

# Opdagelse af og reaktion på cybersikkerhedshændelser

En EU-samarbejdsramme er under udvikling, men på grund af gennemførelsesforsinkelser og begrænset informationsdeling er den kun delvis effektiv



DEN  
EUROPÆISKE  
REVISIONSRET

# Indhold

## Punkt

### 01-23 | **Hovedbudskaber**

01-07 | Hvorfor dette område er vigtigt

08-23 | Hvad vi konstaterede og anbefaler

### 24-01 | **Et nærmere blik på vores bemærkninger**

**24-74 | EU's cybersikkerhedsnetværk og -mekanismer understøtter samarbejde og reaktioner, men begrænset informationsdeling og ufuldstændig gennemførelse svækker effektiviteten**

24-51 | EU-netværkene muliggør samarbejde mellem medlemsstaterne, men begrænset informationsdeling svækker deres merværdi

52-61 | EU's cybersikkerhedsreserve muliggør hurtig levering af indsatstjenester

62-74 | Det europæiske cybersikkerhedsvarslingssystem skal forbedre evnen til at opdage trusler, men det er ikke operationelt

**75-01 | De EU-finansierede DEP-projekter skal styrke cybersikkerheden, men har gennemførelses- og rapporteringsudfordringer**

75-81 | Forsinkelser ved oprettelsen af Kompetencefællesskabet for Cybersikkerhed betød, at det ikke kunne bidrage til at forme DEP

82-96 | De EU-finansierede projekter forfølger relevante mål, men mange af dem er ramt af operationelle problemer

97-01 | De fleste EU-finansierede projekter har utilstrækkelige præstationsrammer, og DEP's cybersikkerhedsrelaterede præstationsdata er ikke nøjagtige

## **Bilag**

**Bilag I - Om revisionen**

**Bilag II - EU's cybersikkerhedslandskab**

**Bilag III - Udvalgte cybersikkerhedsforanstaltninger**

**Bilag IV - Revisionsrettens vurdering af EU-finansierede cybersikkerhedsprojekter**

## **Forkortelser**

## **Glossar**

## **Kommissionens svar**

**Svar fra Det Europæiske Kompetencecenter for Cybersikkerhed (ECCC)**

**Svar fra Den Europæiske Unions Agentur for Cybersikkerhed (ENISA)**

## **Tidslinje**

## **Revisionsholdet**

# 01

## Hovedbudskaber

### Hvorfor dette område er vigtigt

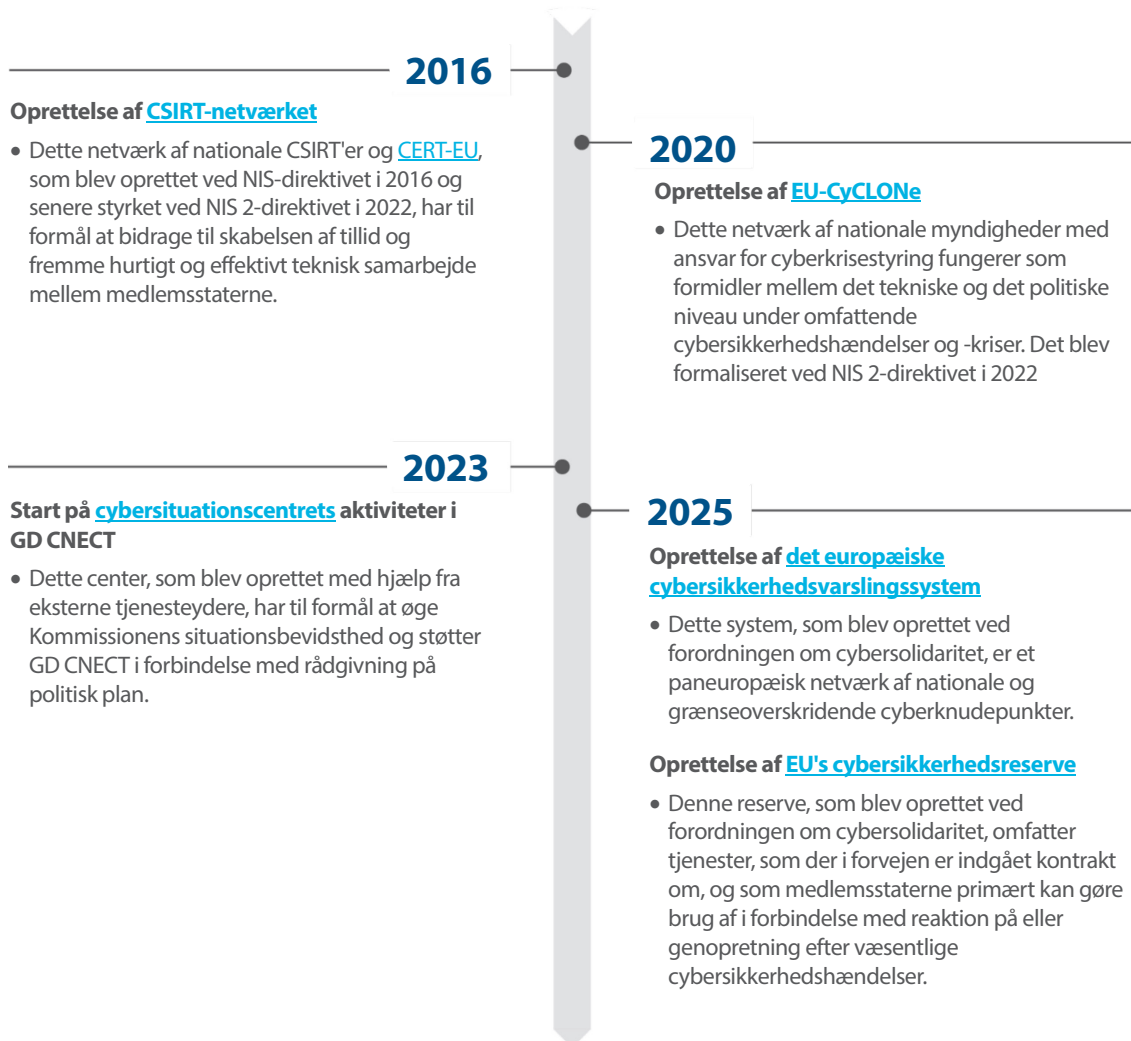
- 01** Risiciene for cyberangreb vokser i takt med, at vores økonomi og vores dagligdag bliver mere og mere digitaliseret. Cybersikkerhed er defineret som "de aktiviteter, der er nødvendige for at beskytte net- og informationssystemer, brugerne af sådanne systemer og andre personer berørt af cybertrusler"<sup>1</sup>. Cybersikkerhed kræver en holistisk tilgang til at forebygge, opdage, reagere på og sikre genopretning efter cybertrusler.
- 02** EU's cybersikkerhedslandskab involverer en lang række offentlige og private enheder på regionalt og nationalt plan samt på EU-plan, som arbejder med cybersikkerhed på det civile område. Cybersikkerhed er også et centralt element i de enkelte medlemsstaters nationale sikkerheds- og forsvarspolitik.
- 03** Medlemsstaterne har det primære ansvar for at forebygge, forberede sig på og reagere på cybersikkerhedshændelser og -kriser, der påvirker dem. Da sådanne hændelser kan påvirke det indre markeds funktion, har EU også en vigtig rolle at spille i forbindelse med væsentlige hændelser eller kriser. I de seneste år har EU styrket og udviklet sin lovgivningsmæssige ramme vedrørende cybersikkerhed<sup>2</sup> og etableret netværk og mekanismer, jf. [figur 1](#) og [bilag II](#).

---

<sup>1</sup> Forordning (EU) 2019/881 ([forordningen om cybersikkerhed](#)).

<sup>2</sup> F.eks. fremsatte Kommissionen forslag til en [digital omnibus](#) i november 2025 og forslag til en revideret [EU-forordning om cybersikkerhed](#) i januar 2026.

**Figur 1 | EU's cybersikkerhedsnetværk og -mekanismer 2016-2025**



**CSIRT'er:** Enheder, der håndterer IT-sikkerhedshændelser

**GD CNECT:** Generaldirektoratet for Kommunikationsnet, Indhold og Teknologi

**EU-CyCLONe:** Det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser

**NIS-direktivet:** Direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen

**NIS 2-direktivet:** Direktiv (EU) 2022/2555 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen

*Kilde:* Revisionsretten.

- 04** Hovedkilden til finansiering af cybersikkerhed under den aktuelle flerårige finansielle ramme for 2021-2027 er [programmet for et digitalt Europa](#) (DEP). Det har et samlet budget på 8,1 milliard euro, hvoraf 1,4 milliarder euro er afsat til at styrke cybersikkerheden.

- 05** Formålet med vores revision var at vurdere, om EU-tiltag effektivt fremmer opdagelse af og reaktion på væsentlige og omfattende cybersikkerhedshændelser. Vi vurderede dette med hensyn til:
- de etablerede netværk og mekanismer på EU-plan (dvs. netværket af enheder, der håndterer IT-sikkerhedshændelser (CSIRT-netværket), Det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser (EU-CyCLONe), det europæiske cybersikkerhedsvarslingssystem, cybersituationscentret og EU's cybersikkerhedsreserve)
  - de DEP-finansierede tiltag.
- 06** Vi forventer, at vores revisionsresultater vil bidrage til at styrke EU's cyberrobusthed ved at sikre større effektivitet og produktivitet i EU's netværk og mekanismer og forbedre den måde, EU-finansierede tiltag udvælges og overvåges på.
- 07** Vores revision dækkede perioden fra 2022 til 2025. Revisionsarbejdet omfattede skrivebordsgennemgang og analyse af relevante dokumenter, revisionsbesøg i tre medlemsstater - Irland, Grækenland og Italien - skriftlige spørgeskemaer og interview med relevante interessenter. Flere baggrundsoplysninger og nærmere detaljer om revisionens omfang og revisionsmetoden kan findes i [bilag I](#).

## Hvad vi konstaterede og anbefaler

- 08** Vi konkluderer samlet set, at EU's tiltag kun delvis fremmer opdagelse af og reaktion på væsentlige og omfattende cybersikkerhedshændelser. Der er gradvis blevet udformet en samarbejdsramme, men arbejdet med at færdiggøre den er stadig i gang. På grund af begrænset informationsdeling, rapporteringssvagheder og store gennemførelsesforsinkelser har EU's netværk og mekanismer ikke opfyldt deres fulde potentiale. De DEP-finansierede projekter forfølger relevante mål, men adskillige er ramt af operationelle udfordringer og forsinkelser, og der er svagheder i den generelle præstationsovervågningsramme.
- 09** Den nuværende ramme af EU-netværk og -mekanismer, der skal fremme opdagelse af og reaktion på væsentlige cybersikkerhedshændelser, er blev opbygget gradvis. I 2025 vedtog Rådet [cyberplanen](#), der fastlægger EU-rammen for cyberkrisestyring. Vi konstaterede, at cyberplanen i vidt omfang præciserer roller og ansvarsområder vedrørende cyberkrisestyring på EU-plan. Ikke desto mindre er de proceduremæssige ordninger for, hvordan CSIRT-netværket (oprettet i 2016) og EU-CyCLONe (formaliseret i 2023) skal samarbejde, endnu ikke formaliseret (punkt [24-30](#)).

- 10** Vi konstaterede, at informationsdelingen i disse netværk er begrænset. Det skyldes hovedsagelig, at gennemførelsen af [direktivet om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele EU](#) (NIS 2-direktivet) er forsinket, at der er problemer med at vurdere, om en hændelse har grænseoverskridende virkninger, og at den nationale sikkerhedslovgivning forhindrer informationsdeling. Netværkenes merværdi svækkes betydeligt, hvis medlemsstaterne ikke er villige til at udveksle rettidige og anvendelige oplysninger (punkt [31-44](#)).



### Anbefaling 1

#### Styrke informationsdelingen mellem medlemsstaterne

Med henblik på at sikre bedre opdagelse af og reaktion på cybersikkerhedshændelser bør Kommissionen med støtte fra Den Europæiske Unions Agentur for Cybersikkerhed (ENISA):

- a) foreslå, at samarbejdsgruppen for net- og informationssikkerhed foretager en detaljeret analyse af de nationale sikkerhedsrestriktioner, der begrænser informationsdelingen og svækker EU's cyberrobusthed, og at den identificerer retlige og tekniske løsninger, der kan øge informationsudvekslingen, samtidig med at beføjelserne vedrørende den nationale sikkerhed respekteres
- b) uden at dette berører fælleslovgivernes afgørelser, i samarbejde med medlemsstaterne sikre, at det centrale kontaktpunkt for indberetning af hændelser, der foreslås i den digitale omnibus, kan opdage potentielle grænseoverskridende hændelser
- c) arbejde på løsninger, der kan muliggøre indberetning af hændelser til ENISA i realtid.

**Måldato for gennemførelsen: a) og b) 2027, c) 2028**

- 11** I 2022 oprettede Kommissionen et "cybersituationscenter" for at øge sin situationsbevidsthed og understøtte udførelsen af opgaver vedrørende sit institutionelle krisestyringsansvar. Centrets drift varetages i vidt omfang af eksterne tjenesteydere, som der er indgået kontrakt med. Vi konstaterede, at de eksterne tjenesteyderes arbejde delvis overlapper med eksisterende kapaciteter i Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) vedrørende situationsbevidsthed og trusselovervågning. Vi mener ikke, at cybersituationscentret er blevet etableret på en sådan måde, at der er tilstrækkelige muligheder for at opnå rationalisering ved at anvende allerede tilgængelige oplysninger fra Kommissionen og ENISA. Det forhold, at der mangler en omfattende, detaljeret plan for tiden efter kontraktens udløb, udgør desuden en risiko vedrørende cybersituationscentrets drift efter 2026 (punkt [45-51](#)).



## Anbefaling 2

### Rationalisere EU's kapaciteter vedrørende situationsbevidsthed om cybersikkerhed og optimere formidlingen af oplysninger

Med henblik på at sikre øget effektivitet bør Kommissionen i samarbejde med ENISA vurdere gennemførligheden af at foretage fælles indsamling og analyse af oplysninger vedrørende situationsbevidsthed. Den bør desuden gøre disse oplysninger og de relaterede cybertrusselsrapporter tilgængelige for de relevante EU-tjenestegrene og -agenturer.

**Måldato for gennemførelsen: 2027**

- 12** Ved [forordningen om cybersolidaritet](#) fra 2024 oprettedes EU's cybersikkerhedsreserve, som har til formål at støtte medlemsstaternes reaktion på og genopretning efter større cybersikkerhedshændelser. Reserven består af tjenester fra bestemte udbydere i hver medlemsstat, som kan reagere på hændelser døgnet rundt. Dette bidrager til at sikre opfyldelse af medlemsstaternes specifikke krav og opbygge tillid, men det disponible budget er fordelt ligeligt mellem dem og tager ikke hensyn til de enkelte medlemsstaters særlige behov (punkt [52-57](#)).
- 13** Vi mener, at brugen af udbydere, som der i forvejen er indgået kontrakt med, muliggør hurtig levering af indsatstjenester. EU's cybersikkerhedsreserve skal primært støtte indsatser og genopretning, men når den ikke bruges til hændelseshåndtering, kan den bruges til beredskabsformål. Denne fleksible tilgang kan forhindre, at der ikke gøres brug af forudbetalte tjenester. Der er dog en risiko for, at reserven primært anvendes til beredskabs- i stedet for indsatsaktiviteter, hvilket er i strid med dens formål (punkt [58-61](#)).

- 14** Det europæiske cybersikkerhedsvarslingssystem er et netværk af nationale og grænseoverskridende cyberknudepunkter, som har til formål at forbedre evnen til at opdage, analysere og reagere på cybertrusler. Vi konstaterede på tidspunktet for vores revision, at de to knudepunkter (ATHENA og ENSOC) - på grund af betydelige forsinkelser vedrørende indkøb af værktøjer og tjenester - endnu ikke var operationelle, og at det europæiske cybersikkerhedsvarslingssystem endnu ikke var i funktion (punkt [62-70](#)).
- 15** Et af de vigtigste mål for det europæiske cybersikkerhedsvarslingssystem er at tilskynde til meningsfuld informationsdeling mellem klynger af medlemsstater. Systemet kan potentielt løse nogle af problemerne vedrørende informationsdeling, men det er en stor udfordring at integrere cyberknudepunkter i det allerede komplekse cybersikkerhedslandskab. Vi konstaterede, at systemet endnu ikke fungerede fuldt ud, fordi der manglede samarbejdsaftaler, en fælles taksonomi og standarder for interoperabilitet (punkt [71-74](#)).



### Anbefaling 3

#### Integrere det europæiske cybersikkerhedsvarslingssystem i EU's cybersikkerhedslandskab

Kommissionen bør sammen med ENISA og medlemsstaterne sikre, at der etableres samarbejdsordninger og indføres standarder for interoperabilitet med henblik på at fremme informationsdeling mellem grænseoverskridende knudepunkter, som er del af det europæiske cybersikkerhedsvarslingssystem, CSIRT-netværket og EU-CyCLONe.

**Måldato for gennemførelsen: 2028**

- 16** Kommissionen foreslog i 2018, at der skulle oprettes et europæisk kompetencecenter for cybersikkerhed (ECCC) med henblik på at forvalte DEP's cybersikkerhedskomponent fra 2021. [ECCC-forordningen](#) fastsatte, at der skulle oprettes et kompetencefællesskab for cybersikkerhed bestående af repræsentanter for industrien, akademiske organisationer og forskningsorganisationer. Udvalgte medlemmer af kompetencefællesskabet skulle udgøre ECCC's Strategiske Rådgivningsgruppe (punkt [75](#) og [76](#)).
- 17** Vi konstaterede, at ECCC's opnåelse af finansiel uafhængighed og oprettelsen af Kompetencefællesskabet for Cybersikkerhed og Den Strategiske Rådgivningsgruppe var blevet forsinket. Det betød, at kompetencefællesskabet og Den Strategiske Rådgivningsgruppe ikke kunne levere input vedrørende udformningen af DEP-arbejdsprogrammerne. Vi betragter dette som en forspildt mulighed (punkt [77-81](#)).

