SPECIAAL VERSLAG 19/2026 **NL**

Opsporing van en respons op cyberbeveiligingsincidenten

EU-samenwerkingskader laat vorderingen zien, maar is slechts deels doeltreffend door vertragingen bij de uitvoering en beperkte informatie-uitwisseling

CURIA RATIONUM

EUROPESE REKENKAMER

Inhoud

Paragraaf

01-23 | Kernboodschappen 01

01-07 | Waarom dit terrein van belang is

08-23 | Wat wij constateerden en aanbevelen

24-01 | Onze bevindingen nader bekeken 02

24-74 | Hoewel EU-cyberbeveiligingsnetwerken en -mechanismen samenwerking en respons ondersteunen, verminderen beperkte informatie-uitwisseling en onvolledige uitvoering de doeltreffendheid ervan

24-51 | EU-netwerken maken samenwerking tussen de lidstaten mogelijk, maar door de beperkte uitwisseling van informatie neemt de toegevoegde waarde ervan af

52-61 | Dankzij de EU-cyberbeveiligingsreserve kunnen incidentresponsdiensten snel worden ingezet

62-74 | Het Europees waarschuwingssysteem voor cyberbeveiliging heeft tot doel de capaciteit voor het opsporen van dreigingen te verbeteren, maar is niet operationeel

75-01 | Door de EU gefinancierde projecten in het kader van DIGITAL hebben tot doel de cyberbeveiliging te versterken, maar worden geconfronteerd met uitdagingen op het gebied van uitvoering en rapportage

75-81 | Vertragingen bij de oprichting ervan verhinderden dat de kennisgemeenschap voor cyberbeveiliging DIGITAL kon vormgeven op basis van haar behoeften

82-96 | Met door de EU gefinancierde projecten worden relevante doelstellingen nagestreefd, maar veel projecten worden geconfronteerd met operationele problemen

97-01 | De meeste door de EU gefinancierde projecten hebben ontoereikende prestatiekaders en de prestatiegegevens van DIGITAL op het gebied van cyberbeveiliging zijn niet nauwkeurig

Bijlagen

Bijlage I — Over de controle

Bijlage II — Het cyberbeveiligingslandschap van de EU

Bijlage III — Geselecteerde acties op het gebied van cyberbeveiliging

Bijlage IV — Beoordeling door de ERK van door de EU gefinancierde cyberbeveiligingsprojecten

Afkortingen

Woordenlijst

Antwoorden van de Commissie

Antwoorden van het Europees Kenniscentrum voor cyberbeveiliging (ECCC)

Antwoorden van het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa)

Tijdlijn

Controleteam

01 Kernboodschappen

Waarom dit terrein van belang is

01 Naarmate onze economie en ons dagelijks leven steeds verder digitaliseren, neemt het risico op cyberaanvallen toe. Cyberbeveiliging wordt gedefinieerd als “de activiteiten die nodig zijn om netwerk- en informatiesystemen, de gebruikers van dergelijke systemen, en andere personen die getroffen worden door cyberdreigingen, te beschermen”[1]. Cyberbeveiliging vereist een holistische aanpak om cyberdreigingen te voorkomen, op te sporen, erop te reageren en ervan te herstellen.

02 Het cyberbeveiligingslandschap van de EU omvat talrijke publieke en particuliere entiteiten op regionaal, nationaal en EU-niveau in de civiele sfeer. Cyberbeveiliging is ook een belangrijk onderdeel van nationale veiligheid en defensie.

03 De lidstaten zijn in de eerste plaats verantwoordelijk voor het voorkomen van, de voorbereiding en het reageren op cyberbeveiligingsincidenten en -crises die hen aangaan. Aangezien deze incidenten de goede werking van de interne markt kunnen verstoren, speelt de EU ook een belangrijke rol bij significante incidenten of crises. De afgelopen jaren heeft de EU haar evoluerende regelgevingskader voor cyberbeveiliging versterkt[2] en netwerken en mechanismen opgezet, zoals weergegeven in ***figuur 1*** hieronder en in ***bijlage II***.

---

[1] Verordening (EU) 2019/881 (cyberbeveiligingsverordening).

[2] Zo heeft de Commissie in november 2025 de digitale omnibus voorgesteld en in januari 2026 een herziene EU-cyberbeveiligingsverordening.

Figuur 1 | EU-cyberbeveiligingsnetwerken en -mechanismen 2016-2025

2016

Oprichting van het CSIRT-netwerk

- Dit netwerk van nationale CSIRT's en CERT-EU, dat in 2016 werd opgericht bij de NIS-richtlijn en in 2022 werd versterkt bij de NIS 2-richtlijn, heeft tot doel bij te dragen tot de ontwikkeling van het vertrouwen en een snelle en doeltreffende technische samenwerking tussen de lidstaten te bevorderen.

2020

Start van EU-CyCLONe

- Dit netwerk van nationale autoriteiten die verantwoordelijk zijn voor cybercrisisbeheer fungeert als schakel tussen de technische en politieke dimensies bij grootschalige cyberbeveiligingsincidenten en -crises. Dit werd in 2022 vastgelegd in de NIS 2-richtlijn.

2023

Start van de activiteiten van het cybersituatiecentrum in DG Connect

- Het centrum, dat is opgericht met de hulp van externe dienstverleners, heeft tot doel het situationeel bewustzijn van de Commissie te vergroten en ondersteunt DG Connect bij het verstrekken van advies op politiek niveau.

2025

Oprichting van het Europees waarschuwingssysteem voor cyberbeveiliging

- Het Europees waarschuwingssysteem voor cyberbeveiliging, opgericht bij de verordening cybersolidariteit, is een pan-Europees netwerk van nationale en landsgrensoverschrijdende cyberhubs.

Instelling van de EU-cyberbeveiligingsreserve

- De EU-cyberbeveiligingsreserve is een vooraf ingehuurde dienst die is opgericht bij de verordening cybersolidariteit, waarop de lidstaten in de eerste plaats een beroep moeten doen voor respons en herstel in geval van cyberbeveiligingsincidenten.

CSIRT's: computer security incident response teams
DG Connect: directoraat-generaal Communicatienetwerken, Inhoud en Technologie
EU-CyCLONe: Europees Netwerk van verbindingsorganisaties voor cybercrises
NIS-richtlijn: Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie
NIS 2-richtlijn: Richtlijn (EU) 2022/2555 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie

Bron: ERK.

04 Binnen het huidige meerjarig financieel kader 2021-2027 is het programma Digitaal Europa (DIGITAL) de belangrijkste financieringsbron voor cyberbeveiliging. Het programma heeft een totale begroting van 8,1 miljard EUR, waarvan 1,4 miljard EUR is bestemd voor het versterken van de cyberbeveiliging.

05 Het doel van onze controle was na te gaan of de EU-maatregelen de opsporing van en de respons op significante en grootschalige cyberbeveiligingsincidenten doeltreffend bevorderen. We hebben onderzocht of dit het geval was voor:

- netwerken en mechanismen op EU-niveau (d.w.z. het netwerk van Computer Security Incident Response teams (CSIRT-netwerk), het Europees netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe), het Europees waarschuwingssysteem voor cyberbeveiliging, het cybersituatiecentrum en de EU-cyberbeveiligingsreserve);
- in het kader van DIGITAL gefinancierde maatregelen.

06 We verwachten dat onze bevindingen zullen bijdragen tot de versterking van de cyberweerbaarheid van de EU door de doeltreffendheid en efficiëntie van de EU-netwerken en -mechanismen te verbeteren en de wijze waarop EU-gefinancierde maatregelen worden geselecteerd en gemonitord, te verbeteren.

07 De controle had betrekking op de periode van 2022 tot en met 2025. Deze is gebaseerd op een controle aan de hand van stukken en een analyse van relevante documenten, controlebezoeken aan drie lidstaten — Ierland, Griekenland en Italië — en schriftelijke vragenlijsten en vraaggesprekken met relevante belanghebbenden. Meer achtergrondinformatie en details over de reikwijdte en aanpak van de controle zijn te vinden in ***bijlage I***.

Wat wij constateerden en aanbevelen

08 In het algemeen concluderen wij dat EU-maatregelen de opsporing van en de respons op significante en grootschalige cyberbeveiligingsincidenten slechts ten dele bevorderen. Hoewel er geleidelijk een samenwerkingskader tot stand is gekomen, wordt er nog steeds gewerkt aan de volledige opzet ervan. Door de beperkte informatie-uitwisseling, tekortkomingen in de rapportage en aanzienlijke vertragingen bij de uitvoering kan het potentieel van de EU-netwerken en -mechanismen niet volledig worden benut. Met de door DIGITAL gefinancierde projecten worden relevante doelstellingen nagestreefd, maar verschillende ervan hebben te kampen met operationele problemen en vertragingen, en er zijn tekortkomingen in het algemene kader voor prestatiemonitoring.

09 Het huidige kader van EU-netwerken en -mechanismen om de opsporing van en de respons op significante cyberbeveiligingsincidenten te bevorderen, is geleidelijk opgebouwd. In 2025 keurde de Raad de cyberblauwdruk goed, waarin het EU-kader voor cybercrisisbeheer wordt uiteengezet. We constateerden dat de cyberblauwdruk de rollen en verantwoordelijkheden met betrekking tot het EU-cybercrisisbeheer in grote lijnen verduidelijkt. Desondanks moeten de procedurele regelingen voor de samenwerking tussen het CSIRT-netwerk (opgericht in 2016) en EU-CyCLONe (geformaliseerd in 2023) nog worden geformaliseerd (zie de paragrafen ***24***-***30***).

10 We constateerden dat het uitwisselen van informatie via deze netwerken beperkt is. Dit is voornamelijk te wijten aan vertragingen bij de omzetting van de richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS 2-richtlijn), aan moeilijkheden bij het bepalen of een incident grensoverschrijdende gevolgen heeft, en aan nationale veiligheidswetgeving die informatie-uitwisseling verhindert. De toegevoegde waarde van de netwerken wordt aanzienlijk verminderd als de lidstaten niet bereid zijn tijdig bruikbare informatie uit te wisselen (zie de paragrafen ***31***-***44***)

Aanbeveling 1

Versterk de uitwisseling van informatie tussen lidstaten

Om de opsporing van en de respons op cyberbeveiligingsincidenten te verbeteren, moet de Commissie, met steun van het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa):

a) de samenwerkingsgroep voor netwerk- en informatiebeveiliging voorstellen dat zij een gedetailleerde analyse uitvoert van de beperkingen op het gebied van nationale veiligheid wat betreft het uitwisselen van informatie die van invloed zijn op de cyberweerbaarheid van de EU, en dat zij juridische en technische oplossingen vindt om meer informatie uit te kunnen wisselen, met inachtneming van de grenzen van de nationale veiligheid;

b) zonder afbreuk te doen aan de besluiten van de medewetgevers, er in samenwerking met de lidstaten voor zorgen dat vanuit het in de digitale omnibus voorgestelde centrale contactpunt voor het melden van incidenten potentiële grensoverschrijdende incidenten kunnen worden opgespoord;

c) werken aan oplossingen om realtime melding van incidenten aan Enisa mogelijk te maken.

Streefdatum voor de uitvoering: a) en b) 2027, c) 2028

11 In 2022 heeft de Commissie haar “cybersituatiecentrum“ opgericht om haar situationeel bewustzijn te vergroten, met als doel haar institutionele verantwoordelijkheden op het gebied van crisisbeheer te ondersteunen. De werking van het centrum wordt grotendeels ondersteund door middel van een contract met externe dienstverleners. We constateerden dat de door de externe dienstverleners verrichte werkzaamheden gedeeltelijk overlappen met de bestaande capaciteit van het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) op het gebied van situationeel bewustzijn en het monitoren van dreigingen. Wij zijn van mening dat bij de oprichting van het cybersituatiecentrum niet het volledige potentieel tot rationalisering is benut door gebruik te maken van informatie die reeds beschikbaar was bij de Commissie en Enisa. Daarnaast vormt het ontbreken van een alomvattend, gedetailleerd plan voor de toekomst na afloop van het contract een risico voor de werking van het cybersituatiecentrum na 2026 (zie de paragrafen ***45***-***51***).

Aanbeveling 2

Rationaliseer de capaciteiten van de EU op het gebied van situationeel bewustzijn inzake cyberveiligheid en optimaliseer de verspreiding van informatie

Om de efficiëntie te vergroten, moet de Commissie, in samenwerking met Enisa, de haalbaarheid van gezamenlijke verwerving en analyse van informatie voor situationeel bewustzijn beoordelen. Zij moet deze informatie en de daarmee verband houdende cyberdreigingsverslagen ook beschikbaar stellen aan alle relevante afdelingen en agentschappen van de EU.

Streefdatum voor de uitvoering: 2027

12 Bij de verordening cybersolidariteit van 2024 werd de EU-cyberbeveiligingsreserve opgericht, die tot doel heeft de lidstaten te ondersteunen bij de respons op en het herstel van grote cyberbeveiligingsincidenten. Deze reserve bestaat uit geselecteerde dienstverleners per lidstaat, die dag en nacht op incidenten kunnen reageren. Hoewel deze aanpak helpt om tegemoet te komen aan de specifieke behoeften van de lidstaten en om vertrouwen op te bouwen, wordt de beschikbare begroting gelijkelijk over de lidstaten verdeeld en wordt er geen rekening gehouden met de specifieke behoeften van elke lidstaat (zie de paragrafen ***52***-***57***).

13 Wij zijn van mening dat gebruikmaking van vooraf gecontracteerde aanbieders een snelle inzet van incidentresponsdiensten mogelijk maakt. Hoewel de EU-cyberbeveiligingsreserve in de eerste plaats tot doel heeft de respons en het herstel te ondersteunen, kan deze, wanneer zij niet wordt gebruikt voor de respons op incidenten, worden gebruikt voor paraatheid. Deze flexibele aanpak kan voorkomen dat vooraf betaalde diensten ongebruikt blijven. Het risico bestaat echter dat de reserve voornamelijk wordt gebruikt voor paraatheid in plaats van respons, wat in strijd is met het beoogde doel ervan (zie de paragrafen *58*-*61*).

14 Het Europees waarschuwingssysteem voor cyberbeveiliging is een netwerk van nationale en landsgrensoverschrijdende cyberhubs die tot doel hebben de opsporing en analyse van en de respons op cyberdreigingen te verbeteren. We hebben vastgesteld dat de twee hubs (ATHENA en ENSOC) ten tijde van de controle nog niet operationeel waren als gevolg van aanzienlijke vertragingen bij de aanbesteding van instrumenten en diensten, en dat het Europees waarschuwingssysteem voor cyberbeveiliging nog niet functioneerde (zie de paragrafen *62*-*70*).

15 Een van de belangrijkste doelstellingen van het Europees waarschuwingssysteem voor cyberbeveiliging is het stimuleren van zinvolle informatie-uitwisseling tussen clusters van lidstaten. Hoewel dit een oplossing zou kunnen bieden voor een aantal problemen op het gebied van informatie-uitwisseling, is het ook een enorme uitdaging om cyberhubs te integreren in het toch al complexe cyberbeveiligingslandschap. We constateerden dat de vereiste samenwerkingsovereenkomsten, gemeenschappelijke taxonomie en interoperabiliteitsnormen die nodig zijn voor de volledige werking van het Europees waarschuwingssysteem voor cyberbeveiliging nog niet bestonden (zie de paragrafen *71*-*74*).

Aanbeveling 3

Integreer het Europees waarschuwingssysteem voor cyberbeveiliging in het cyberbeveiligingslandschap van de EU

De Commissie moet er samen met Enisa en de lidstaten voor zorgen dat er samenwerkingsregelingen en interoperabiliteitsnormen worden vastgesteld om de informatie-uitwisseling te vergemakkelijken tussen landsgrensoverschrijdende hubs die deel uitmaken van het Europees waarschuwingssysteem voor cyberbeveiliging, het CSIRT-netwerk en EU-CyCLONe.

Streefdatum voor de uitvoering: 2028

16 In 2018 heeft de Commissie voorgesteld het Europees Kenniscentrum voor cyberbeveiliging (ECCC) op te richten om de cyberbeveiligingscomponent van DIGITAL vanaf 2021 te beheren. In de ECCC-verordening werd opgeroepen tot de oprichting van een Kennisgemeenschap voor cyberbeveiliging, bestaande uit vertegenwoordigers van de industrie, academische en onderzoeksorganisaties. Geselecteerde leden van de kennisgemeenschap voor cyberbeveiliging zouden dan een strategische adviesgroep (SAG) vormen (zie de paragrafen ***75*** en ***76***).

17 We constateerden dat er vertragingen waren bij het bereiken van financiële autonomie door het ECCC en bij de oprichting van de Kennisgemeenschap voor cyberbeveiliging en de SAG. Dit betekende dat de Kennisgemeenschap voor cyberbeveiliging en de SAG geen input konden leveren om de werkprogramma's van DIGITAL vorm te geven. Wij zien dit als een gemiste kans (zie de paragrafen ***77***-***81***).

18 We constateerden dat bij alle door ons onderzochte projecten relevante doelstellingen werden nagestreefd die bijdragen tot de verwezenlijking van de cyberbeveiligingsdoelstellingen van DIGITAL. Wij troffen echter gevallen aan waarin de kwaliteit of de bereikte resultaten niet bevredigend waren, voornamelijk vanwege vertragingen bij de uitvoering (zie de paragrafen ***82***-***87***).

19 In de DIGITAL-verordening is bepaald dat, om veiligheidsredenen, de financiering voor cyberbeveiliging kan worden beperkt tot entiteiten die zijn gevestigd in de lidstaten en waarover de lidstaten of burgers van de lidstaten zeggenschap hebben. De centrale valideringsdienst van het Europees Uitvoerend Agentschap onderzoek voert deze eigendoms- en zeggenschapsbeoordeling namens het ECCC uit (zie de paragrafen ***88***-***91***).

20 In het geval van financiële steun aan derden is de eigendoms- en zeggenschapsbeoordeling de verantwoordelijkheid van de projectbegunstigden, op basis van hun eigen aanpak en methodologie. We constateerden dat het ECCC zijn methodologie niet valideert en evenmin controles uitvoert om ervoor te zorgen dat geselecteerde derden eigendom zijn van en worden gecontroleerd door de EU. Wij zijn van mening dat er een aanzienlijk risico bestaat dat begunstigden niet over de capaciteit beschikken om deze controles naar behoren uit te voeren. Dit risico is niet voldoende beperkt en kan leiden tot de blootstelling van gevoelige infrastructuur, operationele gegevens en in veiligheidsopzicht kritieke technologieën (zie de paragrafen *92*-*96*).

