Voortgangsrapportage 2025 Nederlandse Cybersecuritystrategie

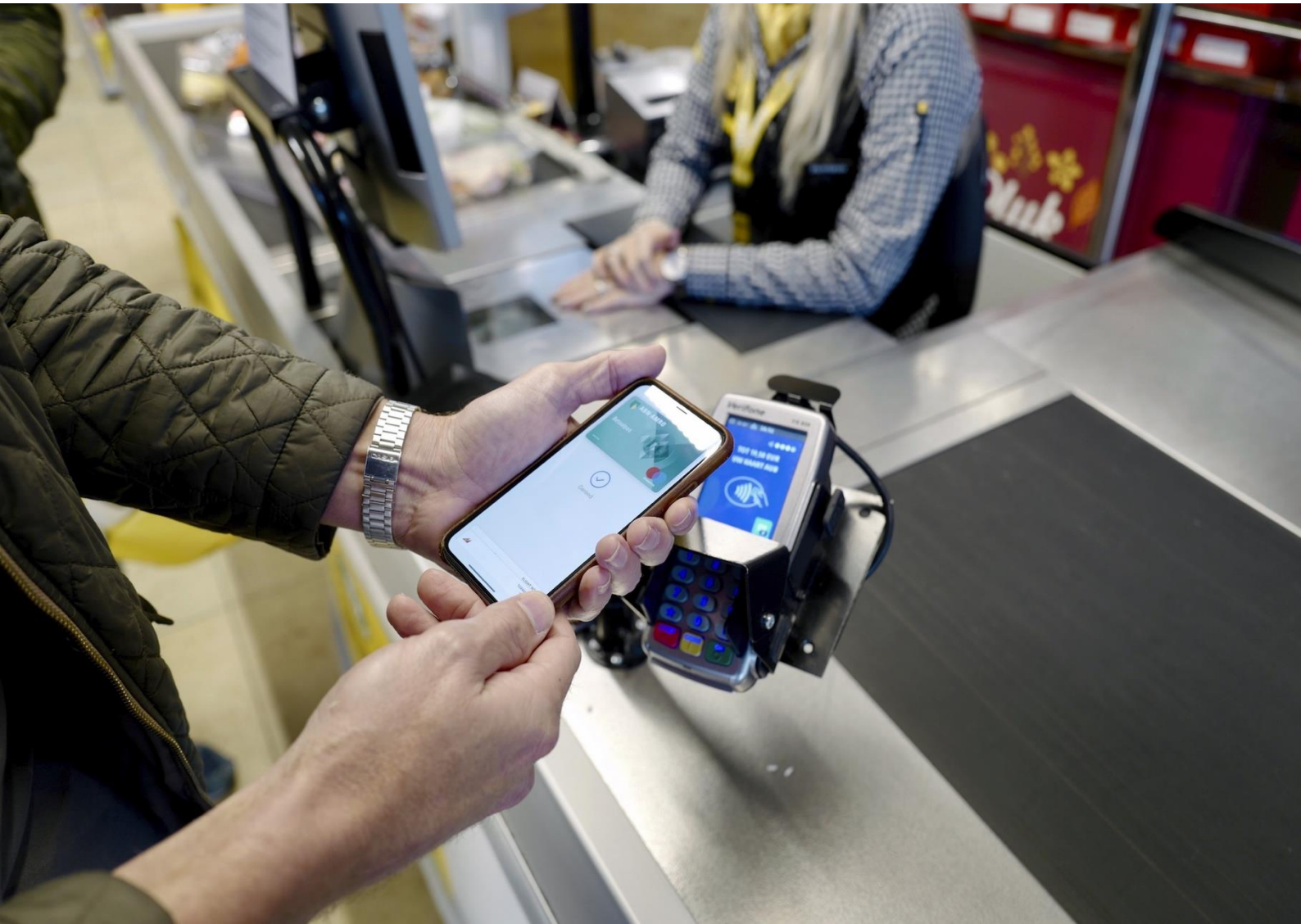

Foto omslag:

We gebruiken steeds minder contant geld. Tegenwoordig gebeurt 81% van de betalingen aan de kassa zelfs contactloos. Dat maakt het nog belangrijker dat ons betalingsverkeer veilig en betrouwbaar is en blijft.

Voortgangsrapportage 2025 Nederlandse Cybersecuritystrategie

Leeswijzer

- De voortgang wordt beschreven op het niveau van de actieclusters uit het actieplan. Dit biedt de mogelijkheid om de acties in samenhang te bespreken. De nummers uit het actieplan corresponderen met de nummers in de voortgangsrapportage.
- Niet elk onderwerp is opgenomen in de rapportage. De focus ligt op de onderwerpen met acties die in 2024 afgerond dienen te zijn en waar belangrijke ontwikkelingen op te melden zijn.
- Wanneer een bepaald onderwerp niet is opgenomen verloopt de uitvoering volgens de planning zoals beschreven in het actieplan.
- Om de voortgangsrapportage overzichtelijk te houden worden de onderwerpen maar beperkt inhoudelijk ingeleid. De voortgangsrapportage wordt daarom het beste gelezen in combinatie met de NLCS en het actieplan.

Inhoudsopgave

Pijler I
Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties 8

Doel 1: Organisaties hebben zicht op cyberincidenten, -dreigingen en -risico's en hoe hiermee om te gaan. 8

I.1.1: Herziening van het stelsel 8

De vernieuwde NCSC organisatie
Cyclotron

I.1.2: Versterken Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden (LDS) 9

I.1.3: Uitbreiden schakelorganisaties binnen het CWN 9

I.1.4: Nationaal Detectie Netwerk 10

I.1.5: Doelwit- en Slachtoffernotificatie 10

Doel 2: Organisaties zijn goed beschermd tegen digitale risico's, en nemen hierin hun belang voor de sector en andere organisaties in de keten mee. 10

I.2.1: Digitale weerbaarheid vitale infrastructuur 10

NIS2-richtlijn
Aanpak vitale infrastructuur
Risicomanagement inkoop door vitale aanbieders

I.2.2: Digitale weerbaarheid MKB en bedrijfsleven 11

I.2.3: Digitale weerbaarheid onderwijs 11

I.2.4: Digitale weerbaarheid zorginstellingen 12

I.2.5: Digitale weerbaarheid sectoren infrastructuur en waterstaat 12

I.2.6: Digitale weerbaarheid Rijksoverheid 13

Versterken SOC Stelsel Rijk-programma 13
Red Teaming testen binnen de Rijksoverheid 13
Quantumcomputing
Verplichte basisopleiding digitale weerbaarheid

I.2.7: Digitale weerbaarheid overheid en Bestuurlijk convenant 14

I.2.8: Digitale weerbaarheid sectoren met operationele technologie- en procesautomatiseringssystemen 14

I.2.9: Zicht op digitale weerbaarheid van overheid en bedrijfsleven 14

Doel 3: Organisaties reageren, herstellen en leren snel en adequaat op en van cyberincidenten en –crises. 15