- 18** Vi konstaterede, at alle de projekter, vi undersøgte, forfølger relevante mål, der bidrager til at opfylde DEP's cybersikkerhedsmål. Vi fandt dog tilfælde, hvor projektkvaliteten eller de opnåede resultater ikke var tilfredsstillende, hvilket hovedsagelig skyldtes forsinkelser i gennemførelsen (punkt [82-87](#)).
- 19** [DEP-forordningen](#) fastsætter, at finansiering til cybersikkerhed af sikkerhedsmæssige årsager kan forbeholdes enheder, der er etableret i en medlemsstat og kontrolleres af en medlemsstat eller statsborgere i en medlemsstat. Den centrale valideringstjeneste i [Det Europæiske Forvaltningsorgan for Forskning](#) udfører ejerskabs- og kontrolvurderinger på ECCC's vegne (punkt [88-91](#)).
- 20** I forbindelse med finansiell støtte til tredjeparter er tilskudsmodtagerne ansvarlige for at udføre ejerskabs- og kontrolvurderinger efter deres egne metoder. Vi konstaterede, at ECCC hverken validerer disse metoder eller foretager kontrol for at sikre, at de udvalgte tredjeparter er EU-ejede og -kontrollerede. Efter vores opfattelse er der en betydelig risiko for, at tilskudsmodtagerne ikke har den nødvendige kapacitet til at udføre disse vurderinger korrekt. Denne risiko er ikke blevet mindsket tilstrækkeligt og kan føre til eksponering af følsom infrastruktur, operationelle data og sikkerhedskritiske teknologier (punkt [92-96](#)).



#### Anbefaling 4

##### **Sikre solide ejerskabs- og kontrolvurderinger af enheder, der modtager EU-finansiering under programmet for et digitalt Europa**

Det Europæiske Kompetencecenter for Cybersikkerhed bør:

- a) opnå rimelig sikkerhed for, at tilskudsmodtagere med ansvar for at yde finansiell støtte til tredjeparter har den nødvendige administrative og tekniske kapacitet til at udføre tilstrækkelige ejerskabs- og kontrolvurderinger ved anvendelse af den eksisterende metode, der er fastlagt for tilskudsmodtagere, som yder finansiell støtte til tredjeparter
- b) på stikprøvebasis kontrollere, om der kun er ydet EU-finansiering til berettigede enheder.

**Måldato for gennemførelsen: a) 2026, b) 2027**

- 21** Tilskudsmodtagere, der forvalter EU-finansierede projekter, skal rapportere til ECCC om deres fremskridt og resultater med henvisning til delmål, leverancer og indikatorer. Disse elementer er afgørende for projektovervågningen og bør fastsættes korrekt. Vi konstaterede, at instrukserne vedrørende udformningen af delmål og leverancer næsten ikke var fulgt i nogen af projekterne i vores stikprøve, og at mange af dem ikke kunne anvendes til måling af fremskridt (punkt [97-99](#)).
- 22** Vi konstaterede, at mange af de præstationsindikatorer, der anvendes af tilskudsmodtagerne, ikke er relevante eller målbare, og at de mangler et mål eller et referencescenario. Desuden er rapporteringen om disse indikatorer utilstrækkelig, og den kan derfor ikke tjene som grundlag for en vurdering af projekternes præstation (punkt [100-102](#)).
- 23** Med henblik på overvågning af DEP som helhed skal der i forbindelse med alle projekter rapporteres om bestemte programindikatorer, der anvendes som input til Kommissionens årlige [programgennemførelseserklæringer](#). ECCC er ansvarligt for at indsamle og kontrollere de indsendte data vedrørende disse indikatorer. Vi konstaterede adskillige problemer med hensyn til den måde, hvorpå dataene blev indsamlet, og deres samlede kvalitet. Vi fandt ingen dokumentation for, at nøjagtigheden af de rapporterede data var blevet kontrolleret af ECCC. På baggrund af vores kontrol af projekterne i vores stikprøve mener vi ikke, at de rapporterede data afspejler de opnåede resultater korrekt (punkt [103-106](#)).



### Anbefaling 5

#### **Styrke præstationsovervågningsrammen vedrørende cybersikkerhedskomponenten i programmet for et digitalt Europa**

Med henblik på at muliggøre passende overvågning af fremskridt og præstationer bør Det Europæiske Kompetencecenter for Cybersikkerhed:

- a) sikre vedrørende alle projekter, at der før underskrivelsen af tilskudsaftalen er fastsat delmål, leverancer og præstationsindikatorer, som er udformet i overensstemmelse med instrukserne i ansøgningsskemaet
- b) udforme og indføre et robust system til indsamling, sporing, kontrol og aggregering af data til beregning af præstationsindikatorerne vedrørende cybersikkerhedskomponenten i programmet for et digitalt Europa, så det kan sikres, at indikatorerne nøjagtigt afspejler de opnåede resultater.

**Måldato for gennemførelsen: 2027**

## Et nærmere blik på vores bemærkninger

**EU's cybersikkerhedsnetværk og -mekanismer understøtter samarbejde og reaktioner, men begrænset informationsdeling og ufuldstændig gennemførelse svækker effektiviteten**

**EU-netværkene muliggør samarbejde mellem medlemsstaterne, men begrænset informationsdeling svækker deres merværdi**

- 24** Den nuværende EU-ramme af netværk og mekanismer, der skal fremme opdagelse af og reaktion på væsentlige cybersikkerhedshændelser, blev opbygget gradvis, begyndende med [direktivet om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen](#)<sup>3</sup> (NIS-direktivet), som trådte i kraft i august 2016. Vi illustrerer det aktuelle EU-landskab i [bilag II](#).

---

<sup>3</sup> Direktiv (EU) 2016/1148.

## EU-netværkene muliggør teknisk og operationelt samarbejde mellem medlemsstaterne

- 25** NIS-direktivet oprettede [CSIRT-netværket](#), som samler [CERT-EU](#) (Cybersikkerhedstjenesten for Unionens Institutioner, Organer, Kontorer og Agenturer) og de CSIRT'er, der er udpeget af medlemsstaterne. Formålet med dette netværk er at skabe tillid mellem de nationale CSIRT'er og fremme et hurtigt og effektivt operationelt samarbejde mellem medlemsstaterne.
- 26** [EU-CyCLONe](#) blev oprettet i 2020 som et uformelt samarbejdsnetværk for nationale myndigheder med ansvar for cyberkrisestyring. Det fungerer som formidler mellem det tekniske niveau, hvor CSIRT-netværket opererer, og det politiske niveau, som udgøres af Rådet for Den Europæiske Union og dets ordninger for [integreret politisk kriserespons](#). NIS 2-direktivet, som trådte i kraft i 2023, formaliserede EU-CyCLONe's rolle og gav det et klart mandat.
- 27** Vi vurderede, om disse EU-netværks roller og ansvarsområder er veldefinerede, og om de fremmer samarbejde mellem medlemsstaterne.
- 28** [ENISA](#) fungerer som sekretariat for CSIRT-netværket og EU-CyCLONe og tilvejebringer ressourcer, ekspertise, infrastruktur og IT-værktøjer vedrørende samarbejde og sikker kommunikation med henblik på informationsdeling. I den tilfredshedsundersøgelse<sup>4</sup>, der blev foretaget blandt ENISA's interessenter i begyndelsen af 2025, fik det en god bedømmelse for sit arbejde som sekretariat for disse netværk. Denne positive feedback blev bekræftet under vores revisionsbesøg, hvor de nationale cybersikkerhedsmyndigheder gav udtryk for deres tilfredshed.
- 29** I 2025 vedtog Rådet [cyberplanen](#), som definerer roller og ansvarsområder for de centrale aktører (herunder CSIRT-netværket og EU-CyCLONe) og mekanismer, der er involveret i håndtering af omfattende cybersikkerhedshændelser og cyberkriser. Vi konstaterede, at cyberplanen i vidt omfang præciserer roller og ansvarsområder vedrørende cyberkrisestyring på EU-plan og tager højde for de ændringer, der er sket i cybersikkerhedslandskabet, siden den første cyberplan blev udarbejdet i 2017. Den definerer tre samarbejdsniveauer: teknisk, operationelt og politisk. Den beskriver de nye netværk og strukturer, der er oprettet siden 2017 - f.eks. EU-CyCLONe, EU-hybridberedskabsholdene og det europæiske cybersikkerhedsvarslingssystem - og hvordan cyberkrisestyring bør integreres i den bredere EU-ramme for håndtering af cybersikkerhedskriser.

---

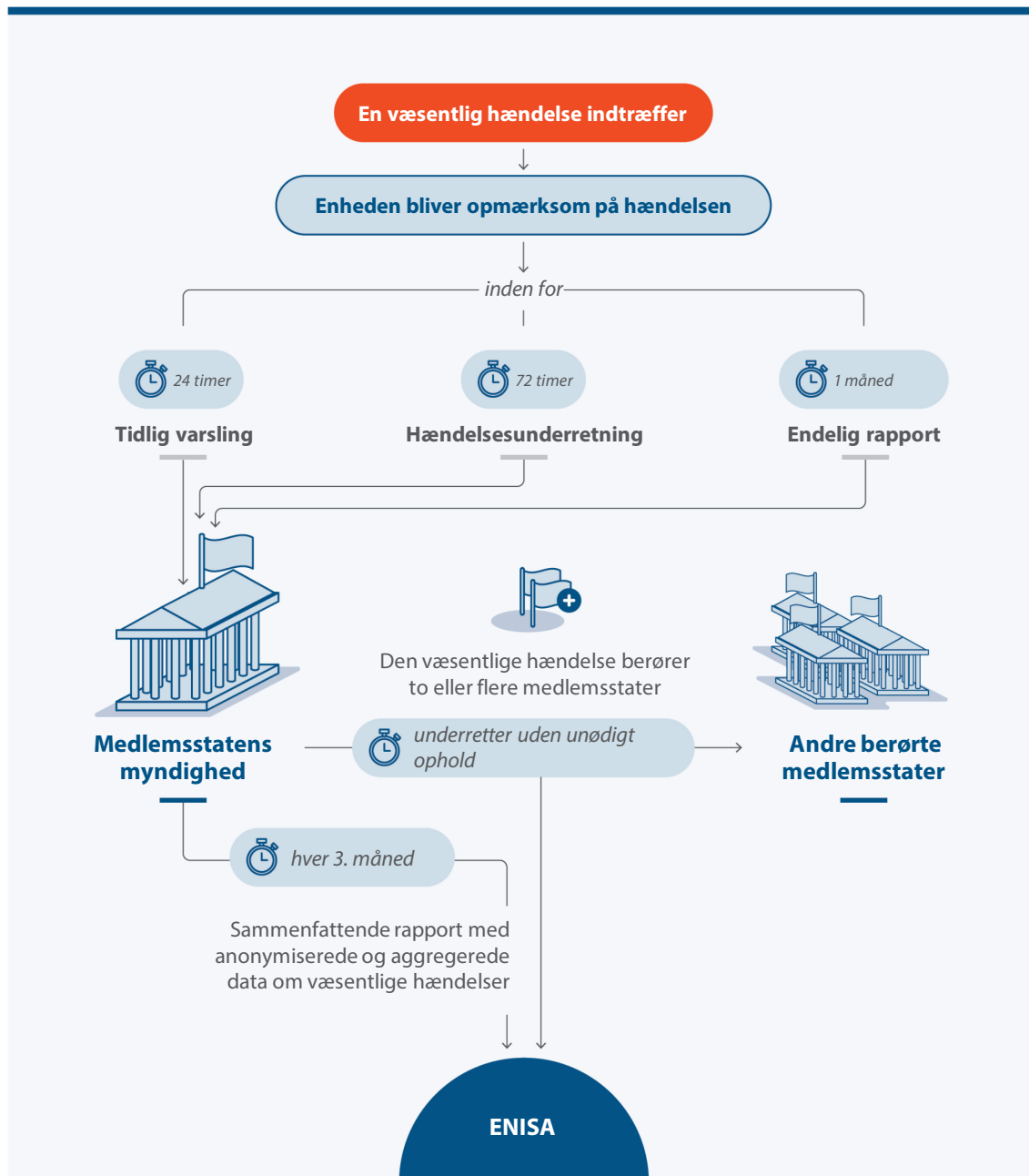
<sup>4</sup> ENISA, "[2024 Consolidated Annual Activity Report](#)", s. 33 og 36.

- 30** Selv om CSIRT-netværket og EU-CyCLONe officielt blev oprettet i henholdsvis 2016 og 2023, har disse to netværk dog endnu ikke formaliseret de proceduremæssige ordninger for, hvordan de skal samarbejde. De har heller ikke vedtaget kriterier for, hvornår CSIRT-netværket skal meddele EU-CyCLONe, at en observeret cybersikkerhedshændelse udgør en potentiel eller aktuel omfattende cybersikkerhedshændelse. Desuden mangler de to netværk at vedtage en fælles taksonomi for hændelsers alvor og at definere nøglebegreber - f.eks. "trussel", "trusselsaktør", "hændelse" og "effekt" - hvilket er nødvendigt for at muliggøre automatiseret udveksling af oplysninger. For nærværende er det et fortolkningsspørgsmål, hvornår en hændelse skal betragtes som væsentlig eller omfattende. Manglen på en fælles taksonomi blev nævnt af cybersikkerhedsmyndighederne i alle de tre medlemsstater, vi besøgte.

### **Begrænset informationsdeling og rapportering svækker netværkenes merværdi betydeligt**

- 31** Geografiske grænser forhindrer ikke cybersikkerhedshændelser og cyberangreb i at indtræffe og sprede sig. Det kan i væsentlig grad bidrage til øget cybersikkerhed, hvis medlemsstaterne deler oplysninger, f.eks. om de taktikker og teknikker, der anvendes af trusselsaktører, og om digitale tegn på indtrængen i et net eller informationssystem ("kompromitteringsindikatorer").
- 32** Vi konstaterede, at informationsdelingen var begrænset, og at dette svækker netværkenes merværdi betydeligt. De begrænsninger, vi konstaterede, var hovedsagelig forbundet med, at gennemførelsen af NIS 2-direktivet var forsinket, at der var problemer med at vurdere, om en hændelse havde grænseoverskridende virkninger, at den nationale sikkerhedslovgivning hæmmede informationsdeling, og at der var tillidsmangler. NIS 2-direktivet indfører adskillige rapporteringskrav for de omfattede enheder og for medlemsstaternes myndigheder, som vist i [figur 2](#).

**Figur 2 | Tidsramme for indberetning af hændelser i henhold til direktivet om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele EU (NIS 2-direktivet)**



Kilde: Revisionsretten, baseret på oplysninger fra ENISA.

- 33** Medlemsstaterne skulle senest i oktober 2024 [gennemføre NIS 2-direktivet](#) i national ret, men kun to overholdt denne frist. Forsinkelserne påvirker i væsentlig grad informationsdelingen, fordi de enheder, der er omfattet af NIS 2-direktivet, ikke er retligt forpligtet til at indberette hændelser, før direktivet er gennemført. Kommissionen har anslået<sup>5</sup>, at 15 500 enheder var omfattet af NIS-direktivet, mens over 110 000 er omfattet af NIS 2-direktivet. F.eks. var enheder i den offentlige forvaltning - som ifølge ENISA's [2025-rapport om trusselsbilledet](#) er den mest udsatte sektor i EU - ikke forpligtet til at indberette hændelser i henhold til NIS-direktivet.
- 34** Hændelsesdata indberettes til ENISA hver tredje måned (dvs. længe efter at hændelserne har fundet sted), hvilket begrænser dataenes merværdi. De anvendes hovedsagelig til statistik og rapportering om historiske tendenser, ikke til at sikre bedre opdagelse og reaktion. ENISA stiller et [onlineværktøj](#) til rådighed, som medlemsstaterne bruger til deres indberetninger. Indberetningsmodellen kræver et minimumssæt af data, f.eks. oplysninger om hændelsestypen og den berørte sektor. ENISA opfordrer desuden medlemsstaterne til at give yderligere oplysninger, som muliggør en mere dybtgående analyse af dataene, f.eks. ved at sammenkæde hændelserne med specifikke sårbarheder. Det er imidlertid ikke alle medlemsstater, der vælger at give sådanne oplysninger, hvilket i væsentlig grad svækker kvaliteten og merværdien af de indsamlede data.
- 35** ENISA anførte i sin [2024-rapport om cybersikkerhedssituationen i EU](#), at hændelserne sandsynligvis underrapporteres, da antallet af indberettede hændelser forekom at være lavt. I årene 2018-2021 indberettede medlemsstaterne årligt mellem 100 og 500 hændelser til ENISA. Antallet er steget gradvis, og i 2024 nåede det op på 1 276<sup>6</sup>.

---

<sup>5</sup> Europa-Kommissionen, [konsekvensanalyse](#), 2020.

<sup>6</sup> [CIRAS](#)-data for 2024.