Aanbeveling 4

Zorg voor een robuuste eigendoms- en zeggenschapsbeoordeling van entiteiten die EU-financiering ontvangen in het kader van het programma Digitaal Europa

Het Europees kenniscentrum voor cyberbeveiliging moet:

a) redelijke zekerheid verkrijgen dat begunstigden die verantwoordelijk zijn voor het verlenen van financiële steun aan derden, over de nodige administratieve en technische capaciteit beschikken om adequate eigendoms- en zeggenschapsbeoordelingen uit te voeren, op basis van de bestaande methodologie die ter beschikking staat van begunstigden die financiële steun aan derden verlenen, en

b) steekproefsgewijs controleren of alleen subsidiabele entiteiten EU-financiering hebben ontvangen.

Streefdatum voor de uitvoering: a) 2026, b) 2027

21 Begunstigden die door de EU gefinancierde projecten beheren, moeten aan het ECCC verslag uitbrengen over de vooruitgang en de resultaten ervan aan de hand van mijlpalen en te leveren prestaties. Deze zijn van cruciaal belang voor projectmonitoring en moeten naar behoren worden gedefinieerd. We constateerden dat bij nagenoeg geen van de projecten in onze steekproef de instructies werden gevolgd voor het opstellen van mijlpalen en te leveren prestaties, en dat veel ervan niet nuttig waren voor het volgen van de vooruitgang (zie de paragrafen *97*-*99*).

22 Wij constateerden dat veel van de door de begunstigden gebruikte prestatie-indicatoren niet relevant of meetbaar zijn en geen streefdoel of referentiewaarde hebben. Bovendien was de rapportage over deze indicatoren ontoereikend en kan deze daarom niet dienen als basis voor de beoordeling van de prestaties van projecten (zie de paragrafen ***100***-***102***).

23 Om de resultaten van DIGITAL als geheel te monitoren, moet bij alle projecten verslag worden uitgebracht over specifieke programma-indicatoren die worden meegenomen in de jaarlijkse prestatieoverzichten van de programma's van de Commissie. Het ECCC is verantwoordelijk voor het verzamelen en verifiëren van de gegevens die over deze indicatoren zijn verstrekt. We troffen verschillende problemen aan met betrekking tot de manier van gegevensverzameling en de algemene kwaliteit ervan. Wij troffen geen bewijs aan dat de nauwkeurigheid van de gerapporteerde gegevens door het ECCC was geverifieerd. Op basis van onze steekproefcontroles zijn wij van mening dat de gerapporteerde gegevens de bereikte resultaten niet nauwkeurig weergeven (zie de paragrafen ***103***-***106***).

Aanbeveling 5

Versterk het kader voor prestatiemonitoring van de cyberbeveiligingscomponent van het programma Digitaal Europa

Om adequate voortgangs- en prestatiemonitoring mogelijk te maken, moet het Europees Kenniscentrum voor cyberbeveiliging:

a) ervoor zorgen dat, voordat de subsidieovereenkomst wordt ondertekend, alle projecten beschikken over vastgestelde mijlpalen, te leveren resultaten en prestatie-indicatoren die voldoen aan de instructies in het aanvraagformulier;

b) een robuust systeem ontwerpen en invoeren voor het verzamelen, traceren, verifiëren en aggregeren van de gegevens voor de prestatie-indicatoren van het onderdeel cyberbeveiliging van het programma Digitaal Europa, om ervoor te zorgen dat de indicatoren een getrouw beeld geven van de bereikte resultaten.

Streefdatum voor de uitvoering: 2027

02 Onze bevindingen nader bekeken

Hoewel EU-cyberbeveiligingsnetwerken en -mechanismen samenwerking en respons ondersteunen, verminderen beperkte informatie-uitwisseling en onvolledige uitvoering de doeltreffendheid ervan

EU-netwerken maken samenwerking tussen de lidstaten mogelijk, maar door de beperkte uitwisseling van informatie neemt de toegevoegde waarde ervan af

24 Het huidige EU-kader van netwerken en mechanismen om de opsporing van en respons op significante cyberbeveiligingsincidenten te bevorderen, is geleidelijk opgebouwd, te beginnen met de richtlijn houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie[3] (NIS-richtlijn), die in augustus 2016 in werking is getreden. In ***bijlage II*** wordt het huidige EU-landschap geïllustreerd.

[3] Richtlijn (EU) 2016/1148.

EU-netwerken maken samenwerking tussen de lidstaten op technisch en operationeel niveau mogelijk

25 Bij de NIS-richtlijn is het CSIRT-netwerk ingesteld, dat CERT-EU (de cyberbeveiligingsdienst voor de instellingen, organen en instanties van de Unie) en de door de lidstaten aangewezen CSIRT's samenbrengt. Dit netwerk heeft tot doel vertrouwen tussen de nationale CSIRT's op te bouwen en een snelle en doeltreffende operationele samenwerking tussen de lidstaten te bevorderen.

26 EU-CyCLONe werd in 2020 opgericht als een informeel samenwerkingsnetwerk voor nationale autoriteiten die belast zijn met cybercrisisbeheer. Het dient als brug tussen de technische laag waar het CSIRT-netwerk actief is en de politieke laag van de Raad van de Europese Unie en zijn geïntegreerde regeling politieke crisisrespons. Met de inwerkingtreding van de NIS 2-richtlijn in 2023 werd de rol van EU-CyCLONe geformaliseerd en kreeg het een duidelijk mandaat.

27 Wij hebben beoordeeld of de rollen en verantwoordelijkheden van deze netwerken op EU-niveau goed zijn omschreven en of zij samenwerking tussen de lidstaten mogelijk maken.

28 Enisa fungeert als secretariaat van het CSIRT-netwerk en EU-CyCLONe en voorziet deze van de middelen, deskundigheid, infrastructuur en IT-instrumenten die nodig zijn voor samenwerking en beveiligde communicatie voor informatie-uitwisseling. In zijn tevredenheidsenquête onder belanghebbenden[4] van begin 2025 ontving Enisa goede scores voor zijn prestaties als secretariaat voor deze netwerken. Deze positieve feedback werd ook bevestigd tijdens onze controlebezoeken, waarbij de nationale cyberbeveiligingsautoriteiten hun waardering uitspraken.

---

[4] Geconsolideerd jaarlijks activiteitenverslag 2024 van Enisa, blz. 33 en 36.

29 In 2025 nam de Raad de cyberblauwdruk aan, waarin de taken en verantwoordelijkheden worden omschreven van de belangrijkste actoren (waaronder het CSIRT-netwerk en EU-CyCLONe) en mechanismen worden vastgelegd die bij grootschalige cyberbeveiligingsincidenten of cybercrises een rol spelen. We constateerden dat in de cyberblauwdruk de rollen en verantwoordelijkheden met betrekking tot cybercrisisbeheer in de EU grotendeels worden verduidelijkt en rekening wordt gehouden met de veranderingen in het landschap sinds de eerste blauwdruk in 2017. In de blauwdruk worden drie niveaus van samenwerking vastgesteld: technisch, operationeel en politiek. Ook worden hierin de nieuwe netwerken en structuren beschreven die sinds 2017 zijn opgezet — zoals EU-CyCLONe, de EU-teams voor snelle reactie op hybride dreigingen en het Europees waarschuwingssysteem voor cyberbeveiliging — en wordt ingegaan op de wijze waarop cybercrisisbeheer moet worden geïntegreerd in het bredere kader voor cybercrisisbeheer van de EU.

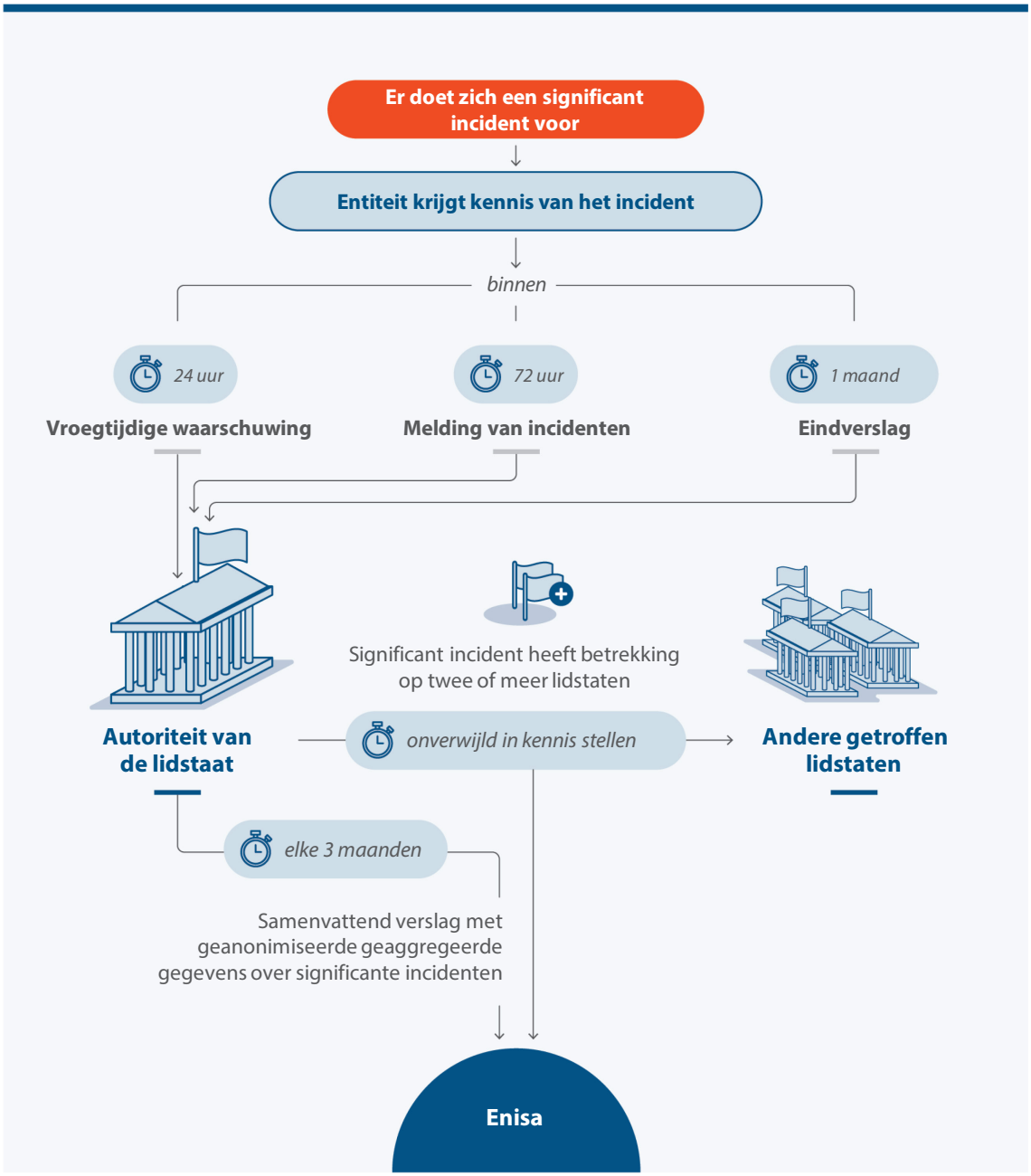
30 Ondanks de officiële oprichting van het CSIRT-netwerk in 2016 en EU-CyCLONe in 2023 moeten de twee netwerken de procedurele regelingen voor de samenwerking echter nog formaliseren. Ze hebben ook geen overeenstemming bereikt over de criteria voor het CSIRT-netwerk om EU-CyCLONe mee te delen dat een waargenomen cyberbeveiligingsincident een mogelijk of lopend grootschalig cyberbeveiligingsincident vormt. De twee netwerken moeten ook overeenstemming bereiken over een gemeenschappelijke taxonomie betreffende de ernst van incidenten en belangrijke concepten — zoals “dreiging”, “dreigingsactor”, “incident” of “impact” — die nodig is om geautomatiseerde informatie-uitwisseling mogelijk te maken. Momenteel is er ruimte voor interpretatie met betrekking tot de vraag wanneer een incident als significant of grootschalig kan worden aangemerkt. Het ontbreken van een gemeenschappelijke taxonomie werd genoemd door de cyberbeveiligingsautoriteiten van alle drie de door ons bezochte lidstaten.

Beperkte informatie-uitwisseling en rapportage verminderen de toegevoegde waarde van deze netwerken aanzienlijk

31 Geografische grenzen voorkomen niet dat cyberbeveiligingsincidenten en cyberaanvallen zich voordoen en verspreiden. Het uitwisselen van informatie tussen de lidstaten over bijvoorbeeld de tactieken en technieken die door dreigingsactoren worden gebruikt en over digitale tekenen dat er is ingebroken in een netwerk- of informatiesysteem (“indicatoren voor aantasting”), kan een aanzienlijke bijdrage leveren aan een betere cyberbeveiliging.

32 We hebben vastgesteld dat de uitwisseling van informatie beperkt was, waardoor de toegevoegde waarde van deze netwerken aanzienlijk werd verminderd. De beperkingen die we hebben vastgesteld hebben voornamelijk betrekking op vertragingen bij de omzetting van de NIS 2-richtlijn, problemen bij het bepalen of een incident grensoverschrijdende gevolgen heeft, nationale veiligheidswetgeving die informatie-uitwisseling beperkt, en een gebrek aan vertrouwen. Bij de NIS 2-richtlijn worden verschillende rapportagevereisten ingevoerd voor entiteiten die onder het toepassingsgebied ervan vallen en voor autoriteiten van de lidstaten, zoals geïllustreerd in ***figuur 2***.

Figuur 2 | Tijdschema voor het melden van incidenten in het kader van de richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de EU (NIS 2)



Bron: ERK, op basis van Enisa.

33 De lidstaten hadden tot oktober 2024 de tijd om de NIS 2-richtlijn in nationaal recht om te zetten, maar slechts twee lidstaten voldeden aan deze termijn. Vertragingen bij de omzetting hebben aanzienlijke gevolgen voor de uitwisseling van informatie, omdat de entiteiten die onder de NIS 2-richtlijn vallen, intussen niet wettelijk verplicht zijn incidenten te melden. De Commissie schatte[5] dat 15 500 entiteiten onder de NIS-richtlijn vielen, terwijl meer dan 110 000 entiteiten onder het toepassingsgebied van de NIS 2-richtlijn vielen. Zo waren overheidsinstanties, die volgens het verslag van 2025 over het dreigingslandschap van Enisa de meest getroffen sector in de EU vormden, op grond van de NIS-richtlijn niet verplicht om incidenten te melden.

34 Het feit dat incidentgegevens slechts om de drie maanden aan Enisa worden gemeld (d.w.z. lang nadat een incident zich mogelijk heeft voorgedaan), beperkt de toegevoegde waarde ervan. Deze gegevens dienen voornamelijk voor statistische doeleinden en de rapportage van historische trends, en niet om de opsporing en respons te verbeteren. Enisa biedt de lidstaten een online-instrument om hun meldingen in te dienen. Het meldingsmodel bevat een minimale reeks gegevens die moeten worden verstrekt, zoals het soort incident en de betrokken sector. Daarnaast stelt Enisa voor dat de lidstaten aanvullende informatie verstrekken om een grondiger analyse van de gegevens mogelijk te maken, bijvoorbeeld door incidenten te koppelen aan specifieke kwetsbaarheden. Niet alle lidstaten kiezen er echter voor deze informatie te verstrekken, waardoor de kwaliteit en de toegevoegde waarde van de verzamelde gegevens aanzienlijk afnemen.

35 Enisa heeft in zijn verslag van 2024 over de staat van de cyberbeveiliging in de EU verklaard dat incidenten waarschijnlijk te weinig worden gemeld, aangezien het aantal gemelde incidenten laag leek te zijn. In de jaren 2018 tot en met 2021 meldden de lidstaten jaarlijks tussen de 100 en 500 incidenten aan Enisa. Het aantal is geleidelijk toegenomen en steeg in 2024 tot 1 276[6].

---

[5] Europese Commissie, effectbeoordelingsverslag van 2020.

[6] CIRAS-gegevens voor 2024.

36 In zijn verslag van 2025 over het dreigingslandschap, dat betrekking heeft op de periode van juni 2024 tot juni 2025, heeft Enisa ongeveer 4 800 cyberbeveiligingsincidenten[7] geïdentificeerd aan de hand van inlichtingen uit open bronnen, zoals nieuwsartikelen. Deze incidenten zouden niet allemaal onder de NIS 2-richtlijn vallen, aangezien Enisa bij het verzamelen van de gegevens een breder spectrum aan incidenten in aanmerking neemt. Omgekeerd worden veel significante incidenten niet gemeld aan de hand van inlichtingen uit open bronnen. Aangezien de door de lidstaten gemelde gegevens geanonimiseerd zijn, kan Enisa de zelf vastgestelde incidenten niet koppelen aan de incidenten die door de lidstaten zijn gemeld. Het is daarom niet mogelijk de mate van onderrapportage nauwkeurig te bepalen, maar naar onze mening toont het verschil tussen het aantal door de lidstaten gemelde incidenten en de incidenten in het verslag over het dreigingslandschap aan dat niet alle significante incidenten worden gemeld.

37 Een andere aanwijzing voor onderrapportage is het aantal meldingen aan andere getroffen lidstaten en Enisa over significante grensoverschrijdende incidenten. Een soortgelijke vereiste bestond in het kader van de NIS-richtlijn, maar werd ondoeltreffend geacht, aangezien de Commissie in 2020 concludeerde[8] dat kennisgevingen ondanks de verplichting zelden werden verzonden. Zij weet het uitblijven van de kennisgeving aan het ontbreken van duidelijke regels voor het uitwisselen van informatie en het ontbreken van gemeenschappelijke doelstellingen die de uitwisseling zouden stimuleren.

