument om utmaningar för en ändamålsenlig EU politik för cybersäkerhet, s. 12.

⁸ T.ex. Europeiska unionens arbete på cyberområdet (2022), ram för en samordnad EU-reaktion på hybridkampanjer (2022), EU:s politik för cyberförsvar (2023) och den reviderade verktygslådan för cyberdiplomati (2023).

Figur 3 | Relevant EU-lagstiftning och relevanta politiska instrument

- Antagande av lagstiftning och politiska instrument
- Skapande av nätverk och strukturer



Källa: Revisionsrätten.

Roller och ansvarsområden

- 07** EU:s cybersäkerhetslandskap omfattar ett stort antal privata och offentliga aktörer på regional och nationell nivå och EU-nivå inom det civila området, däribland brottsbekämpande myndigheter. Cybersäkerhet är också en viktig del av nationella säkerhets- och försvarssystem⁹. Vi ger en översikt över den aktuella situationen inom EU i [bilaga II](#).
- 08** Medlemsstaterna har det primära ansvaret för förebyggande av, beredskap inför och hantering av cybersäkerhetsincidenter och cyberkriser som påverkar dem. Enligt [artikel 4.2 i fördraget om Europeiska unionen](#) ska den nationella säkerheten vara varje medlemsstats eget ansvar. Eftersom cyberincidenter skulle kunna störa och skada kritisk informationsinfrastruktur, som är en förutsättning för att den inre marknaden ska fungera väl, spelar EU också en viktig roll i händelse av en betydande incident eller kris¹⁰. De viktigaste entiteterna på EU-nivå presenteras i [figur 4](#) nedan.

⁹ Yttrande 02/2023 om den föreslagna cybersolidaritetsakten.

¹⁰ EU-planen för hantering av cyberkriser.

Figur 4 | Entiteter på EU-nivå med en nyckelroll inom cybersäkerhet



Källa: Revisionsrätten.

EU-finansiering

- 09** Enligt den nuvarande fleråriga budgetramen för 2021–2027 är den viktigaste finansieringskällan för cybersäkerhet [programmet för ett digitalt Europa \(Digital\)](#). Det lanserades 2021 och är det första EU-program som specifikt syftar till att driva på EU:s digitala omställning. Programmet har en total budget på 8,1 miljarder euro¹¹.

¹¹ Programmet för ett digitalt Europa.

- 10** Digital finansierar cybersäkerhetsåtgärder inom ramen för sitt särskilda mål 3 – ”Cybersäkerhet och förtroende”. Närmare bestämt finns det en budget på 1,4 miljarder euro för att
- stärka cybersäkerhetssamordningen mellan medlemsstaternas verktyg och datainfrastruktur,
 - främja ett brett införande av cybersäkerhetslösningar i hela ekonomin.
- 11** Merparten av finansieringen av cybersäkerhet från Digital tilldelas genom ansökningsomgångar, och mellan november 2021 och december 2025 genomfördes 12 ansökningsomgångar. Den tillgängliga EU-finansieringen för dessa ansökningsomgångar uppgår till 825 miljoner euro. Nya ansökningsomgångar planeras för 2026 och 2027, då ytterligare 212 miljoner euro ska delas ut i bidrag.
- 12** Ett annat viktigt EU-program till stöd för cybersäkerhet är [Horisont Europa](#). Cybersäkerhetsprojekt finansieras främst inom ramen för [kluster 3](#) – ”Civil säkerhet för samhället” – och befinner sig vanligtvis i ett tidigt mognadsstadium på grund av Horisont Europas inriktning på forskning och innovation. [Faciliteten för återhämtning och resiliens](#) tillhandahåller också finansiering för cybersäkerhetsåtgärder.

Revisionens inriktning och omfattning samt revisionsmetod

- 13** Den ökande förekomsten av cyberhot och deras potentiella konsekvenser har tydliggjort behovet av att stärka vår gemensamma cyberresiliens. Syftet med vår revision var att bedöma om EU:s åtgärder gör det lättare att upptäcka och hantera betydande och storskaliga cybersäkerhetsincidenter på ett ändamålsenligt sätt. Vi undersökte särskilt om detta gällde för
- nätverk och mekanismer på EU-nivå (dvs. CSIRT-nätverket, EU-CyCLONe, det europeiska systemet för cybersäkerhetsvarningar, cyberlägescentralen och EU-cybersäkerhetsreserven),
 - åtgärder som finansieras inom ramen för Digital.