- 36** I sin [2025-rapport om trusselsbilledet](#), som dækker perioden fra juni 2024 til juni 2025, identificerede ENISA ca. 4 800 cybersikkerhedshændelser<sup>7</sup> baseret på åbne kilder såsom nyhedsartikler. Ikke alle disse hændelser skulle være indberettet i henhold til NIS 2-direktivet, eftersom ENISA's dataindsamling dækkede et bredere spektrum af hændelser. Omvendt bliver mange væsentlige hændelser ikke omtalt i åbne kilder. Da de data, som medlemsstaterne indberetter, er anonymiseret, kan ENISA ikke sammenholde de hændelser, som det selv identificerer, med dem, som medlemsstaterne indberetter. Det er derfor ikke muligt at fastslå underrapporteringens omfang nøjagtigt, men efter vores opfattelse viser forskellen mellem det antal hændelser, der er indberettet af medlemsstaterne, og det antal, der er anført i rapporten om trusselsbilledet, at ikke alle væsentlige hændelser indberettes.
- 37** Et andet tegn på underrapportering er antallet af underretninger til andre berørte medlemsstater og til ENISA om væsentlige grænseoverskridende hændelser. Et underretningskrav fandtes allerede i NIS-direktivet, men det blev anset for at være ineffektivt, da Kommissionen i 2020 konkluderede<sup>8</sup>, at der sjældent blev sendt underretninger. Kommissionen tilskrev dette, at der manglede klare metoder til informationsdeling, og at der ikke var fastsat fælles mål, som tilskyndede til deling.
- 38** Forpligtelsen til at underrette andre medlemsstater er afgørende for at forhindre, at hændelser får afsmittende virkninger - manglende underretning påvirker EU's cybersikkerhed negativt. I 2025 blev kun 14 væsentlige grænseoverskridende hændelser rapporteret af syv medlemsstater. Medlemsstaterne rapporterede i 2024 to hændelser med mulige grænseoverskridende virkninger, ingen i 2023 og tre i 2022. Dette viser, at rapporteringen af væsentlige grænseoverskridende hændelser er meget lav og ikke afspejler det reelle antal af sådanne angreb. Til sammenligning identificerede ENISA i sin [2024-rapport om trusselsbilledet](#) 322 hændelser, der specifikt var rettet mod to eller flere medlemsstater. F.eks. var hændelsen vedrørende Collins Aerospace (jf. [tekstboks 1](#)) en hændelse, der ikke blev rapporteret, selv om den havde væsentlige grænseoverskridende virkninger.

---

<sup>7</sup> ENISA's [2025-rapport om trusselsbilledet](#).

<sup>8</sup> Europa-Kommissionen, [konsekvensanalyse](#), 2020.

## Tekstboks 1

### En cybersikkerhedshændelse forstyrrede lufthavnsdriften

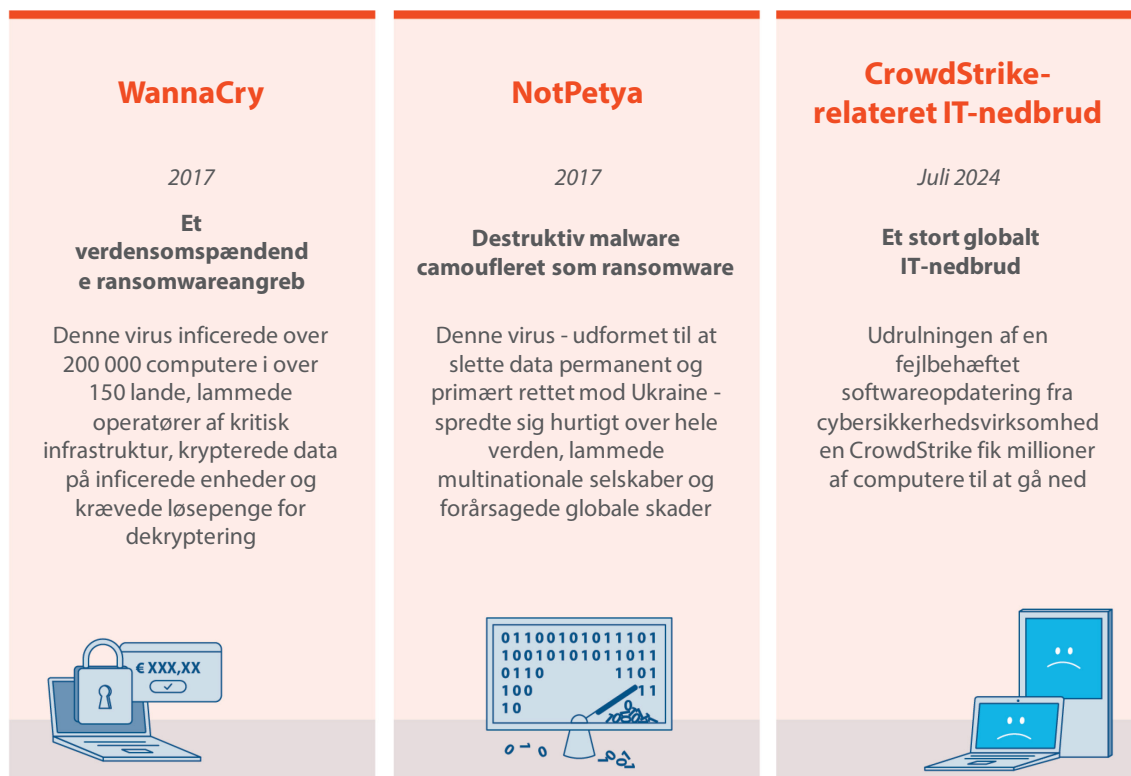
I september 2025 blev Collins Aerospace, som er en vigtig leverandør af teknologi til luftfartsindustrien, udsat for et væsentligt ransomwareangreb rettet mod selskabets passagerbehandlingssoftware. Angrebet tvang store europæiske lufthavne til at vende tilbage til manuel drift, hvilket forårsagede mange flyforsinkelser og aflysninger. Forstyrrelserne var værst i London Heathrow lufthavn, Bruxelles lufthavn, Berlin Brandenburg lufthavn og Dublin lufthavn.

I henhold til NIS 2-direktivet anses en hændelse for at være "væsentlig", hvis den f.eks. forårsager alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed. Alligevel behandlede ingen medlemsstater denne hændelse som en væsentlig eller omfattende grænseoverskridende hændelse. Der var derfor ingen af de berørte medlemsstater, der formelt underrettede ENISA eller andre medlemsstater om hændelsen. Endvidere underrettede CSIRT-netværket ikke EU-CyCLONe, som derfor ikke støttede den koordinerede håndtering af hændelsen.

*Kilde:* Revisionsrettens analyse baseret på interview med ENISA.

- 39** En anden årsag til den begrænsede rapportering af grænseoverskridende hændelser er, at det er op til de enkelte medlemsstaters myndigheder at afgøre, om en hændelse har grænseoverskridende virkninger, og at identificere de øvrige berørte medlemsstater. I forbindelse med nogle angreb har den indberettende enhed eller medlemsstatens myndighed måske ikke oplysninger nok til at vide, at der er grænseoverskridende virkninger. For nærværende findes der ingen EU-dækkende platform, som i realtid modtager hændelsesrapporter fra alle medlemsstaterne, og som kan sammenholde oplysninger om sektorer eller kompromitteringsindikatorer med henblik på opdagelse af grænseoverskridende hændelser. Der er derfor en betydelig risiko for, at nogle grænseoverskridende hændelser ikke bliver identificeret og rapporteret.
- 40** Siden 2016 har ingen medlemsstat anset en cybersikkerhedshændelse for at være "omfattende". Enhver hændelse, der har en væsentlig indvirkning på mindst to medlemsstater, er ellers i princippet omfattet af denne definition. Men selv cybersikkerhedshændelser, der har forårsaget globale nedbrud og betydelige skader - f.eks. som beskrevet i [figur 3](#) - er ikke blevet anset for at være omfattende. Som følge heraf er EU-CyCLONe's eskaleringsprocedure aldrig blevet aktiveret fuldt ud i forbindelse med en omfattende cybersikkerhedshændelse.

**Figur 3 | Eksempler på større cybersikkerhedshændelser**



Kilde: Revisionsretten, baseret på oplysninger fra [Cloudflare](#), [ENISA](#), [Europol](#), [Wired](#), [IBM](#) og [CrowdStrike](#).

- 41 Som supplement til enhedernes og medlemsstaternes rapporteringsforpligtelser blev CSIRT-netværket oprettet for at fremme informationsdeling. Tillid mellem medlemsstaterne er afgørende for CSIRT-netværket, hvor oplysninger udveksles på frivillig basis. Netværkets merværdi svækkes betydeligt, hvis medlemsstaterne ikke er villige til at udveksle rettidige og anvendelige oplysninger.
- 42 Informationsdelingen på EU-plan er begrænset af de enkelte medlemsstats nationale sikkerhedslovgivning. Hvis en medlemsstat vurderer, at cyberangrebsrelaterede oplysninger om en kritisk enhed er klassificerede, eller at rapportering om en specifik hændelse vil være til skade for den nationale sikkerhed, er den ikke forpligtet til at dele oplysningerne. Under vores besøg i medlemsstaterne udtalte repræsentanter for CSIRT-netværket og EU-CyCLONe, at informationsdeling kun kan ske inden for de grænser, der er fastsat i den nationale sikkerhedslovgivning. Der er ikke på EU-plan foretaget en analyse af medlemsstaternes nationale retlige rammer og disses betydning for informationsdelingen.

- 43** I 2016 bestod CSIRT-netværket af 28 nationale CSIRT'er med to repræsentanter pr. medlemsstat. Den mangelfulde informationsdeling har været et vedvarende problem. Kommissionen bemærkede således i sin [evaluering af NIS-direktivet](#), at medlemsstaterne ikke systematisk deler oplysninger med hinanden, og at dette navnlig forringer effektiviteten af cybersikkerhedsforanstaltningerne og niveauet af fælles situationsbevidsthed på EU-plan. Under NIS 2-direktivet har mange medlemsstater udpeget sektorspecifikke CSIRT'er ud over deres nationale CSIRT'er, så netværket er blevet udvidet betydeligt. På tidspunktet for vores revision bestod det af 42 CSIRT'er og over 700 individuelle deltagere. Dette gør det endnu mere udfordrende at opbygge tillid, da det er vanskeligt at opretholde tætte forbindelser mellem alle medlemmerne.
- 44** CSIRT-netværket er opmærksom på problemet vedrørende informationsdeling og overvejer forskellige tiltag, der kan øge tilliden i det voksende netværk. En alternativ metode til adressering af denne udfordring kunne være at skabe et EU-dækkende netværk bestående af mindre klynger af medlemsstater, som udgør grænseoverskridende knudepunkter, jf. beskrivelsen i punkt [62-74](#).

**De eksterne tjenesteyderes arbejde for cybersituationscentret overlapper delvis med eksisterende kapaciteter, og der er uklarhed om centrets fremtidige funktionsmåde**

- 45** I henhold til NIS 2-direktivet er Kommissionen medlem af EU-CyCLONe i tilfælde, hvor en potentiel eller igangværende omfattende cybersikkerhedshændelse har eller sandsynligvis vil have en betydelig indvirkning<sup>9</sup>. Denne nye rolle og udviklingen i trusselsbilledet fik Kommissionen til i 2022 at oprette en taskforce for cyberkoordinering i GD CNECT. Taskforcen omfatter et cybersituationscenter, som skal øge Kommissionens situationsbevidsthed og understøtte udførelsen af opgaver vedrørende dens institutionelle krisestyringsansvar. Centret skal også sætte GD CNECT i stand til at yde rådgivning på politisk plan.

---

<sup>9</sup> Artikel 16, stk. 2, i [NIS 2-direktivet](#).

- 46** Cybersituationscentrets drift varetages i vidt omfang af eksterne tjenesteydere, som Kommissionen i december 2022 indgik en 4-årig **kontrakt** med til en værdi af næsten 18 millioner euro. Vi vurderede centrets oprettelse, dets output og Kommissionens planer for dets fremtidige funktionsmåde.
- 47** En af kontrahenternes tjenesteydelser er et dashboard baseret på kommercielle cybertrusselsefterretningsfeeds, som muliggør visning og deling af trusselsoplysninger. Kontrahenterne udarbejder også forskellige efterretningsrapporter, herunder daglige og ugentlige rapporter, og tematiske rapporter om lande eller økonomiske sektorer. Det fysiske cybersituationscenter - et lokale med arbejdsstationer, som er forbundet med kontrahenternes dashboard - er placeret i en af Kommissionens bygninger. På tidspunktet for vores revision var cybersituationscentret bemanded af nogle få ansatte fra Kommissionen, som blev støttet af mange analytikere fra kontrahenterne samt af eksperter fra ENISA.
- 48** Vi konstaterede, at de eksterne tjenesteyderes arbejde for cybersituationscentret delvis overlapper med eksisterende kapaciteter i ENISA. ENISA har en fast kapacitet vedrørende situationsbevidsthed og trusselovervågning. Den offentliggør regelmæssigt rapporter om cybertrusler, herunder "flash reports" om specifikke hændelser og ugentlige rapporter med trusseloversigter. Rapporterne er baseret på åbne kilder og svarer til dem, der udarbejdes af kontrahenterne. Desuden udarbejder eller bidrager ENISA til højniveaubriefinger givet til politiske beslutningstagere i krisetider, som også svarer til output fra cybersituationscentret.
- 49** Hertil kommer, at de data, som cybersituationscentret anvender ved udarbejdelsen af sine rapporter, stammer fra kommercielle cybertrusselsefterretningsfeeds og svarer til de data, der anvendes af andre tjenestegrene i Kommissionen, f.eks. Generaldirektoratet for Digitale Tjenester og CERT-EU. Vi mener ikke, at cybersituationscentret er blevet etableret på en sådan måde, at der er tilstrækkelige muligheder for at opnå rationalisering ved at anvende allerede tilgængelige oplysninger fra Kommissionen og ENISA.
- 50** Kontrakten vedrørende cybersituationscentret udløber i december 2026, hvorefter kontrahenterne ikke længere vil levere de relaterede tjenesteydelser. Det drejer sig bl.a. om tilvejebringelse af data til dashboardet, udarbejdelse af trusselsrapporter og bemanning af de fleste stillinger i centret. Kommissionen vil overtage ansvaret for dashboardet, men det vil miste sin merværdi, hvis det ikke løbende ajourføres med cybertrusselsefterretninger.

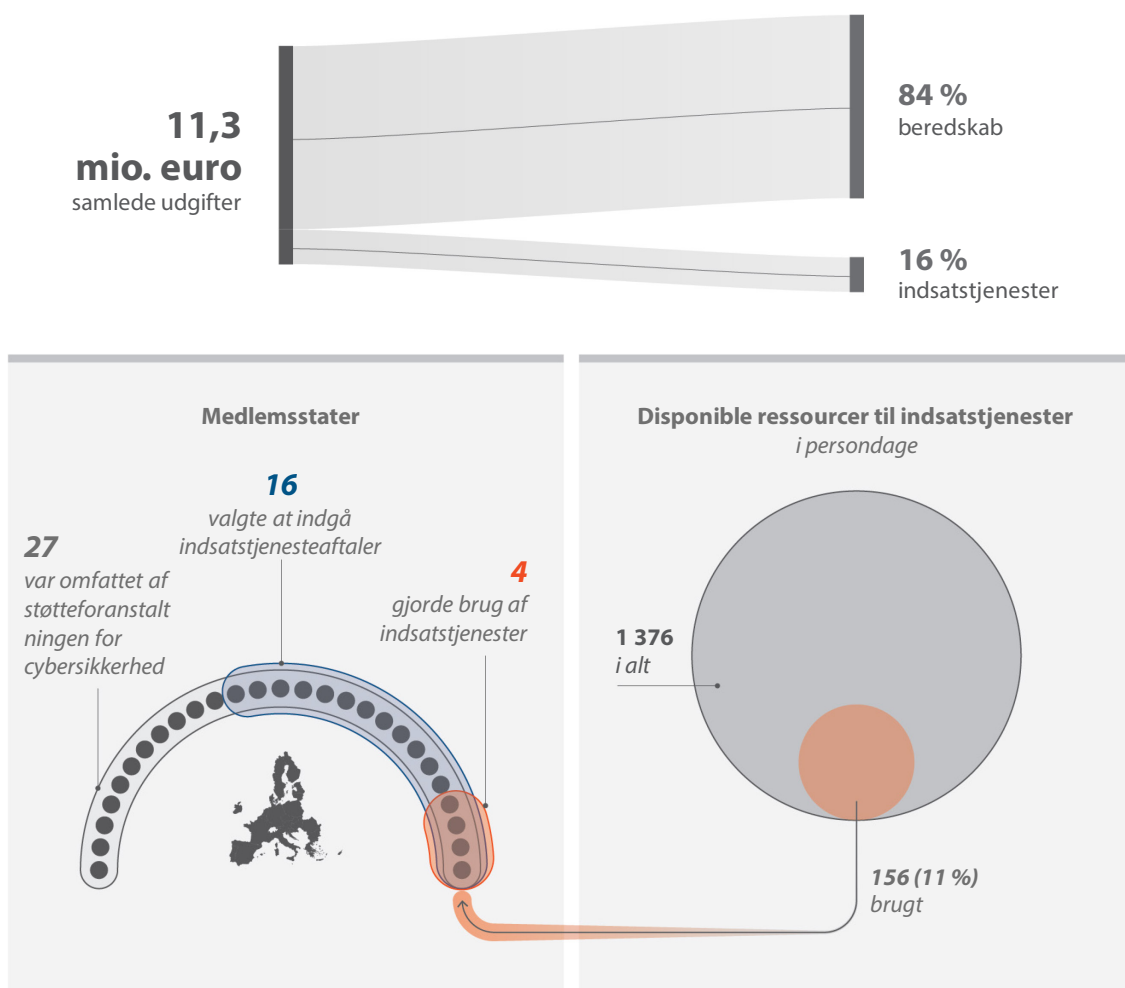
- 51** På tidspunktet for vores revision havde Kommissionen ingen planer for, hvad der efter kontraktens udløb skal ske med de eksterne tjenesteyderes støtte til cybersituationscentrets drift. Det forhold, at der mangler en omfattende, detaljeret plan for tiden efter kontraktens udløb, udgør efter vores mening en risiko vedrørende cybersituationscentrets drift efter 2026.