I.3.1: Incident- en crisispreparatie en I.3.2 oefenen 15

Evaluatie ISIDOOR IV
Crisisplannen en oefenen

Pijler II
Veilige en innovatie digitale producten en diensten 17

Doel 1: Digitale producten en diensten zijn veiliger 17

II.1.1: Europese wetgeving voor digitale producten en diensten 17
II.1.2: Toezicht en handhaving op digitale producten en diensten 17
II.1.3: Certificering en standaarden 18
II.1.4: Algemene beveiligingseisen rijksoverheid (ABRO) en overheidsinkoopbeleid 18

Doel 2: Nederland heeft een sterke cybersecuritykennis- en innovatieketen. 19

II.2.1: Veilige cryptografie 19
II.2.2: Nationale samenwerking kennis- en innovatie-onderzoekssamenwerking 19
II.2.3: Europese onderzoekssamenwerking en fondsen 20

Pijler III
Tegengaan van digitale dreigingen van staten en criminelen 22

Doel 1: Nederland heeft zicht op digitale dreigingen van staten en criminelen. 22

III.1.1: Zicht op statelijke actoren 22
III.1.2: Onderzoeks- en opsporingscapaciteit cybercriminelen 22
III.1.3: Versterken diplomatiek netwerk 23

Doel 2: Nederland heeft grip op digitale dreigingen van staten en criminelen 24

III.2.1: Attributie en respons 24
III.2.2: Defensieve en offensieve cybercapaciteiten 24

Doel 3: Staten houden zich aan het normatief kader voor verantwoordelijk statelijk gedrag in de digitale ruimte 25

III.3.1: Normatief kader 25
III.3.2: Internet governance 25

Pijler IV
Cybersecurity arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers 28

Doel 1: Burgers zijn goed beschermd tegen digitale risico's 28

IV.1.1: Voorlichtingscampagnes 28
IV.1.2: Beveiligingsadvies burgers 28
IV.1.3: Betrouwbaarheid digitale overheidsvoorzieningen 29

Doel 2: Burgers reageren snel en adequaat op cyberincidenten 29

IV.2.1: Melding of aangifte doen van cybercrime fenomenen 29

Doel 3: Leerlingen krijgen onderwijs in digitale vaardigheden gericht op veiligheid 29

IV.3.1: Curriculum 29

Doel 4: De Nederlandse arbeidsmarkt kan voldoen aan de toenemende vraag naar cybersecurity-experts 29

IV.4.1: Cybersecurity arbeidsmarkt 29

Digitalisering is een belangrijke stap om zorg voor iedereen toegankelijk te houden en de druk op zorgprofessionals te verminderen. Het maakt het mogelijk om zorg op afstand te verlenen, maar biedt ook sneller toegang tot informatie.

Pijler I

Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties

Het verhogen van de weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties is een opgave die een vergaande publiek-private samenwerking vergt. Onder pijler I van de Nederlandse Cybersecuritystrategie (NLCS) worden verschillende acties uitgevoerd die deze samenwerking verdiepen en uitbreiden. Deze acties dragen bij aan het realiseren van de ambitie van het kabinet om alle organisaties binnen Nederland in staat te stellen om hun weerbaarheidsniveau te verhogen.

Doel 1: Organisaties hebben zicht op cyberincidenten, -dreigingen en -risico's en hoe hiermee om te gaan.

I.1.1: Herziening van het stelsel

De vernieuwde NCSC organisatie

De integratie van het Nationaal Cyber Security Centrum (NCSC), Digital Trust Center (DTC) en Computer Security Incident Response Team voor digitale diensten (CSIRT-DSP) ligt op koers. In 2026 zal het vernieuwde NCSC alle organisaties in Nederland als doelgroep hebben. Om dit te realiseren gaat het NCSC samen met het DTC en CSIRT-DSP momenteel door een intensieve transitie, waarin hard wordt gewerkt om producten, processen en mensen te laten landen in de vernieuwde organisatie. Daarnaast wordt ook het aansturingsmodel, interne governance en de merkstrategie geactualiseerd. Het DTC en het NCSC werken nu al op tal van terreinen intensief samen. Door kennis, ervaring en netwerken te verbinden, ontstaat een gezamenlijke aanpak die zichtbaar is in de producten en dienstverlening. Concrete voorbeelden van de samenwerking zijn de gezamenlijke adviesraad met daarin vertegenwoordiging uit het bedrijfsleven en het cyberdomein, de gezamenlijke aanpak van doelwit- en slachtoffernotificatie, de ontwikkeling en het gezamenlijk uitdragen van de vijf basisprincipes voor cyberweerbaarheid, en de nauwe samenwerking gedurende de NAVO-top. In het najaar van 2025 zullen ook de uitingen via de diverse communicatiekanalen van beide organisaties zichtbaar maken dat er wordt toegewerkt naar één nationale cybersecurityorganisatie.

Het vernieuwde NCSC heeft vier rollen: Nationaal CSIRT, Sectoraal CSIRT, Kennis- en adviescentrum en Uitvoeringscoördinator binnen het cybersecuritystelsel. Vanuit die rollen werkt de organisatie aan een digitaal weerbaar Nederland.

Om de integratie mogelijk te maken wordt er voor schakelorganisaties bepaald welke taken bij het NCSC en welke taken sectoraal worden belegd.[1] Het uitgangspunt hierbij is

[1] Organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek over dreigingen en incidenten met betrekking tot netwerk- en informatiesystemen te informeren. Zie Regeling aanwijzing schakelorganisaties cybersecurity.

'centraal tenzij'. Om dit te bereiken wordt het CSIRT-stelsel ingericht binnen de kaders van de Cyberbeveiligingswet (Cbw) en in overeenstemming met het rapport "Een beleidskader voor het herinrichten van het stelsel met een nationale en sectorale CSIRT's in Nederland".[2] De sectorale CSIRT's zullen onderling samenwerkingsafspraken maken die worden vastgelegd in een samenwerkingsprotocol. Dit zorgt voor transparantie over de gemaakte afspraken en maakt voor de betrokken entiteiten helder op welke wijze de CSIRTs invulling geven aan hun taken. Het samenwerkingsprotocol zal samenhangen met de implementatie van de Cbw en naar verwachting in Q2 2026 worden opgeleverd.[3]

De huidige hybride en constante dreiging vraagt om vergaande publiek-private samenwerking. De verkenning naar de oprichting van een House of Cyber, waarbinnen het NCSC, het ministerie van Defensie, publieke veiligheidsdiensten, wetenschappelijke organisaties, kennisinstituten en private cybersecuritypartijen nauw samenwerken onder één dak aan de digitale weerbaarheid van Nederland, is inmiddels afgerond. De verkenning heeft geleid tot een uitvraag bij het Rijksvastgoedbedrijf naar beschikbare locaties. Vanuit het NCSC wordt er nauw samengewerkt aan de verdere visievorming en de realisatie van publiek-private samenwerking onder één dak.