Vi har inte behandlat samarbete inom brottsbekämpning på EU-nivå, och inte heller de avskräckande åtgärder på cyberområdet som vidtas på EU-nivå genom diplomatiska åtgärder eller försvarsverksamhet.

- 14** Revisionen omfattar perioden 2022–2025. Den bygger på en skrivbordsgranskning och analys av relevanta handlingar, revisionsbesök i tre medlemsstater, nämligen Irland, Grekland och Italien, samt skriftliga frågeformulär och intervjuer med berörda intressenter. [Figur 5](#) visar hur vi inhämtade bevis för våra iakttagelser.

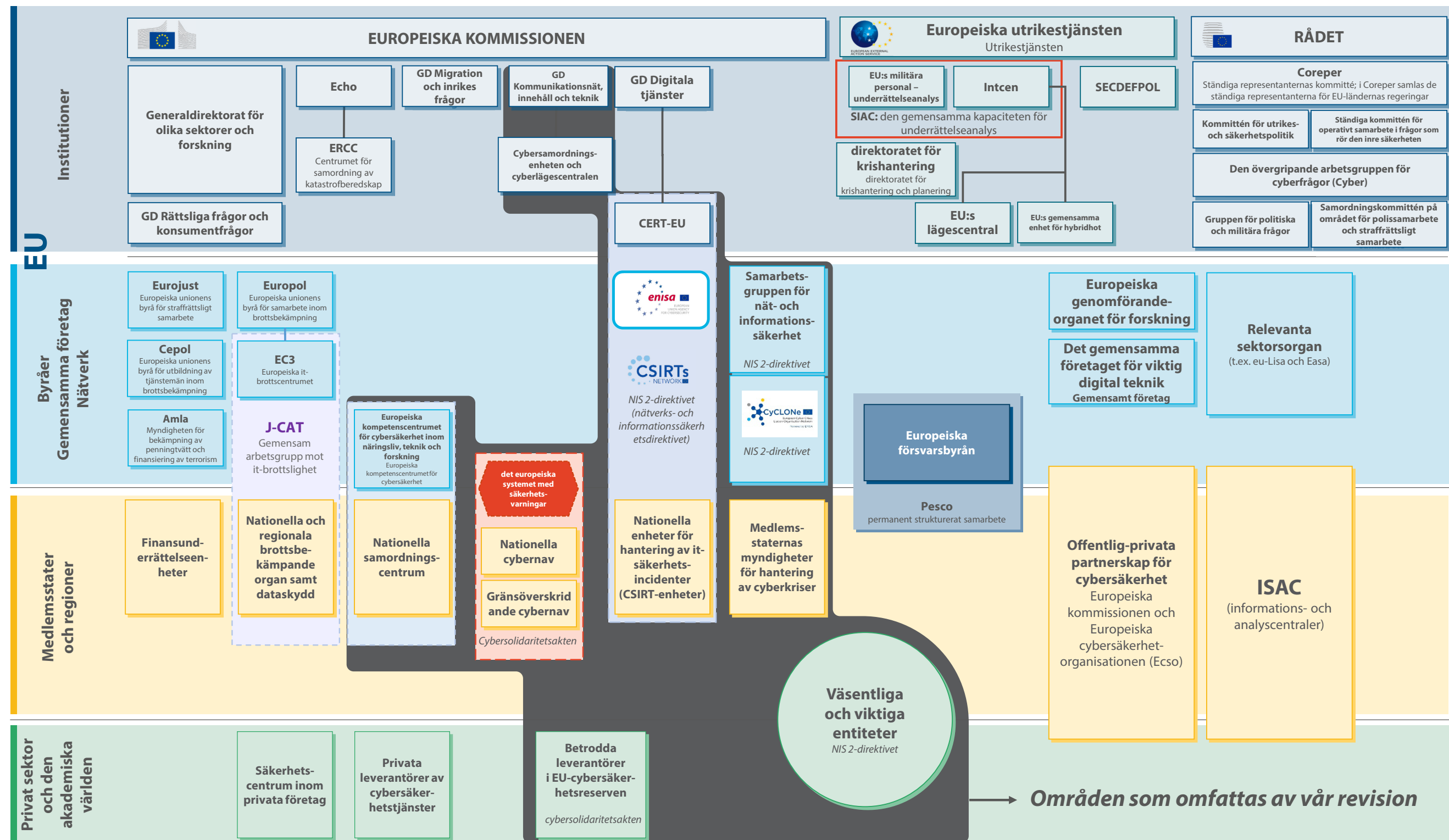
Figur 5 | Utfört revisionsarbete

Vi granskade	• den rättsliga ramen som gäller för upptäckt och hantering av betydande och storskaliga cybersäkerhetsincidenter, • roller och ansvarsområden för nätverk och strukturer som inrättats på EU-nivå.
Vi analyserade	• dokument om hur CSIRT-nätverket och EU-CyCLONe fungerar, • dokumentation om ramen för programplanering och prestationsövervakning inom ramen för Digital, • dokumentation om 13 utvalda EU-finansierade åtgärder (11 bidrag och 2 kontrakt – se detaljerad förteckning i bilaga III). * Vi har valt ut EU-finansierade åtgärder i tre länder (Irland, Grekland och Italien) där den relevanta finansieringen från Digital var mer betydande. De 11 bidragen valdes ut från en lista med 137 EU-finansierade projekt inom området upptäckt och hantering av hot, i syfte att täcka en bred uppsättning projekt.
Vi intervjuade	• mottagare av de 11 EU-finansierade bidrag som ingick i urvalet, • företrädare för de nationella cybersäkerhetsmyndigheterna i tre medlemsländer (Irland, Grekland och Italien), • företrädare för Europeiska kommissionen (GD Kommunikationsnät, innehåll och teknik), Enisa och Europeiska kompetenscentrumet för cybersäkerhet.

Källa: Revisionsrätten.

- 15** Vi räknar med att våra slutsatser ska bidra till att förbättra ändamålsenligheten och effektiviteten i EU:s upptäckt och hantering av betydande och storskaliga cybersäkerhetsincidenter, samt till att förbättra urvals- och övervakningsprocessen för EU-finansierade åtgärder. Vår [revisionsmetod](#) följer de internationella revisionsstandarder som utfärdats av [Internationella organisationen för högre revisionsorgan \(Intosai\)](#).