38 De verplichting om andere lidstaten op de hoogte te stellen is van cruciaal belang om overloopeffecten van incidenten te voorkomen; het nalaten hiervan heeft een negatieve invloed op de cyberbeveiliging van de EU. In 2025 werden door zeven lidstaten slechts veertien significante grensoverschrijdende incidenten gemeld. De lidstaten hebben in 2024 twee incidentmeldingen met mogelijke grensoverschrijdende gevolgen ingediend, geen enkele in 2023 en drie in 2022. Hieruit blijkt dat het aantal meldingen van significante grensoverschrijdende incidenten zeer laag is en niet de werkelijke omvang van dergelijke aanvallen weerspiegelt. Om dit in perspectief te plaatsen, heeft Enisa in zijn verslag van 2024 over het dreigingslandschap 322 incidenten geïdentificeerd die specifiek gericht waren op twee of meer lidstaten. Het Collins Aerospace-incident (zie ***kader 1***) is een voorbeeld van lidstaten die een incident niet melden, ondanks het feit dat het een significante grensoverschrijdende impact heeft.

---

[7] Verslag van 2025 over het dreigingslandschap van Enisa.

[8] Europese Commissie, effectbeoordelingsverslag van 2020.

Kader 1

Cyberbeveiligingsincident dat luchthavenactiviteiten verstoort

In september 2025 kreeg Collins Aerospace, een belangrijke technologieleverancier voor de luchtvaartsector, te maken met een grote ransomwareaanval op zijn software voor passagiersverwerking. Door de aanval waren grote Europese luchthavens gedwongen om terug te keren naar handmatige activiteiten, wat leidde tot massale vertragingen en annuleringen van vluchten. De verstoring was het ernstigst op de luchthavens Londen Heathrow, Brussel, Berlijn Brandenburg en Dublin.

Volgens de NIS 2-richtlijn wordt een incident als “significant” beschouwd indien het onder meer ernstige operationele verstoring van de diensten of financieel verlies voor de betrokken entiteit veroorzaakt. Geen enkele lidstaat behandelde dit incident echter als significant of grootschalig grensoverschrijdend. Daarom heeft geen van de getroffen lidstaten Enisa of andere lidstaten formeel in kennis gesteld van het incident. Het CSIRT-netwerk heeft EU-CyCLONe niet geïnformeerd, waardoor dit netwerk het gecoördineerde beheer van het incident niet heeft ondersteund.

Bron: Analyse van de ERK op basis van gegevens uit vraaggesprekken met Enisa.

39 Een andere reden waarom grensoverschrijdende incidenten slechts in beperkte mate worden gemeld, is dat het aan de autoriteiten van elke lidstaat is om te bepalen of een gemeld incident grensoverschrijdende gevolgen heeft, en om vast te stellen welke andere lidstaten hierdoor worden getroffen. Op basis van de informatie waarover zij beschikken, is het mogelijk dat de entiteit of de lidstaatautoriteit die de melding doet zich niet bewust is van het grensoverschrijdende karakter van sommige aanvallen. Momenteel is er geen EU-breed platform dat realtimemelding van incidenten van alle lidstaten ontvangt en dat informatie over sectoren of indicatoren voor aantasting kan koppelen om grensoverschrijdende incidenten op te sporen. Daarom bestaat er een aanzienlijk risico dat sommige grensoverschrijdende incidenten niet als grensoverschrijdend worden geïdentificeerd en gemeld.

40 Sinds 2016 heeft geen enkele lidstaat een cyberbeveiligingsincident als “grootschalig” aangemerkt. In principe valt elk incident dat significante gevolgen heeft voor ten minste twee lidstaten onder die definitie. Desalniettemin worden zelfs cyberbeveiligingsincidenten die wereldwijde storingen en aanzienlijke schade hebben veroorzaakt, zoals die in ***figuur 3***, niet als grootschalig beschouwd. Als gevolg daarvan is de escalatieprocedure EU-CyCLONe nooit volledig geactiveerd als gevolg van een grootschalig cyberbeveiligingsincident.

Figuur 3 | Voorbeelden van grote cyberbeveiligingsincidenten

WannaCry

2017

Een wereldwijde ransomware-aanval

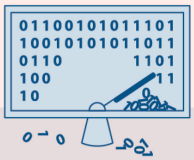
Hierbij werden ruim 200 000 computers in meer dan 150 landen geïnfecteerd, waardoor exploitanten van kritieke infrastructuur werden lamgelegd; gegevens op geïnfecteerde apparaten werden versleuteld en er werd losgeld geëist voor ontsleuteling

NotPetya

2017

Een schadelijke malware die zich voordoet als ransomware

Ontworpen om gegevens definitief te wissen en voornamelijk gericht op Oekraïne; de malware verspreidde het zich razendsnel over de hele wereld waardoor multinationale ondernemingen werden lamgelegd en wereldwijd schade werd aangericht



IT-storing in verband met CrowdStrike

juli 2024

Een wereldwijde massale IT-storing

Veroorzaakt door een foutieve software-update van het cyberbeveiligingsbedrijf CrowdStrike, waardoor miljoenen computers crashten

Bron: ERK, aangepast op basis van Cloudflare, Enisa, Europol, Wired, IBM, CrowdStrike.

41 Naast de meldingsverplichting voor entiteiten en lidstaten is het CSIRT-netwerk opgericht om de uitwisseling van informatie te vergemakkelijken. Vertrouwen tussen de lidstaten vormt de kern van het CSIRT-netwerk, waarbinnen informatie op vrijwillige basis wordt gedeeld. De toegevoegde waarde van het netwerk wordt aanzienlijk verminderd als de lidstaten niet bereid zijn tijdig bruikbare informatie uit te wisselen.

42 Het uitwisselen van informatie op EU-niveau wordt beperkt door de nationale veiligheidswetgeving van elke lidstaat. Indien een lidstaat van mening is dat informatie over een cyberaanval op een kritieke entiteit vertrouwelijk is, of dat het melden van een specifiek incident schadelijk zou zijn voor zijn nationale veiligheid, is hij niet verplicht deze informatie te delen. Tijdens onze bezoeken aan de lidstaten verklaarden vertegenwoordigers van het CSIRT-netwerk en EU-CyCLONe dat informatie-uitwisseling alleen mogelijk is binnen de grenzen van de nationale veiligheidswetgeving. Er is op EU-niveau geen analyse uitgevoerd van de nationale rechtskaders van de lidstaten en de gevolgen daarvan voor de informatie-uitwisseling.

43 In 2016 bestond het CSIRT-netwerk uit 28 nationale CSIRT's, met twee vertegenwoordigers per lidstaat. Het gebrek aan informatie-uitwisseling is een hardnekkig probleem, en in de evaluatie van de NIS-richtlijn door de Commissie wordt erkend dat de lidstaten niet systematisch informatie met elkaar uitwisselen, wat met name van invloed is op de doeltreffendheid van de cyberbeveiligingsmaatregelen en het niveau van gezamenlijk situationeel bewustzijn op EU-niveau. In het kader van de NIS 2-richtlijn hebben veel lidstaten naast hun nationale CSIRT sectorale CSIRT's aangewezen, waardoor het netwerk aanzienlijk is uitgebreid. Ten tijde van de controle bestond het uit 42 CSIRT's en meer dan 700 individuele deelnemers. Dit maakt het nog moeilijker vertrouwen op te bouwen, aangezien het onderhouden van nauwe betrekkingen tussen alle leden moeilijk is.

44 Het CSIRT-netwerk is zich bewust van het probleem rond het uitwisselen van informatie en overweegt verschillende maatregelen om het vertrouwen in het groeiende netwerk te vergroten. Het opzetten van kleinere clusters van lidstaten die landsgrensoverschrijdende hubs vormen, zoals uiteengezet in de paragrafen ***62-74***, is een alternatieve aanpak voor een EU-breed netwerk waarmee deze uitdaging kan worden aangepakt.

Er is een gedeeltelijke overlapping tussen de gecontracteerde diensten van het cybersituatiecentrum en de bestaande capaciteiten, en de toekomstige werking ervan is niet duidelijk

45 In het kader van de NIS 2-richtlijn, in gevallen waarin een mogelijk of lopend grootschalig cyberbeveiligingsincident een aanzienlijke impact heeft of dreigt te hebben, wordt de Commissie lid van EU-CyCLONe[9]. Deze nieuwe rol en de ontwikkeling van het dreigingslandschap hebben de Commissie ertoe gebracht om in 2022 binnen DG Connect een taskforce voor cybercoördinatie op te richten. Deze taskforce omvat een cybersituatiecentrum, dat de Commissie moet helpen haar situationeel bewustzijn te vergroten, met als doel om haar institutionele verantwoordelijkheden op het gebied van crisisbeheer te ondersteunen. De taskforce moet ook DG Connect helpen om advies te verstrekken op politiek niveau.

[9] Artikel 16, lid 2, van de NIS 2-richtlijn.

46 Voor de oprichting van het cybersituatiecentrum wordt de Commissie grotendeels ondersteund door externe dienstverleners die in december 2022 zijn gecontracteerd voor bijna 18 miljoen EUR over een periode van vier jaar. We beoordeelden de oprichting van het centrum, de output ervan en de plannen van de Commissie voor de toekomstige werking ervan.

47 Als onderdeel van de verleende diensten hebben de contractanten een dashboard opgezet op basis van commerciële informatiebronnen over cyberdreigingen om dreigingsinformatie te presenteren en te delen. Zij stellen ook verschillende inlichtingenverslagen over cyberdreigingen op, waaronder dagelijkse en wekelijkse verslagen en thematische verslagen over landen of sectoren van de economie. Het fysieke cybersituatiecentrum, dat bestaat uit een ruimte met werkstations die op afstand zijn aangesloten op het dashboard dat door de contractanten wordt gehost, is opgezet in een van de gebouwen van de Commissie. Ten tijde van de controle bestond het cybersituatiecentrum uit een klein aantal medewerkers van de Commissie, die werden ondersteund door een groot aantal analisten van de contractanten en door deskundigen van Enisa.

48 We constateerden dat er een gedeeltelijke overlapping is tussen de door de externe dienstverleners verrichte werkzaamheden voor het cybersituatiecentrum en de bestaande capaciteit van Enisa. Enisa heeft een permanente capaciteit voor situationeel bewustzijn en dreigingsmonitoring. Het publiceert regelmatig verslagen over cyberdreigingen, met inbegrip van korte overzichten ("flash reports") over specifieke incidenten, en wekelijkse verslagen met een overzicht van dreigingen. De verslagen zijn gebaseerd op inlichtingen uit open bronnen en zijn vergelijkbaar met die van de contractanten. Daarnaast verstrekt Enisa — of draagt het bij aan — briefings op hoog niveau voor beleidsmakers in tijden van crisis, die ook vergelijkbaar zijn met wat het cybersituatiecentrum produceert.

49 Bovendien zijn de gegevens die door het cybersituatiecentrum worden gebruikt om deze verslagen op te stellen, gebaseerd op commerciële informatiebronnen over cyberdreigingen en zijn zij vergelijkbaar met de gegevens die worden gebruikt door andere diensten van de Commissie, zoals het directoraat-generaal Digitale Diensten en CERT-EU. Wij zijn van mening dat bij de oprichting van het cybersituatiecentrum niet het volledige potentieel is benut van de mogelijkheden tot rationalisering door gebruik te maken van informatie die reeds beschikbaar was bij de Commissie en Enisa.

50 Het contract loopt af in december 2026, waarna de contractanten de diensten voor het cybersituatiecentrum niet langer zullen verlenen. Deze diensten omvatten het beschikbaar stellen van de gegevens in het dashboard, het opstellen van de dreigingsverslagen en het feit dat de diensten het grootste deel van het centrum uitmaken. Het dashboard wordt aan de Commissie overgedragen, maar verliest zijn toegevoegde waarde als het niet voortdurend wordt bijgewerkt met inlichtingen over cyberdreigingen.

51 Ten tijde van de controle had de Commissie geen plannen met betrekking tot de ondersteuning door de externe dienstverleners bij de werking van het cybersituatiecentrum na afloop van het contract. We zijn van mening dat het ontbreken van een alomvattend, gedetailleerd plan voor de toekomst na afloop van het contract een risico inhoudt voor de werking van het cybersituatiecentrum na 2026.

Dankzij de EU-cyberbeveiligingsreserve kunnen incidentresponsdiensten snel worden ingezet

52 In 2022, onmiddellijk na de militaire agressie van Rusland tegen Oekraïne en in het besef dat grootschalige cyberaanvallen steeds vaker voorkomen, heeft de Commissie Enisa 15 miljoen EUR aan uitzonderlijke financiering verstrekt om de in 2023 gelanceerde ondersteunende actie op het gebied van cyberbeveiliging te testen. In 2023 verstrekte de Commissie aanvullende financiering (ongeveer 20 miljoen EUR) om het programma tot eind 2026 te verlengen.

53 De Commissie heeft ook de verordening cybersolidariteit voorgesteld, die in december 2024 werd vastgesteld, ter voorbereiding op grootschalige cyberbeveiligingsincidenten. Bij de verordening wordt een EU-cyberbeveiligingsreserve ingesteld die incidentresponsdiensten van betrouwbare aanbieders omvat. Deze reserve is in 2025 geleidelijk in werking getreden, met een budget van 36 miljoen EUR voor de periode 2025-2027.

54 We beoordeelden hoe het actieprogramma ter ondersteuning van cyberbeveiliging was georganiseerd, aangezien het de basis vormt voor de EU-cyberbeveiligingsreserve. Wij zijn ook nagegaan of de lessen die sinds 2022 zijn getrokken, zijn meegenomen in het ontwerp van de EU-cyberbeveiligingsreserve.

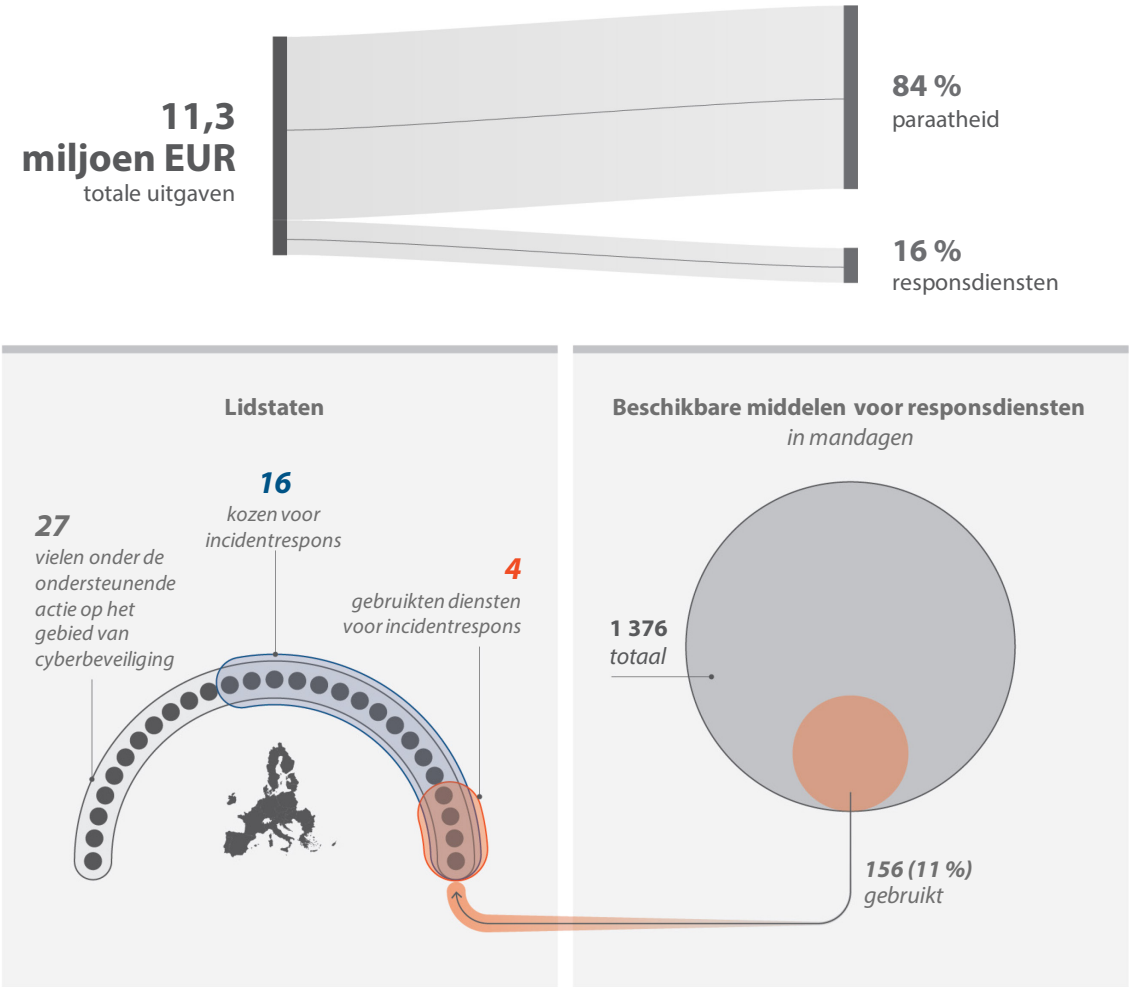
55 Enisa heeft de actie ter ondersteuning van cyberbeveiliging opgezet als een mechanisme om diensten te verlenen ter ondersteuning van de paraatheid voor en respons van de lidstaten op grootschalige cyberbeveiligingsincidenten of -crises. Alle diensten zijn vooraf door Enisa gecontracteerd, wat betekent dat dienstverleners aan de slag kunnen zodra de lidstaten hen nodig hebben. Dit is ook te danken aan de opzet van Enisa, die ervoor zorgt dat er dag en nacht een medewerker klaarstaat om verzoeken van de lidstaten te behandelen.

56 Enisa heeft ervoor gekozen het beschikbare budget gelijkelijk over de lidstaten te verdelen. In de praktijk heeft het agentschap een openbare aanbestedingsprocedure uitgeschreven, verdeeld in 27 percelen, één per lidstaat, om maximaal drie particuliere beveiligingsbedrijven te selecteren voor het verlenen van diensten tot eind 2026. Daarnaast heeft Enisa in het kader van een pan-Europees perceel een aantal aanbieders geselecteerd om diensten te verlenen aan in aanmerking komende niet-EU-landen en aan EU-instellingen, -organen en -agentschappen, of om de respons op grensoverschrijdende incidenten te ondersteunen.

57 Dankzij deze aanpak kon Enisa rekening houden met specifieke nationale vereisten, waaronder taal, nationale veiligheidsmachtigingen of gevestigde aanwezigheid in de lidstaten. Aangezien de aanbieders echter niet zijn geselecteerd om in de hele EU diensten te kunnen verlenen, is een belangrijk nadeel van deze aanpak dat, als een lidstaat geen gebruik maakt van de vooraf gecontracteerde diensten, de voor die diensten voor een specifieke lidstaat vastgelegde begroting niet kan worden gebruikt om een andere lidstaat te ondersteunen.