Cyclotron

Het programma Cyclotron verbindt publiek-private partijen met een hoge cybersecurity volwassenheid en realiseert de uitwisseling van informatie over cyberdreiging en incidenten tussen deze partijen. De eerste technische voorzieningen zijn gerealiseerd en in gebruik genomen bij het NCSC. Cyclotron heeft inmiddels 35 aangesloten organisaties die deelnemen in deze publiek-private samenwerkingen. Van de 35 aangesloten organisaties delen nu negentien partijen actief informatie met elkaar. Naast zicht op de dreigingen en incidenten leidt dit ook tot meer onderlinge kennisuitwisseling en samenwerking. Op dit moment zijn er elf publiek-private samenwerkingen opgestart, waarvan vijf in een verkennende fase.

De juridische vereisten voor deze publiek-private samenwerking zijn onderzocht en hierover is een rapport gepubliceerd door het NCSC en gedeeld met de Governance Board Cyclotron. De conclusies zijn gebundeld in een gezamenlijk convenant, dat tijdens One Conference op 30 september is ondertekend.

Het afgelopen jaar is vanuit verschillende publiek-private partijen de wens uitgesproken de resultaten van het Cyclotron programma te versnellen. Door de publieke deelnemers zijn daarvoor ook extra middelen ter beschikking gesteld. Het programma is bovendien geëvalueerd middels een Gateway Review om ook de volgende fase van het programma succesvol te kunnen uitvoeren.[4] Dit rapport is gelijktijdig met deze voortgangsrapportage NLCS 2025 met uw Kamer gedeeld. De Gateway Review geeft een stevig oordeel en stelt dat er meer strategische en inhoudelijke richting gegeven moet worden aan het programma. Tegelijkertijd is er een breed draagvlak waargenomen voor de doelstelling van Cyclotron: bijdragen aan een verhoogde maatschappelijke cyberweerbaarheid door verbetering van het zicht op cyberdreigingen. Het Gateway Reviewteam doet in haar rapport concrete aanbevelingen omtrent het meetbaar maken van de resultaten en het intensiveren van de inhoudelijke regie. De aanbevelingen in het rapport bieden een goede basis voor de verdere inrichting van het publiek-private samenwerkingsplatform. Het Gateway reviewteam en alle geïnterviewde partijen worden dan ook graag bedankt voor hun inzet en het goede rapport. Het programmateam Cyclotron gaat aan de slag met de aanbevelingen. Volgend jaar zal in de Voortgangsrapportage NLCS 2026 gerapporteerd worden hoe de aanbevelingen zijn geïmplementeerd. Het is het streven dat de uitvoering van het programma vanaf 1 januari 2026 volledig bij het NCSC belegd is.

I.1.2: Versterken Cyberweerbaarheidsnetwerk (CWN) (voorheen Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden (LDS)) en

I.1.3: Uitbreiden schakelorganisaties binnen het CWN

Het Cyberweerbaarheidsnetwerk (CWN), als opvolger van het LDS, is een publiek-private samenwerking binnen het Koninkrijk der Nederlanden. Het CWN faciliteert en coördineert samenwerking op gebied van:

1. Informatiedeling,
2. doelwit- en slachtoffernotificatie,
3. incidentafhandeling,
4. kennisuitwisseling,
5. opleiden, trainen en oefenen (OTO).

Het CWN wordt gecoördineerd door het NCSC als uitvoeringscoördinator. Het NCSC zal in deze rol initiërend,

[2] Een beleidskader voor het herinrichten van het stelsel met een nationale en sectorale CSIRT's in Nederland
[3] Kamerstuk, 2024-2025, 36764-6
[4] Uitleg Gateway Review

regisserend en coördinerend zijn, maar de uitvoering is nadrukkelijk een publiek-private samenwerking tussen meerdere publieke en private netwerkpartners. Het bouwplan voor het CWN is op 10 september gepubliceerd op de website van het NCSC en geeft daarmee een eerste invulling aan de implementatie van de Toekomstvisie Cyberweerbaarheidsnetwerk waarin het beleidsmatige kader voor de doorontwikkeling van het LDS is vastgelegd.[5] De volgende stap is het netwerk op te bouwen met de publieke en private netwerkpartners en voor ieder van de bovengenoemde functies te werken aan concrete resultaten. Daarbij zal steeds worden bekeken of in de toekomst mogelijke aanpassingen nodig zijn. Hiermee is actie I.1.3.1 afgedaan.

De Wet bevordering digitale weerbaarheid bedrijven (Wbdwb) is op 1 oktober 2024 in werking getreden. Deze wet zet de taken en bevoegdheden van de minister van Economische Zaken (EZ) uiteen op het terrein van digitale weerbaarheid van niet-vitale bedrijven in Nederland, zoals het verwerken en verspreiden van informatie over kwetsbaarheden, dreigingen en incidenten en het samenwerken met andere bestuursorganen en organisaties. Deze wet vormt een grondslag om vanuit de overheid niet-vitale Nederlandse bedrijven te kunnen waarschuwen over digitale kwetsbaarheden, cyberdreigingen en beveiligingslekken. Met de inwerkingtreding van de Wbdwb is actie I.1.2.1 van de NLCS afgerond.

I.1.4: Nationaal Detectie Netwerk

Via het Nationaal Detectie Netwerk (NDN) werken overheidsorganisaties en bedrijven samen om geavanceerde digitale aanvallen eerder en beter waar te nemen. Verschillende ontwikkelingen zoals (aanstaande) verandering in wetgeving en technische uitdagingen vragen om een andere aanpak. Het afgelopen jaar is een nieuwe aanpak ontwikkeld waarin de vernieuwde toekomstvisie tot aan 2028 is beschreven voor monitoring en detectie van geavanceerde digitale aanvallen. Onderdeel van deze aanpak is het mogelijk maken van veiliger cloudgebruik, het ontwikkelen van een eigen cyber threat intelligence (CTI) capaciteit en wordt er versterkt ingezet op kennisdeling tussen aangesloten partijen.

I.1.5: Doelwit- en Slachtoffernotificatie

Met de aanpassing van het Besluit politiegegevens is het nu mogelijk om op structurele wijze informatie uit te wisselen vanuit de politie met het NCSC ten behoeve van slachtoffer- en doelwitnotificatie. Het NCSC kan de verkregen informatie verder delen met organisaties die wettelijk zijn aangemerkt als doelgroep van het NCSC, die vanwege de integratie en de inwerkingtreding van de Cbw, beide voorzien in 2026, aanzienlijk wordt uitgebreid. Het NCSC kan daarnaast de informatie delen met het EU CSIRT-netwerk. Ook is gesproken over nut en noodzaak van gezamenlijke standaarden en gezamenlijke tooling om informatie-uitwisseling te bevorderen. Met de komst van de Cbw ontstaan er op internationaal vlak meer mogelijkheden voor slachtoffer- en doelwitnotificatie, omdat de Cbw het delen van informatie vanuit het CSIRT's, waaronder het NCSC, met andere EU CSIRT's of gelijkwaardige organisaties buiten de EU onder strikte voorwaarden mogelijk maakt.

Doel 2: Organisaties zijn goed beschermd tegen digitale risico's, en nemen hierin hun belang voor de sector en andere organisaties in de keten mee.