## **EU's cybersikkerhedsreserve muliggør hurtig levering af indsats tjenester**

- 52** Umiddelbart efter Ruslands militære aggression mod Ukraine og i erkendelse af, at omfattende cyberangreb er blevet mere udbredte, tildelte Kommissionen i 2022 ENISA 15 millioner euro i ekstraordinær finansiering til at udvikle [støtteforanstaltningen for cybersikkerhed](#), som blev iværksat i 2023. Kommissionen afsatte i 2023 yderligere finansiering (ca. 20 millioner euro) til at forlænge programmet indtil udgangen af 2026.
- 53** Kommissionen fremsatte desuden forslag til [forordningen om cybersolidaritet](#) - som blev vedtaget i december 2024 - med henblik på at sikre forberedelser på håndtering af omfattende cybersikkerhedshændelser. Ved forordningen oprettedes en EU-cybersikkerhedsreserve bestående af indsats tjenester fra betroede udbydere. Reserven blev gradvis operationel i 2025 med et budget på 36 millioner euro for perioden 2025-2027.
- 54** Vi vurderede etableringen af støtteforanstaltningen for cybersikkerhed, da den danner grundlag for EU's cybersikkerhedsreserve. Vi undersøgte også, om de erfaringer, der er gjort siden 2022, har bidraget til udformningen af EU's cybersikkerhedsreserve.
- 55** ENISA udformede støtteforanstaltningen for cybersikkerhed som en mekanisme til levering af tjenester med henblik på at støtte medlemsstaternes beredskab og indsats over for omfattende cybersikkerhedshændelser og -kriser. Der er i forvejen indgået kontrakt om samtlige tjenester, og udbydere kan derfor straks gå i gang, så snart medlemsstaterne har brug for det. Dette skyldes også ENISA's egen struktur, som sikrer, at der døgnet rundt er en medarbejder til rådighed til at behandle medlemsstaternes anmodninger.
- 56** ENISA valgte at fordele det disponible budget ligeligt mellem medlemsstaterne. I praksis iværksatte agenturet et åbent udbud opdelt i 27 delkontrakter, én pr. medlemsstat, med henblik på at udvælge op til tre private sikkerhedsudbydere, der skulle levere tjenester indtil udgangen af 2026. Derudover udvalgte ENISA under en paneuropæisk delkontrakt nogle udbydere, der skulle levere tjenester til støtteberettigede ikke-EU-lande og EU's institutioner, organer og agenturer eller støtte reaktioner på grænseoverskridende hændelser.

- 57** Denne metode indebærer, at ENISA kunne tage hensyn til specifikke nationale krav - f.eks. vedrørende sprog, nationale sikkerhedsgodkendelser eller forudgående tilstedeværelse i medlemsstaterne. Eftersom udbydere ikke blev udvalgt til at kunne levere tjenester i hele EU, er det på den anden side en væsentlig ulempe ved denne metode, at hvis en medlemsstat ikke gør brug af de tjenester, som der i forvejen er indgået kontrakt om, kan de afsatte midler til denne medlemsstat ikke bruges til at bistå en anden medlemsstat.
- 58** I forbindelse med støtteforanstaltningen for cybersikkerhed kunne medlemsstaterne vælge beredskabs- eller indsats tjenester eller en kombination af begge. Medlemsstaterne valgte primært at bruge de disponible midler på at forbedre deres beredskab (84 % af udgifterne i 2023). De medlemsstater, der valgte at indgå indsats tjenesteaftaler (dvs. foruddefinerede aftaler med udbydere, som sikrer umiddelbar adgang til disse tjenester vedrørende hurtig reaktion på cybersikkerhedshændelser), gjorde kun beskednen brug af dem, jf. figur 4. I de tre besøgte medlemsstater udtrykte myndighederne tilfredshed med ENISA's forvaltning af støtteforanstaltningen for cybersikkerhed.

**Figur 4 | ENISA's støtteforanstaltning for cybersikkerhed indtil 2023**



Kilde: Revisionsretten, baseret på data fra ENISA.

- 59** Kun ni medlemsstater har indgået indsats tjeneste aftaler for perioden 2024-2026. I vores interview med ENISA og myndighederne i de tre besøgte medlemsstater blev det bekræftet, at medlemsstaterne har en stærk præference for beredskabsaktiviteter.
- 60** EU's cybersikkerhedsreserve skal primært støtte håndtering af og genopretning efter større cybersikkerhedshændelser, men uudnyttede indsats tjenester fra reserven kan konverteres til beredskabstjenester. Denne fleksible tilgang kan forhindre, at der ikke gøres brug af forudbetalte tjenester.
- 61** Vi mener, at den valgte model til gennemførelse af EU's cybersikkerhedsreserve trækker på erfaringerne fra støtteforanstaltningen for cybersikkerhed. Dataene om anvendelsen af støtteforanstaltningen for cybersikkerhed indikerer dog en risiko for, at EU's cybersikkerhedsreserve hovedsagelig vil blive anvendt til beredskabs- i stedet for indsatsaktiviteter, hvilket er i strid med det formål, der er fastsat i forordningen om cybersolidaritet.

## **Det europæiske cybersikkerhedsvarslingssystem skal forbedre evnen til at opdage trusler, men det er ikke operationelt**

- 62** Et af de vigtigste mål for det europæiske cybersikkerhedsvarslingssystem er at tilskynde til meningsfuld informationsdeling med henblik på at forbedre evnen til at opdage, analysere og reagere på cybertrusler. Det er frivilligt at deltage i varslingssystemet, men de medlemsstater, der vælger at tilslutte sig et grænseoverskridende cyberknudepunkt, skal forpligte sig til at dele relevante oplysninger med de andre medlemmer. Ved at arbejde sammen i klynger i et pålideligt og sikkert miljø kan medlemsstaterne undgå nogle af de problemer vedrørende informationsdeling, der er beskrevet i punkt [31-44](#).
- 63** På tidspunktet for vores revision havde 13 medlemsstater valgt at deltage i det europæiske cybersikkerhedsvarslingssystem og oprettet to grænseoverskridende knudepunkter: ATHENA og ENSOC. Der var afsat midler til i 2026 at oprette et tredje grænseoverskridende cyberknudepunkt, NBCC, som bringer antallet af lande i systemet op på 20 (18 medlemsstater plus Island og Norge<sup>10</sup>), jf. [figur 5](#).

---

<sup>10</sup> Associerede lande i henhold til artikel 10, stk. 1, litra a), i forordning (EU) 2021/694.

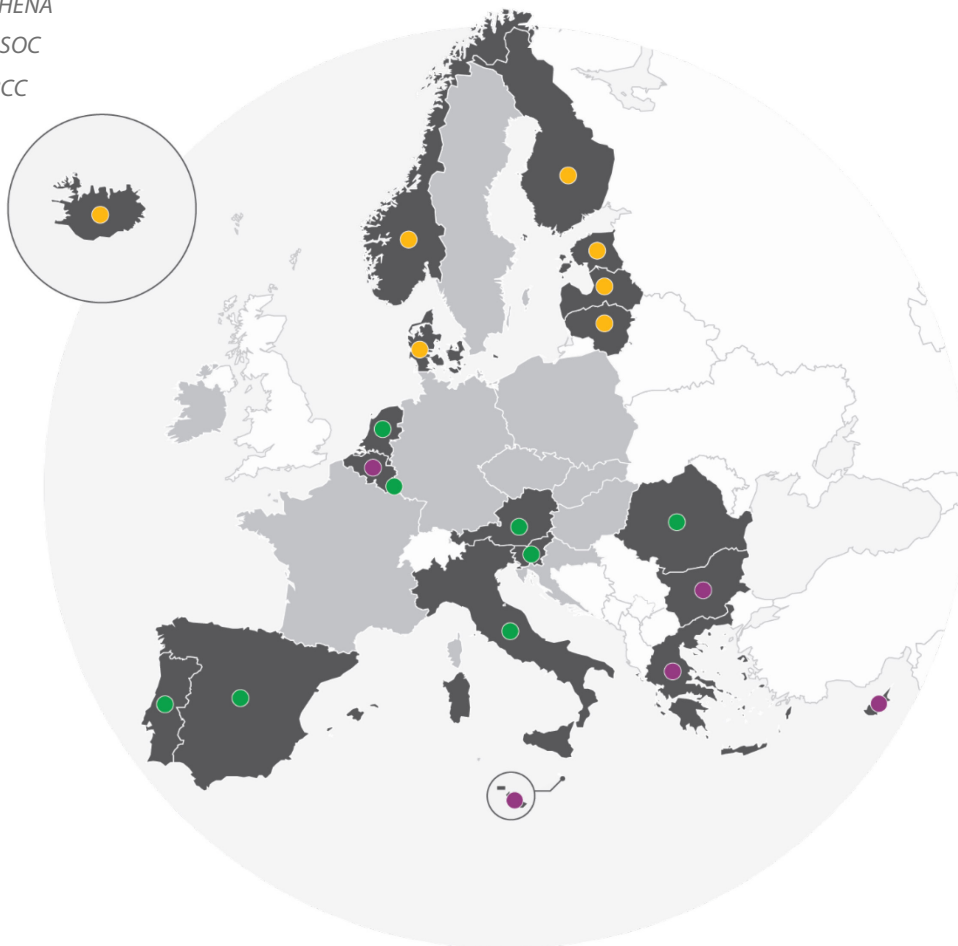
**Figur 5 | Lande i det europæiske cybersikkerhedsvarslingssystem**

■ Lande i det europæiske cybersikkerhedsvarslingssystem

● ATHENA

● ENSOC

● NBCC



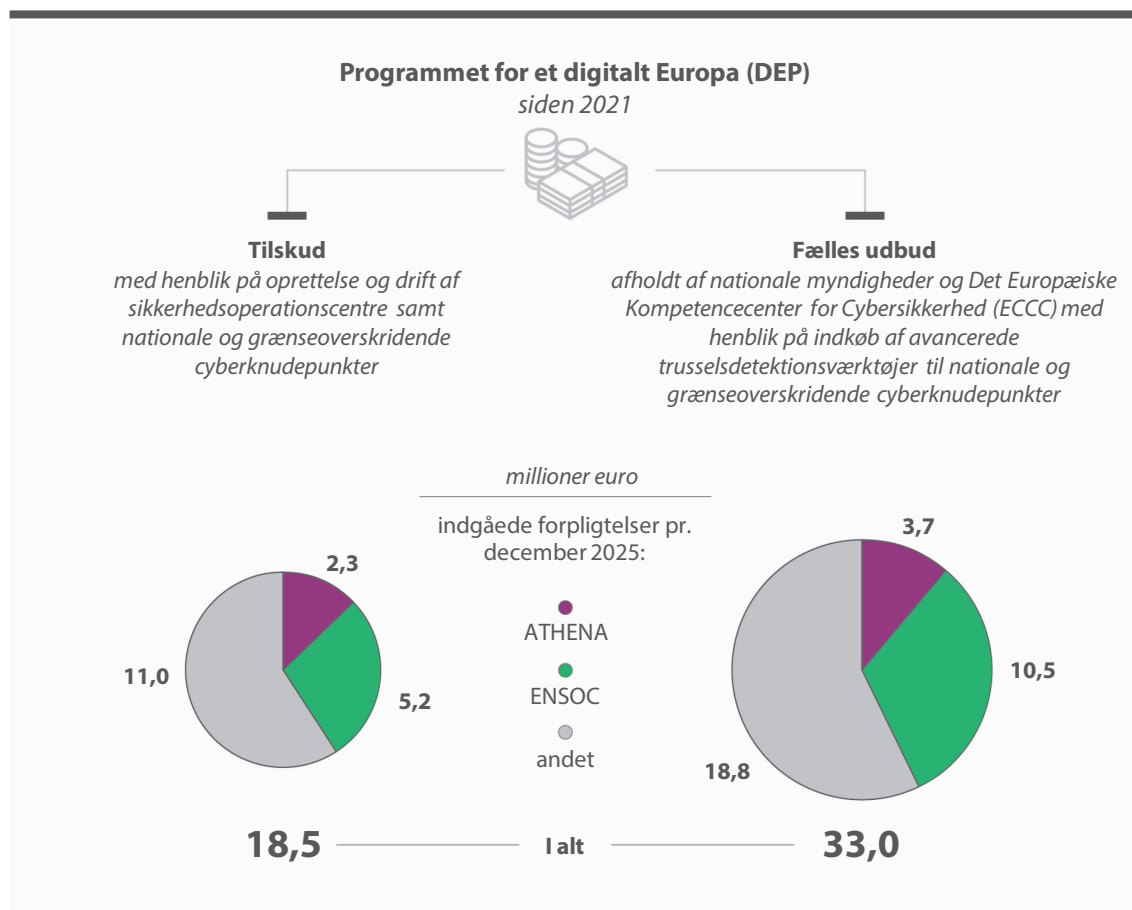
Kilde: Revisionsretten.

**64** Vi vurderede etableringen af de første to grænseoverskridende cyberknodepunkter og deres fremskridt med hensyn til at opfylde målene for det europæiske cybersikkerhedsvarslingssystem. Vi undersøgte også, hvordan oprettelsen af de grænseoverskridende cyberknodepunkter passer ind i det bredere cybersikkerhedslandskab, og hvordan de spiller sammen med de eksisterende netværk og strukturer.

## På grund af betydelige indkøbsforsinkelser er der endnu ikke opnået konkrete resultater

- 65** Siden 2021 har der under DEP kunnet ydes finansiering til at støtte oprettelse af nationale og grænseoverskridende cyberknodepunkter. Finansieringen ydes efter en kompleks procedure med to parallelle elementer: dels traditionelle tilskud til oprettelse og drift af knodepunkterne, dels fælles udbud med henblik på indkøb af avancerede trusselsdetektionsværktøjer, jf. [figur 6](#). Efter en indkaldelse af forslag i november 2022 påbegyndte ATHENA og ENSOC deres arbejde i januar 2024.

**Figur 6 | Finansiering af cyberknodepunkter fra programmet for et digitalt Europa**



Kilde: Revisionsretten, baseret på data fra ECCC.

- 66** De begrænsede udbud i to faser<sup>11</sup> blev tilrettelagt af medlemmerne af ATHENA og ENSOC i samarbejde med GD CNECT (første fase) og det nyoprettede ECCC (anden fase). Der anvendes to faser for at begrænse udbredelsen af følsomme oplysninger - det er kun ansøgere, som udvælges i første fase, der får de detaljerede tekniske specifikationer.
- 67** Første fase blev iværksat i maj 2024 vedrørende ENSOC og i juli 2024 vedrørende ATHENA. Interesserede virksomheder havde en måned til at ansøge. De udvalgte ansøgere blev imidlertid først underrettet om deres udvælgelse i april 2025, næsten et år efter iværksættelsen af udbuddene.
- 68** Desuden kunne hverken ENSOC's eller ATHENA's udbud gå videre til anden fase på dette tidspunkt, eftersom knudepunkternes medlemmer og ECCC stadig var ved at udarbejde de tekniske specifikationer, som de udvalgte virksomheder skulle opfylde ved afgivelsen af deres tilbud.
- 69** Anden fase blev først iværksat i august 2025 vedrørende nogle af ENSOC-delkontrakterne, og den skulle efter planen iværksættes i begyndelsen af 2026 vedrørende ATHENA. På tidspunktet for vores revision - 18 måneder efter iværksættelsen af udbuddene - var der ikke underskrevet nogen delkontrakter. Vi mener, at den mangelfulde forberedelse af udbuddene og disses kompleksitet var til hinder for, at de kunne afsluttes rettidigt.
- 70** Vi konstaterede følgelig, at de grænseoverskridende knudepunkter ikke er på rette vej til at opfylde deres mål. Uden værktøjer til at opdage trusler og udveksle oplysninger er de operationelt på standby, og det europæiske cybersikkerhedsvarslingssystem er endnu ikke i funktion, hvilket forsinker den konkrete udvikling af avanceret kapacitet til at opdage og forebygge cybertrusler og -hændelser. Der er foretaget ændringer med henblik på at forlænge tilskudsaftalens varighed i lyset af de hidtidige forsinkelser i udbuddene (15 måneder vedrørende ATHENA og 18 måneder vedrørende ENSOC).

---

<sup>11</sup> ENSOC's udbud og ATHENA's udbud.

## De grænseoverskridende cyberknodepunkter skaber nye kommunikationskanaler, som øger kompleksiteten

- 71** En af de grænseoverskridende cyberknodepunkters centrale opgaver er at dele relevante oplysninger for at sikre bedre opdagelse af og reaktion på trusler. Det kan f.eks. være oplysninger om cybertrusler, sårbarheder, kompromitteringsindikatorer og trusselsaktører. De grænseoverskridende cyberknodepunkters opgaver overlapper delvis med de opgaver, der udføres af de nationale CSIRT'er og CSIRT-netværket, navnlig hvad angår informationsdeling om cybertrusler og sårbarheder. Der er ingen klar rollefordeling mellem de grænseoverskridende cyberknodepunkter og CSIRT'erne. I henhold til cyberplanen fra 2025 (punkt 29) skal de grænseoverskridende cyberknodepunkter operere både på teknisk niveau (som de nationale CSIRT'er og CSIRT-netværket) og på operationelt niveau (som EU-CyCLONe).
- 72** Forordningen om cybersolidaritet fastsætter, at de grænseoverskridende cyberknodepunkter skal indgå samarbejdsaftaler med hinanden for at fremme informationsdeling. I henhold til denne forordning skulle ENISA senest i februar 2026 have udstedt retningslinjer for interoperabilitet mellem de grænseoverskridende cyberknodepunkter. I december 2025 fik et konsortium (som bl.a. omfatter ENSOC- og ATHENA-medlemmer) tildelt et ECCC-tilskud med henblik på udarbejdelse af en teknisk ramme for interoperabilitet mellem de grænseoverskridende cyberknodepunkter. Retningslinjerne og rammen vil dog først blive færdiggjort, når de grænseoverskridende cyberknodepunkter er operationelle. Som vi påpegede i vores udtalelse fra 2023 om forslaget til forordningen om cybersolidaritet<sup>12</sup>, kan det føre til parallel udvikling af inkompatible systemer og dermed øgede omkostninger, hvis der ikke hurtigt opnås enighed.
- 73** De grænseoverskridende cyberknodepunkter skal også uden unødigt forsinkelse dele relevante oplysninger om omfattende cybersikkerhedshændelser med EU-CyCLONe og CSIRT-netværket. På medlemsstatsniveau skaber oprettelsen af nationale cyberknodepunkter og deltagelsen i grænseoverskridende cyberknodepunkter således nye kommunikationslag. Koordineringen med ikke-EU-lande<sup>13</sup>, som ikke er medlemmer af CSIRT-netværket eller EU-CyCLONe, øger også kompleksiteten.

<sup>12</sup> Udtalelse 02/2023 om forslag til Europa-Parlamentets og Rådets forordning om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser, punkt 26.

<sup>13</sup> Island og Norge.