58 Voor de actie ter ondersteuning van cyberbeveiliging konden de lidstaten kiezen tussen paraatheids- of responsdiensten, of een combinatie van beide. De lidstaten hebben er in de eerste plaats voor gekozen de beschikbare financiering te gebruiken om hun paraatheid te verbeteren (84 % van de uitgaven in 2023). De lidstaten die ervoor kozen een incidentrespons te hebben (d.w.z. een vooraf bepaalde overeenkomst met een aanbieder die ervoor zorgt dat de lidstaat op verzoek toegang heeft tot de diensten van de aanbieder met het oog op een snelle respons op cyberbeveiligingsincidenten), maakten er spaarzaam gebruik van, zoals blijkt uit ***figuur 4***. In de drie bezochte lidstaten spraken de autoriteiten hun waardering uit voor het beheer door Enisa van de actie ter ondersteuning van cyberbeveiliging.

Figuur 4 | Actie van Enisa ter ondersteuning van cyberbeveiliging tot 2023



Bron: ERK, op basis van gegevens van Enisa.

59 Voor de periode 2024-2026 hebben slechts negen lidstaten om een incidentrespons verzocht. Onze vraaggesprekken met Enisa en de autoriteiten in drie lidstaten hebben bevestigd dat er een sterke voorkeur bestaat voor paraatheidsactiviteiten.

60 Hoewel de EU-cyberbeveiligingsreserve in de eerste plaats tot doel heeft de respons op en het herstel van grote cyberbeveiligingsincidenten te ondersteunen, kunnen vooraf vastgelegde diensten uit de EU-cyberbeveiligingsreserve die niet voor incidentrespons worden gebruikt, worden omgezet in paraatheidsdiensten. Deze flexibele aanpak kan voorkomen dat vooraf betaalde diensten ongebruikt blijven.

61 Wij zijn van mening dat het voor de EU-cyberbeveiligingsreserve gekozen model voortbouwt op de lessen die zijn getrokken uit het actieprogramma ter ondersteuning van cyberbeveiliging. De gegevens over het gebruik van het actieprogramma ter ondersteuning van cyberbeveiliging wijzen echter op het risico dat de EU-cyberbeveiligingsreserve in de eerste plaats wordt gebruikt voor paraatheid en niet voor respons, wat in strijd is met het doel van de verordening cybersolidariteit.

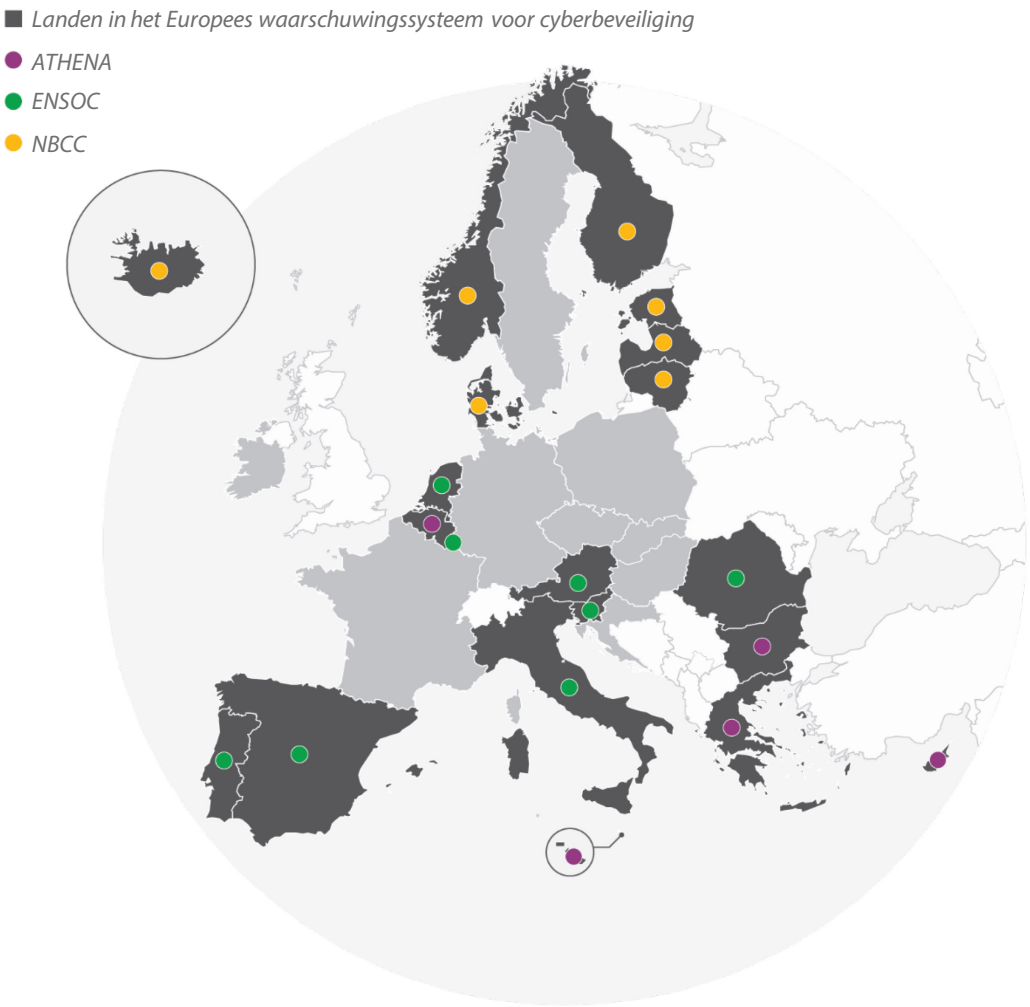
Het Europees waarschuwingssysteem voor cyberbeveiliging heeft tot doel de capaciteit voor het opsporen van dreigingen te verbeteren, maar is niet operationeel

62 Een van de belangrijkste doelstellingen van het Europees waarschuwingssysteem voor cyberbeveiliging is het stimuleren van zinvolle informatie-uitwisseling om de opsporing en analyse van en de respons op cyberdreigingen te verbeteren. Deelname aan het waarschuwingssysteem is vrijwillig, maar lidstaten die ervoor kiezen zich bij een landsgrensoverschrijdende cyberhub aan te sluiten, moeten zich ertoe verbinden relevante informatie met de andere leden te delen. Door samen te werken in clusters in een betrouwbare en veilige omgeving, zouden de lidstaten sommige van de in de paragrafen ***31***-***44*** genoemde problemen in verband met informatie-uitwisseling kunnen vermijden.

63 Ten tijde van de controle hadden 13 lidstaten ervoor gekozen deel te nemen aan het Europees waarschuwingssysteem voor cyberbeveiliging, waarbij twee landsgrensoverschrijdende hubs werden opgericht: ATHENA en ENSOC. Een derde landsgrensoverschrijdende cyberhub, NBCC, had in 2026 financiering toegewezen gekregen voor de oprichting ervan, zodat er in totaal 20 landen (18 lidstaten, alsook Ijsland en Noorwegen[10]) lid waren van het netwerk, zoals weergegeven in ***figuur 5***.

[10] Geassocieerde derde landen overeenkomstig artikel 10, lid 1, punt a), van Verordening (EU) 2021/694.

Figuur 5 | Landen in het Europees waarschuwingssysteem voor cyberbeveiliging



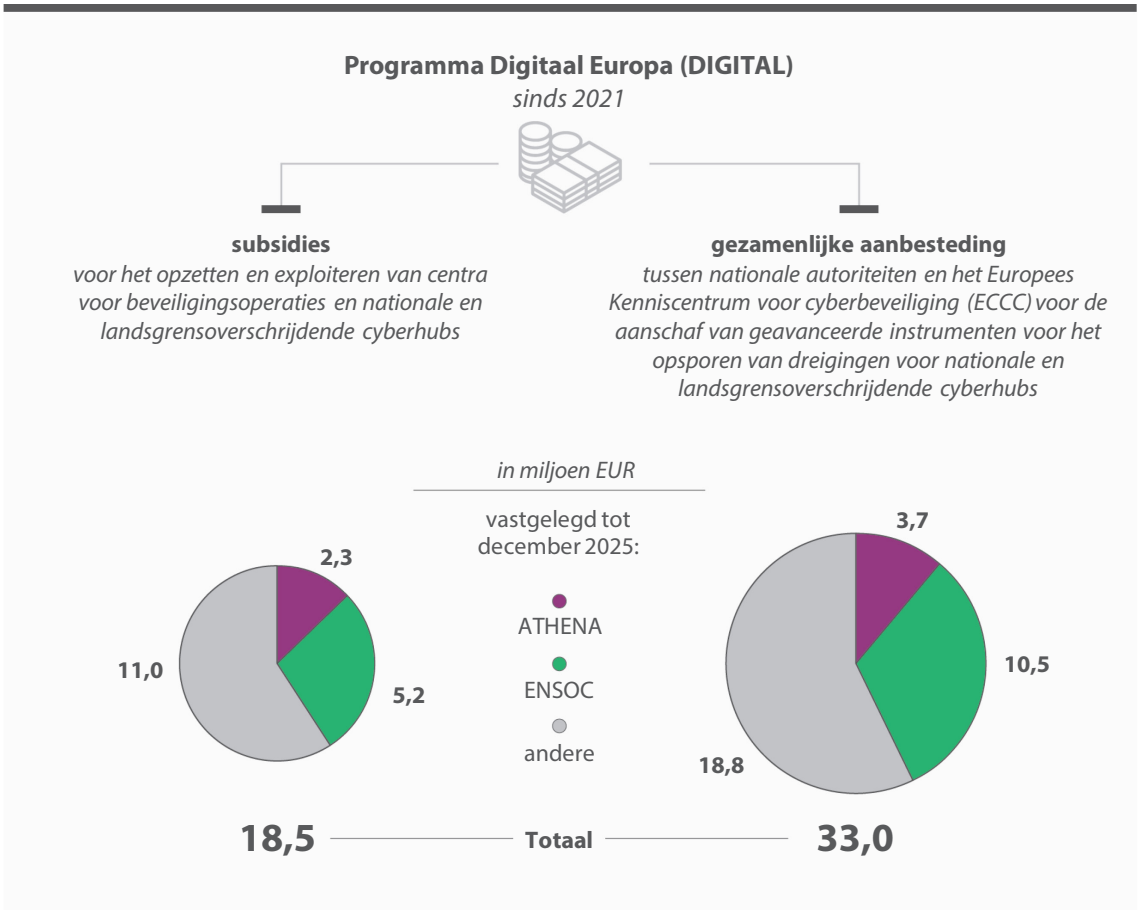
Bron: ERK.

64 Wij hebben beoordeeld hoe de eerste twee landsgrensoverschrijdende cyberhubs zijn opgezet en welke vooruitgang ermee is geboekt bij de verwezenlijking van de doelstellingen van het Europees waarschuwingssysteem voor cyberbeveiliging. We onderzochten ook hoe de oprichting van de landsgrensoverschrijdende cyberhubs past in het bredere cyberbeveiligingslandschap alsmede de wisselwerking ervan met bestaande netwerken en structuren.

Tot dusver zijn er geen concrete resultaten geboekt wegens aanzienlijke vertragingen bij aanbesteding

65 Sinds 2021 is er vanuit DIGITAL financiering beschikbaar voor de oprichting van nationale en landsgrensoverschrijdende cyberhubs. Deze financiering verloopt via een complexe procedure met twee parallelle trajecten: traditionele subsidies ter ondersteuning van de oprichting en exploitatie van de hubs, en gezamenlijke aanbestedingen voor de aanschaf van geavanceerde instrumenten voor het opsporen van dreigingen, zoals weergegeven in *figuur 6*. Na een oproep tot het indienen van voorstellen in november 2022 zijn ATHENA en ENSOC in januari 2024 met hun werkzaamheden begonnen.

Figuur 6 | Financiering van cyberhubs in het kader van het programma Digitaal Europa



Bron: ERK, op basis van gegevens van het ECCC.

66 De niet-openbare aanbestedingsprocedures in twee fasen[11] werden georganiseerd door de leden van ATHENA en ENSOC, alsook door DG Connect (de eerste fase) en het onlangs opgerichte ECCC (de tweede fase). De tweefasenaanpak heeft tot doel de verspreiding van gevoelige informatie te beperken door de gedetailleerde technische specificaties alleen te verstrekken aan kandidaten die in de eerste fase zijn geselecteerd.

67 De eerste fase ging in mei 2024 van start voor ENSOC en in juli 2024 voor ATHENA. Geïnteresseerde bedrijven hadden een maand de tijd om een aanvraag in te dienen. De geslaagde kandidaten werden echter pas in april 2025 op de hoogte gebracht, bijna een jaar na de start van de procedure.

68 Bovendien konden op dat moment noch de ENSOC- noch de ATHENA-aanbestedingsprocedures naar de tweede fase overgaan, aangezien de leden van de hub en het ECCC de geselecteerde bedrijven niet de technische specificaties konden verstrekken die nodig waren om een offerte in te dienen, omdat zij nog bezig waren met het afronden daarvan.

69 De tweede fase van de aanbestedingsprocedures ging pas in augustus 2025 van start voor sommige ENSOC-percelen en was gepland voor begin 2026 voor ATHENA. Ten tijde van de controle, 18 maanden na de start van de aanbestedingsprocedure, was voor geen van de percelen een contract ondertekend. Wij zijn van mening dat het gebrek aan adequate voorbereiding en de complexiteit van de aanbestedingsprocedures nadelig waren voor de tijdige voltooiing ervan.

70 Daarom stelden we vast dat de landsgrensoverschrijdende hubs niet op schema liggen om hun doelstellingen te verwezenlijken. Zonder de middelen om bedreigingen op te sporen en informatie uit te wisselen, liggen hun activiteiten stil en is het Europees waarschuwingssysteem voor cyberbeveiliging nog niet operationeel, waardoor de doeltreffende ontwikkeling van geavanceerde capaciteiten voor het opsporen en voorkomen van cyberdreigingen en -incidenten vertraging oploopt. Er zijn wijzigingen ondertekend om de looptijd van de subsidieovereenkomst te verlengen, teneinde rekening te houden met de vertragingen die tot nu toe bij de aanbestedingsprocedures zijn opgetreden (15 maanden voor ATHENA en 18 maanden voor ENSOC).

---

[11] Aanbesteding van ENSOC en aanbesteding van ATHENA.

Landsgrensoverschrijdende cyberhubs zorgen voor aanvullende communicatiekanalen waardoor de complexiteit verder toeneemt

71 Een van de belangrijkste taken van de landsgrensoverschrijdende cyberhubs is het delen van relevante informatie om de opsporing van en respons op dreigingen te verbeteren. Dit omvat informatie over cyberdreigingen, kwetsbaarheden, indicatoren voor aantasting en dreigingsactoren. De taken van de landsgrensoverschrijdende cyberhubs overlappen gedeeltelijk met die van de nationale CSIRT's en het CSIRT-netwerk, met name wat betreft de uitwisseling van informatie over cyberdreigingen en kwetsbaarheden. Er is geen duidelijke grens tussen de rollen van landsgrensoverschrijdende cyberhubs en CSIRT's. Volgens de cyberblauwdruk van 2025 (punt ***29***) zijn landsgrensoverschrijdende cyberhubs bedoeld om op zowel technisch (zoals de nationale CSIRT's en het CSIRT-netwerk) als operationeel niveau (zoals EU-CyCLONe) te opereren.

72 Op grond van de verordening cybersolidariteit moeten landsgrensoverschrijdende cyberhubs samenwerkingsovereenkomsten met elkaar sluiten om de uitwisseling van informatie te vergemakkelijken. Enisa had uiterlijk in februari 2026 richtsnoeren voor interoperabiliteit tussen landsgrensoverschrijdende cyberhubs moeten uitvaardigen, zoals vereist door de verordening cybersolidariteit. Ondertussen heeft het ECCC in december 2025 een subsidie toegekend aan een consortium (met inbegrip van bepaalde ENSOC- en ATHENA-leden) om een technisch kader voor interoperabiliteit tussen landsgrensoverschrijdende cyberhubs vast te stellen. De richtsnoeren en het kader zullen echter pas worden voltooid wanneer de landsgrensoverschrijdende cyberhubs operationeel zijn. Zoals wij in ons advies van 2023 over het voorstel voor de verordening cybersolidariteit hebben opgemerkt[12], bestaat het risico dat zonder een snel akkoord systemen worden ontwikkeld die onderling onverenigbaar zijn, wat tot hogere kosten leidt.

[12] Advies 02/2023 over het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van maatregelen ter versterking van de solidariteit en de capaciteit in de Unie om cyberdreigingen en -incidenten op te sporen, zich erop voor te bereiden en erop te reageren, paragraaf 26.

73 Landsgrensoverschrijdende cyberhubs moeten ook onverwijld relevante informatie over grootschalige cyberbeveiligingsincidenten delen met EU-CyCLONe en het CSIRT-netwerk. Op het niveau van de lidstaten zorgen de oprichting van nationale cyberhubs en de deelname aan landsgrensoverschrijdende cyberhubs voor extra communicatielagen. De coördinatie met niet-EU-lidstaten[13] die geen lid zijn van het CSIRT-netwerk of EU-CyCLONe, vergroot ook de complexiteit.

74 Er zijn duidelijke samenwerkingsovereenkomsten nodig om overeenstemming te bereiken over een gemeenschappelijke taxonomie en over de wijze waarop informatie moet worden uitgewisseld, en om interoperabiliteit te waarborgen. Uit de lessen die zijn getrokken uit het CSIRT-netwerk blijkt dat dit een aanzienlijke uitdaging is. We constateerden dat er ten tijde van de controle geen procedurele regelingen inzake samenwerking en informatie-uitwisseling waren overeengekomen. We zijn van mening dat de oprichting van nationale en landsgrensoverschrijdende cyberhubs een doeltreffendere informatie-uitwisseling kan bevorderen. De integratie van de landsgrensoverschrijdende hubs in het reeds complexe cyberbeveiligingslandschap zal echter een uitdaging vormen en extra communicatiekanalen en samenwerkingsregelingen vereisen.

[13] IJsland en Noorwegen.