I.2.1: Digitale weerbaarheid vitale infrastructuur

De Cbw en de Wet weerbaarheid kritieke entiteiten (Wwke), die respectievelijk de NIS2- en de CER-richtlijn implementeren, zijn op 2 juni 2025 aangeboden aan de Tweede Kamer.[6] De concept algemene maatregelen van bestuur (amvb's) zijn de nadere uitwerkingen van de Cbw en Wwke. De concept-amvb's zijn op 30 juni 2025 onverplicht naar de Tweede Kamer gestuurd. De Cbw en de Wwke zien toe op het verhogen van de fysieke en digitale weerbaarheid van de vitale infrastructuur. De verwachting dat de wetten in Q2 2026, afhankelijk van parlementaire behandeling, in werking treden.[7]

Momenteel draait de voorlichtingscampagne gericht op *wat* een organisatie nu al kan doen, en *hoe* men de juiste maatregelen kan treffen, zowel voor de Cbw als de Wwke. Er worden concrete handreikingen en tools aangeboden waarmee een organisatie een inschatting kan maken of men onder de Cbw of Wwke valt. Daarnaast worden handreikingen ontwikkeld aan de hand waarvan NIS2-sectoren hun beveiligingsmaatregelen kunnen versterken. Deze handreikingen worden bijvoorbeeld via de website van de

[5] Bouwplan Cyberweerbaarheidsnetwerk
[6] Kamerstukken, 2024-2025, 36764
[7] Kamerstuk, 2024-2025, 36764-6

NCTV gedeeld.[8] Er is daarnaast ook sectorspecifieke informatie beschikbaar vanuit de vakdepartementen.[9] Ook de NIS2-Zelfevaluatietool en de NIS2-Quickscan ontwikkeld door de Rijksdienst Digitale Inspectie (RDI) blijven veelgebruikte tools.[10]

Er wordt daarnaast vanuit de NCTV in samenwerking met de vakdepartementen gewerkt aan de herziening van het huidige beleidsinstrumentarium voor de Aanpak vitaal. Dit instrumentarium zorgt o.a. voor ondersteuning van de vakdepartementen bij het uitvoeren van de risicobeoordeling. Deze herziening heeft enerzijds als doel om het instrumentarium in lijn te brengen met de wettelijke vereisten vanuit de Wwke en anderzijds om scherper aan te sluiten bij het continue veranderende dreigingslandschap. In deze herziening is expliciet aandacht voor sector overschrijdende risico's, cascade-effecten en risicovolle afhankelijkheden.

Eén van de onderdelen van de Cbw is de invoering van een meldplicht, die geldt voor 'significante incidenten'. Dit zijn incidenten die een ernstige operationele verstoring van de diensten of financiële verliezen voor de organisatie (kunnen) veroorzaken. Ook gaat het om incidenten die (kunnen) leiden tot aanzienlijke materiële of immateriële schade bij andere organisaties. De exacte drempelwaarden voor significante incidenten worden nog uitgewerkt. De meldplicht is pas van kracht zodra de Cbw in werking treedt. Tot die tijd is het voor alle organisaties mogelijk vrijwillige meldingen te doen bij het NCSC. Sinds 17 oktober 2024 is hiervoor een meldformulier beschikbaar op www.ncsc.nl.

Om kwaliteit en consistentie van het toezicht op organisaties na de implementatie van de NIS2 te verzekeren, wordt het Samenhangend Inspectiebeeld Cybersecurity Vitale Processen (SIB) en de bijhorende governance doorontwikkeld. Eerder werd het SIB jaarlijks gepubliceerd. Om tot een meer inhoudelijk product te komen heeft het Directeurenoverleg Toezicht Digitale Weerbaarheid (DTDW) in april 2025 besloten de publicatie van het SIB voor 2 jaar te pauzeren. In 2026 starten de inhoudelijke activiteiten voor het SIB. Daarnaast werken de betrokken toezichthouders sinds september 2024 aan een intensivering van de samenwerking.

I.2.2: Digitale weerbaarheid MKB en bedrijfsleven

Vanaf 2026 zal het DTC samengaan met het NCSC en CSIRT-DSP tot een nieuwe cybersecurity organisaties met heel Nederland als doelgroep.

Het Digital Trust Centre (DTC) zet zich op verschillende manieren in voor de digitale weerbaarheid van het midden- en kleinbedrijf (mkb) en het bedrijfsleven. Het DTC heeft afgelopen jaar het gebruik van risicoscans en de opvolging van concrete beveiligingsadviezen en handelingsperspectieven actief gestimuleerd binnen het mkb, onder andere via brancheorganisaties, samenwerkingsverbanden en publiek-private platforms zoals Samen Digitaal Veilig.[11] Via verschillende (ondernemers)verhalen uit de praktijk is het belang van digitale weerbaarheid en de aanbevolen tools op een herkenbare manier onder de aandacht gebracht. Verder is via de subsidieregeling Mijn Cyberweerbare Zaak voor micro- en kleine ondernemingen een financiële compensatie beschikbaar gesteld voor de aanschaf en implementatie van één of meerdere belangrijke cyberweerbaarheidsmaatregelen.

I.2.3: Digitale weerbaarheid onderwijs

Binnen de onderwijssector is intensief overleg gevoerd met alle betrokken stakeholders over de toenemende digitale dreiging en een effectieve aanpak voor de verdere versterking van de cyberweerbaarheid. De Minister van Onderwijs, Cultuur en Wetenschap heeft, na overleg met de Minister van Justitie en Veiligheid (JenV), besloten om de hogescholen en universiteiten onder toepassing van de Cbw te brengen.[12] Dit besluit wordt momenteel in nauw overleg met de betrokken stakeholders nader uitgewerkt.

In de gehele onderwijssector is er het afgelopen jaar aandacht besteed aan awareness programma's. Er wordt continu ingezet op de 'factor mens' door verschillende bewustwordings-campagnes voor studenten, medewerkers én bestuurders, door deelname aan oefeningen en weerbaarheidstesten, maar ook door trainingen voor de Raden van Toezicht. Ook heeft SURF een informatiepunt opgezet middels de website cybersaveyourself.nl voor zowel docenten, studenten als de voor de security en privacy professionals binnen de school.[13] Dit komt voort uit het eerder opgezette programma Cybersave yourself.[14]

In het afgelopen jaar zijn de meeste instellingen in het mbo, hbo en wo extern geaudit. Bijna alle instellingen doen mee aan

8 Documenten | Nationaal Coördinator Terrorismebestrijding en Veiligheid
9 Bijvoorbeeld NIS2 impact toeleveringsketen Chemische sector door Berenschot, uit opdracht I&W
10 NIS2 Zelfevaluatie NL en NIS2 Quickscan
11 Samen Digitaal Veilig - Samen Digitaal Veilig
12 Kamerstuk 31288, nr. 1189
13 SURF is de ICT-coöperatie van Nederlandse onderwijs- en onderzoeksinstellingen
14 Website Cybersave yourself

het sectorbeeld digitale veiligheid. Dit wordt gedaan op basis van het gezamenlijke SURF-toetsingskader.