Bilaga II – EU:s cybersäkerhetslandskap



CNECT: generaldirektoratet för kommunikationsnät, innehåll och teknik
Echo: generaldirektoratet för europeiskt civilskydd och humanitära biståndsåtgärder
GD HOME: generaldirektoratet för migration och inrikes frågor

GD JUST: kommissionens generaldirektorat för rättsliga frågor och konsumentfrågor
DIGIT: generaldirektoratet för digitala tjänster
Easa: Europeiska unionens byrå för luftfartssäkerhet

EU-CyCLONe: Europeiska kontaktnätverket för cyberkriser
eu-Lisa: Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa
Intcen: EU:s underrättelse- och lägescentral

SECDEFPOL: Säkerhets- och försvarspolitik
SOC: säkerhetscentrum

Bilaga III – Utvalda cybersäkerhetsåtgärder

ID	Avdelning	Länder	Startdatum	Slutdatum	Total kostnad (i miljoner euro) och EU-bidrag (i %)	Länk till EU:s finansierings- och anbudsportal
Bidrag till gränsöverskridande cybernav som ingår i det europeiska systemet för cybersäkerhetsvarningar						
1	Inrättande av gränsöverskridande säkerhetscentrum (ATHENA)	Bulgarien, Grekland, Cypern och Malta	1.1.2024	31.3.2028	4,7 (50 %)	
2	GRÄNSÖVERSKRIDANDE PLATTFORMEN ENSOC	Spanien, Italien, Luxemburg, Nederländerna, Österrike, Portugal, Rumänien	1.1.2024	30.6.2028	10,4 (50 %)	
Bidrag för utbyggnad av nätverket av nationella samordningscentrum i medlemsstaterna						
3	Utveckling och inrättande av det nationella centrumet för samordning och utveckling av cybersäkerhet i Irland (NCC-IE)	Irland	2.10.2023	1.10.2026	4,2 (47 %)	
4	Italiens nationella samordningscentrum (NCC-IT)	Italien	1.11.2023	31.10.2025	2,0 (50 %)	
Bidrag för att bygga upp kapaciteten hos säkerhetscentrum, främja nya tillämpningar av AI och annan möjliggörande teknik för säkerhetscentrum samt tillhandahålla beredskapsstöd och ömsesidigt bistånd						
5	Stärkande av kapaciteten hos det grekiska konsoliderade säkerhetscentrumet (EL-SOC)	Grekland, Cypern	1.1.2024	31.12.2026	9,7 (50 %)	
6	Grekiska säkerhetscentrumet för små och medelstora företag (GR-SME-SOC)	Grekland	1.1.2024	31.12.2026	12,1 (50 %)	