Door de EU gefinancierde projecten in het kader van DIGITAL hebben tot doel de cyberbeveiliging te versterken, maar worden geconfronteerd met uitdagingen op het gebied van uitvoering en rapportage

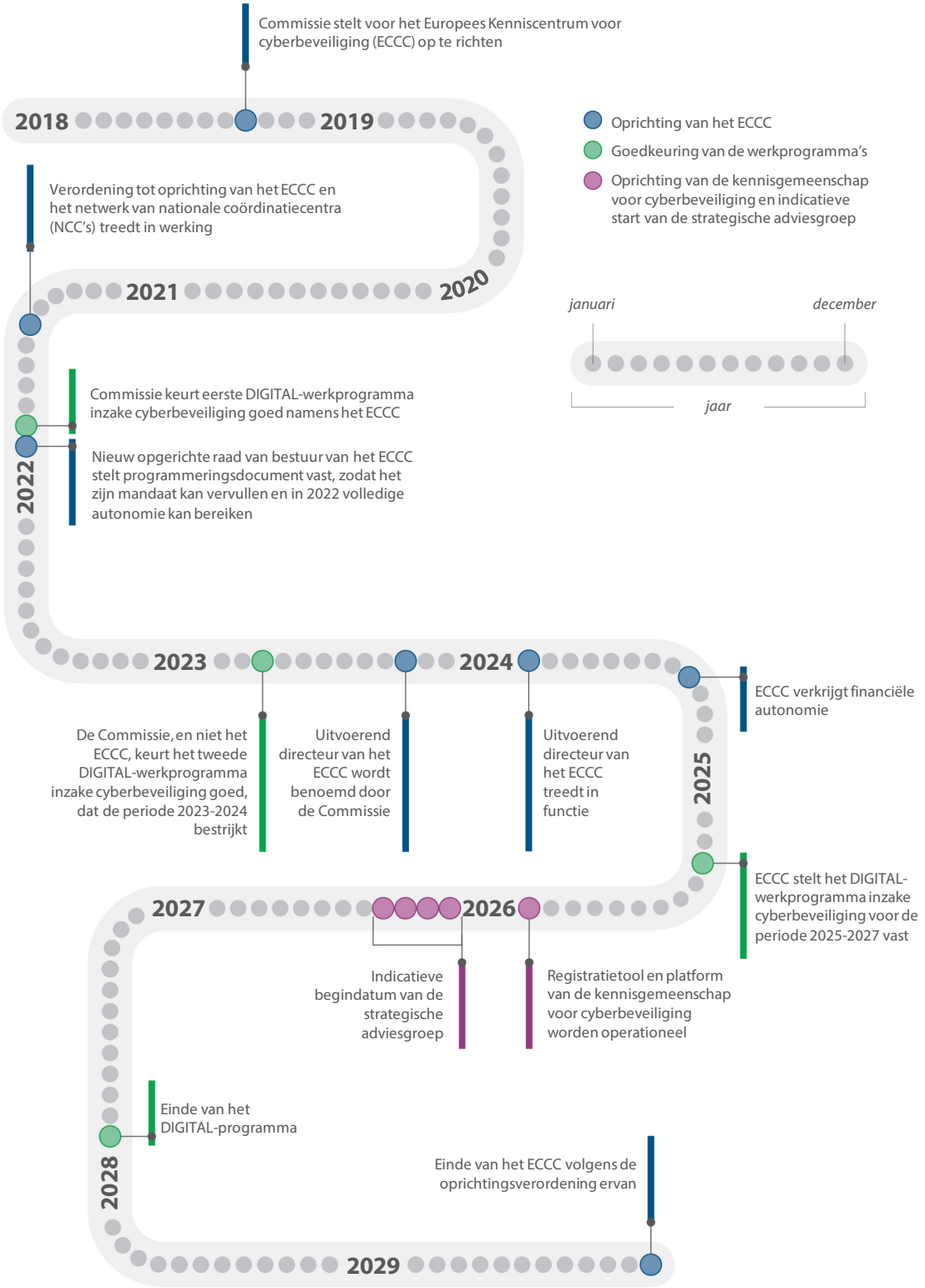
Vertragingen bij de oprichting ervan verhinderden dat de kennisgemeenschap voor cyberbeveiliging DIGITAL kon vormgeven op basis van haar behoeften

75 Om de cyberbeveiligingscomponent van DIGITAL te beheren, heeft de Commissie in 2018 voorgesteld het Europees Kenniscentrum voor cyberbeveiliging (ECCC) op te richten. Volgens de ECCC-verordening zou het ECCC worden ondersteund door een netwerk van 29 nationale coördinatiecentra (NCC's), een voor elke lidstaat, en IJsland en Noorwegen. Het drong ook aan op de oprichting van de kennisgemeenschap voor cyberbeveiliging (de gemeenschap), bestaande uit vertegenwoordigers van het bedrijfsleven, academische en onderzoeksorganisaties en andere relevante verenigingen uit het maatschappelijk middenveld.

76 Maximaal twintig leden van de gemeenschap zouden worden benoemd in de strategische adviesgroep (SAG), een van de drie componenten van de structuur van het ECCC. Een van de belangrijkste taken van de SAG is het organiseren van openbare raadplegingen als input voor de agenda van het ECCC en de DIGITAL-werkprogramma's.

77 Wij beoordeelden of DIGITAL en zijn werkprogramma's werden vastgesteld op basis van een gedegen behoeftenanalyse, en hoe het ECCC, het netwerk van NCC's, de gemeenschap en de SAG konden bijdragen aan de werkprogramma's. In de praktijk zijn het ECCC, het netwerk van NCC's, de gemeenschap en de SAG in de loop der jaren geleidelijk opgericht (zie figuur *7*).

Figuur 7 | Tijdlijn van de oprichting van het Europees Kenniscentrum voor cyberbeveiliging, het netwerk van nationale coördinatiecentra, de gemeenschap en de strategische adviesgroep



Bron: ERK.

78 Aangezien het ECCC pas in september 2024 volledig operationeel werd, heeft de Commissie namens het ECCC de werkprogramma's voor de perioden 2021-2022 en 2023-2024 vastgesteld. De twee door de Commissie goedgekeurde werkprogramma's konden geen voordelen genieten van de inbreng van de gemeenschap.

79 Ondertussen zijn de lidstaten begonnen met de oprichting van hun NCC's, die fungeren als contactpunten op nationaal niveau voor de gemeenschap. De oprichting en werking ervan zijn gecofinancierd door DIGITAL, waarbij ten tijde van de controle meer dan 90 miljoen EUR aan EU-financiering was toegekend, waarvan ongeveer 44 miljoen EUR verder zal worden verdeeld door middel van financiële steun aan derden. Er is tot 2027 38 miljoen EUR extra begroot om NCC's te ondersteunen.

80 We constateerden dat de gemeenschap in december 2025, vier jaar na de oprichting van het ECCC en het netwerk van NCC's, nog niet was opgericht en de SAG nog niet was benoemd. Het ECCC heeft op 14 maart 2025 het meest recente DIGITAL-werkprogramma inzake cyberbeveiliging voor de periode 2025-2027 vastgesteld. Hoewel het ECCC zijn werkprogramma heeft opgesteld en vastgesteld na uitgebreid overleg met de lidstaten en het netwerk van NCC's, kon het niet profiteren van input en advies van de gemeenschap of de SAG. Dit is in strijd met de bepalingen van de oprichtingsverordening ervan en wij beschouwen dit als een gemiste kans.

81 DIGITAL zal in 2027 aflopen en als zijn mandaat niet wordt verlengd, zal het ECCC naar verwachting in 2029 worden opgeheven. Zodoende is de steun van het netwerk van NCC's, de gemeenschap en de SAG, zodra deze is opgezet, mogelijk slechts voor een korte periode relevant.

Met door de EU gefinancierde projecten worden relevante doelstellingen nagestreefd, maar veel projecten worden geconfronteerd met operationele problemen

82 We selecteerden een steekproef van elf projecten die relevant waren voor de opsporing van en respons op cyberbeveiligingsincidenten en die werden gefinancierd in het kader van DIGITAL in de periode 2022-2025 (zie ***figuur 5*** in ***bijlage I*** en ***bijlage III***). Wij hebben beoordeeld of:

- de doelstellingen van de projecten strookten met de verwachte resultaten in de oproepen tot het indienen van voorstellen en die van DIGITAL in het algemeen;
- de projecten tot dusver hun geplande output en resultaten hebben bereikt;
- de resultaten van de projecten tijdig zijn geleverd.

We presenteren het resultaat van deze beoordeling in ***bijlage IV***.

Sommige projecten leveren in een vroeg stadium resultaten op, maar veel ervan worden geconfronteerd met operationele uitdagingen en vertragingen

83 We constateerden dat alle projecten doelstellingen nastreven die bijdragen tot de verwezenlijking van de doelstellingen van DIGITAL op het gebied van cyberbeveiliging[14] en dat zij betrekking hebben op de meeste doelstellingen van de oproepen tot het indienen van voorstellen[15].

84 Van de elf projecten in onze steekproef bevonden twee projecten zich in een vroeg stadium van uitvoering, waardoor we geen conclusies konden trekken over de prestaties ervan. Van de overige beoordeelden we vier als bevredigend wat betreft de verwezenlijking van hun geplande output en resultaten. We waren van mening dat twee projecten enkele tekortkomingen vertoonden en we beoordeelden drie projecten als onbevredigend (zie ***bijlage IV***).

---

[14] Artikel 6 van Verordening (EU) 2021/694 tot oprichting van het programma Digitaal Europa.

[15] Oproepen: Capacity building of security operation centres; Deploying the network of national coordination centres with member states; Preparedness support and mutual assistance; en Novel applications of AI and other enabling technologies for security operation centres.

85 Digitalisering heeft uitdrukkelijk tot doel het cyberbeveiligingsniveau van kleine en middelgrote ondernemingen (kmo's) te verhogen. In dat verband bieden verschillende projecten concrete oplossingen voor kmo's (zie ***kader 2***).

Kader 2

Voorbeelden van projecten die tastbare resultaten opleveren voor kmo's

Het GR-SME-SOC-project (project 6 in ***bijlage III***) heeft tot doel cyberbeveiligingsinstrumenten en -diensten te verstrekken aan kmo's in Griekenland door een centrum voor beveiligingsoperaties op te richten dat is afgestemd op hun behoeften. Het project is in januari 2024 van start gegaan en wordt uitgevoerd door een consortium van vijf Griekse organisaties. Het plan is om 120 kmo's gedurende één jaar gratis cyberbeveiligingsdiensten aan te bieden, waarna de diensten commercieel beschikbaar zullen worden. Het project biedt kmo's geavanceerde diensten zoals realtimemonitoring, AI-gestuurde opsporing van dreigingen en flexibele incidentrespons.

Met het NCC-IE-project (project 3 in ***bijlage III***) verstrekte de projectcoördinator ongeveer 1,8 miljoen EUR aan subsidies aan meer dan vijftig Ierse kmo's om hun cyberbeveiliging te verbeteren. De subsidieregeling kwam ten goede aan ondernemingen met twee tot ongeveer 200 werknemers, waaronder familiebedrijven, start-ups en mondiale exporteurs in verschillende sectoren. De subsidies waren uitsluitend bestemd voor bedrijven die eerder een cyberbeveiligingsevaluatie hadden ondergaan die werd beheerd door de overheidsinstantie Enterprise Ireland. De subsidie dekte 80 % van de kosten (tot 60 000 EUR) voor de uitvoering van de aanbevelingen van de evaluatie.

Bron: ERK.

86 Bij veel projecten in onze steekproef is het lastig om de termijnen te halen of doen zich operationele uitdagingen voor (zie ***bijlage IV***). We constateerden dat vier projecten werden geconfronteerd met aanzienlijke vertragingen. Dit omvat ENSOC en ATHENA, zoals uiteengezet in de paragrafen ***65***-***70***. In ***kader 3*** geven we andere voorbeelden.

Kader 3

Voorbeelden van projecten die met operationele uitdagingen en vertragingen worden geconfronteerd

In Ierland is de Local Government Management Authority (LGMA) de enige begunstigde van de subsidie voor het ILG-SOC-project (project 8 in ***bijlage III***). Het doel van het project is de oprichting van een centraal centrum voor beveiligingsoperaties voor 31 lokale autoriteiten om geavanceerde instrumenten voor de opsporen van en de respons op dreigingen te gebruiken. Het project is in oktober 2023 van start gegaan en heeft een looptijd van drie jaar. De tussentijdse evaluatie leidde ertoe dat alle te leveren prestaties werden afgewezen. Het project omvat verschillende aanbestedingsprocedures die zijn mislukt of vertraging hebben opgelopen. De duur van het project zal worden verlengd (zonder aanvullende financiering), waardoor het project voldoende tijd zou kunnen krijgen om met succes te worden afgerond.

In Griekenland heeft het EL-SOC-project (project 5 in ***bijlage III***) tot doel een geconsolideerd SOC op nationaal niveau op te zetten, waarin informatie van sectorale SOC's wordt samengebracht. Dit zou een realtime en volledig overzicht van de cyberbeveiligingssituatie opleveren. Het project loopt van januari 2024 tot en met december 2026. De geplande aanbesteding van hardware en diensten liep vertraging op als gevolg van problemen bij het afronden en publiceren van de technische specificaties voor de aanbesteding. Als reden voor de vertraging noemde de projectcoördinator ook kwesties in verband met het verkrijgen van nationale cofinanciering en de beperkte beschikbaarheid van aanbestedingspersoneel.

Bron: ERK.

87 Twee andere projecten in onze steekproef hebben te kampen met beperkte vertragingen. Drie projecten hebben hun output op tijd geleverd. Tot slot bevinden twee projecten zich in een vroeg stadium van uitvoering en kunnen we daarom niet tot een conclusie komen.

Beveiligingsbeperkingen hebben geleid tot operationele uitdagingen, en er zijn aanzienlijke risico's wanneer controles worden uitgevoerd door begunstigden

88 In de DIGITAL-verordening is bepaald dat, om veiligheidsredenen, de financiering voor cyberbeveiliging kan worden beperkt tot entiteiten die zijn gevestigd in de EU en waarover de lidstaten of EU-burgers zeggenschap hebben. Deze beperking heeft tot doel het risico van inmenging of invloed door niet-EU-landen te beperken en te voorkomen dat gevoelige beveiligingsinformatie wordt gedeeld met autoriteiten van buiten de EU.

89 De eigendoms- en zeggenschapsverplichting van de EU geldt niet alleen voor begunstigden van subsidies, maar ook voor hun subcontractanten en alle ontvangers van financiële steun aan derden. Met uitzondering van deze laatste categorie (zie de paragrafen ***92-96***) voert de centrale valideringsdienst van het Europees Uitvoerend Agentschap onderzoek de beoordeling uit. Het definitieve besluit over de subsidiabiliteit voor deelname aan beperkte oproepen ligt echter nog steeds bij de steunverlenende autoriteit, d.w.z. DG Connect of het ECCC.

90 Tijdens onze controlewerkzaamheden hebben begunstigden herhaaldelijk gewezen op de praktische uitdagingen die de eigendoms- en zeggenschapsbeoordelingen met zich meebrengen. Het beoordelen van EU-eigendom en -zeggenschap kan een complex en langdurig proces zijn. Hiervoor moet de volledige eigendomsstructuur en zeggenschapsketen van elke organisatie worden geanalyseerd, met inbegrip van alle eigendomsniveaus tot aan de uiteindelijke eigenaren. De centrale valideringsdienst vereist dat elke entiteit uitgebreide bewijsstukken verstrekt van haar eigendomsstructuur en specifieke rechten, corporate governance en alle commerciële, financiële of andere banden waarmee zeggenschap wordt verkregen.

91 Bij drie door de EU gefinancierde projecten in onze steekproef werd ten minste één begunstigde van een consortium achteraf uitgesloten omdat deze werd beschouwd als eigendom van of onder zeggenschap staand van partijen buiten de EU. De uitsluiting van consortiumleden toont aan dat het begrip EU-eigendom en -zeggenschap niet door alle DIGITAL-deelnemers volledig wordt begrepen. In totaal is, blijkens gegevens van de centrale valideringsdienst, 7 % van alle aanvragers van DIGITAL-subsidies voor cyberbeveiliging of subcontractanten in de periode 2022-2025 niet door de beoordeling gekomen. Het indienen van aanvragen door niet-subsidiabele deelnemers in het kader van een oproep tot het indienen van voorstellen leidt tot vertragingen, zoals weergegeven in ***kader 4***.

Kader 4

Voorbeeld van een geval waarin begunstigden werden uitgesloten nadat zij niet door de beveiligingscontroles waren gekomen

Twee van de consortiumleden van het NG-SOC-project (project 7 in ***bijlage III***) kwamen niet door de eigendoms- en zeggenschapsbeoordeling. Het resultaat werd ongeveer een maand voor de uiterste datum voor de ondertekening van de subsidieovereenkomst bekendgemaakt. De projectcoördinator moest instemmen met de overname van de werkzaamheden die aan de twee uitgesloten leden waren toegewezen, aangezien er geen tijd was om een nieuwe partner te vinden. Een van de uitgesloten leden bevond zich in een specifieke sector waar de ontwikkelde oplossing zou worden getest. Daarom kon een aanzienlijk deel van het project, dat betrekking had op het testen van de oplossingen in de praktijk, niet volgens plan worden uitgevoerd. Deze situatie werd later verholpen door de subsidieovereenkomst aan te passen en nieuwe leden toe te voegen.

Bron: ERK.

92 Twee van de door ons onderzochte projecten (NCC-IE en CYberSynchrony) bieden financiële steun aan derden. Dit financieringsmechanisme stelt begunstigden van subsidies in staat een deel van de subsidiefinanciering te gebruiken om andere entiteiten te financieren via openbare oproepen. Financiële steun aan derden kan de toegang tot EU-financiering vergemakkelijken. In dit geval zijn de begunstigden als enigen verantwoordelijk voor de uitvoering van de eigendoms- en zeggenschapsbeoordelingen en is de centrale valideringsdienst hier niet bij betrokken.