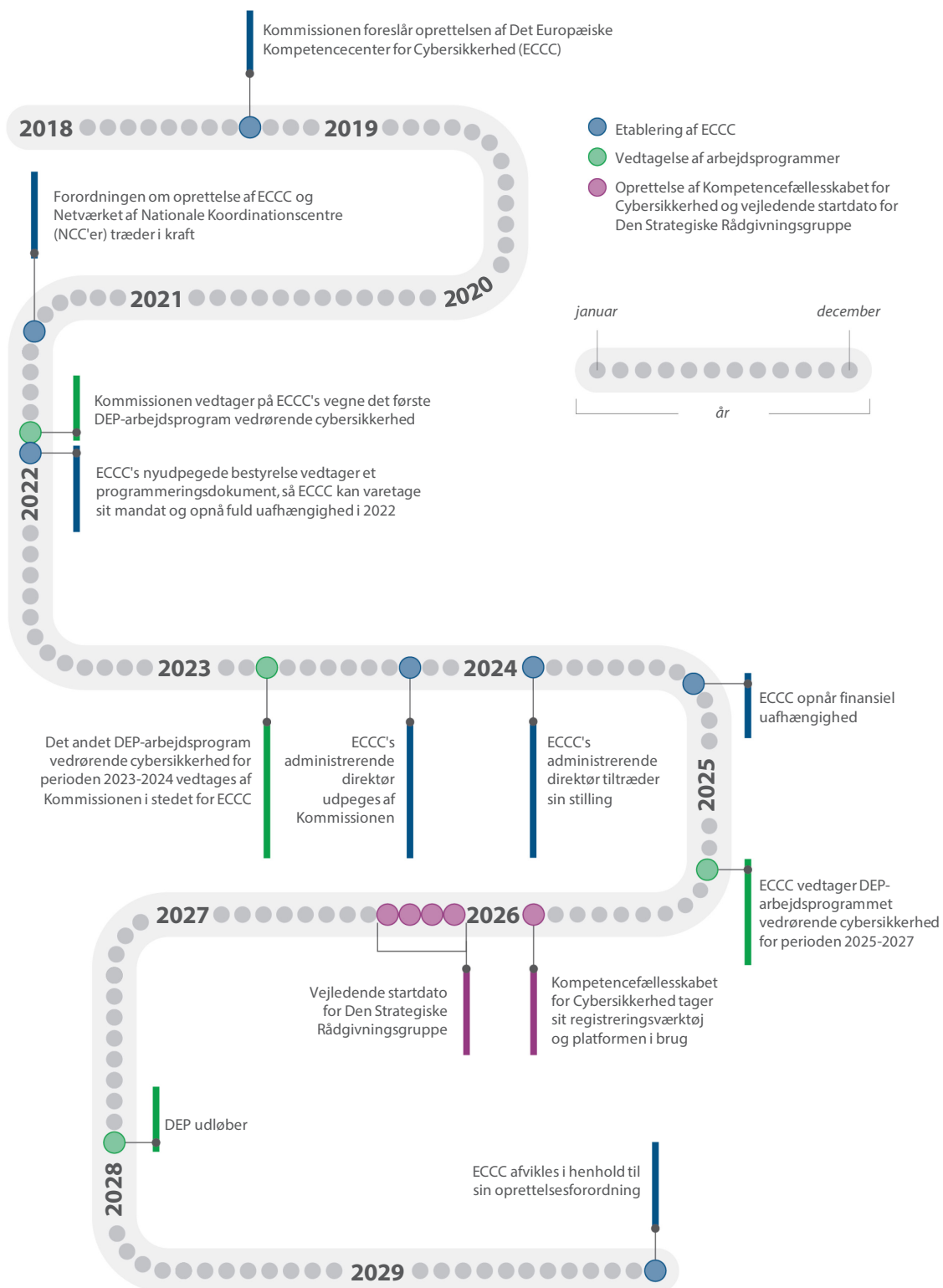
- 74** Det kræver klare samarbejdsaftaler at fastlægge en fælles taksonomi og regler for informationsdeling samt at sikre interoperabilitet. Erfaringerne fra CSIRT-netværket viser, at dette er en stor udfordring. Vi konstaterede, at der på tidspunktet for vores revision ikke var fastlagt nogen proceduremæssige ordninger vedrørende samarbejde og informationsdeling. Vi mener, at oprettelsen af nationale og grænseoverskridende cyberknudepunkter kan fremme mere effektiv informationsdeling. Men integreringen af de grænseoverskridende knudepunkter i det allerede komplekse cybersikkerhedslandskab vil være en udfordring og kræve nye kommunikationskanaler og samarbejdsordninger.

## De EU-finansierede DEP-projekter skal styrke cybersikkerheden, men har gennemførelses- og rapporteringsudfordringer

### Forsinkelser ved oprettelsen af Kompetencefællesskabet for Cybersikkerhed betød, at det ikke kunne bidrage til at forme DEP

- 75** Kommissionen foreslog i 2018, at der skulle oprettes et europæisk kompetencecenter for cybersikkerhed (ECCC) med henblik på at forvalte DEP's cybersikkerhedskomponent. I henhold til ECCC-forordningen skulle ECCC støttes af et netværk af 29 nationale koordinationscentre (NCC'er) - et for hver medlemsstat samt Island og Norge. Forordningen fastsatte også, at der skulle oprettes et kompetencefællesskab for cybersikkerhed bestående af repræsentanter for industrien, akademiske organisationer, forskningsorganisationer og andre relevante civilsamfundssammenslutninger.
- 76** Op til 20 medlemmer af kompetencefællesskabet skulle udgøre Den Strategiske Rådgivningsgruppe, som er det ene af ECCC's tre organer. En af Den Strategiske Rådgivningsgruppes opgaver er at organisere offentlige høringer for at indsamle input til ECCC's dagsorden og DEP's arbejdsprogrammer.
- 77** Vi vurderede, om DEP og dets arbejdsprogrammer blev vedtaget på grundlag af en grundig behovsanalyse, og om ECCC, NCC-netværket, Kompetencefællesskabet for Cybersikkerhed og Den Strategiske Rådgivningsgruppe kunne bidrage til arbejdsprogrammerne. I praksis er ECCC, NCC-netværket, kompetencefællesskabet og Den Strategiske Rådgivningsgruppe blevet oprettet gradvis over flere år (jf. [figur 7](#)).

**Figur 7 | Tidslinje for oprettelsen af Det Europæiske Kompetencecenter for Cybersikkerhed, Netværket af Nationale Koordinationscentre, Kompetencefællesskabet for Cybersikkerhed og Den Strategiske Rådgivningsgruppe**



Kilde: Revisionsretten.

- 78** Eftersom ECCC først blev fuldt operationelt i september 2024, vedtog Kommissionen på dets vegne arbejdsprogrammerne for perioderne 2021-2022 og 2023-2024. Da Kommissionen vedtog disse to arbejdsprogrammer, kunne den endnu ikke modtage input fra kompetencefællesskabet.
- 79** Medlemsstaterne begyndte at oprette deres NCC'er, der fungerer som kontaktpunkter for kompetencefællesskabet. DEP har medfinansieret oprettelsen og driften af NCC'erne - på tidspunktet for vores revision var der ydet over 90 millioner euro i EU-midler, herunder ca. 44 millioner euro, der skulle videreformidles som finansiel støtte til tredjeparter. Der er budgetteret med yderligere 38 millioner euro i NCC-støtte til og med 2027.
- 80** Vi konstaterede i december 2025 - fire år efter oprettelsen af ECCC og NCC-netværket - at kompetencefællesskabet endnu ikke var blevet oprettet, og at Den Strategiske Rådgivningsgruppe endnu ikke var blevet udpeget. ECCC vedtog den 14. marts 2025 det seneste DEP-arbejdsprogram vedrørende cybersikkerhed, der dækker perioden 2025-2027. ECCC udarbejdede og vedtog sit arbejdsprogram efter omfattende høringer af medlemsstaterne og NCC-netværket, men kunne endnu ikke modtage input og rådgivning fra kompetencefællesskabet og Den Strategiske Rådgivningsgruppe. Dette var i strid med bestemmelserne i ECCC's oprettelsesforordning, og vi betragter det som en forspildt mulighed.
- 81** DEP udløber i 2027, og ECCC forventes afviklet i 2029, hvis dets mandat ikke forlænges. Måske vil støtten fra NCC-netværket, kompetencefællesskabet og Den Strategiske Rådgivningsgruppe derfor kun være relevant i en kort periode, når den engang er på plads.

## De EU-finansierede projekter forfølger relevante mål, men mange af dem er ramt af operationelle problemer

- 82** Vi udtog en stikprøve på 11 projekter, som vedrørte opdagelse af og reaktion på cybersikkerhedshændelser, og som blev finansieret under DEP i perioden 2022-2025 (jf. [figur 5](#) i [bilag I](#) samt [bilag III](#)). Vi vurderede:
- om projekternes mål var i overensstemmelse med de ønskede resultater, der var beskrevet i indkaldelserne af forslag, og med DEP's overordnede mål
  - om projekterne indtil videre havde leveret de planlagte output og resultater
  - om projekterne havde leveret deres output til tiden.

Vi præsenterer resultatet af denne vurdering i [bilag IV](#).

## Nogle projekter viser tidlige resultater, men mange er ramt af operationelle udfordringer og forsinkelser

- 83** Vi konstaterede, at alle projekterne forfølger mål, der bidrager til at opfylde DEP's cybersikkerhedsmål<sup>14</sup>, og at de adresserer de fleste af målene i indkaldelserne af forslag<sup>15</sup>.
- 84** Af de 11 projekter i vores stikprøve befandt to sig på et tidligt gennemførelsesstadium, og vi kunne derfor ikke drage konklusioner om deres præstationer. Af de resterende vurderede vi, at fire på tilfredsstillende vis havde leveret deres planlagte output og resultater. Vi vurderede, at der var svagheder i to projekter, og at tre havde leveret utilfredsstillende præstationer (jf. [bilag IV](#)).
- 85** DEP har udtrykkeligt til formål at øge cybersikkerhedsniveauet i små og mellemstore virksomheder (SMV'er). Adskillige projekter tilbyder derfor konkrete løsninger for SMV'er (jf. [tekstboks 2](#)).

---

<sup>14</sup> Artikel 6 i [forordning \(EU\) 2021/694](#) om programmet for et digitalt Europa.

<sup>15</sup> Indkaldelser vedrørende: kapacitetsopbygning i sikkerhedsoperationscentre; etablering af Netværket af Nationale Koordinationscentre i medlemsstaterne; beredskabsstøtte og gensidig bistand; nye anvendelser af kunstig intelligens og andre støtteteknologier i sikkerhedsoperationscentre.

## Tekstboks 2

### Eksempler på projekter, der giver håndgribelige resultater for SMV'er

**GR-SME-SOC**-projektet (projekt 6 i [bilag III](#)) har til formål at sikre levering af cybersikkerhedsværktøjer og -tjenester til SMV'er i Grækenland ved oprettelse af et sikkerhedsoperationscenter (SOC), der er skræddersyet til deres behov. Projektet startede i januar 2024 og gennemføres af et konsortium bestående af fem græske organisationer. Planen er at tilbyde cybersikkerhedstjenester gratis til 120 SMV'er i et år, hvorefter tjenesterne vil blive kommercielt tilgængelige. Projektet tilbyder SMV'er avancerede tjenester såsom realtidsovervågning, AI-drevet trusselsdetektion og fleksibel reaktion på hændelser.

Under **NCC-IE**-projektet (projekt 3 i [bilag III](#)) ydede projektkoordinatoren ca. 1,8 millioner euro i tilskud til over 50 irske SMV'er med henblik på forbedring af deres cybersikkerhed. Tilskudsordningen omfattede virksomheder med fra 2 til ca. 200 ansatte, herunder familievirksomheder, nystartede virksomheder og globale eksportører i forskellige sektorer. Tilskuddene blev udelukkende givet til virksomheder, der tidligere havde været genstand for en cybersikkerhedsundersøgelse foretaget af det statslige agentur Enterprise Ireland. Tilskuddene dækkede 80 % af omkostningerne (op til 60 000 euro) ved at gennemføre anbefalingerne fra undersøgelsen.

Kilde: Revisionsretten.

- 86** I mange af projekterne i vores stikprøve er der problemer med at overholde fristerne eller operationelle udfordringer (jf. [bilag IV](#)). Vi konstaterede, at fire projekter er ramt af betydelige forsinkelser. Det gælder bl.a. ENSOC og ATHENA, jf. punkt [65-70](#). Vi beskriver de to andre projekter i [tekstboks 3](#).

### Tekstboks 3

#### Eksempler på projekter, der er ramt af operationelle udfordringer og forsinkelser

I Irland er Local Government Management Authority (LGMA) den eneste tilskudsmodtager vedrørende **ILG-SOC**-projektet (projekt 8 i **bilag III**). Formålet med projektet er at oprette et centralt sikkerhedsoperationscenter, som kan give 31 lokale myndigheder mulighed for at anvende avancerede værktøjer til opdagelse af og reaktion på trusler. Projektet startede i oktober 2023 med en varighed på tre år. Ved midtvejsevalueringen blev samtlige resultater fundet utilfredsstillende. Projektet omfatter adskillige udbud, som er slået fejl eller blevet forsinket. Projektet vil blive forlænget (uden yderligere finansiering), hvilket kan give mulighed for en vellykket afslutning.

I Grækenland har **EL-SOC**-projektet (projekt 5 i **bilag III**) til formål at oprette et konsolideret SOC på nationalt plan, som skal samle oplysninger fra sektorspecifikke SOC'er. Dette vil give et omfattende realtidsoverblik over cybersikkerhedssituationen. Projektet gennemføres fra januar 2024 til december 2026. Det planlagte indkøb af hardware og tjenesteydelser blev forsinket på grund af problemer med at færdiggøre og offentliggøre udbuddets tekniske specifikationer. Ifølge projektkoordinatoren skyldtes forsinkelsen også, at der var problemer med hensyn til at sikre national medfinansiering, og at der var for få ansatte til at forvalte udbuddet.

Kilde: Revisionsretten.

- 87** Yderligere to projekter i vores stikprøve er ramt af moderate forsinkelser. Tre projekter har leveret deres output til tiden. Endelig befinder to projekter sig på et tidligt gennemførelsesstadium, og vi kan derfor ikke drage konklusioner om dem.

#### Sikkerhedsrestriktioner har ført til operationelle udfordringer, og der er betydelige risici, når tilskudsmodtagere selv står for kontrollen

- 88** DEP-forordningen fastsætter, at finansiering til cybersikkerhed af sikkerhedsmæssige årsager kan forbeholdes enheder, der er etableret i EU og kontrolleres af en medlemsstat eller af EU-borgere. Formålet med denne restriktion er at mindske risikoen for indtrængen eller påvirkning fra ikke-EU-landes side og at forhindre, at følsomme sikkerhedsoplysninger deles med myndigheder i ikke-EU-lande.

- 89** Kravet om EU-ejerskab og -kontrol gælder ikke kun tilskudsmodtagere, men også deres underleverandører og eventuelle modtagere af finansiel støtte til tredjeparter. Undtagen vedrørende sidstnævnte kategori (jf. punkt [92-96](#)) vurderes det af den centrale valideringstjeneste i [Det Europæiske Forvaltningsorgan for Forskning](#), om kravet er overholdt. Den endelige afgørelse om en enheds berettigelse til at deltage i et begrænset udbud træffes dog af den tildelende myndighed, dvs. GD CNECT eller ECCC.
- 90** Under vores revisionsarbejde omtalte tilskudsmodtagerne gentagne gange de praktiske udfordringer i forbindelse med ejerskabs- og kontrolvurderinger. Det kan være en kompleks og langvarig proces at vurdere, om en enhed er EU-ejet og -kontrolleret. Der skal foretages en analyse af hele enhedens ejerskabsstruktur og af kontrolkæden i hvert ejerskabslag helt op til de reelle ejere. Den centrale valideringstjeneste kræver, at hver enhed fremlægger omfattende [dokumentation](#) vedrørende ejerskabsstruktur og specifikke rettigheder, virksomhedsledelse og eventuelle kommercielle, finansielle eller andre forbindelser, der giver kontrol.
- 91** I tre EU-finansierede projekter i vores stikprøve var der foretaget efterfølgende udelukkelse af mindst én tilskudsmodtager i et konsortium, fordi de pågældende enheder vurderedes at være ejet eller kontrolleret fra lande uden for EU. Denne udelukkelse af konsortiemedlemmer viser, at begrebet EU-ejerskab og -kontrol ikke forstås fuldt ud af alle DEP-deltagere. Ifølge data fra den centrale valideringstjeneste vedrørende DEP-tilskud til cybersikkerhed i perioden 2022-2025 fik i alt 7 % af alle ansøgere og underleverandører en negativ vurdering. Det fører til forsinkelser, når uberettigede ansøgere deltager i indkaldelser af forslag, jf. eksemplet i [tekstboks 4](#).

#### Tekstboks 4

##### Eksempel på et tilfælde, hvor tilskudsmodtagere blev udelukket efter en negativ sikkerhedsvurdering

To medlemmer af konsortiet bag [NG-SOC](#)-projektet (projekt 7 i [bilag III](#)) fik en negativ ejerskabs- og kontrolvurdering. Resultatet blev meddelt ca. en måned før fristen for tilskudsafतालens indgåelse. Projektkoordinatoren måtte acceptere at overtage det arbejde, der skulle være udført af de to udelukkede medlemmer, da der ikke var tid til at finde en ny partner. Det ene af de udelukkede medlemmer tilhørte en specifik industri, hvor den udviklede løsning skulle afprøves. En betydelig del af projektet, som vedrørte afprøvning af løsningen i praksis, kunne derfor ikke gennemføres som planlagt. Denne situation blev senere afhjulpet ved at ændre tilskudsafतालen, så nye medlemmer kunne indtræde.