Het CERT voor het funderend onderwijs is nu ook toegankelijk voor schoolbesturen buiten de pilot. Stapsgewijs sluiten er steeds meer scholen aan die dreigingsinformatie ontvangen en hulp krijgen als ze te maken krijgen met een cyberincident.

Het onderwerp informatiebeveiliging en privacy is in 2025 opgenomen als maatschappelijk thema in het bestuursverslag. Daarmee zijn scholen vanaf dit jaar verplicht om verantwoording af te leggen over welke acties ze hebben ondernomen op het gebied van de borging van informatiebeveiliging en privacy.

I.2.4: Digitale weerbaarheid zorginstellingen

Zorgaanbieders zijn op grond van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) verplicht om te voldoen aan de NEN-7510 norm. De herziene norm is eind 2024 gepubliceerd. Hiermee is actie I.2.4.1 afgerond. De Stichting Koninklijk Nederlands Normalisatie Instituut (NEN) heeft reeds 4 implementatietools gratis beschikbaar gesteld om het zorgveld te ondersteunen bij de implementatie van de norm. Eind 2025 zal er daar een gratis risico-tool bijkomen die organisaties ondersteunt bij het maken van risico inschattingen.

In het kader van het project risicogestuurde aanpak worden zorgsectoren stapsgewijs aangesloten bij het expertisecentrum voor cybersecurity in de zorg Z-CERT, waar nu 373 organisaties deelnemer van zijn.[15] In 2025 zijn ook de ambulancezorg, gehandicaptenzorg en Verpleeg- en Verzorgingshuizen en Thuiszorg (VVT) aangesloten. Z-CERT publiceert regelmatig verschillende kennisproducten en stelt deze zowel publiek als specifiek voor deelnemers beschikbaar. In het eerste halfjaar van 2025 heeft Z-CERT zich met oefenen en testen voorbereid op de NAVO top met achttien organisaties in de regio. Er zijn in totaal vijfitg tabletop oefeningen gehouden gericht op de techniek waarbij een fictief maar realistisch scenario werd nagespeeld door de instellingen. Daarnaast is de nieuwe red teaming systematiek ZORRO by ART bij drie instellingen getest.[16]

De open-source software Kwetsbaarheden Analyse Tool (OpenKAT) wordt door een aantal zorgorganisaties actief gebruikt. In het eerste halfjaar van 2025 is OpenKAT verder doorontwikkeld door het ministerie van Volksgezondheid, Welzijn en Sport (VWS). In het tweede halfjaar van 2025 ligt de focus op het uitbreiden van het deelnemersveld binnen overheidsorganisaties, met als doel het versterken van de community en het borgen van de continuïteit van OpenKAT. Per 1 januari 2026 wilt het ministerie van VWS de doorontwikkeling en het beheer en onderhoud overdragen aan een geschikte beheerpartij.

Het programma Informatieveilig gedrag in de zorg, gericht op zorgbestuurders en professionals die bezig zijn met privacy en cybersecurity risico's in zorginstellingen, blijft groeien.[17] Aan de Masterclass in het voorjaar van 2025 namen 25 experts informatieveiligheid, uit veertien verschillende zorginstellingen vanuit vijf sub sectoren binnen de zorgsector deel, waarmee het bereik in de hele zorgsector steeds verder reikt.

In januari 2025 heeft de Europese Commissie een actieplan gepresenteerd om de cyberbeveiliging van ziekenhuizen en zorginstellingen binnen de EU te verbeteren, omdat de zorgsector het hoogste aantal cyberincidenten meldt van alle kritieke sectoren en de sector in toenemende mate afhankelijk is van digitale systemen. Het actieplan richt zich op het versterken van de capaciteit van de sector om cybersecurity-incidenten te voorkomen, op efficiëntere informatie-uitwisseling en op het sneller detecteren en reageren op cyberdreigingen en incidenten om herstel te bevorderen. Nederland benadrukt in haar reactie het belang van speciale aandacht voor kleine zorgaanbieders, omdat zij vaak beperkte middelen hebben en daardoor de zwakste schakel vormen binnen de keten. Daarnaast onderstreept Nederland de grote meerwaarde van training en bewustwording binnen de zorgsector. Het actieplan moet ook goed aansluiten bij de implementatie van de Cbw en dubbelingen met nationaal beleid moeten voorkomen worden. Eind 2025 wordt het door de Europese Commissie een bijgewerkte actieplan verwacht.

I.2.5: Digitale weerbaarheid sectoren infrastructuur en waterstaat

Het ministerie van Infrastructuur en Waterstaat (IenW) zorgt met het programma Versterken Cyberweerbaarheid voor de cyberveiligheid van de sectoren waarvoor IenW systeemverantwoordelijk is. Alle vitale sectoren vallen onder de Cyberweerbaarheidsprogramma's van het ministerie van

15 Stand van zaken juli 2025: Z-CERT heeft ruim 373 deelnemers, inclusief uitbreiding naar de ambulancezorg (7), gehandicaptenzorg (35) en VVT (55)
16 ZORRO by ART staat voor ZOrg Redteaming Resilience Oefeningen (ZORRO) en Advanced Red Teaming (ART).
17 Stand van zaken juli 2025: LinkedIn volgers (1491, met groei van 72.17% sinds juli 2024), aantal inschrijvingen op nieuwsbrief (971). Het aantal deelnemers aan activiteiten van juni 2024 tot juli 2025 (648), met uitzondering van workshops en lezingen op externe events.

IenW. De Cyberweerbaarheidsprogramma's voor de luchtvaart en maritieme sector, de weg- en spoorvervoersectoren, en de watersector zijn opgestart. Rode draad door alle activiteiten voor de IenW-sectoren is de cybersecurity van Operationele Technologie (OT). Uitgangspunt hierbij is dat initiatieven waar mogelijk sector-overstijgend worden geïnitieerd en aangeboden. Op de website publiceert IenW regelmatig informatie over het programma Versterken Cyberweerbaarheid.[18]

De cyberweerbaarheidsprogramma's voor de sectoren Chemie, Nucleair, Afvalstoffenbeheer en Plaats- en tijdsbepaling zijn in 2025 van start gegaan, waarbij de focus ligt op het ophalen van knelpunten binnen de sectoren. Hiervoor is een externe kick-off gepland. Het ministerie van IenW geeft aan dat dit programma zal lopen tot 2028 en daarmee licht vertraagd is.

Als actiehouder organiseert het ministerie van Infrastructuur en Waterstaat jaarlijks samen met alle Cyberweerbaarheidsprogramma's en Concerndirectie Informatiebeleid, de cyberweerbaarheidsconferentie IenW. Op 26 mei 2025 organiseerde het ministerie van IenW de tweede cyberweerbaarheidsconferentie met als thema: Samen verder, samen weerbaar. De conferentie droeg op die manier bij aan de nationale veiligheid en het versterken van de cyberweerbaarheid van de vitale sectoren.