93 In 2021 heeft de Commissie algemene publieke richtsnoeren gepubliceerd voor aanvragers van beperkte oproepen; deze zijn in 2026 geactualiseerd. Hoewel er sinds 2021 financiële steun aan derden bestaat voor DIGITAL-oproepen, heeft noch de Commissie, noch het ECCC begunstigden een gedetailleerde methodologie verstrekt over de wijze waarop controles in het kader van eigendoms- en zeggenschapsbeoordelingen moeten worden uitgevoerd bij de beoordeling van de derden aan wie zij financiële steun verlenen.
In juli 2025 deelde het ECCC niet-verplichte richtsnoeren, waardoor het netwerk van NCC's een gestructureerde aanpak van eigendoms- en zeggenschapsbeoordelingen kreeg.
De richtsnoeren bevatten algemene beginselen en maatregelen die kunnen worden genomen. In de richtsnoeren wordt echter niet gespecificeerd hoe de controles moeten worden uitgevoerd, waardoor de begunstigden verantwoordelijk blijven voor de ontwikkeling van hun eigen aanpak.

94 We constateerden dat het ECCC de door de begunstigden vastgestelde methodologie niet valideert en evenmin steekproefsgewijze controles uitvoert om ervoor te zorgen dat de methodologie robuust genoeg is en dat de geselecteerde ontvangers van financiële steun inderdaad eigendom zijn van en gecontroleerd worden door de EU.

95 In ons Jaarverslag 2024 hebben we geconstateerd dat de begunstigden die door de Commissie zijn belast met het beheer van financiële steun aan derden (op het gebied van onderzoek) niet verplicht zijn de doeltreffendheid van hun controles aan te tonen om de regelmatigheid van de EU-uitgaven te waarborgen. Evenmin beoordeelt het ECCC de administratieve en technische capaciteit van de begunstigden om de eigendoms- en zeggenschapsbeoordelingen naar behoren te beheren. Zoals uiteengezet in paragraaf ***90***, kan deze beoordeling complex zijn en wordt zij op EU-niveau uitgevoerd door een specifieke dienst met gespecialiseerde deskundigheid.

96 In dit verband zijn wij van mening dat er een aanzienlijk risico bestaat dat de begunstigden, die verantwoordelijk zijn voor de uitvoering van de controles in het kader van eigendoms- en zeggenschapsbeoordeling, niet over de capaciteit beschikken om deze naar behoren uit te voeren. Gezien de aard van de gefinancierde activiteiten zou deze tekortkoming gevoelige infrastructuur, operationele gegevens en kritieke technologieën op het gebied van veiligheid aan het licht kunnen brengen.

De meeste door de EU gefinancierde projecten hebben ontoereikende prestatiekaders en de prestatiegegevens van DIGITAL op het gebied van cyberbeveiliging zijn niet nauwkeurig

De meeste door de EU gefinancierde projecten hebben ontoereikende prestatiekaders

97 Begunstigden die door de EU gefinancierde projecten beheren, moeten aan het ECCC verslag uitbrengen over de vooruitgang en de resultaten ervan aan de hand van mijlpalen, te leveren prestaties en indicatoren, zoals weergegeven in ***figuur 8***. We hebben beoordeeld of de mijlpalen en te leveren prestaties die voor elk project zijn vastgesteld, toereikend zijn voor projectmonitoring. We beoordeelden ook of hun prestatie-indicatoren relevant en meetbaar zijn en een referentiewaarde en een streefdoel hebben.

Figuur 8 | Mijlpalen, te leveren prestaties en prestatie-indicatoren in DIGITAL-projecten

	Mijlpalen	Te bereiken prestaties	Prestatie-indicatoren
Wat ze zijn	controlepunten gedurende het hele project die helpen de vooruitgang in kaart te brengen	projectoutput wordt ingediend om vooruitgang te tonen	worden gebruikt om resultaten te meten
Hoe stel je ze in?	zijn alleen gekoppeld aan belangrijke output (beperkt in aantal)	alleen grote output (maximaal 10 tot 15 per project)	specifiek, meetbaar, haalbaar, realistisch en tijdgebonden
Voorbeelden	"start van de proeffase van het platform"	"handleiding voor platformgebruikers"	"30 % kortere responstijd bij incidenten"
	Gestructureerde aanpak, onderdeel van het onlinesysteem voor subsidiebeheer		**Ongestructureerde aanpak**

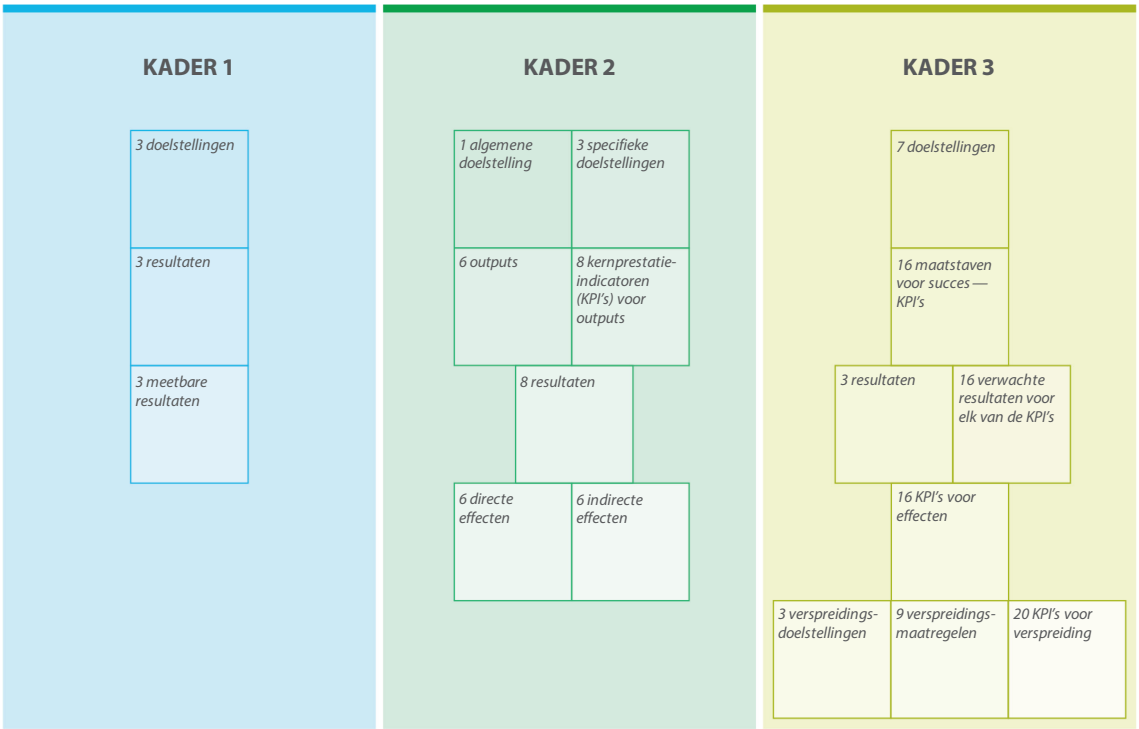
Bron: ERK, op basis van het subsidieaanvraagformulier.

98 In hun projectvoorstel moeten de begunstigden een reeks mijlpalen en te leveren prestaties vastleggen volgens een gestructureerde aanpak die wordt gespecificeerd in de instructies voor aanvragers. Alle mijlpalen en te leveren prestaties zijn opgenomen in het onlinesysteem voor subsidiebeheer om de follow-up ervan te vergemakkelijken. Het ECCC evalueert elk project doorgaans twee keer: eenmaal halverwege het project en eenmaal nadat het is afgerond. Tijdens deze evaluaties verifiëren externe deskundigen of de mijlpalen en te bereiken prestaties zijn verwezenlijkt en valideert het ECCC deze. Mijlpalen en te bereiken prestaties zijn van cruciaal belang voor projectmonitoring en moeten naar behoren worden vastgelegd.

99 We hebben vastgesteld dat vrijwel geen enkel project in onze steekproef de richtlijnen met betrekking tot het aantal mijlpalen en te bereiken prestaties volgde: het aantal mijlpalen per project varieert van 8 tot 39, terwijl het aantal te bereiken prestaties varieert van 8 tot 45. Veel van de mijlpalen en te leveren prestaties voldoen niet aan de instructies over de wijze waarop zij moeten worden opgesteld en zijn daarom niet nuttig voor het volgen van de vooruitgang (bv. “vergadering om het opstellen van oproepen tot het indienen van onderzoeksvoorstellen in gang te zetten” of “formele notulen van projectvergaderingen”). Voor drie projecten had het evaluatiecomité deze problemen vastgesteld vóór de ondertekening van de subsidieovereenkomst. In twee gevallen stelden de begunstigden slechts geringe wijzigingen voor (bv. van de termijnen) zonder de belangrijkste kwesties aan te pakken, terwijl in het derde geval geen wijzigingen werden aangebracht. Voor zes andere projecten in onze steekproef blijkt uit onze analyse dat de mijlpalen of te leveren prestaties niet in overeenstemming zijn met de instructies en niet altijd toereikend zijn. Wij zijn van mening dat het moeilijk is om de vooruitgang te volgen als er slecht gedefinieerde resultaten of mijlpalen zijn, of als er te veel zijn.

100 In tegenstelling tot de mijlpalen en te bereiken prestaties volgen de prestatie-indicatoren geen gestructureerde aanpak en zijn zij niet geconsolideerd in een tabel in het subsidiebeheersysteem, maar zijn deze te vinden in verschillende hoofdstukken van het voorstel. Deze aanpak heeft geleid tot een overvloed aan prestatiekaders die door de begunstigden worden voorgesteld. Sommige hebben alleen projectdoelstellingen vastgesteld die gekoppeld zijn aan prestatie-indicatoren, terwijl andere veel complexere prestatiekaders hebben opgezet. In ***kader 9*** hieronder geven we enkele voorbeelden.

Figuur 9 | Voorbeeld van de verscheidenheid aan prestatiekaders die voor de projecten zijn ontworpen



Bron: ERK.

101 Uit onze analyse kan worden geconcludeerd dat veel van de door de begunstigden gebruikte prestatie-indicatoren niet relevant of meetbaar zijn en geen streefdoel of referentiewaarde hebben (zie ***kader 5***). Bovendien zijn er bij zeven projecten twintig of meer indicatoren vastgesteld, terwijl één project er 52 heeft. We presenteren het resultaat van deze beoordeling in ***bijlage IV***.

Kader 5

Voorbeelden van ontoereikende prestatie-indicatoren

Niet meetbaar:

- "Indicator voor aantasting en andere geleverde diensten versterken de cyberbeveiligingscapaciteiten van kmo's"
- "Levering van instrumenten en methoden voor incidentrespons die integratie met de communicatiekanalen van EU-CyCLONe mogelijk maken"

Niet voorzien van een referentiewaarde of streefdoel:

- "≥ 20 % verbetering van de paraatheid van het personeel"
- "≥ 20 % vermindering van de inspanningen die nodig zijn om aan te sluiten bij en te voldoen aan relevante EU-initiatieven op het gebied van cyberbeveiliging"

Niet prestatiegerelateerd:

- "Eindverslag over het project aan het einde van de financieringsfase"
- "Aantal stagiairs dat aan alle opleidingssessies zal deelnemen"

Bron: ERK, op basis van projectdocumentatie.

102 Over het algemeen zijn wij van mening dat de brede waaier aan prestatiekaders, de slechte opzet van de indicatoren en het buitensporige aantal ervan de prestatiemonitoring aanzienlijk bemoeilijken. Het is daarom niet mogelijk om de prestaties van het project naar behoren te beoordelen. Dit wordt verder bemoeilijkt door het feit dat het rapportagemodel geen specifiek onderdeel over de prestatie-indicatoren van projecten bevat en dat de meeste projecten in onze steekproef er bijgevolg geen verslag over hebben uitgebracht.

Prestatiegegevens over de cyberbeveiligingscomponent van DIGITAL zijn niet nauwkeurig

103 Om de resultaten van DIGITAL te monitoren, voorziet de verordening in programma-indicatoren waarover alle projecten verslag moeten uitbrengen, zoals beschreven in ***kader 6***.

Kader 6

DIGITAL-indicatoren voor cyberbeveiliging

1.a Het aantal gezamenlijk aangekochte infrastructuurvoorzieningen en/of instrumenten, ook in het kader van het Europees waarschuwingssysteem voor cyberbeveiliging

1.b Het aantal gezamenlijk ingezette infrastructuurvoorzieningen en/of instrumenten inzake cyberbeveiliging

2 Het aantal gebruikers en gemeenschappen van gebruikers die toegang hebben tot Europese voorzieningen inzake cyberbeveiliging

3. Het aantal maatregelen ter ondersteuning van de paraatheid voor en de respons op cyberbeveiligingsincidenten in het kader van het noodmechanisme voor cyberbeveiliging

Bron: Bijlage II bij Verordening (EU) 2021/694 tot oprichting van het programma Digitaal Europa; het monitoring- en evaluatiekader voor het programma Digitaal Europa (SWD(2024) 37).

104 We beoordeelden of de projecten in onze steekproef over deze indicatoren verslag hadden uitgebracht en onderzochten hoe het ECCC deze gegevens verzamelt en verifieert.

105 Alle projecten moeten vóór hun tussentijdse en eindevaluatie verslag uitbrengen over de DIGITAL-indicatoren in het systeem voor subsidiebeheer. We constateerden dat van de zeven projecten die tijdens onze controle halverwege hun tijdlijn zaten en daarom over deze indicatoren verslag hadden moeten uitbrengen, slechts drie dat hadden gedaan. Van deze drie waren er bij twee geen correcte gegevens verstrekt: bij een project waren er gegevens over de verkeerde indicator gerapporteerd, bij de andere twee waren er streefwaarden opgegeven in plaats van behaalde resultaten.

106 Elk jaar brengt de Commissie in haar verklaringen over de prestaties van de programma's verslag uit over deze indicatoren. Dit stelt belanghebbenden in staat te beoordelen of de doelstellingen van het programma worden verwezenlijkt. Volgens de verklaringen over de prestaties van de programma's van 2024 liggen de DIGITAL-indicatoren voor cyberbeveiliging op schema. Het ECCC heeft ons uitgelegd dat het gebruik heeft gemaakt van een reeks enquêtes die naar begunstigden van projecten zijn gestuurd om deze indicatoren samen te stellen, in plaats van ze te baseren op het subsidiebeheersysteem. We evalueerden de door het ECCC verstrekte uitgesplitste gegevens en troffen talrijke problemen aan met betrekking tot de manier waarop gegevens werden verzameld en de algemene kwaliteit ervan. We constateerden dat de verzamelde gegevens niet overeenkomen met de waarden in de verklaring over de prestaties van de programma's, waardoor het onduidelijk is hoe de gerapporteerde waarden zijn berekend. We troffen geen bewijs aan dat de nauwkeurigheid van de gerapporteerde gegevens door het ECCC was geverifieerd. Op basis van onze controle van de projecten in onze steekproef, waarbij de meeste waarden ontbreken of onjuist zijn, zijn wij van mening dat de gerapporteerde gegevens geen getrouw beeld geven van de behaalde resultaten.

Dit verslag werd door kamer III onder leiding van de heer George Marius Hyzler, lid van de Rekenkamer, te Luxemburg vastgesteld op haar vergadering van 16 juni 2026.

Voor de Rekenkamer

Tony Murphy
President

Bijlagen

Bijlage I — Over de controle

01 Cyberbeveiliging wordt gedefinieerd als “de activiteiten die nodig zijn om netwerk- en informatiesystemen, de gebruikers van dergelijke systemen, en andere personen die getroffen worden door cyberdreigingen, te beschermen”[1]. Een cyberdreiging is “elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden”[2]. Cyberbeveiliging vereist een holistische aanpak, bestaande uit een reeks onderling verbonden activiteiten om cyberdreigingen te voorkomen, op te sporen, erop te reageren en ervan te herstellen, zoals weergegeven in ***figuur 1***.

[1] Verordening (EU) 2019/881 (cyberbeveiligingsverordening).

[2] Artikel 2 van de cyberbeveiligingsverordening.

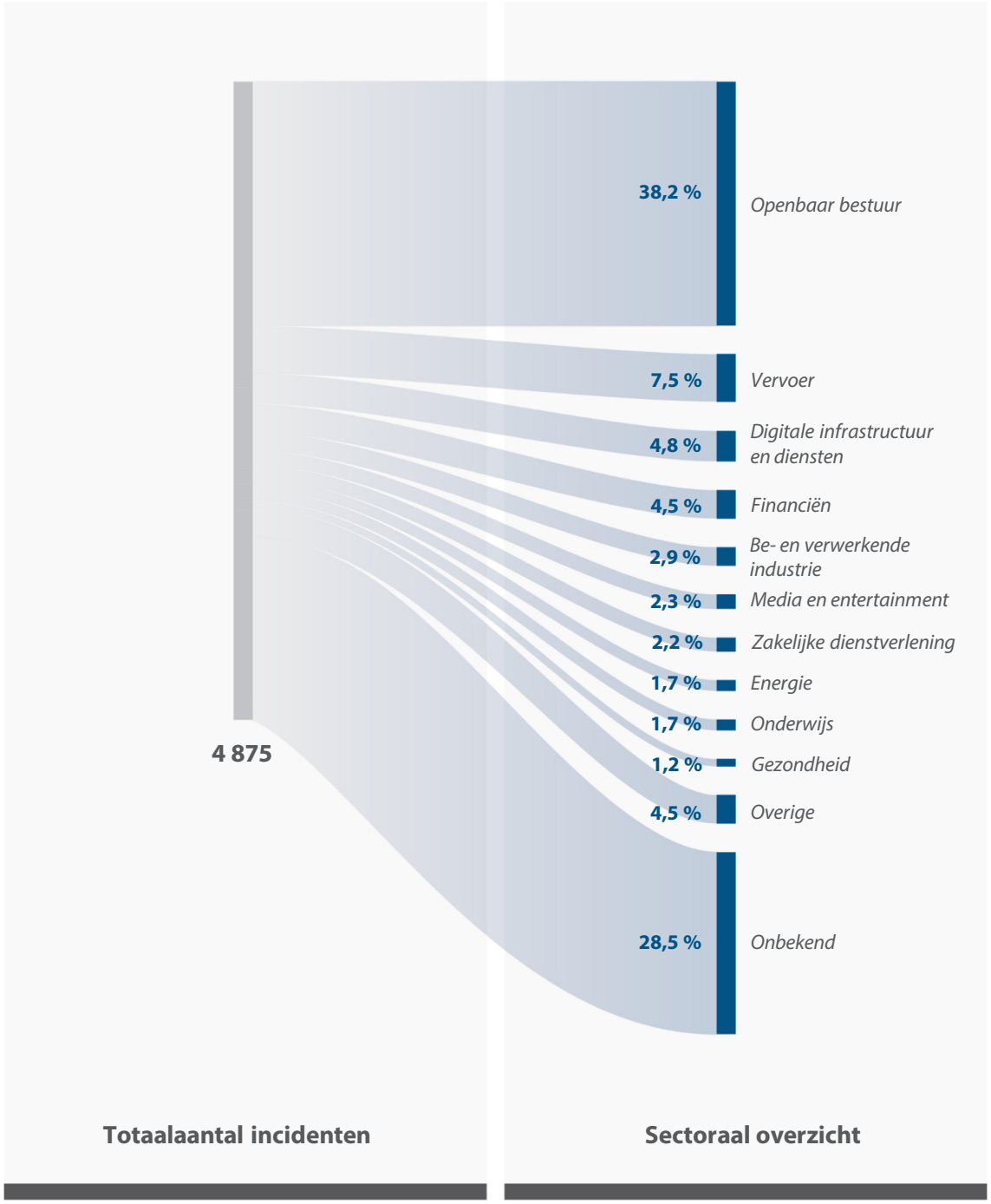
Figuur 1 | Voorbeelden van cyberbeveiligingsactiviteiten

Bron: ERK, op basis van overweging 78 van Richtlijn (EU) 2022/2555 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging (NIS 2-richtlijn).