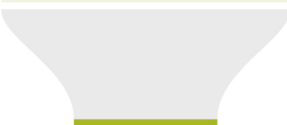
- 92** To af de projekter, vi undersøgte (NCC-IE og CYberSynchrony), yder finansiel støtte til tredjeparter. Denne finansieringsmekanisme gør det muligt for tilskudsmodtagere at bruge en del af deres tilskudsmidler på at finansiere andre enheder via åbne indkaldelser. Finansiel støtte til tredjeparter kan give disse adgang til EU-finansiering. I forbindelse med denne type støtte er tilskudsmodtagerne eneansvarlige for ejerskabs- og kontrolvurderingerne, og den centrale valideringstjeneste involveres ikke.
- 93** Kommissionen offentliggjorde en generel vejledning for deltagere i begrænsede udbud i 2021 og ajourførte den i 2026. Selv om muligheden for finansiel støtte til tredjeparter har eksisteret i forbindelse med DEP-indkaldelser siden 2021, har hverken Kommissionen eller ECCC udarbejdet en detaljeret metode, som tilskudsmodtagerne skal følge, når de udfører ejerskabs- og kontrolvurderinger af de tredjeparter, som de yder finansiel støtte. ECCC sendte i juli 2025 NCC-netværket en ikkeobligatorisk vejledning med en struktureret tilgang til udførelse af ejerskabs- og kontrolvurderinger. Vejledningen indeholder generelle principper og beskriver skridt, der kan tages. Den angiver imidlertid ikke specifikt, hvordan vurderingerne skal udføres, og det er således tilskudsmodtagernes eget ansvar at udvikle en metode.
- 94** Vi konstaterede, at ECCC hverken validerer de udviklede metoder eller foretager stikprøvebaseret kontrol for at sikre, at de er robuste nok, og at de udvalgte modtagere af finansiel støtte faktisk er EU-ejede og -kontrollerede.
- 95** I vores [årsberetning for 2024](#) bemærkede vi, at de tilskudsmodtagere, der af Kommissionen havde fået til opgave at forvalte finansiel støtte til tredjeparter (på forskningsområdet), ikke havde pligt til at dokumentere effektiviteten af den kontrol, som de udfører for at sikre, at EU-udgifterne er formelt rigtige. Tilsvarende vurderer ECCC ikke, om tilskudsmodtagerne har den nødvendige administrative og tekniske kapacitet til at udføre ejerskabs- og kontrolvurderinger. Som beskrevet i punkt [90](#) kan der være tale om en kompleks opgave, som på EU-plan udføres af en særlig tjeneste med specialiseret ekspertise.
- 96** I lyset af dette er der efter vores opfattelse en betydelig risiko for, at tilskudsmodtagerne - som er ansvarlige for at udføre ejerskabs- og kontrolvurderinger - ikke har den nødvendige kapacitet til at udføre dem korrekt. Grundet de finansierede aktiviteter karakter kan denne svaghed føre til eksponering af følsom infrastruktur, operationelle data og sikkerhedskritiske teknologier.

## De fleste EU-finansierede projekter har utilstrækkelige præstationsrammer, og DEP's cybersikkerhedsrelaterede præstationsdata er ikke nøjagtige

De fleste EU-finansierede projekter har utilstrækkelige præstationsrammer

- 97** Tilskudsmodtagere, der forvalter EU-finansierede projekter, skal rapportere til ECCC om deres fremskridt og resultater med henvisning til delmål, leverancer og indikatorer, jf. [figur 8](#). Vi vurderede, om de enkelte projekters fastsatte delmål og leverancer muliggør tilstrækkelig overvågning. Vi vurderede også, om deres præstationsindikatorer er relevante og målbare og har et referencescenario og et mål.

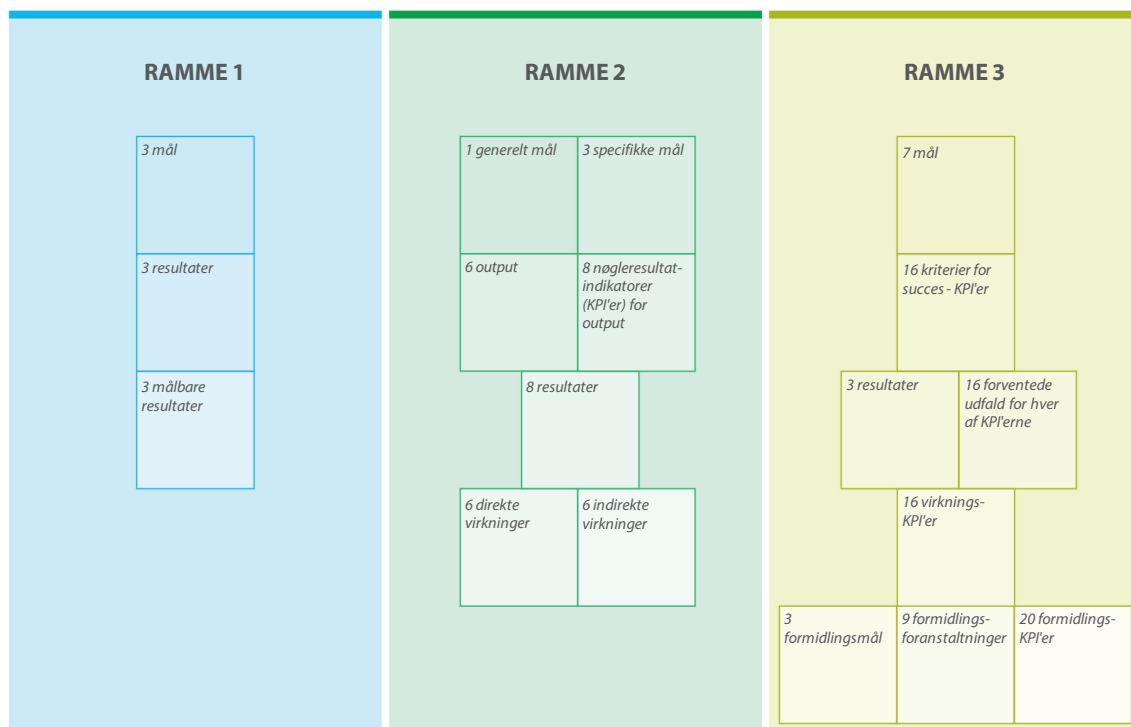
**Figur 8 | Delmål, leverancer og præstationsindikatorer i DEP-projekter**

|                     |  <b>Delmål</b>                                                                 |  <b>Leverancer</b> |  <b>Præstationsindikatorer</b>  |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Definition</b>   | kontrolpunkter gennem hele projektet, der bruges til at kortlægge fremskridt                                                                                    | projektoutput, der fremlægges for at vise fremskridt                                                | bruges til at måle resultater                                                                                      |
| <b>Fastsættelse</b> | kun knyttet til større output (begrænset antal)                                                                                                                 | kun større output (højest 10-15 pr. projekt)                                                        | specifikke, målbare, opnåelige, relevante og tidsbestemte                                                          |
| <b>Eksempler</b>    | "iværksættelse af platformens pilotfase"                                                                                                                        | "brugervejledning til platformen"                                                                   | "30 % reduceret reaktionstid ved hændelser"                                                                        |
|                     |  <b>Struktureret tilgang, del af onlinesystemet til tilskudsforvaltning</b> |                                                                                                     |  <b>Ustruktureret tilgang</b> |

Kilde: Revisionsretten, baseret på [tilskudsansøgningsskemaet](#).

- 98** I deres projektforslag skal tilskudsmodtagerne fastsætte en række delmål og leverancer ved anvendelse af en struktureret tilgang, som er angivet i ansøgningsinstrukserne. Alle delmål og leverancer registreres i onlinesystemet til tilskudsforvaltning, så det er let at følge op på dem. ECCC gennemgår normalt hvert projekt to gange: halvvejs i gennemførelsen og efter afslutningen. Ved disse gennemgange kontrollerer eksterne eksperter opfyldelsen af delmål og leverancer, og ECCC validerer kontrolresultaterne. Delmål og leverancer er således afgørende for projektovervågningen og bør fastsættes korrekt.
- 99** Vi konstaterede, at instrukserne vedrørende antallet af delmål og leverancer næsten ikke er fulgt i nogen af projekterne i vores stikprøve: Antallet af delmål pr. projekt varierer fra 8 til 39, mens antallet af leverancer varierer fra 8 til 45. Mange af delmålene og leverancerne er ikke udformet efter instrukserne og kan derfor ikke anvendes til måling af fremskridt (f.eks. "møde for at iværksætte udarbejdelsen af indkaldelsen af forskningsforslag" eller "formelle referater fra projektmøder"). Vedrørende tre projekter havde evalueringsudvalget identificeret disse problemer før underskrivelsen af tilskudsftalen. To tilskudsmodtagere foreslog kun mindre ændringer (f.eks. af datoer) uden at adressere de egentlige problemer, og den tredje foretog ingen ændringer. Med hensyn til seks andre projekter i vores stikprøve viser vores analyse, at delmålene og leverancerne ikke er udformet efter instrukserne og ikke altid er anvendelige. Efter vores opfattelse gør det overvågningen af fremskridt vanskelig, hvis delmålene eller leverancerne er dårligt udformet, eller hvis der er for mange.
- 100** I modsætning til delmål og leverancer fastsættes præstationsindikatorer ikke ved anvendelse af en struktureret tilgang, og de registreres ikke i en tabel i tilskudsforvaltningssystemet, men optræder i stedet spredt omkring i projektforslagene. På grund af denne tilgang har tilskudsmodtagerne foreslået vidt forskellige præstationsrammer. Nogle omfatter kun projektmål knyttet til præstationsindikatorer, mens andre er meget mere komplekse. Vi giver nogle eksempler i [figur 9](#).

**Figur 9 |** Eksempler på uensartetheden af projekternes præstationsrammer



Kilde: Revisionsretten.

**101** Vores analyse viser, at mange af de præstationsindikatorer, der anvendes i projekterne, ikke er relevante eller målbare, og at de mangler et mål eller et referencescenario (jf. [tekstboks 5](#)). Desuden er der i syv projekter fastsat 20 indikatorer eller derover, og i ét projekt er der 52. Vi præsenterer resultatet af vores vurdering i [bilag IV](#).

## Tekstboks 5

### Eksempler på utilstrækkelige præstationsindikatorer

#### Ikke målbare:

- "Kompromitteringsindikator og andre leverede tjenester styrker SMV'ernes cybersikkerhedskapacitet"
- "Levering af værktøjer og metoder til reaktion på hændelser, som muliggør integration med EU-CyCLONe-kommunikationskanaler"

#### Mangler referencescenario eller mål:

- "≥ 20 % forbedring af personalets beredskab"
- "≥ 20 % reduktion af den indsats, det kræver at følge og overholde relevante EU-cybersikkerhedsinitiativer"

#### Ikke præstationsrelaterede:

- "Endelig rapport om projektet ved finansieringsfasens udløb"
- "Antal praktikanter, der vil deltage i alle kurser"

Kilde: Revisionsretten, baseret på projektdokumentation.

**102** Samlet set mener vi, at det komplicerer præstationsovervågningen betydeligt, at præstationsrammerne er meget uensartede, samt at indikatorerne er dårligt udformet, og at der er for mange af dem. Det er derfor ikke muligt at foretage en hensigtsmæssig vurdering af projekternes præstation. Opgaven kompliceres yderligere af, at rapporteringsmodellen ikke indeholder et særligt afsnit om projekternes præstationsindikatorer, og at der vedrørende de fleste af projekterne i vores stikprøve derfor ikke blev rapporteret om dem.

## Præstationsdataene om DEP's cybersikkerhedskomponent er ikke nøjagtige

- 103** Med henblik på overvågning af DEP's resultater fastsætter forordningen programindikatorer, som der skal rapporteres om i forbindelse med alle projekter, jf. [tekstboks 6](#).

### Tekstboks 6

#### DEP-indikatorer vedrørende cybersikkerhed

1.a Antal cybersikkerhedsinfrastrukturer eller værktøjer eller begge dele, som er indkøbt i fællesskab, herunder inden for rammerne af det europæiske cybersikkerhedsvarslingssystem

1.b Antal cybersikkerhedsinfrastrukturer eller værktøjer eller begge dele, som er taget i brug

2. Antal brugere og brugersamfund, som får adgang til europæiske cybersikkerhedsfaciliteter

3. Antal foranstaltninger til støtte for beredskab og reaktion på cybersikkerhedshændelser inden for rammerne af cyberberedskabsmekanismen

Kilde: Bilag II til [forordning \(EU\) 2021/694 om programmet for et digitalt Europa](#) og "Monitoring and Evaluation Framework for the Digital Europe Programme" ([SWD\(2024\) 37](#)).

- 104** Vi vurderede, om der i forbindelse med projekterne i vores stikprøve var blevet rapporteret om disse indikatorer, og undersøgte, hvordan ECCC indsamler og kontrollerer de pågældende data.
- 105** For alle projekter skal der i tilskudsforvaltningssystemet rapporteres om DEP-indikatorerne før midtvejsevalueringen og den endelige evaluering. Der burde være rapporteret om disse indikatorer vedrørende syv projekter, som under vores revision var halvvejs i deres tidsplan, men vi konstaterede, at det kun var sket vedrørende tre. For to af disse tre projekter var der rapporteret unøjagtige oplysninger: Vedrørende det ene var der rapporteret om den forkerte indikator, og vedrørende det andet var der rapporteret målværdier i stedet for opnåede resultater.

**106** Hvert år rapporterer Kommissionen om disse indikatorer i sine [programgennemførelseserklæringer](#). Dette gør det muligt for interessenter at vurdere, om programmet opfylder sine mål. Ifølge programgennemførelseserklæringerne for 2024 er der gjort tilfredsstillende fremskridt med DEP-indikatorerne vedrørende cybersikkerhed. ECCC forklarede os, at det havde beregnet indikatorerne på grundlag af en række spørgeundersøgelser henvendt til tilskudsmodtagerne i stedet for at basere dem på tilskudsforvaltningssystemet. Vi gennemgik de disaggregerede data, som vi modtog fra ECCC, og konstaterede talrige problemer med hensyn til den måde, hvorpå dataene blev indsamlet, og deres samlede kvalitet. Vi konstaterede, at de indsamlede data ikke passer sammen med værdierne i programgennemførelseserklæringen, og det er således uklart, hvordan de rapporterede værdier er blevet beregnet. Vi fandt ingen dokumentation for, at nøjagtigheden af de rapporterede data var blevet kontrolleret af ECCC. På baggrund af vores kontrol af projekterne i vores stikprøve mener vi ikke, at de rapporterede data afspejler de opnåede resultater korrekt, eftersom de fleste værdier mangler eller er unøjagtige.

Vedtaget af Afdeling III, der ledes af George-Marius Hyzler, medlem af Revisionsretten, i Luxembourg på mødet den 16. juni 2026.

*På Revisionsrettens vegne*

Tony Murphy  
*Formand*

# Bilag

## Bilag I - Om revisionen

- 01** Cybersikkerhed er defineret som "de aktiviteter, der er nødvendige for at beskytte net- og informationssystemer, brugerne af sådanne systemer og andre personer berørt af cybertrusler"<sup>1</sup>. En cybertrussel er "enhver potentiel omstændighed, begivenhed eller handling, som kan skade, forstyrre eller på anden måde have en negativ indvirkning på net- og informationssystemer, brugerne af sådanne systemer og andre personer"<sup>2</sup>. Cybersikkerhed kræver en holistisk tilgang bestående af en række indbyrdes forbundne aktiviteter, der gør det muligt at forebygge, opdage, reagere på og sikre genopretning efter cybertrusler, jf. *figur 1*.

---

<sup>1</sup> Forordning (EU) 2019/881 ([forordningen om cybersikkerhed](#)).

<sup>2</sup> Artikel 2 i [forordningen om cybersikkerhed](#).