I.2.6: Digitale weerbaarheid Rijksoverheid

De ambitie op de digitale weerbaarheid van de Rijksoverheid wordt uiteengezet in de I-strategie Rijk en de bijbehorende routekaart digitale weerbaarheid. Over de voortgang op de routekaart en de mijlpalen die zijn behaald is de Tweede Kamer geïnformeerd via de jaarrapportage Bedrijfsvoering Rijk in mei 2025.[19]

Versterken SOC Stelsel Rijk (VSSR)

Het Versterken SOC Stelsel Rijk (VSSR) programma zorgt voor stabiele Security Operations Centres (SOC). De VSSR-organisatie richt zich op het versterken van en ondersteunen bij het inrichten van SOC's bij rijksoverheidsorganisaties door het ontwikkelen van generieke aanpakken en kennisproducten. Inmiddels is een breed aantal expertisediensten en kennisproducten ontwikkeld op gebied van monitoring en detectie, kwetsbaarhedenbeheer, operational readiness, incident response en inkoop van SOC-dienstverlening.

Daarnaast vervult VSSR een netwerk- en schakelfunctie tussen organisaties binnen de Rijksoverheid die bezig zijn met SOC-dienstverlening. Binnen het NCSC wordt gedurende 2025 de programmaorganisatie omgevormd tot een staande lijnorganisatie, onderdeel van de nieuwe NCSC-organisatie. Het is van belang om de komende jaren middels producten de SOC's binnen de rijksoverheid verder te blijven versterken. Het versterken van detectie en respons capaciteiten is ook prioriteit binnen de Nederlandse Digitaliseringsstrategie (NDS).[20]

Red Teaming testen binnen de Rijksoverheid

Om de veiligheid van kritieke functies te testen past de Rijksoverheid red teaming testen toe via de TIBER-aanpak.[21] TIBER staat voor Threat Intelligence Based Ethical Red-teaming. Deze aanpak zorgt ervoor dat een test realistisch en gebaseerd op huidige dreiging is. Het centrale team dat tijdens deze testen adviseert is gegroeid om zo steeds meer testen te kunnen begeleiden. In 2025 zijn er verschillende TIBER-testen afgerond. Bovendien is in 2024 afgesproken met alle departementen dat zij in 2024 of 2025 een test organiseren via deze methodiek.

Quantumveilige cryptografie

Om risico's door het beschikbaar komen van quantumcomputers te mitigeren is de Rijksoverheid het programma Quantumveilige Cryptografie Rijk gestart. In 2024 is het Rijksbreed beleidskader cryptografie vastgesteld en gepubliceerd. Daarnaast is in de Nederlandse Digitaliseringsstrategie (NDS) de volgende versneller opgenomen: Cyberveiligheidsbouwstenen zoals quantumveilige encryptie worden collectief ontwikkeld en geïntegreerd. Ook heeft het Rijk een e-learning voor IT-gerelateerd personeel ontwikkeld en zijn er verschillende gesprekken met allerlei doelgroepen, zoals gemeenten, waterschappen en vitale sectoren gevoerd om het bewustzijn te vergroten. Tot slot is er een eerste verkenning uitgevoerd om de scope van het programma stapsgewijs uit te breiden naar alle doelgroepen van de Cbw. Deze uitbreiding vind plaats naar aanleiding van een kabinetsbesluit en de Europese aanbeveling.[22]

In december 2024 is door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), TNO en het Centrum Wiskunde & Informatica (CWI) de herziene versie van het Post Quantum Encryptie (PQC) handboek gepubliceerd.[23] Dit handboek biedt organisaties concrete stappen en advies om de dreiging van

18 Home | Versterken cyberweerbaarheid
19 Kamerstukken II, 2024–2025, 31 490, nr. 365
20 Acties prioriteiten 2.5 Iedereen kan de digitale wereld vertrouwen - Digitale Overheid
21 Hierover is de Kamer geïnformeerd: Kamerstukken II, 2023/24, 26643, nr. 1149.
22 Bijlage bij Kamerstukken II, 2023/24 22112 nr. 3945 en Aanbeveling van de Commissie over een routekaart voor een gecoördineerde uitvoering van de transitie naar post-kwantumcryptografie.
23 Het PQC-migratie handboek | Publicatie | AIVD

quantumcomputers voor cryptografie te beperken. Deze nieuwe editie bevat ook een nieuwe adviestool, de PQChoiceAssistant, die bedrijven helpt bij hun keuze van PQC-methode.[24]

Ransomware

Fase 1 van het project 'Bescherming tegen ransomware en datadiefstal' is inmiddels afgerond en de kennisproducten die digitale weerbaarheid van de Rijksoverheid vergroten zijn ontwikkeld. In 2025 is fase 2 van het project gestart, dat is gericht op daadwerkelijke verbetering van de weerbaarheid door toepassing van de ontwikkelde kennisproducten in de praktijk. De inzet van deze kennisproducten is niet verplicht; Rijksoverheidsorganisaties bepalen zelf hoe zij hier invulling aan geven. De stimulering bestaat uit twee onderdelen:

- Aandacht voor het moeten: een meetbare norm op basis van de afgesproken strategische prioriteit, waarbij organisaties de vrijheid hebben om een eigen invulling te kiezen.
- Aandacht voor het willen en kunnen: communicatie over het nut, de noodzaak en de beschikbaarheid van de ontwikkelde hulpmiddelen.

Verplichte basisopleiding digitale weerbaarheid

Het ministerie van BZK heeft leermateriaal en een e-learning laten ontwikkelen met als doel de digitale weerbaarheid van alle Rijksmedewerkers te verhogen. De e-learning is bedoeld voor de organisaties die niet zelf al een basisopleiding hebben die voldoet aan het vastgestelde beleid.[25] Actie I-2.6.1 is daarmee afgedaan.

I.2.7: Digitale weerbaarheid overheid en Bestuurlijk convenant

In opdracht van de ministeries van BZK en JenV, VNG en de G4 is een onderzoek uitgevoerd dat zicht geeft in het cyberlandschap van gemeenten en de verantwoordelijkheden van het lokale bevoegd gezag in het digitale domein. Momenteel wordt in kaart gebracht op welke punten nog moet worden versterkt. Over de opvolging van de aanbevelingen wordt gerapporteerd middels de Voortgangsrapportage van de Nederlandse Digitaliseringsstrategie (NDS).

De Baseline Informatiebeveiliging Overheid (BIO) 2 is op 25 september 2025 vastgesteld en gepubliceerd. Deze zal niet in de Wet Digitale Overheid (WDO) maar in de Cbw worden verankerd, die naar verwachting in het tweede kwartaal van 2026 in werking zal treden.[26] De uitvoering van het ondersteuningsprogramma BIO is gecontinueerd in 2025.

De doorontwikkeling van de verantwoordingssystematiek voor informatieveiligheid van gemeenten, ook wel Eenduidige Normatiek Single Information Audit (ENSIA), is in 2025 voortgezet.

I.2.8: Digitale weerbaarheid sectoren met operationele technologie- en procesautomatiseringssystemen

In de IenW beleidsagenda voor 2026 staat dat IenW zich inzet voor het lanceren van een Kennis en Expertise centrum voor OT & cybersecurity. Om te onderzoeken of een OT expertisecentrum gewenst is zal eerst een verkenning worden uitgevoerd. Wanneer uit de verkenning blijkt dat een OT expertisecentrum van toegevoegde waarde is, is het streven om de activiteiten en doelstellingen van de cyberweerbaarheidsprogramma's zo veel als mogelijk op te laten gaan in het expertisecentrum, met als doel de tijdelijke programma's verantwoord te kunnen beëindigen.