ID	Avdelning	Länder	Startdatum	Slutdatum	Total kostnad (i miljoner euro) och EU-bidrag (i %)	Länk till EU:s finansierings- och anbudsportal
7	Nästa generations säkerhetscentrum (NG-SOC)	Grekland, Spanien, Cypern, Luxemburg, Slovenien, Norge	1.1.2024	31.12.2026	4,8 (50 %)	
8	Irländska säkerhetscentrumet för lokala myndigheter (ILG-SOC)	Irland	1.10.2023	30.9.2026	8,3 (50 %)	
9	Ett sammanlänkat ekosystem av nätverk för samordning och insatser på cybersäkerhetsområdet (Cyber-CORE-nätverket)	Irland	1.1.2024	31.12.2026	3,6 (50 %)	
10	Harmonisering av människor, processer och teknik för en robust cybersäkerhet (CYberSynchrony)	Belgien, Grekland, Italien, Cypern, Nederländerna	1.6.2024	31.5.2027	7,0 (100 %)	
11	Avancerade samverkande säkerhetscentrum (ACSOC)	Grekland, Italien, Rumänien	1.1.2025	31.12.2027	3,0 (50 %)	
Ramavtal för Enisas stödåtgärd för cybersäkerhet						
12	Stöd till Enisa för tillhandahållande av tjänster inom ramen för stödåtgärden för cybersäkerhet (28 delupphandlingar)	27 delupphandlingar för medlemsstaterna 1 alleuropeisk delupphandling	1.12.2022 ¹	31.12.2025	28,3 (100 %)	
Tjänsteavtal för cyberlägescentralen för GD Kommunikationsnät, innehåll och teknik						
13	Skräddarsydd tjänst för att stödja Europeiska kommissionens läges- och analyscentral på cyberområdet	–	30.12.2022	30.12.2026	18,0 (100 %)	

Källa: Revisionsrätten.

¹ Flera avtal undertecknades under december 2022.

Bilaga IV – Revisionsrättens bedömning av EU-finansierade cybersäkerhetsprojekt

ID	Projekt	Tillfredsställande Vissa brister Otillfredsställande Ingen slutsats kan dras (eftersom det är för tidigt)			
		Projektet tillgodoser de flesta av de behov som identifierats i ansökningsomgången	Projektet har hittills uppnått planerade output och resultat	Projektets output har levererats senast på förfallodagen	Projektets prestationsindikatorer är relevanta, mätbara och har ett utgångsvärde och ett mål.
1	Inrättande av gränsöverskridande säkerhetscentrum (ATHENA)	Tillfredsställande	Otillfredsställande	Otillfredsställande	Otillfredsställande
2	DEN GRÄNSÖVERSKRIDANDE PLATTFORMEN ENSOC	Tillfredsställande	Otillfredsställande	Otillfredsställande	Otillfredsställande
3	Utveckling och inrättande av det nationella samordnings- och utvecklingscentrumet för cybersäkerhet i Irland (NCC-IE)	Tillfredsställande	Tillfredsställande	Vissa brister	Vissa brister
4	Italiens nationella samordningscentrum (NCC-IT)	Tillfredsställande	Tillfredsställande	Tillfredsställande	Vissa brister
5	Att stärka kapaciteten hos det grekiska samordnade säkerhetsoperationscentret (EL-SOC)	Tillfredsställande	Vissa brister	Otillfredsställande	Otillfredsställande
6	Grekiska säkerhetscentrumet för små och medelstora företag (GR-SME-SOC)	Tillfredsställande	Tillfredsställande	Tillfredsställande	Vissa brister
7	Nästa generations säkerhetscentrum (NG-SOC)	Tillfredsställande	Tillfredsställande	Tillfredsställande	Vissa brister
8	Irländska säkerhetscentrumet för lokala myndigheter (ILG-SOC)	Tillfredsställande	Otillfredsställande	Otillfredsställande	Otillfredsställande
9	Ett sammanlänkat ekosystem av nätverk för samordning och insatser på cybersäkerhetsområdet (Cyber-CORE-nätverket)	Tillfredsställande	Vissa brister	Vissa brister	Vissa brister
10	Harmonisering avseende människor, processer och teknik för en robust cybersäkerhet (CYberSynchrony)	Vissa brister	Ingen slutsats kan dras (eftersom det är för tidigt)	Ingen slutsats kan dras (eftersom det är för tidigt)	Vissa brister
11	Avancerade samverkande säkerhetscentrum (ACSOC)	Tillfredsställande	Ingen slutsats kan dras (eftersom det är för tidigt)	Ingen slutsats kan dras (eftersom det är för tidigt)	Otillfredsställande