02 Het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) is van mening dat het cyberdreigingsniveau aanzienlijk is en merkt op dat het cyberdreigingslandschap aanzienlijk complexer is geworden en nog steeds is[3]. Deze dreigingen onderstrepen het cruciale belang van cyberbeveiliging in steeds digitalere economieën en samenlevingen. In zijn dreigingslandschapsverslag van 2025 heeft Enisa ransomware aangemerkt als de meest kritieke dreiging in de EU. In ***figuur 2*** worden de sectoren getoond die het doelwit van de aanvallen zijn.

[3] Verslag van 2024 over de stand van zaken op het gebied van de cyberbeveiliging in de Unie, Enisa.

Figuur 2 | Sectoren die het doelwit van cyberaanvallen zijn



Bron: ERK, op basis van Enisa.

Significante en grootschalige cyberbeveiligingsincidenten

03 Cyberbeveiligingsincidenten, waaronder cyberdreigingen en onbedoelde gebeurtenissen (zoals die welke worden genoemd in ***figuur 3*** en paragraaf ***40***), "kunnen de verlening van openbare diensten (…) [en] de uitoefening van economische activiteiten [belemmeren], (…) aanzienlijke financiële verliezen veroorzaken, het vertrouwen van de gebruikers ondermijnen, grote schade toebrengen aan de economie en de democratische systemen van de Unie, en zelfs gevolgen voor de gezondheid of levensbedreigende gevolgen hebben"[4]. Een cyberbeveiligingsincident wordt beschouwd als[5]:

- **significant** indien het een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken, of indien het andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken;

- **grootschalig**, als het een verstoringsniveau veroorzaakt dat te groot is om door een getroffen lidstaat alleen te worden verholpen of dat significante gevolgen heeft voor ten minste twee lidstaten.

04 Een grootschalig cyberbeveiligingsincident kan escaleren tot een volwaardige **cybercrisis in de EU** als het de goede werking van de interne markt verhindert of ernstige risico's voor de openbare veiligheid en beveiliging met zich meebrengt voor entiteiten of burgers in verschillende lidstaten, of voor de EU als geheel[6].

---

[4] Overweging 2 van Verordening (EU) 2025/38 (de verordening cybersolidariteit).

[5] Artikelen 6 en 23 van de NIS 2-richtlijn, nader gespecificeerd in Uitvoeringsverordening (EU) 2024/2690 van de Commissie voor een aantal aanbieders in de sector digitale infrastructuur.

[6] Overweging 69 van de NIS 2-richtlijn.

Beleidskader van de EU

05 Het ecosysteem voor cyberbeveiliging van de EU is complex en bestaat uit verschillende lagen, en heeft raakvlakken met diverse interne beleidsterreinen, zoals justitie en binnenlandse zaken, de digitale eengemaakte markt en onderzoeksbeleid[7]. Wat het externe beleid betreft, speelt cyberbeveiliging een rol in de diplomatie en maakt het in toenemende mate deel uit van het defensiebeleid van de EU dat momenteel wordt ontwikkeld[8].

06 De afgelopen jaren heeft de EU haar regelgevingskader voor cyberbeveiliging versterkt. ***Figuur 3*** toont de meest relevante wetgeving en beleidsinstrumenten op EU-niveau. Overeenkomstig onze reikwijdte van de controle (zie de paragrafen ***13*** en ***14***) hebben we ons gericht op instrumenten voor de opsporing van en de respons op significante en grootschalige cyberbeveiligingsincidenten.

---

[7] Uitdagingen voor een doeltreffend EU-beleid inzake cyberbeveiliging, ERK-briefingdocument, blz. 14.

[8] Bijvoorbeeld de cyberstrategie van de Europese Unie (2022), het kader voor een gecoördineerde EU-respons op hybride campagnes (2022), het EU-beleid inzake cyberdefensie (2023) en het herziene instrumentarium voor cyberdiplomatie (2023).

Figuur 3 | Relevante EU-wetgeving en -beleidsinstrumenten

- Goedkeuring van wetgeving en beleidsinstrumenten
- Oprichting van netwerken en structuren

2016

- **Goedkeuring van de richtlijn netwerk- en informatiebeveiliging (NIS-richtlijn)**
  De NIS-richtlijn vereist dat aanbieders van bepaalde essentiële diensten en digitaledienstverleners risicobeheerpraktijken toepassen en significante incidenten melden.
- **Oprichting van de NIS-samenwerkingsgroep**
  De groep ondersteunt en bevordert strategische samenwerking en informatie-uitwisseling tussen de lidstaten.
- **Oprichting van het netwerk van Computer Security Incident Response Teams (CSIRT's)**
  Dit netwerk van nationale CSIRT's en CERT-EU heeft tot doel bij te dragen tot de ontwikkeling van het vertrouwen en een snelle en doeltreffende technische samenwerking tussen de lidstaten te bevorderen.

2017

- **Goedkeuring van de eerste cyberblauwdruk**
  In de blauwdruk wordt de visie van de Commissie op de totstandbrenging van een EU-kader voor respons op cybercrises uiteengezet.

2019

- **Goedkeuring van de cyberbeveiligingsverordening**
  De verordening verleent Enisa een sterker en permanent mandaat.

2020

- **Start van het Europees Netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe)**
  Dit informele netwerk van nationale verbindingsfunctionarissen voor cybercrisisbeheer fungeert als schakel tussen de technische en politieke dimensies bij grootschalige cyberbeveiligingsincidenten en -crises.
- **Presentatie van de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk**
  De strategie is erop gericht de collectieve weerbaarheid tegen cyberdreigingen te versterken, omvat wereldwijde samenwerking in cyberspace en wijst op toekomstige wetsvoorstellen.

2021

- **Goedkeuring van het programma Digitaal Europa (DIGITAL)**
- **Oprichting van het Europees Kenniscentrum voor cyberbeveiliging en het Netwerk van nationale coördinatiecentra**

2022

- **Start van de DIGITAL-oproep tot het indienen van voorstellen voor landsgrensoverschrijdende centra voor beveiligingsoperaties**
  Deze centra brengen groepen lidstaten op vrijwillige basis samen.
- **Goedkeuring van de NIS 2-richtlijn**
  Met de NIS 2-richtlijn wordt het toepassingsgebied van de vorige NIS-richtlijn uitgebreid tot publieke en particuliere entiteiten in 18 sectoren van de economie die onderworpen zijn aan strenge beveiligingseisen, met inbegrip van de behandeling van incidenten en de respons op en bekendmaking van kwetsbaarheden.
- **Formalisering van EU-CyCLONe**
  Het netwerk krijgt een rechtsgrondslag.

2024

- **Goedkeuring van de verordening cyberweerbaarheid**
  Bij deze verordening worden cyberbeveiligingsnormen ingevoerd voor producten die een digitale component bevatten. De belangrijkste verplichtingen ervan zijn van toepassing met ingang van 11 december 2027.

2025

- **Goedkeuring van de verordening cybersolidariteit**
  De verordening heeft tot doel de capaciteit van de EU te versterken om cyberdreigingen en -incidenten op te sporen, zich erop voor te bereiden en erop te reageren. De verordening voorziet in de oprichting van het Europees waarschuwingssysteem voor cyberbeveiliging, een pan-Europees netwerk van nationale en landsgrensoverschrijdende cyberhubs. Ook wordt hierbij de EU-cyberbeveiligingsreserve ingesteld.
- **Presentatie van de EU-strategie voor een paraatheidsunie en de Europese strategie voor interne veiligheid (ProtectEU)**
  Cyberbeveiliging speelt in beide strategieën een prominente rol.
- **Goedkeuring van een herziene cyberblauwdruk**
  In deze aanbeveling van de Raad wordt de blauwdruk van 2017 geactualiseerd en het EU-kader voor cybercrisisbeheer vastgesteld in de context van de algemene paraatheid van de EU voor grootschalige cyberbeveiligingsincidenten en cybercrises.

Bron: ERK.

Rollen en verantwoordelijkheden

07 Het cyberbeveiligingslandschap van de EU omvat tal van particuliere en publieke actoren op regionaal, nationaal en EU-niveau in de civiele sfeer, met inbegrip van rechtshandhavingsinstanties. Cyberbeveiliging is ook een belangrijk onderdeel van nationale veiligheid en defensie[9]. In ***bijlage II*** wordt het huidige EU-landschap geïllustreerd.

08 De lidstaten zijn in de eerste plaats verantwoordelijk voor het voorkomen van, de voorbereiding en het reageren op cyberbeveiligingsincidenten en -crises die hen aangaan. Overeenkomstig artikel 4, lid 2, van het Verdrag betreffende de Europese Unie blijft de nationale veiligheid de uitsluitende verantwoordelijkheid van elke lidstaat. Aangezien cyberbeveiligingsincidenten de kritieke informatie-infrastructuur kunnen verstoren en aantasten waarvan de goede werking van de interne markt afhankelijk is, speelt de EU ook een belangrijke rol bij een significant incident of een crisis[10]. De belangrijkste entiteiten op EU-niveau worden weergegeven in ***kader 4***.

[9] Advies 02/2023 over de voorgestelde verordening cybersolidariteit.

[10] EU-blauwdruk voor cybercrisisbeheer.

Figuur 4 | Entiteiten op EU-niveau met een sleutelrol op het gebied van cyberbeveiliging

Directoraat-generaal Communicatienetwerken, Inhoud en Technologie (DG Connect)

ontwikkelt het EU-beleid inzake cyberbeveiliging en voert het uit, onder meer door relevante wetgeving te formuleren en de cyberbeveiligingscapaciteiten van de EU op te bouwen

Agentschap van de Europese Unie voor cyberbeveiliging (Enisa)

heeft een breed mandaat, maar heeft als hoofddoel een hoog gezamenlijk niveau van cyberbeveiliging in de hele EU tot stand te brengen

Europees Kenniscentrum voor cyberbeveiliging (ECCC)

opgericht in 2021; is verantwoordelijk voor de uitvoering van de cyberbeveiligingscomponent van DIGITAL en relevante projecten in het kader van Horizon Europa

Raad van de Europese Unie

kan de geïntegreerde regelingen voor politieke crisisrespons activeren om de politieke respons op grote crises op EU-niveau te coördineren

Bron: ERK.

EU-financiering

09 Binnen het huidige meerjarig financieel kader 2021-2027 is het programma Digitaal Europa (DIGITAL) de belangrijkste financieringsbron voor cyberbeveiliging. Het programma, dat in 2021 van start ging, is het eerste EU-programma dat specifiek gericht is op het stimuleren van de digitale transformatie van de EU, en heeft een totale begroting van 8,1 miljard EUR[11].

10 DIGITAL financiert acties op het gebied van cyberbeveiliging in het kader van specifieke doelstelling 3 — "Cyberbeveiliging en vertrouwen". Meer in het bijzonder is er een budget van 1,4 miljard EUR voor:

- het versterken van de coördinatie op het gebied van cyberbeveiliging tussen de instrumenten en data-infrastructuur van de lidstaten;
- het ondersteunen van de brede uitrol van de cyberbeveiligingsoplossingen in de hele economie.

11 Het grootste deel van de DIGITAL-financiering voor cyberbeveiliging wordt verstrekt via oproepen tot het indienen van voorstellen. Tussen november 2021 en december 2025 zijn er twaalf oproepen gedaan. De beschikbare EU-financiering voor deze oproepen bedroeg 825 miljoen EUR. Voor 2026 en 2027 staan er nieuwe oproepen gepland, waarbij nog eens 212 miljoen EUR aan subsidies zal worden toegekend.

12 Een ander belangrijk EU-programma ter ondersteuning van cyberbeveiliging is Horizon Europa. Cyberbeveiligingsprojecten worden voornamelijk gefinancierd in het kader van cluster 3 — "Civiele veiligheid voor de samenleving" en bevinden zich gewoonlijk in een vroege maturiteitsfase als gevolg van de focus van Horizon Europa op onderzoek en innovatie. Vanuit de herstel- en veerkrachtfaciliteit wordt ook financiering voor cyberbeveiligingsmaatregelen verstrekt.

[11] Programma Digitaal Europa.

Reikwijdte en aanpak van de controle

13 De toename van cyberdreigingen en de mogelijke gevolgen daarvan hebben duidelijk gemaakt dat we onze gezamenlijke cyberweerbaarheid moeten versterken. Het doel van onze controle was na te gaan of de EU-maatregelen de opsporing van en de respons op significante en grootschalige cyberbeveiligingsincidenten doeltreffend bevorderen. We hebben met name onderzocht of dit het geval was voor:

- netwerken en mechanismen op EU-niveau (namelijk het CSIRT-netwerk, EU-CyCLONe, het Europees waarschuwingssysteem voor cyberbeveiliging, het cybersituatiecentrum en de EU-cyberbeveiligingsreserve);
- in het kader van DIGITAL gefinancierde maatregelen.

We hebben ons niet gebogen over de samenwerking op het gebied van wetshandhaving op EU-niveau, noch over afschrikkingsmaatregelen op cybergebied die op EU-niveau worden genomen door middel van diplomatieke maatregelen of defensieactiviteiten.

14 De controle had betrekking op de periode van 2022 tot en met 2025. Deze is gebaseerd op een controle aan de hand van stukken en een analyse van relevante documenten, controlebezoeken aan drie lidstaten — Ierland, Griekenland en Italië — en schriftelijke vragenlijsten en vraaggesprekken met relevante belanghebbenden. ***Figuur 5*** laat zien hoe we bewijs hebben verkregen voor onze bevindingen.

Figuur 5 | Uitgevoerde controlewerkzaamheden

We onderzochten

- Het **rechtskader** dat van toepassing is op de opsporing van en respons op significante en grootschalige cyberbeveiligingsincidenten
- De **taken en verantwoordelijkheden** van de op EU-niveau opgezette netwerken en structuren

We analyseerden

- Documenten over de werking van het **CSIRT-netwerk** en **EU-CyCLONe**
- Documentatie over het **kader voor programmering en prestatiemonitoring van DIGITAL**
- Documentatie over **13 geselecteerde door de EU gefinancierde acties** (elf subsidies en twee overeenkomsten — zie gedetailleerde lijst in bijlage III)

* We hebben door de EU gefinancierde acties geselecteerd in drie landen (Ierland, Griekenland en Italië) waar de relevante DIGITAL-financiering een grotere rol speelde. De elf subsidies waren geselecteerd uit een lijst van 137 door de EU gefinancierde projecten die relevant zijn voor het opsporen van en reageren op dreigingen, om zo een breed scala aan projecten te bestrijken.

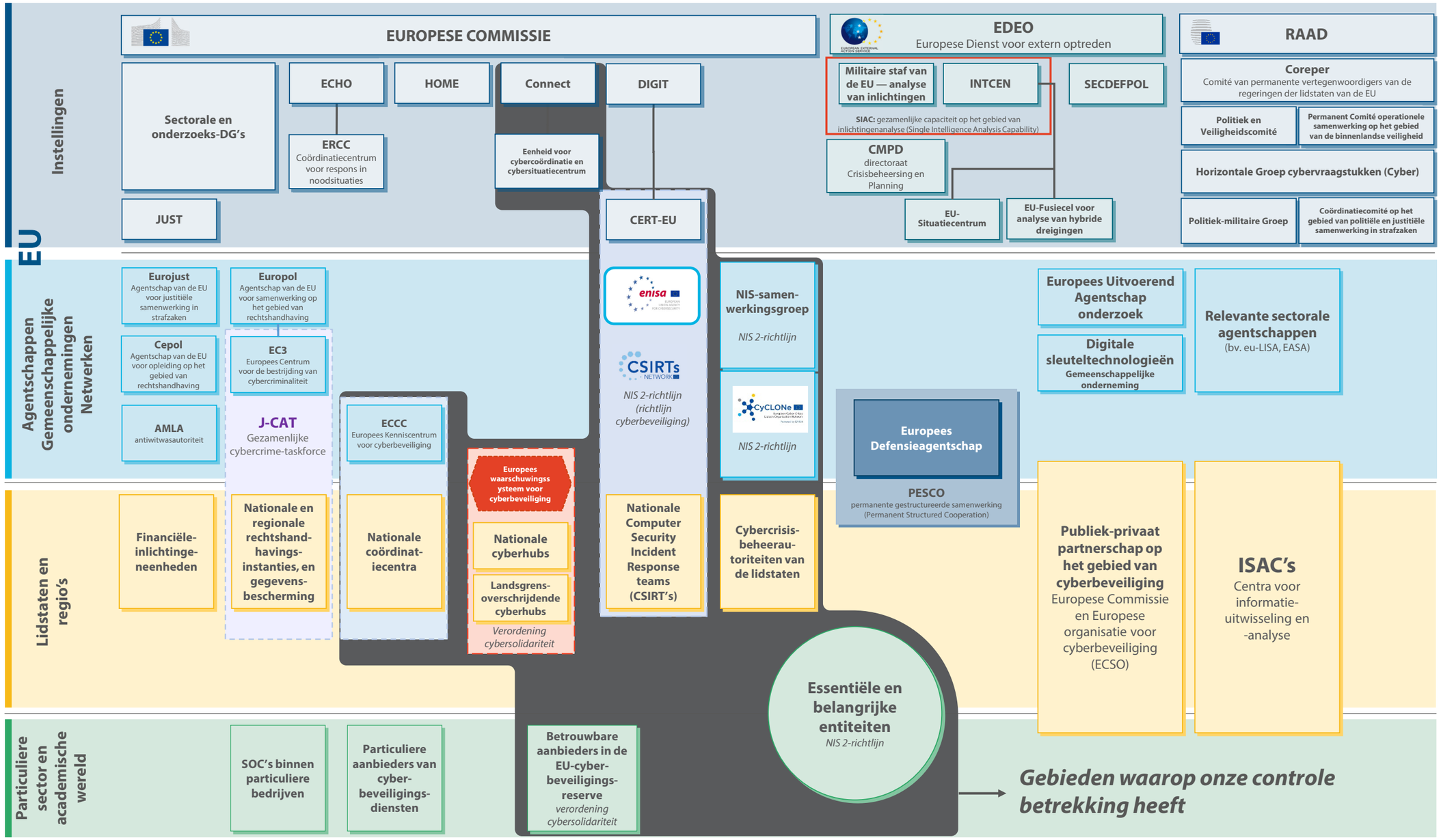
We spraken met

- Begunstigden van de **11 in de steekproef opgenomen door de EU gefinancierde subsidies**
- Vertegenwoordigers van de nationale cyberbeveiligingsautoriteiten in **drie lidstaten** (Ierland, Griekenland en Italië)
- Vertegenwoordigers van de Europese Commissie (**DG Connect**), **Enisa** en het **ECCC**

Bron: ERK.