I.2.9: Zicht op digitale weerbaarheid van overheid en bedrijfsleven

Norea Reporting Initiative

De Nederlandse beroepsorganisatie van IT-auditors (NOREA) heeft een generiek format voor een IT-jaarverslag en een IT-auditverklaring ontwikkeld als onderdeel van het NOREA Reporting Initiative (NRI). De eerste pilots met dit format hebben inmiddels plaatsgevonden. Het ministerie van BZK werkt aan het organiseren van aanvullende pilots. Daarnaast sluit het ministerie van BZK aan bij de initiatiefgroep voor het International Digital Reporting Standards (IDRS) van ECP Platform voor de Informatiesamenleving om de standaard verder te ontwikkelen.

Basisbeveiliging.nl

Via het Centrum voor Informatiebeveiliging en Privacy (CIP), dat wordt gecontinueerd in 2025, geeft het ministerie van BZK een bijdrage aan de Stichting Internet Cleanup Foundation (ICF) voor het onderhoud en de verdere ontwikkeling van de site Basisbeveiliging.nl. Zo blijft de website actueel. Deze website faciliteert kennisdeling tussen overheidsorganisaties en maakt zo concrete verbeteringen mogelijk.

[24] PQC Choice Assistant
[25] Kamerstukken II, 2024–2025, 31 490, nr. 365
[26] Baseline Informatiebeveiliging Overheid (BIO) 2

Monitoringssystematiek

Cybersecurity is een beleidsterrein dat de afgelopen jaren doorontwikkeld is binnen de overheid en het bedrijfsleven. Doel van de monitoringssystematiek is om de digitale weerbaarheid van Nederland over meerdere jaren te kunnen meten en uiteindelijk ook de effecten van beleid inzichtelijk te maken. Om te komen tot een monitoringssystematiek is een onderzoek uitgezet via het WODC. De uitkomsten van dit onderzoek worden betrokken bij de tussentijdse evaluatie van de NLCS in 2026.

Doel 3: Organisaties reageren, herstellen en leren snel en adequaat op en van cyberincidenten en –crises.

I.3.1: Incident- en crisispreparatie en I.3.2: Oefenen

Update Landelijk Crisisplan Digitaal (LCP-D)

In de aankomende update van het Landelijk Crisisplan Digitaal (LCP-D) worden onder andere de ervaringen van de NAVO-top en de cyberoefening ISIDOOR IV, en stelselwijzigingen zoals de integratie van het NCSC met het CSIRT-DSP en het DTC meegenomen.

Ook de implementatie van de Cbw en de stelselwijzigingen die als gevolg hiervan plaatsvinden, hebben een belangrijke uitwerking op het LCP-D. Om die reden is besloten om in 2026, na inwerkingtreding van de Cbw, een geüpdatete versie van het LCP-Digitaal te publiceren. Verschillende publieke en private stakeholders en partners op het vlak van (digitale) crisisbeheersing worden nauw bij de aankomende update betrokken.

Crisisplannen en oefenen

Het afgelopen jaar hebben er verschillende oefeningen plaatsgevonden waarin de aansluiting van het LCP-D op de departementale crisisplannen werd beoefend. Zo werd door het ministerie van BZK het afgelopen jaar de 6e editie van de overheidsbrede cyberoefening georganiseerd. Hier nemen de Rijksoverheid, provincies, gemeenten en waterschappen aan deel. In deze editie zijn aanvullend specifieke activiteiten georganiseerd in samenwerking met Caribisch Nederland. Voorafgaand hieraan oefenden vele deelnemende organisaties binnen hun eigen organisatie al met hetzelfde scenario. Regionale crisisplannen sluiten door deze oefeningen steeds beter aan het op LCP-D en worden doorlopend doorontwikkeld. Het NCSC en de NCTV organiseren de volgende editie van de grootschalige ISIDOOR oefening, ISIDOOR V, op zijn vroegst in 2027. Dit stelt organisaties in staat om de eigen planvorming voor te bereiden na publicatie van de update van het LCP-D. Ook zorgt de aankomende Cbw voor een uitbreiding van de doelgroep van het NCSC. Daarom wordt in de komende periode de vorm en omvang van ISIDOOR V verder uitgewerkt.

Ook werd er door verschillende departementen deel genomen aan verschillende internationale oefeningen waaronder Port Defender, Locked Shields en het Virtual Cyber Incident Support Capability (VCISC) en NAVO gestuurde Crisis Management Exercise (CMX). Aan de CMX namen vrijwel alle departementen van de Rijksoverheid in 2025 deel. In deze NAVO oefening, waarbij de interne en NAVO-brede besluitvormingsprocessen werden geoefend en getest, waren cyberaspecten een belangrijk onderdeel van het scenario. In november staat BlueOlex op de agenda.

Inlichtingen-gebaseerde incidentencoördinatie

De op inlichtingen-gebaseerde incidentencoördinatie vanuit de AIVD en de MIVD is in 2025 verder uitgebouwd, onder andere via de samenwerking in de Cyber Intel/Info Cel (CIIC) en het cyberincident team van de AIVD en de MIVD dat de Intelligence Based Incident Coordination (IBIC) uitvoert. De Nederlandse overheid was in 2024 regelmatig doelwit van statelijke cyberactoren. Het IBIC-team heeft in 2024 verschillende organisaties, bedrijven en individuen in Nederland genotificeerd over geavanceerde en persistente digitale aanvallen van deze cyberactoren en advies gegeven over het mitigeren van deze concrete dreigingen. Bij het coördineren van cyberincidenten heeft het IBIC-team, daar waar nodig, samengewerkt in de CIIC, het NCSC en andere partners.

In de loop van 2025 worden de aanbevelingen uit de tweede evaluatie van de CIIC geïmplementeerd.[27] In Q1 2026 wordt vervolgens onder leiding van de AIVD en MIVD een uitvoerige evaluatie van de CIIC uitgevoerd. Tijdens de NAVO-top heeft de CIIC een belangrijke rol gespeeld als verbindende schakel tussen de CIIC-partijen (NCSC, openbaar ministerie, nationale politie, MIVD en AIVD). Hierdoor kon operationele afstemming goed plaatsvinden en een bijdrage worden geleverd aan het situationeel beeld van het NCSC.

[27] In 2024 heeft een 'lichtvoetige' evaluatie plaatsgevonden ter voorbereiding op de uitgebreide evaluatie voorzien in Q1 2026.

Het einde van de OV-chipkaart is nabij. Binnenkort is inchecken met een betaalpas of smartphone mogelijk in het openbaar vervoer. Dit moet zorgen voor meer reis- en betalings-gemak. Een dergelijke verandering is een behoorlijke operatie. Ruim 60.000 poortjes en kaartlezers moeten worden omgebouwd.