Förkortningar

Förkortning	Definition/förklaring
CNECT	Generaldirektoratet för kommunikationsnät, innehåll och teknik
CSIRT	enhet för hantering av it-säkerhetsincidenter
Digital	Programmet för ett digitalt Europa.
Enisa	Europeiska unionens cybersäkerhetsbyrå
EU-CyCLONe	Europeiska kontaktnätverket för cyberkriser
Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning	Europeiska kompetenscentrumet för cybersäkerhet
FSTP	Ekonomiskt stöd till tredje parter
NIS	Nät- och informationssäkerhet
NSC	Nationellt samordningscentrum
SMF	Små och medelstora företag
SOC	Säkerhetscentrum

Ordlista

Term	Definition/förklaring
Betydande cybersäkerhetsincident	Cybersäkerhetsincident som har orsakat eller kan orsaka allvarliga störningar eller ekonomiska förluster för en organisation eller stor skada för andra enheter eller enskilda individer.
cyberhot	Potentiell användning av cyberrymden för att undergräva uppgifters eller informationssystemers tillgänglighet, äkthet, integritet eller konfidentialitet.
Cybernav	En central plattform som samlar olika tjänster, verktyg och it-expertiser för att förbättra övervakningen, upptäckten och analysen av cyberhot, förebygga cybersäkerhetsincidenter och stödja framtagningen av underrättelser om cyberhot.
Cybersäkerhetsincident	Händelse som undergräver uppgifters eller informationssystemers tillgänglighet, äkthet, integritet eller konfidentialitet.
Fientlig aktör	Enskild person eller grupp som avsiktligt orsakar skada, stör tjänster eller stjälar data genom att utnyttja sårbarheter i it-system, it-nätverk och it-enheter.
Storskalig cybersäkerhetsincident	En cybersäkerhetsincident som orsakar störningar som är så omfattande att den berörda medlemsstaten inte kan hantera dem eller som har en betydande påverkan på minst två medlemsstater.
Säkerhetscentrum	Organisatorisk enhet som arbetar för att förhindra cyberhot och cyberincidenter och samlar in underrättelser.
Taxonomi	Inom cybersäkerhet, ett klassificeringssystem som används för att organisera, kategorisera och strukturera kunskap om centrala begrepp som hot och incidenter.
Utpressningstrojan	Skadlig kod som nekar offer åtkomst till ett datorsystem eller krypterar filer för att göra dem oläsliga och vanligen tvingar offret att betala en lösensumma för att återställa åtkomsten.

Kommissionens svar

<https://www.eca.europa.eu/sv/publications/sr-2026-19>

Svaren från Europeiska kompetenscentrumet för cybersäkerhet (ECCC).

<https://www.eca.europa.eu/sv/publications/sr-2026-19>

Svar från Europeiska unionens cybersäkerhetsbyrå (Enisa)

<https://www.eca.europa.eu/sv/publications/sr-2026-19>

Tidsplan

<https://www.eca.europa.eu/sv/publications/sr-2026-19>

Vi som arbetat med revisionen

I våra särskilda rapporter redovisar vi resultatet av våra revisioner av EU:s politik och program eller av förvaltningsteman som är kopplade till specifika budgetområden. För att uppnå så stor effekt som möjligt väljer vi ut och utformar granskningsuppgifterna med hänsyn till riskerna när det gäller prestation eller regelefterlevnad, storleken på de aktuella intäkterna eller kostnaderna, framtida utveckling och politiskt intresse och allmänintresse.

Denna effektivitetsrevision utfördes av revisionsrättens avdelning III yttre åtgärder, säkerhet och rättvisa, där ledamoten George-Marius Hyzler är ordförande. Revisionen leddes av revisionsrättens ledamot George-Marius Hyzler, med stöd av Romuald Kayibanda, chef för kansliet, och Annette Farrugia, kansliassistent; Cyril Messein, huvudansvarig chef; Frédéric Soblet, projektledare; samt Jurgen Manjé och Flavia Di Marco, revisorer. Zoe Amador Martínez bidrog med språkligt stöd. Dunja Weibel bidrog med grafiskt stöd.