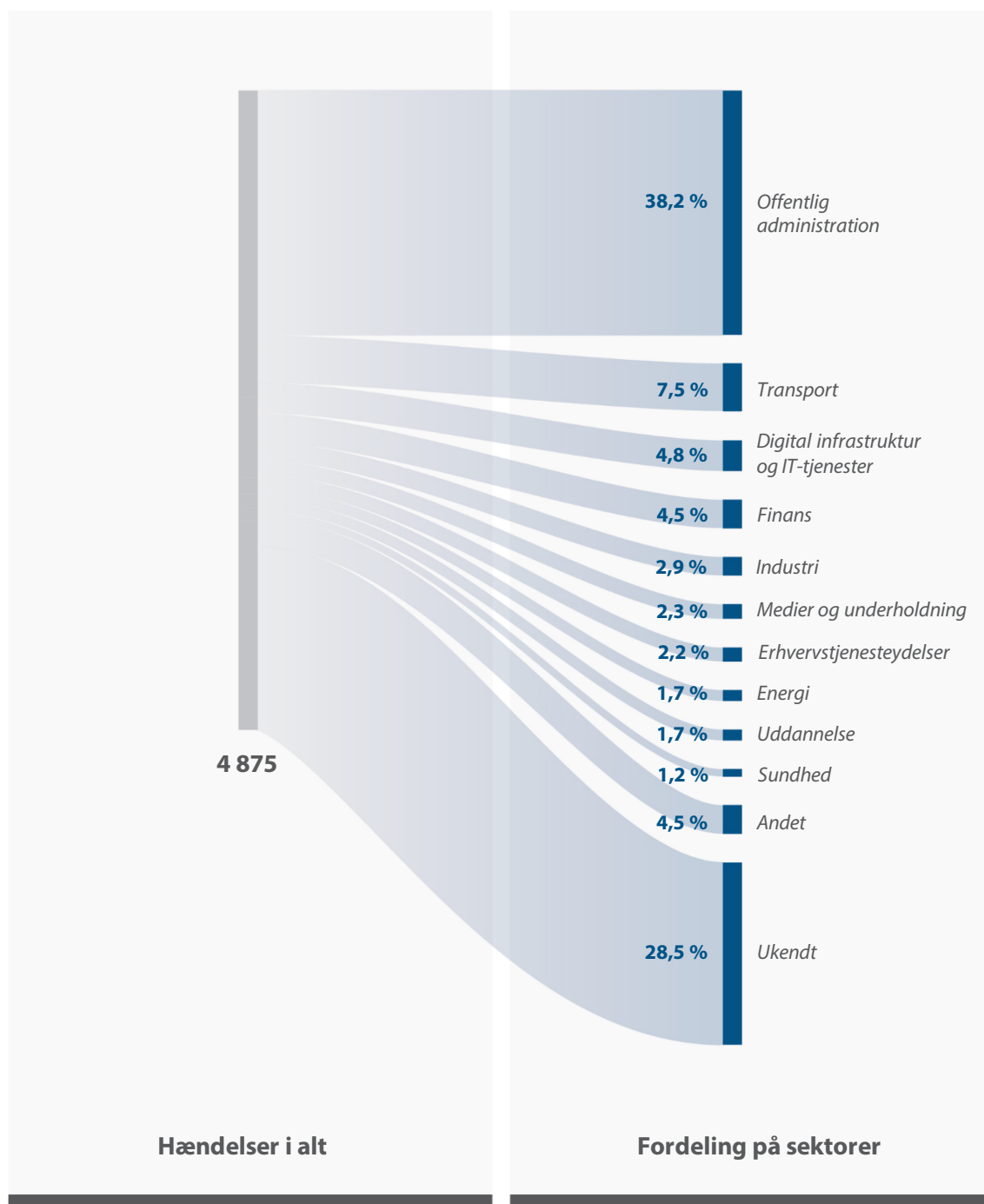
**Figur 1 | Eksempler på cybersikkerhedsaktiviteter**

|                                                                                                                |                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Forebyggelse</b></p>    | <p><b>Reducere risikoen for cybersikkerhedshændelser og minimere deres potentielle effekt</b></p> <p><i>Eksempler: antivirus, firewalls, kryptering, tofaktorgodkendelse, styring af softwareopdateringer, kurser i sikkerhedsbevidsthed for personale</i></p>             |
| <p><b>Opdagelse</b></p>       | <p><b>Opdage ondsindet aktivitet</b></p> <p><i>Eksempler: netværksovervågning, situationsbevidsthed</i></p>                                                                                                                                                                |
| <p><b>Reaktion</b></p>       | <p><b>Håndtere og afbøde en cybersikkerhedshændelse ved at inddæmme truslen og forebygge yderligere skade</b></p> <p><i>Eksempler: fjernelse af trussel, inddæmning ved isolering af servere, deaktivering af kompromitterede konti og nulstilling af adgangskoder</i></p> |
| <p><b>Genopretning</b></p>  | <p><b>Genoprette berørte systemer, data og tjenester, så de er sikre og operationelle</b></p> <p><i>Eksempler: geninstallering af operativsystemer på berørte servere, gendannelse af data fra backup, kortlægning af erfaringer, ajourføring af politikker</i></p>        |

*Kilde: Revisionsretten, baseret på betragtning 78 i direktiv (EU) 2022/2555 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau (NIS 2-direktivet).*

**02** Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) vurderer, at cybertrusselsniveauet er højt, og bemærker, at cybertrusselsbilledet bliver mere og mere komplekst<sup>3</sup>. Dette understreger, at cybersikkerhed har afgørende betydning for vores stadig mere digitale økonomier og samfund. I sin [2025-rapport om trusselsbilledet](#) identificerede ENISA ransomware som den mest kritiske trussel i EU. [Figur 2](#) viser de sektorer, der er udsat for angreb.

<sup>3</sup> ENISA, "2024 Report on the State of the Cybersecurity in the Union".

**Figur 2 | Sektorer udsat for cyberangreb**

Kilde: Revisionsretten, baseret på oplysninger fra [ENISA](#).

## Væsentlige og omfattende cybersikkerhedshændelser

**03** Cybersikkerhedshændelser, herunder cybertrusler og utilsigtede hændelser (f.eks. som dem, der er nævnt i [figur 3](#) og punkt [40](#)), "kan hindre leveringen af offentlige tjenester [og] udøvelsen af økonomiske aktiviteter [...], medføre betydelige finansielle tab, underminere brugernes tillid, forårsage betydelig skade på Unionens økonomi og demokratiske systemer og muligvis få sundhedsmæssige eller livstruende konsekvenser"<sup>4</sup>. En cybersikkerhedshændelse anses for at være<sup>5</sup>:

- **væsentlig**, hvis den har forårsaget eller kan forårsage alvorlige driftsmæssige forstyrrelser af den berørte enheds tjenester eller forårsage økonomiske tab for enheden eller påvirke andre fysiske eller juridiske personer ved at forvolde dem betydelig materiel eller immateriel skade
- **omfattende**, hvis den forårsager en forstyrrelse på et niveau, som overstiger en medlemsstats kapacitet til at reagere på den, eller som har en væsentlig indvirkning på mindst to medlemsstater.

**04** En omfattende cybersikkerhedshændelse kan eskalere til en fuldgældig **EU-cyberkrise**, hvis den forhindrer det indre markeds korrekte funktion eller udgør alvorlige risici for den offentlige sikkerhed for enheder eller borgere i flere medlemsstater eller for EU som helhed<sup>6</sup>.

---

<sup>4</sup> Betragtning 2 i forordning (EU) 2025/38 ([forordningen om cybersolidaritet](#)).

<sup>5</sup> Artikel 6 og 23 i [NIS 2-direktivet](#), præciseret i [Kommissionens gennemførelsesforordning \(EU\) 2024/2690](#) for så vidt angår en række udbydere i sektoren for digital infrastruktur.

<sup>6</sup> Betragtning 69 i [NIS 2-direktivet](#).

## EU's politikramme

- 05** EU har et komplekst cyberøkosystem med mange lag, som spænder over en lang række interne politikker, f.eks. retlige og indre anliggender, det digitale indre marked og forskning<sup>7</sup>. Hvad angår eksterne politikker er cybersikkerhed et fokuspunkt for diplomatiet og i stigende grad en del af EU's nye forsvarspolitik<sup>8</sup>.
- 06** I de seneste år har EU styrket sin lovgivningsmæssige ramme vedrørende cybersikkerhed. **Figur 3** viser de mest relevante EU-retsakter og -politikinstrumenter. I overensstemmelse med revisionens omfang (jf. punkt **13-14**) fokuserede vi på de instrumenter, der vedrører opdagelse af og reaktion på væsentlige og omfattende cybersikkerhedshændelser.

---

<sup>7</sup> Revisionsrettens briefingpapir "Udfordringer for en effektiv cybersikkerhedspolitik i EU", s. 12.

<sup>8</sup> Jf. f.eks. Den Europæiske Unions cyberposition (2022), rammen for en koordineret EU-reaktion på hybride kampagner (2022), EU's politik for cyberforsvar (2023) og den reviderede cyberdiplomatiske værktøjsskabe (2023).

**Figur 3 | Relevante EU-retsakter og -politikinstrumenter**

- Vedtagelse af lovgivning og politiske instrumenter
- Oprettelse af netværk og strukturer



Kilde: Revisionsretten.

## Roller og ansvarsområder

- 07** EU's cybersikkerhedslandskab involverer en lang række private og offentlige enheder på regionalt og nationalt plan samt EU-plan, som arbejder med cybersikkerhed på det civile område, herunder retshåndhævende myndigheder. Cybersikkerhed er også et centralt element i de enkelte medlemsstaters nationale sikkerheds- og forsvarspolitik<sup>9</sup>. Vi illustrerer det aktuelle EU-landskab i [bilag II](#).
- 08** Medlemsstaterne har det primære ansvar for at forebygge, forberede sig på og reagere på cybersikkerhedshændelser og -kriser, der påvirker dem. I henhold til [artikel 4, stk. 2, i traktaten om Den Europæiske Union](#) forbliver den nationale sikkerhed den enkelte medlemsstats eneansvar. Da cybersikkerhedshændelser kan forstyrre og skade kritiske informationsinfrastrukturer, som det indre markeds funktion afhænger af, har EU også en vigtig rolle at spille i forbindelse med væsentlige hændelser eller kriser<sup>10</sup>. De vigtigste enheder på EU-plan præsenteres i [figur 4](#).

---

<sup>9</sup> Udtalelse 02/2023 om forslaget til forordningen om cybersolidaritet.

<sup>10</sup> EU's plan for cyberkrisestyring.

**Figur 4 | Enheder på EU-plan med vigtige roller inden for cybersikkerhed**

Kilde: Revisionsretten.

## EU-finansiering

- 09** Hovedkilden til finansiering af cybersikkerhed under den aktuelle flerårige finansielle ramme for 2021-2027 er [programmet for et digitalt Europa \(DEP\)](#). Det blev iværksat i 2021 som det første EU-program, der specifikt har til formål at fremme EU's digitale omstilling, og det har et samlet budget på 8,1 milliard euro<sup>11</sup>.
- 10** DEP finansierer cybersikkerhedstiltag under specifikt mål nr. 3 "Cybersikkerhed og tillid". Nærmere bestemt er der afsat 1,4 milliard euro til:
- at styrke cybersikkerhedskoordineringen mellem medlemsstaternes værktøjer og datainfrastruktur
  - at støtte en bred udrulning af cybersikkerhedsløsninger på tværs af økonomien.
- 11** Størstedelen af DEP-finansieringen til cybersikkerhed ydes efter indkaldelser af forslag, og 12 sådanne indkaldelser blev iværksat mellem november 2021 og december 2025. Den disponible finansiering under disse indkaldelser udgør 825 millioner euro. Der er planlagt nye indkaldelser i 2026 og 2027 med henblik på tildeling af yderligere 212 millioner euro i tilskud.
- 12** Et andet væsentligt EU-program, som støtter cybersikkerhed, er [Horisont Europa](#). Cybersikkerhedsprojekter finansieres hovedsagelig under [klynge 3](#) - "Civil sikkerhed for samfundet" - og befinder sig typisk på et tidligt modenhedstrin, fordi Horisont Europa fokuserer på forskning og innovation. [Genopretnings- og resiliensfaciliteten](#) finansierer også cybersikkerhedsforanstaltninger.

---

<sup>11</sup> [Programmet for et digitalt Europa](#).

## Revisionens omfang og revisionsmetoden

**13** De tiltagende cybertrusler og deres potentielle effekt har understreget behovet for at styrke vores kollektive cyberrobusthed. Formålet med vores revision var at vurdere, om EU-tiltag effektivt fremmer opdagelse af og reaktion på væsentlige og omfattende cybersikkerhedshændelser. Nærmere bestemt vurderede vi, om dette gjorde sig gældende for:

- de oprettede netværk og mekanismer på EU-plan (CSIRT-netværket, EU-CyCLONe, det europæiske cybersikkerhedsvarslingssystem, cybersituationscentret og EU's cybersikkerhedsreserve)
- de DEP-finansierede tiltag.

Revisionen omfattede ikke retshåndhævelsessamarbejde på EU-plan og heller ikke cyberafskrækkelsestiltag på EU-plan knyttet til diplomatiske foranstaltninger eller forsvarsaktiviteter.

**14** Vores revision dækkede perioden fra 2022 til 2025. Revisionsarbejdet omfattede skrivebordsgennemgang og analyse af relevante dokumenter, revisionsbesøg i tre medlemsstater - Irland, Grækenland og Italien - skriftlige spørgeskemaer og interview med relevante interessenter. [Figur 5](#) viser, hvordan vi indhentede revisionsbevis med henblik på vores bemærkninger.

Figur 5 | Udført revisionsarbejde

## Vi undersøgte

- Den **retlige ramme** vedrørende opdagelse af og reaktion på væsentlige og omfattende cybersikkerhedshændelser
- De **roller og ansvarsområder**, som er fastlagt for de netværk og strukturer, der er oprettet på EU-plan

## Vi analyserede

- Dokumenter om **CSIRT-netværkets** og **EU-CyCLONes** funktionsmåde
  - Dokumentation vedrørende **DEP's programmerings- og præstationsovervågningsramme**
  - Dokumentation vedrørende **13 udvalgte EU-finansierede tiltag** (11 tilskud og 2 kontrakter - jf. den detaljerede liste i bilag III)
- \* Vi udvalgte EU-finansierede tiltag i tre lande (Irland, Grækenland og Italien), hvor den relevante DEP-finansiering var særlig væsentlig. De 11 tilskud stod på en liste over 137 EU-finansierede projekter med relevans vedrørende opdagelse af og reaktion på trusler, og vi udvalgte dem med fokus på at dække en varieret blanding af projekter.

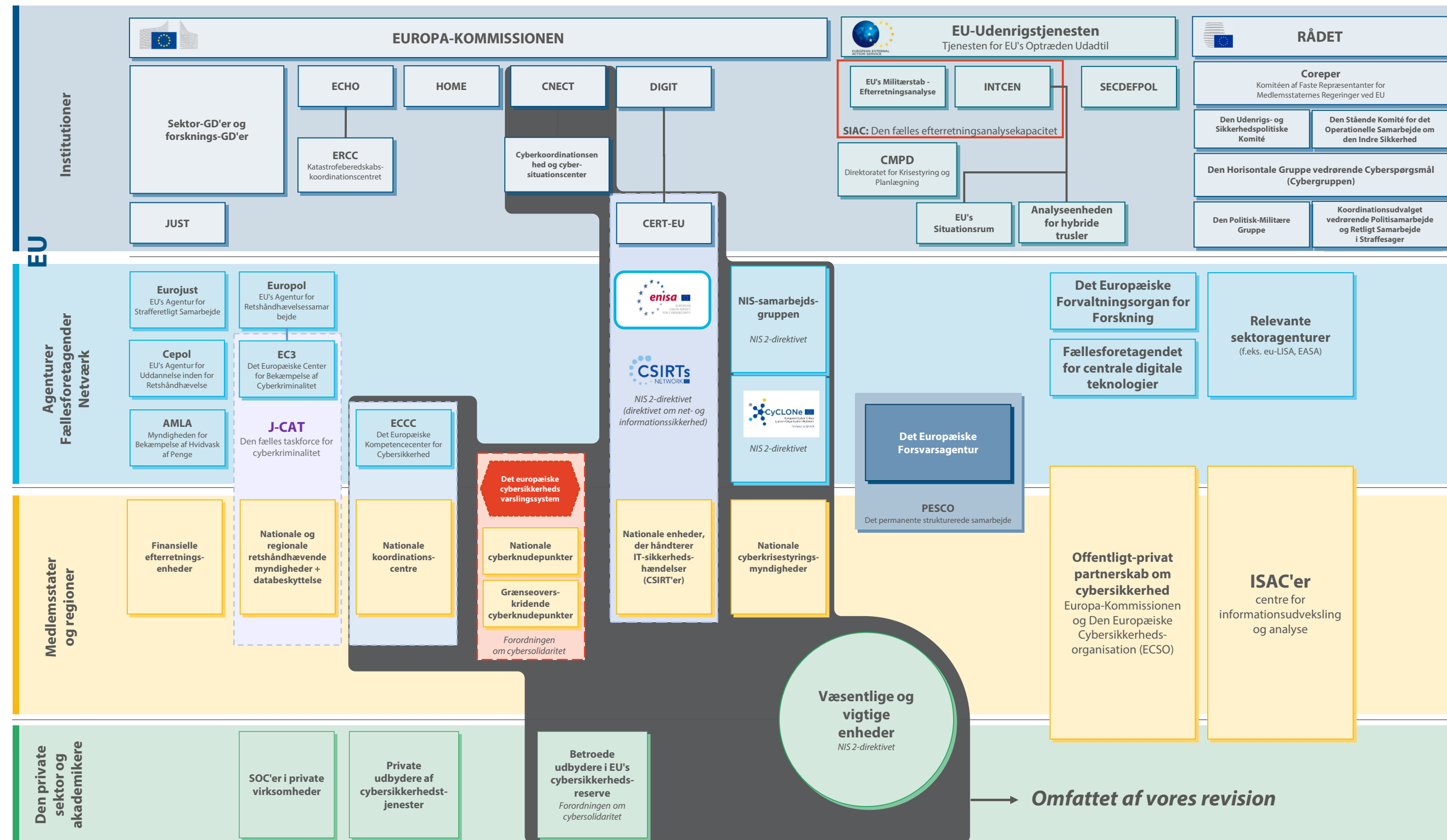
## Vi interviewede

- Modtagerne af de **11 EU-finansierede tilskud** i vores stikprøve
- Repræsentanter for de nationale cybersikkerhedsmyndigheder i **tre medlemsstater** (Irland, Grækenland og Italien)
- Repræsentanter for Europa-Kommissionen (**GD CNECT**), **ENISA** og **ECCC**

Kilde: Revisionsretten.

**15** Vi forventer, at vores revisionsresultater vil bidrage til at sikre større effektivitet og produktivitet i EU's opdagelse af og reaktion på væsentlige og omfattende cybersikkerhedshændelser og forbedre den måde, EU-finansierede tiltag udvælges og overvåges på. Vores [revisionsmetode](#) er i overensstemmelse med de internationale revisionsstandarder, som er vedtaget af [International Organisation of Supreme Audit Institutions \(INTOSAI\)](#).