15 Wij verwachten dat onze bevindingen zullen bijdragen tot verbeterde doeltreffendheid en efficiëntie van de opsporing van en de respons van de EU op significante en grootschalige cyberbeveiligingsincidenten, en tot verbetering van de wijze waarop door de EU gefinancierde acties worden geselecteerd en gemonitord. Onze controlemethodologie is in overeenstemming met de internationale auditstandaarden die zijn uitgevaardigd door de internationale organisatie van hoge controle-instanties (International Organization of Supreme Audit Institutions — INTOSAI).

Bijlage II — Het cyberbeveiligingslandschap van de EU



DG Connect: directoraat-generaal Communicatienetwerken, Inhoud en Technologie
DG ECHO: directoraat-generaal Europese Civiele Bescherming en Humanitaire Hulp
DG HOME: directoraat-generaal Migratie en Binnenlandse Zaken

DG JUST: directoraat-generaal Justitie en Consumentenzaken
DIGIT: directoraat-generaal Digitale Diensten
EASA: Agentschap van de Europese Unie voor de veiligheid van de luchtvaart

EU-CyCLONe: Europees Netwerk van verbindingsorganisaties voor cybercrises
Eu-LISA: Agentschap van de Europese Unie voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht

EU-Intcen: Inlichtingen- en situatiecentrum van de Europese Unie
SECDEFPOL: veiligheids- en defensiebeleid
SOC: centrum voor beveiligingsoperaties (security operations centre)

Bijlage III — Geselecteerde acties op het gebied van cyberbeveiliging

ID	Titel	Landen	Begindatum	Einddatum	Totale kosten (in miljoen EUR) en EU-bijdrage (in %)	Link naar EU-portaal voor financiering en aanbestedingen
Subsidies voor landsgrensoverschrijdende cyberhubs die deel uitmaken van het Europees waarschuwingssysteem voor cyberbeveiliging						
1	**Oprichting van landsgrensoverschrijdende SOC's (ATHENA)**	Bulgarije, Griekenland, Cyprus, Malta	1.1.2024	31.3.2028	4,7 (50 %)	
2	**GRENSOVERSCHRIJDEND PLATFORM VAN ENSOC (ENSOC)**	Spanje, Italië, Luxemburg, Nederland, Oostenrijk, Portugal, Roemenië	1.1.2024	30.6.2028	10,4 (50 %)	
Subsidies voor de uitrol van het netwerk van nationale coördinatiecentra (NCC's) in de lidstaten						
3	**Ontwikkeling en uitvoering van het National Cyber Security Coordination and Development Centre voor Ierland (NCC-IE)**	Ierland	2.10.2023	1.10.2026	4,2 (47 %)	
4	**Italiaans nationaal coördinatiecentrum (NCC-IT)**	Italië	1.11.2023	31.10.2025	2,0 (50 %)	
Subsidies voor het opbouwen van de capaciteit van centra voor beveiligingsoperaties, het bevorderen van nieuwe toepassingen van AI en andere ontsluitende technologieën voor deze centra, en het bieden van ondersteuning op het gebied van paraatheid en wederzijdse bijstand						
5	**Versterking van de capaciteit van het Helleens geconsolideerd centrum voor beveiligingsoperaties (EL-SOC)**	Griekenland, Cyprus	1.1.2024	31.12.2026	9,7 (50 %)	
6	**Grieks centrum voor beveiligingsoperaties voor kleine en middelgrote ondernemingen (GR-SME-SOC)**	Griekenland	1.1.2024	31.12.2026	12,1 (50 %)	

ID	Titel	Landen	Begindatum	Einddatum	Totale kosten (in miljoen EUR) en EU-bijdrage (in %)	Link naar EU-portaal voor financiering en aanbestedingen
7	**Centra voor beveiligingsoperaties van de volgende generatie (NG-SOC)**	Griekenland, Spanje, Cyprus, Luxemburg, Slovenië, Noorwegen	1.1.2024	31.12.2026	4,8 (50 %)	
8	**Iers centrum voor beveiligingsoperaties van lokale overheden (ILG-SOC)**	Ierland	1.10.2023	30.9.2026	8,3 (50 %)	
9	**Een onderling verbonden ecosysteem van coördinatie- en responsnetwerken op het gebied van cyberbeveiliging (Cyber-CORE-netwerk)**	Ierland	1.1.2024	31.12.2026	3,6 (50 %)	
2010	**Harmonisatie van mensen, processen en technologie voor robuuste cyberbeveiliging (CYberSynchrony)**	België, Griekenland, Italië, Cyprus, Nederland	1.6.2024	31.5.2027	7,0 (100 %)	
2011	**Geavanceerde coöperatieve centra voor beveiligingsoperaties**	Griekenland, Italië, Roemenië	1.1.2025	31.12.2027	3,0 (50 %)	
Kaderovereenkomst voor de actie ter ondersteuning van cyberbeveiliging van Enisa						
2012	**Ondersteuning van Enisa voor het verlenen van diensten in het kader van de actie ter ondersteuning van cyberbeveiliging (28 percelen)**	27 percelen van lidstaten 1 pan-Europees perceel	1.12.2022[1]	31.12.2025	28,3 (100 %)	
Dienstverleningsovereenkomst voor het cybersituatiecentrum van DG Connect						
13	**Dienstverlening op maat ter ondersteuning van het cybersituatie- en -analysecentrum voor de Europese Commissie**	–	30.12.2022	30.12.2026	18,0 (100 %)	

Bron: ERK.

[1] Meerdere contracten ondertekend in december 2022.

Bijlage IV — Beoordeling door de ERK van door de EU gefinancierde cyberbeveiligingsprojecten

Bevredigend *Enkele zwakke punten*
Onbevredigend *Geen conclusie mogelijk (te vroeg om te beoordelen)*

ID	Project	Het project komt tegemoet aan de meeste in de oproep vastgestelde behoeften	Met het project zijn tot dusver de geplande output en resultaten gerealiseerd	De output van het project is binnen de termijn geleverd	De prestatie-indicatoren van het project zijn relevant en meetbaar en hebben een referentiewaarde en streefdoel
1	Oprichting van landsgrensoverschrijdende SOC's (ATHENA)	Bevredigend	Onbevredigend	Onbevredigend	Onbevredigend
2	GRENSOVERSCHRIJDEND PLATFORM VAN ENSOC (ENSOC)	Bevredigend	Onbevredigend	Onbevredigend	Onbevredigend
3	Ontwikkeling en uitvoering van het National Cyber Security Coordination and Development Centre voor Ierland (NCC-IE)	Bevredigend	Bevredigend	Enkele zwakke punten	Enkele zwakke punten
4	Italiaans nationaal coördinatiecentrum (NCC-IT)	Bevredigend	Bevredigend	Bevredigend	Enkele zwakke punten
5	Versterking van de capaciteit van het Helleens geconsolideerd centrum voor beveiligingsoperaties (EL-SOC)	Bevredigend	Enkele zwakke punten	Onbevredigend	Onbevredigend
6	Grieks centrum voor beveiligingsoperaties voor kleine en middelgrote ondernemingen (GR-SME-SOC)	Bevredigend	Bevredigend	Bevredigend	Enkele zwakke punten
7	Centra voor beveiligingsoperaties van de volgende generatie (NG-SOC)	Bevredigend	Bevredigend	Bevredigend	Enkele zwakke punten
8	Iers centrum voor beveiligingsoperaties van lokale overheden (ILG-SOC)	Bevredigend	Onbevredigend	Onbevredigend	Onbevredigend
9	Een onderling verbonden ecosysteem van coördinatie- en responsnetwerken op het gebied van cyberbeveiliging (Cyber-CORE-netwerk)	Bevredigend	Enkele zwakke punten	Enkele zwakke punten	Enkele zwakke punten
10	Harmonisatie van mensen, processen en technologie voor robuuste cyberbeveiliging (CYberSynchrony)	Enkele zwakke punten	Geen conclusie mogelijk (te vroeg om te beoordelen)	Geen conclusie mogelijk (te vroeg om te beoordelen)	Enkele zwakke punten
11	Geavanceerde coöperatieve centra voor beveiligingsoperaties	Bevredigend	Geen conclusie mogelijk (te vroeg om te beoordelen)	Geen conclusie mogelijk (te vroeg om te beoordelen)	Onbevredigend

Afkortingen

Afkorting	Definitie/verklaring
CSIRT	computercalamiteitenteam (Computer Security Incident Response Team)
DG Connect	directoraat-generaal Communicatienetwerken, Inhoud en Technologie
DIGITAL	programma Digitaal Europa
ECCC	Europees kenniscentrum voor cyberbeveiliging
Enisa	Agentschap van de Europese Unie voor cyberbeveiliging
EU-CyCLONe	Europees Netwerk van verbindingsorganisaties voor cybercrises
Kmo	kleine en middelgrote onderneming (mkb-bedrijf)
NCC	nationaal coördinatiecentrum
NIB	netwerk- en informatiebeveiliging
SAG	strategische adviesgroep
SOC	centrum voor beveiligingsoperaties

Woordenlijst

Term	Definitie/verklaring
Centrum voor beveiligingsoperaties	Organisatorische eenheid die zich bezighoudt met het voorkomen van cyberbedreigingen en -incidenten en het verzamelen van inlichtingen hierover.
Cyberbeveiligingsincident	Gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens of informatiesystemen in gevaar brengt.
Cyberdreiging	Potentieel gebruik van cyberspace om de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens of informatiesystemen in gevaar te brengen.
Cyberhub	Centraal platform waarop verschillende diensten, instrumenten en IT-professionals worden samengebracht om de monitoring, opsporing en analyse van cyberdreigingen te verbeteren, cyberbeveiligingsincidenten te voorkomen en de productie van inlichtingen over cyberdreigingen te ondersteunen.
Dreigingsactor	Persoon of groep die opzettelijk schade toebrengt, diensten verstoort of gegevens steelt door misbruik te maken van kwetsbaarheden in IT-systemen, netwerken en apparaten.
Grootschalig cyberbeveiligingsincident	Cyberbeveiligingsincident dat te ontwrichtend is voor een lidstaat om alleen af te handelen of dat een significante impact heeft op ten minste twee lidstaten.
Ransomware	Malware die slachtoffers de toegang tot een computersysteem ontzegt of bestanden versleutelt waardoor ze onleesbaar worden, zodat het slachtoffer doorgaans gedwongen wordt losgeld te betalen om de toegang te herstellen.
Significant cyberbeveiligingsincident	Cyberbeveiligingsincident dat ernstige ontwrichting of financieel verlies voor een organisatie, of aanzienlijke schade voor andere entiteiten of personen heeft veroorzaakt of kan veroorzaken.
Taxonomie	In de context van cyberbeveiliging, een classificatiesysteem dat wordt gebruikt om kennis over belangrijke concepten zoals dreigingen en incidenten te organiseren, te categoriseren en te structureren.

Antwoorden van de Commissie

https://www.eca.europa.eu/nl/publications/SR-2026-19

Antwoorden van het Europees Kenniscentrum voor cyberbeveiliging (ECCC)

https://www.eca.europa.eu/nl/publications/SR-2026-19

Antwoorden van het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa)

https://www.eca.europa.eu/nl/publications/SR-2026-19

Tijdlijn

https://www.eca.europa.eu/nl/publications/SR-2026-19

Controleteam

In de speciale verslagen van de ERK worden de resultaten van haar controles van EU-beleid en -programma's, of van beheerskwesties met betrekking tot specifieke begrotingsterreinen uiteengezet. Bij haar selectie en opzet van deze controletaken zorgt de ERK ervoor dat deze een maximale impact hebben door rekening te houden met de risico's voor de doelmatigheid of de naleving, de omvang van de betrokken inkomsten of uitgaven, de verwachte ontwikkelingen alsook de politieke en publieke belangstelling.

Deze doelmatigheidscontrole werd verricht door controlekamer III "Externe maatregelen, veiligheid en justitie", die onder leiding staat van ERK-lid George-Marius Hyzler. De controle werd geleid door ERK-lid George-Marius Hyzler, ondersteund door Romuald Kayibanda, kabinetschef en Annette Farrugia, kabinetsattaché; Cyril Messein, hoofdmanager; Frédéric Soblet, taakleider; Jurgen Manjé en Flavia Di Marco, auditors.
Zoe Amador Martínez verleende taalkundige ondersteuning. Dunja Weibel verleende grafische ondersteuning.

Van links naar rechts: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé, Cyril Messein.

AUTEURSRECHT

© Europese Unie, 2026

Het beleid van de Europese Rekenkamer (ERK) inzake hergebruik is uiteengezet in Besluit nr. 6-2019 van de ERK over het opendatabeleid en het hergebruik van documenten.

Tenzij anders aangegeven (bv. in afzonderlijke auteursrechtelijke mededelingen), wordt voor inhoud van de ERK die eigendom is van de EU een licentie verleend in het kader van de Creative Commons Attribution 4.0 International (CC BY 4.0)-licentie. Als algemene regel geldt daarom dat hergebruik is toegestaan mits de bron correct wordt vermeld en eventuele wijzigingen worden aangegeven. De hergebruiker van ERK-inhoud mag de oorspronkelijke betekenis of boodschap niet wijzigen. De ERK is niet aansprakelijk voor mogelijke gevolgen van hergebruik.

Aanvullende toestemming moet worden verkregen indien specifieke inhoud personen herkenbaar in beeld brengt, bijvoorbeeld op foto's van personeelsleden van de ERK, of werken van derden bevat.

Indien dergelijke toestemming wordt verkregen, wordt de bovengenoemde algemene toestemming opgeheven en zullen beperkingen van het gebruik daarin duidelijk worden aangegeven.

Wilt u inhoud gebruiken of reproduceren die geen eigendom van de EU is, dan dient u de auteursrechthebbende mogelijk rechtstreeks om toestemming te vragen.

Foto op de omslag: © 4AXY — stock.adobe.com.

Figuren 6 en 8 — iconen: deze figuren zijn ontworpen met behulp van Flaticon.com.
© Freepik Company S.L. Alle rechten voorbehouden.

Figuur 5 — kaarten: Eurostat.

Software of documenten waarop industriële-eigendomsrechten rusten, zoals octrooien, handelsmerken, geregistreerde ontwerpen, logo's en namen, zijn uitgesloten van het beleid van de ERK inzake hergebruik.

De groep institutionele websites van de Europese Unie met de domeinnaam "europa.eu" bevat links naar sites van derden. Aangezien de ERK geen controle heeft over deze sites, wordt u aangeraden kennis te nemen van hun privacy- en auteursrechtbeleid.

Gebruik van het ERK-logo

Het logo van de ERK mag niet worden gebruikt zonder voorafgaande toestemming van de ERK.

HTML	ISBN 978-92-849-7883-0	ISSN 1977-575X	doi:10.2865/0384933	QJ-01-26-032-NL-Q
PDF	ISBN 978-92-849-7884-7	ISSN 1977-575X	doi:10.2865/9025902	QJ-01-26-032-NL-N

CITEERWIJZE

Europese Rekenkamer, Speciaal verslag 19/2026 “Opsporing van en respons op cyberbeveiligingsincidenten — EU-samenwerkingskader laat vorderingen zien, maar is slechts deels doeltreffend door vertragingen bij de uitvoering en beperkte informatie-uitwisseling”, Bureau voor publicaties van de Europese Unie, 2026.

De afgelopen jaren heeft de EU haar regelgevingskader voor cyberbeveiliging versterkt en netwerken en mechanismen opgezet om cyberbeveiligingsincidenten aan te pakken. De EU financiert ook cyberbeveiligingsprojecten via het programma Digitaal Europa.

Wij concluderen dat EU-maatregelen de opsporing van en de respons op significante en grootschalige cyberbeveiligingsincidenten slechts ten dele bevorderen. Hoewel er geleidelijk een samenwerkingskader tot stand is gekomen, wordt er nog steeds gewerkt aan de volledige opzet ervan. Door de beperkte informatie-uitwisseling, tekortkomingen in de rapportage en aanzienlijke vertragingen bij de uitvoering kan het potentieel van de EU-netwerken en -mechanismen niet volledig worden benut. De projecten zijn gericht op relevante doelstellingen, maar verschillende ervan worden geconfronteerd met operationele uitdagingen en vertragingen. Bovendien zijn er tekortkomingen in het algemene kader voor prestatiemonitoring. We doen aanbevelingen om deze tekortkomingen verhelpen.

Speciaal verslag van de ERK, uitgebracht krachtens artikel 287, lid 4, tweede alinea, VWEU.

EUROPESE REKENKAMER

Bureau voor publicaties van de Europese Unie

EUROPESE REKENKAMER
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBURG

Tel. +352 4398-1

Inlichtingen: eca.europa.eu/nl/contact
Website: eca.europa.eu
Social media: @EUauditors