Från vänster: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé, Cyril Messein.

UPPHOVSRÄTT

© Europeiska unionen, 2026

Europeiska revisionsrättens policy för vidareutnyttjande av handlingar fastställs i [Europeiska revisionsrättens beslut nr 6-2019](#) om öppen datapolitik och vidareutnyttjande av handlingar.

Om inget annat anges (t.ex. i enskilda meddelanden om upphovsrätt) omfattas revisionsrättens innehåll som ägs av EU av den [internationella licensen Creative Commons Erkännande 4.0 Internationell \(CC BY 4.0\)](#). Det innebär att det är tillåtet att återanvända innehållet under förutsättning att ursprunget anges korrekt och att det framgår om ändringar har gjorts. Om du återanvänder revisionsrättens innehåll får du inte förvanska den ursprungliga innebörden eller det ursprungliga budskapet. Revisionsrätten ansvarar inte för eventuella konsekvenser av återanvändningen.

När enskilda privatpersoner kan identifieras i ett specifikt sammanhang, exempelvis på bilder av revisionsrättens personal, eller om verk av tredje part används, måste ytterligare tillstånd inhämtas.

Om ett sådant tillstånd beviljas upphävs och ersätts det allmänna godkännande som nämns ovan, och eventuella begränsningar av materialets användning måste tydligt anges.

Tillstånd för användning eller mångfaldigande av innehåll som inte ägs av EU kan behöva sökas direkt från upphovsrättsinnehavarna.

Omslagsfoto: © Fotokon – stock.adobe.com.

Figur 6 och 8 - ikoner: Dessa har tagits fram med hjälp av resurser från [Flaticon.com](#).

© Freepik Company S.L. Alla rättigheter förbehålls.

Figur 5 - kartor: [Eurostat](#).

Programvara eller handlingar som omfattas av immateriella rättigheter, till exempel patent, varumärkesskydd, mönsterskydd samt upphovsrätt till logotyper eller namn, omfattas inte av revisionsrättens policy för vidareutnyttjande.

EU-institutionernas webbplatser inom domänen europa.eu innehåller länkar till webbplatser utanför den domänen. Eftersom revisionsrätten inte har någon kontroll över dem uppmanas du att ta reda på vilken integritets- och upphovsrättspolicy de tillämpar.

Användning av revisionsrättens logotyp

Revisionsrättens logotyp får inte användas utan revisionsrättens förhandsgodkännande.

HTML	ISBN 978-92-849-7895-3	ISSN 1977-5830	doi:10.2865/2922381	QJ-01-26-032-SV-Q
Pdf	ISBN 978-92-849-7896-0	ISSN 1977-5830	doi:10.2865/9025285	QJ-01-26-032-SV-N

SÅ HÄNVISAR DU

Europeiska revisionsrätten, [specialrapport 19/2026](#) "EU:s samarbetsram gör framsteg, men är endast delvis ändamålsenlig på grund av förseningar i genomförandet och begränsat informationsutbyte", Europeiska unionens publikationsbyrå 2026.

Under de senaste åren har EU förstärkt sina rättsliga ramar för cybersäkerhet och inrättat nätverk och mekanismer för att hantera cybersäkerhetsincidenter. EU finansierar även cybersäkerhetsprojekt genom programmet för ett digitalt Europa.

Vi drar slutsatsen att EU:s åtgärder endast delvis underlättar upptäckten och hanteringen av betydande och storskaliga cybersäkerhetsincidenter. En samarbetsram har stegvis införts, men arbetet mot att uppnå fullständigt upprättande pågår dock fortfarande. Begränsat informationsutbyte, rapportering av brister och avsevärda förseningar i genomförandet hindrar EU:s nätverk och mekanismer från att uppnå sin fulla potential. Projekten eftersträvar relevanta mål, men ett flertal står inför operativa utmaningar och förseningar. Dessutom finns det brister i den övergripande ramen för prestationsövervakning. Vi lägger fram rekommendationer för att åtgärda dessa brister.

Revisionsrättens särskilda rapport i enlighet med artikel 287.4 andra stycket i EUF-fördraget.



EUROPEISKA
REVISIONSRÄTTEN



Europeiska unionens
publikationsbyrå

EUROPEISKA REVISIONSRÄTTEN
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBURG

Tfn +352 4398-1

Frågor: eca.europa.eu/sv/contact
Webbplats: eca.europa.eu
Sociala medier: @EUauditors