## Bilag II - EU's cybersikkerhedslandskab



**GD CNECT:** Generaldirektoratet for Kommunikationsnet, Indhold og Teknologi  
**GD ECHO:** Generaldirektoratet for Civilbeskyttelse og Humanitære Bistandsforanstaltninger på Europæisk Plan  
**GD HOME:** Generaldirektoratet for Migration og Indre Anliggender

**GD JUST:** Generaldirektoratet for Retlige Anliggender og Forbrugere  
**DIGIT:** Generaldirektoratet for Digitale Tjenester  
**EASA:** Den Europæiske Unions Luftfartssikkerhedsagentur

**EU-CyCLONe:** Det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser  
**eu-LISA:** Den Europæiske Unions Agentur for den Operationelle Forvaltning af Store IT-systemer inden for Området med Frihed, Sikkerhed og Retfærdighed  
**INTCEN:** EU's Efterretnings- og Situationscenter

**SECDEFPOL:** Direktoratet for Sikkerheds- og Forsvarspolitik  
**SOC:** Sikkerhedsoperationscenter

## Bilag III - Udvalgte cybersikkerhedsforanstaltninger

| ID                                                                                                                                                                                                         | Titel                                                                                                                  | Lande                                                                  | Startdato | Slutdato   | Samlede omkostninger (i mio. euro) og EU-bidrag (i %) | Link til EU's finansierings- og udbudsportal                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|-----------|------------|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Tilskud vedrørende grænseoverskridende cyberknudepunkter, som indgår i det europæiske cybersikkerhedsvarslingssystem                                                                                       |                                                                                                                        |                                                                        |           |            |                                                       |                                                                                                       |
| 1                                                                                                                                                                                                          | Establishing Cross-border SOCs (ATHENA)                                                                                | Bulgarien, Grækenland, Cypern, Malta                                   | 1.1.2024  | 31.3.2028  | 4,7 (50 %)                                            | <a href="#"></a>   |
| 2                                                                                                                                                                                                          | ENSOC-CROSSBORDER PLATFORM (ENSOC)                                                                                     | Spanien, Italien, Luxembourg, Nederlandene, Østrig, Portugal, Rumænien | 1.1.2024  | 30.6.2028  | 10,4 (50 %)                                           | <a href="#"></a>   |
| Tilskud vedrørende etablering af Netværket af Nationale Koordinationscentre (NCC'er) i medlemsstaterne                                                                                                     |                                                                                                                        |                                                                        |           |            |                                                       |                                                                                                       |
| 3                                                                                                                                                                                                          | Development and Implementation of the National Cyber Security Coordination and Development Centre for Ireland (NCC-IE) | Irland                                                                 | 2.10.2023 | 1.10.2026  | 4,2 (47 %)                                            | <a href="#"></a>   |
| 4                                                                                                                                                                                                          | Italian National Coordination Centre (NCC-IT)                                                                          | Italien                                                                | 1.11.2023 | 31.10.2025 | 2,0 (50 %)                                            | <a href="#"></a> |
| Tilskud vedrørende kapacitetsopbygning i sikkerhedsoperationscentre (SOC'er), nye anvendelser af kunstig intelligens og andre støtteteknologier i SOC'er og ydelse af beredskabsstøtte og gensidig bistand |                                                                                                                        |                                                                        |           |            |                                                       |                                                                                                       |
| 5                                                                                                                                                                                                          | Enhancing the capacity of the Hellenic Consolidated Security Operation Center (EL-SOC)                                 | Grækenland, Cypern                                                     | 1.1.2024  | 31.12.2026 | 9,7 (50 %)                                            | <a href="#"></a> |
| 6                                                                                                                                                                                                          | Greek Security Operations Centre for Small and Medium Enterprises (GR-SME-SOC)                                         | Grækenland                                                             | 1.1.2024  | 31.12.2026 | 12,1 (50 %)                                           | <a href="#"></a> |

| ID                                                                     | Titel                                                                                                    | Lande                                                                     | Startdato              | Slutdato   | Samlede omkostninger (i mio. euro) og EU-bidrag (i %) | Link til EU's finansierings- og udbudsportal |
|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|------------------------|------------|-------------------------------------------------------|----------------------------------------------|
| 7                                                                      | Next Generation Security Operation Centres (NG-SOC)                                                      | Grækenland, Spanien, Cypern, Luxembourg, Slovenien, Norge                 | 1.1.2024               | 31.12.2026 | 4,8 (50 %)                                            | <a href="#">🔗</a>                            |
| 8                                                                      | Irish Local Government Security Operations Centre (ILG-SOC)                                              | Irland                                                                    | 1.10.2023              | 30.9.2026  | 8,3 (50 %)                                            | <a href="#">🔗</a>                            |
| 9                                                                      | An Interconnected Ecosystem of Cyber Security Coordination and Response Networks (Cyber-CORE-Network)    | Irland                                                                    | 1.1.2024               | 31.12.2026 | 3,6 (50 %)                                            | <a href="#">🔗</a>                            |
| 10                                                                     | Harmonizing People, Processes, and Technology for Robust Cybersecurity (CYberSynchrony)                  | Belgien, Grækenland, Italien, Cypern, Nederlandene                        | 1.6.2024               | 31.5.2027  | 7,0 (100 %)                                           | <a href="#">🔗</a>                            |
| 11                                                                     | Advanced Cooperative Security Operation Centres (ACSOC)                                                  | Grækenland, Italien, Rumænien                                             | 1.1.2025               | 31.12.2027 | 3,0 (50 %)                                            | <a href="#">🔗</a>                            |
| Rammeaftale vedrørende ENISA's støtteforanstaltning for cybersikkerhed |                                                                                                          |                                                                           |                        |            |                                                       |                                              |
| 12                                                                     | Supporting ENISA for the Provision of Services under the Cybersecurity Support Action (28 delkontrakter) | 27 delkontrakter vedrørende medlemsstaterne<br>1 paneuropæisk delkontrakt | 1.12.2022 <sup>1</sup> | 31.12.2025 | 28,3 (100 %)                                          | <a href="#">🔗</a>                            |
| Tjenesteydelseskontrakt vedrørende GD CNECT's cybersituationscenter    |                                                                                                          |                                                                           |                        |            |                                                       |                                              |
| 13                                                                     | Bespoke Service to Support the Cyber Situation and Analysis Centre for the European Commission           | -                                                                         | 30.12.2022             | 30.12.2026 | 18,0 (100 %)                                          | <a href="#">🔗</a>                            |

Kilde: Revisionsretten.

<sup>1</sup> Flere kontrakter indgået i løbet af december 2022.

## Bilag IV - Revisionsrettens vurdering af EU-finansierede cybersikkerhedsprojekter

| ID | Projekt                                                                                                                | <div> <div>Tilfredsstillende</div> <div>Utilfredsstillende</div> <div>Visse svagheder</div> <div>Ingen konklusion mulig (for tidligt at vurdere)</div> </div> |                                                                       |                                                 |                                                                                               |
|----|------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|-------------------------------------------------|-----------------------------------------------------------------------------------------------|
|    |                                                                                                                        | Projektet adresserer de fleste af de behov, der er beskrevet i indkaldelsen                                                                                   | Projektet har indtil videre leveret de planlagte output og resultater | Projektet har leveret sine output rettidigt     | Projektets præstationsindikator er relevante og målbare og har et referencescenario og et mål |
| 1  | Establishing Cross-border SOCs (ATHENA)                                                                                | Tilfredsstillende                                                                                                                                             | Utilfredsstillende                                                    | Utilfredsstillende                              | Utilfredsstillende                                                                            |
| 2  | ENSOC-CROSSBORDER PLATFORM (ENSOC)                                                                                     | Tilfredsstillende                                                                                                                                             | Utilfredsstillende                                                    | Utilfredsstillende                              | Utilfredsstillende                                                                            |
| 3  | Development and Implementation of the National Cyber Security Coordination and Development Centre for Ireland (NCC-IE) | Tilfredsstillende                                                                                                                                             | Tilfredsstillende                                                     | Visse svagheder                                 | Visse svagheder                                                                               |
| 4  | Italian National Coordination Centre (NCC-IT)                                                                          | Tilfredsstillende                                                                                                                                             | Tilfredsstillende                                                     | Tilfredsstillende                               | Visse svagheder                                                                               |
| 5  | Enhancing the capacity of the Hellenic Consolidated Security Operation Center (EL-SOC)                                 | Tilfredsstillende                                                                                                                                             | Visse svagheder                                                       | Utilfredsstillende                              | Utilfredsstillende                                                                            |
| 6  | Greek Security Operations Centre for Small and Medium Enterprises (GR-SME-SOC)                                         | Tilfredsstillende                                                                                                                                             | Tilfredsstillende                                                     | Tilfredsstillende                               | Visse svagheder                                                                               |
| 7  | Next Generation Security Operation Centres (NG-SOC)                                                                    | Tilfredsstillende                                                                                                                                             | Tilfredsstillende                                                     | Tilfredsstillende                               | Visse svagheder                                                                               |
| 8  | Irish Local Government Security Operations Centre (ILG-SOC)                                                            | Tilfredsstillende                                                                                                                                             | Utilfredsstillende                                                    | Utilfredsstillende                              | Utilfredsstillende                                                                            |
| 9  | An Interconnected Ecosystem of Cyber Security Coordination and Response Networks (Cyber-CORE-Network)                  | Tilfredsstillende                                                                                                                                             | Visse svagheder                                                       | Visse svagheder                                 | Visse svagheder                                                                               |
| 10 | Harmonizing People, Processes, and Technology for Robust Cybersecurity (CYberSynchrony)                                | Visse svagheder                                                                                                                                               | Ingen konklusion mulig (for tidligt at vurdere)                       | Ingen konklusion mulig (for tidligt at vurdere) | Visse svagheder                                                                               |
| 11 | Advanced Cooperative Security Operation Centres (ACSOC)                                                                | Tilfredsstillende                                                                                                                                             | Ingen konklusion mulig (for tidligt at vurdere)                       | Ingen konklusion mulig (for tidligt at vurdere) | Utilfredsstillende                                                                            |

## Forkortelser

| Forkortelse | Definition/forklaring                                                |
|-------------|----------------------------------------------------------------------|
| CSIRT       | Enhed, der håndterer IT-sikkerhedshændelser                          |
| DEP         | Programmet for et digitalt Europa                                    |
| ECCC        | Det Europæiske Kompetencecenter for Cybersikkerhed                   |
| ENISA       | Den Europæiske Unions Agentur for Cybersikkerhed                     |
| EU-CyCLONe  | Det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser |
| GD CNECT    | Generaldirektoratet for Kommunikationsnet, Indhold og Teknologi      |
| NCC         | Nationalt koordinationscenter                                        |
| NIS         | Net- og informationssikkerhed                                        |
| SMV'er      | Små og mellemstore virksomheder                                      |
| SOC         | Sikkerhedsoperationscenter                                           |

# Glossar

| Term                                      | Definition/forklaring                                                                                                                                                                                                                          |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Cyberknodepunkt</b>                    | Central platform, som samler forskellige tjenester, værktøjer og IT-fagfolk for at styrke overvågningen, opdagelsen og analysen af cybertrusler, forebygge cybersikkerhedshændelser og støtte tilvejebringelse af cybertrusselsefterretninger. |
| <b>Cybersikkerhedshændelse</b>            | Begivenhed, hvor datas eller informationssystemers tilgængelighed, ægthed, integritet eller fortrolighed kompromitteres.                                                                                                                       |
| <b>Cybertrussel</b>                       | Potentiel anvendelse af cyberspace med henblik på at kompromittere datas eller informationssystemers tilgængelighed, ægthed, integritet eller fortrolighed.                                                                                    |
| <b>Omfattende cybersikkerhedshændelse</b> | Cybersikkerhedshændelse, som er så forstyrrende, at en medlemsstat ikke kan håndtere den alene, eller som har en væsentlig indvirkning på mindst to medlemsstater.                                                                             |
| <b>Ransomware</b>                         | Malware, som nægter offeret adgang til et computersystem eller krypterer datafiler for at gøre dem ulæselige, typisk med det formål at tvinge offeret til at betale en løsesum for genetablering af adgangen.                                  |
| <b>Sikkerhedsoperationscenter</b>         | Organisatorisk enhed, som arbejder med forebyggelse af cybertrusler og -hændelser og indsamler relaterede efterretningsoplysninger.                                                                                                            |
| <b>Taksonomi</b>                          | I forbindelse med cybersikkerhed en klassificeringsordning, som anvendes til at organisere, kategorisere og strukturere viden om centrale begreber såsom trusler og hændelser.                                                                 |
| <b>Trusselsaktør</b>                      | Enkeltperson eller gruppe, som forsætligt forvolder skade, forstyrrer tjenester eller stjæler data ved at udnytte sårbarheder i IT-systemer, -net og -udstyr.                                                                                  |
| <b>Væsentlig cybersikkerhedshændelse</b>  | Cybersikkerhedshændelse, som har medført eller kan medføre alvorlige forstyrrelser eller finansielle tab for en organisation eller betydelige skader for andre enheder eller for enkeltpersoner.                                               |

## **Kommissionens svar**

<https://www.eca.europa.eu/da/publications/SR-2026-19>

## **Svar fra Det Europæiske Kompetencecenter for Cybersikkerhed (ECCC)**

<https://www.eca.europa.eu/da/publications/SR-2026-19>

## **Svar fra Den Europæiske Unions Agentur for Cybersikkerhed (ENISA)**

<https://www.eca.europa.eu/da/publications/SR-2026-19>

## **Tidslinje**

<https://www.eca.europa.eu/da/publications/SR-2026-19>

## Revisionsholdet

Revisionsrettens særberetninger præsenterer resultaterne af dens revisioner vedrørende EU-politikker og -programmer eller forvaltningsspørgsmål i forbindelse med specifikke budgetområder. Med henblik på at opnå maksimal effekt udvælger og udformer Revisionsretten sine revisionsopgaver under hensyntagen til de risici, der knytter sig til forvaltningens resultatopnåelse eller regelefterlevelsen, de pågældende indtægters eller udgifters omfang, den fremtidige udvikling samt den politiske og offentlige interesse.

Denne forvaltningsrevision blev udført af Afdeling III - Foranstaltninger udadtil, sikkerhed og retfærdighed, der ledes af George-Marius Hyzler, medlem af Revisionsretten. Revisionsarbejdet blev udført under ledelse af George-Marius Hyzler, medlem af Revisionsretten, med støtte fra kabinetschef Romuald Kayibanda, attaché Annette Farrugia, ledende administrator Cyril Messein, opgaveansvarlig Frédéric Soblet og revisorerne Jurgen Manjé og Flavia Di Marco. Zoe Amador Martínez ydede sproglig støtte. Dunja Weibel ydede grafisk støtte.



*Fra venstre til højre: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé, Cyril Messein.*

# MEDDELELSE OM OPHAVSRET

© Den Europæiske Union, 2026

Den Europæiske Revisionsrets politik for videreanvendelse er fastsat i [Revisionsrettens afgørelse nr. 6-2019](#) om den åbne datapolitik og videreanvendelse af dokumenter.

Medmindre andet er oplyst (f.eks. i individuelle meddelelser om ophavsret), er det af Revisionsrettens indhold, der ejes af EU, licenseret i henhold til [Creative Commons Attribution 4.0 International \(CC BY 4.0\)](#). Det betyder, at videreanvendelse generelt er tilladt med korrekt angivelse af kilde og eventuelle ændringer. Ved videreanvendelse af Revisionsrettens indhold må den oprindelige betydning eller det oprindelige budskab ikke fordrejes. Revisionsretten er ikke ansvarlig for eventuelle konsekvenser af videreanvendelsen.

Yderligere tilladelse skal indhentes, hvis specifikt indhold afbilder identificerbare privatpersoner, f.eks. på billeder af ansatte i Revisionsretten, eller omfatter tredjeparts værker.

Hvis en sådan tilladelse opnås, erstatter denne tilladelse ovenstående generelle tilladelse, og den skal klart anføre eventuelle begrænsninger i anvendelsen.

Tilladelse til at anvende eller gengive indhold, der ikke ejes af EU, skal eventuelt indhentes direkte hos indehaveren af ophavsretten.

Forsidefoto: © 4AXY - stock.adobe.com.

Figur 6 og 8 - ikoner: Disse figurer er udformet ved anvendelse af ressourcer fra [Flaticon.com](#). © Freepik Company S.L. Alle rettigheder forbeholdes.

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

Software og dokumenter, der er omfattet af industriel ejendomsret såsom patenter, varemærker, registrerede design, logoer og navne, er ikke omfattet af Revisionsrettens videreanvendelsespolitik.

EU-institutionernes websteder på europa.eu-domænet har links til websteder uden for europa.eu-domænet. Da Revisionsretten ikke har kontrol over disse websteder, anbefales det at gennemse deres privatlivspolitik og ophavsretspolitik.

## Anvendelse af Revisionsrettens logo

Revisionsrettens logo må ikke anvendes uden Revisionsrettens forudgående samtykke.

|      |                        |                |                     |                   |
|------|------------------------|----------------|---------------------|-------------------|
| HTML | ISBN 978-92-849-7853-3 | ISSN 1977-5636 | doi:10.2865/4523220 | QJ-01-26-032-DA-Q |
| PDF  | ISBN 978-92-849-7854-0 | ISSN 1977-5636 | doi:10.2865/1142353 | QJ-01-26-032-DA-N |

## HVORDAN DER HENVISES TIL DENNE PUBLIKATION

Den Europæiske Revisionsret, [særberetning 19/2026](#) "Opdagelse af og reaktion på cybersikkerhedshændelser - En EU-samarbejdsramme er under udvikling, men på grund af gennemførelsesforsinkelser og begrænset informationsdeling er den kun delvis effektiv", Den Europæiske Unions Publikationskontor, 2026.

I de seneste år har EU styrket sin lovgivningsmæssige ramme vedrørende cybersikkerhed og etableret netværk og mekanismer til håndtering af cybersikkerhedshændelser. EU finansierer desuden cybersikkerhedsprojekter via programmet for et digitalt Europa.

Vi konkluderer, at EU's tiltag kun delvis fremmer opdagelse af og reaktion på væsentlige og omfattende cybersikkerhedshændelser. Der er gradvis blevet udformet en samarbejdsramme, men arbejdet med at færdiggøre den er stadig i gang. På grund af begrænset informationsdeling, rapporteringssvagheder og store gennemførelsesforsinkelser har EU's netværk og mekanismer ikke opfyldt deres fulde potentiale. Projekterne forfølger relevante mål, men adskillige er ramt af operationelle udfordringer og forsinkelser. Desuden er der svagheder i den generelle præstationsovervågningsramme. Vi fremsætter anbefalinger vedrørende disse forhold.

*Særberetning fra Revisionsretten udarbejdet i medfør af artikel 287, stk. 4, andet afsnit, TEUF.*



DEN  
EUROPÆISKE  
REVISIONSRET



Den Europæiske Unions  
Publikationskontor

DEN EUROPÆISKE REVISIONSRET  
12, rue Alcide De Gasperi  
1615 Luxembourg  
LUXEMBOURG

Tlf. +352 4398-1

Kontakt: [eca.europa.eu/da/contact](https://eca.europa.eu/da/contact)  
Websted: [eca.europa.eu](https://eca.europa.eu)  
Sociale medier: @EUauditors