Pijler II

Veilige en innovatie digitale producten en diensten

Doel 1: Digitale producten en diensten zijn veiliger

II.1.1: Europese wetgeving voor digitale producten en diensten

Eind 2024 is de Cyber Resilience Act (CRA) gepubliceerd. De CRA bevat een zorgplicht voor fabrikanten, importeurs en distributeurs voor de cybersecurity van producten met digitale elementen (alle hard- en software producten en losse componenten) die zij vanaf 11 december 2027 in de EU op de markt aanbieden. Deze zorgplicht geldt voor de gehele verwachte levensduur van het product. De zorgplicht is vastgelegd in essentiële eisen waar het product aan moet voldoen. Deze eisen worden omgezet in Europese normen. De nationale markttoezichthouders zullen hier toezicht op houden. In Nederland is dat de RDI. De uitvoeringswet die deze eisen voor Nederland vastlegt wordt dit najaar aangeboden aan de Tweede Kamer.

In de CRA is aandacht besteed aan een goede aansluiting op sectorspecifieke cybersecurityregulering.[28] De digitale producten die onder deze sectorspecifieke cybersecuritywetgeving vallen worden uitgesloten van de CRA. Daarnaast worden de in de CRA genoemde cybersecurityeisen door CEN/CENELEC en ETSI vertaald in concrete technische maatregelen waarmee een product aan de eis kan voldoen. Ook wordt er bij de uitvoering aandacht besteed aan de aansluiting op andere cybersecurityregelgeving. Zo zal het meldloket, waar fabrikanten op grond van de CRA actief uitgebuite kwetsbaarheden en incidenten moeten melden, onderdeel worden van het meldportaal voor Cbw entiteiten bij het NCSC.

De Europese eisen voor de digitale veiligheid van radioapparatuur (alle apparaten die contactloos kunnen communiceren, inclusief IoT-apparatuur) zijn reeds in 2021 vastgesteld in een gedelegeerde handeling onder de Richtlijn Radioapparatuur (RED) en van kracht sinds 1 augustus 2025. Inmiddels zijn hiervoor geharmoniseerde technische normen ontwikkeld. Aan de totstandkoming van deze normen heeft het kabinet bijgedragen met een subsidie aan NEN, zodat het secretariaat voor de werkgroep bestaande uit experts vanuit het kabinet en private partijen gevoerd kon worden. Voor de CRA, in het kader waarvan de eisen onder de RED worden opgenomen en verder uitgebreid, wordt dezelfde aanpak gehanteerd.

II.1.2: Toezicht en handhaving op digitale producten en diensten

Radio Equipment Directive (RED)

[28] Voor medische hulpmiddelen en auto's bestaat al sectorspecifieke regelgeving en zijn dus uitgezonderd van de CRA. De CRA zorgt voor alle andere producten waar geen sectorspecifieke regels voor bestaan.

De RDI houdt toezicht op de toepassing van de cybersecurityeisen op producten die onder de RED vallen, evenals op de uitbreiding van de eisen onder de CRA. In aanloop naar de inwerkingtreding van de eisen onder de RED (die van kracht zijn sinds 1 augustus 2024) heeft de RDI actief voorbereidingen getroffen en continueert zij dit voor de CRA. Zo is capaciteit opgebouwd en een testlab ingericht. Voor de RED-cybersecurityeisen is onderzoek gedaan naar de kwetsbaarheid van diverse productcategorieën, zoals omvormers voor zon-PV-installaties, om fabrikanten aan te sporen zich beter voor te bereiden op de RED-eisen.

Daarnaast voert de RDI een actieve bewustwordingsstrategie richting fabrikanten en andere relevante marktspelers. Ook deze inspanningen worden de komende jaren voortgezet ter voorbereiding op de uitvoering van taken die voortkomen uit de bredere reikwijdte van de CRA.

Het normalisatieproces voor de RED heeft, door de inhoudelijke complexiteit en de grote diversiteit aan producten, langer geduurd dan voorzien. Dit heeft geleid tot uitstel van de inwerkingtreding van de cybersecurityeisen onder de RED tot 1 augustus 2025. Ondanks het verleende uitstel is de tijdige toepassing van de betreffende normen een uitdaging voor de markt. De RDI houdt hier rekening mee bij het toezicht en besteedt ook aandacht aan de dienstverlening van conformiteitsbeoordelingsinstanties die hierin een rol spelen.

II.1.3: Certificering en standaarden

In 2024 is in het kader van de Europese Cybersecurity Act (CSA) door de Europese Commissie, in samenwerking met het Europese agentschap voor cybersecurity (ENISA), gewerkt aan de uitwerking van een Europees certificeringsschema voor clouddiensten (EUCS). Eind april 2025 heeft de Europese Commissie aan ENISA het verzoek gedaan om een kandidaat-Europese cybersecuritycertificeringsregeling te ontwikkelen voor beheerde beveiligingsdiensten (Managed Security Services – MSS). Deze regeling beoogt de bestaande diversiteit en versnippering in aanpak en vereisten voor de levering van MSS binnen de EU-lidstaten tegen te gaan. Doel van het schema is enerzijds het versterken van het algehele beveiligingsniveau tegen cyberdreigingen, en anderzijds het bevorderen van harmonisatie binnen de interne markt. De Europese regeling zal bestaande nationale certificeringen op dit terrein geleidelijk vervangen. Begin 2025 heeft de Europese Commissie het verdere besluitvormingsproces rond het EUCS gepauzeerd, met als doel om de evaluatie en herziening van de CSA tot prioriteit te verklaren. In het kader van deze herziening heeft het kabinet een non-paper opgesteld met de Nederlandse standpunten. De verwachting is dat de Europese Commissie nog in de loop van 2025 met een voorstel komt voor een herziene CSA.[29] Daarna zal het verdere besluitvormingsproces rond het EUCS weer worden opgepakt.

Voor het certificeringschema voor beveiligingselementen in producten (common criteria) is de RDI toezichthouder. Met de transitie van het hiervoor geldende multilaterale schema NSCIB naar het Europese certificeringschema EUCC begin 2025, is de RDI primair verantwoordelijk voor de uitgifte van certificaten.[30] NSCIB zal vanaf februari 2026 volledig overgaan in EUCC. De AIVD behoudt een adviserende rol op de evaluatie van producten op het hoogste beveiligingsniveau van EUCC. Ter bevordering van de bewustwording en ondersteuning van de implementatie van certificeringsschema's in het kader van de CSA, heeft de RDI meerdere overlegtafels en informatieve bijeenkomsten georganiseerd.

II.1.4: Algemene beveiligingseisen rijksoverheid (ABRO) en overheidsinkoopbeleid

De beveiligingseisen van de ABRO zijn opgesteld en doorlopen momenteel een interdepartementaal goedkeuringsproces dat naar verwachting in het najaar van 2025 zal zijn afgerond. Er komt één instantie, tevens aanspreekpunt, die toetst of leveranciers voldoen aan de gestelde eisen en die gedurende de looptijd van de opdracht toezicht houdt op de naleving door opdrachtnemer: het Nationaal Bureau Industrieveiligheid (NBIV) van de MIVD en AIVD. Het NBIV is op 28 maart 2025 opgericht.[31] De afspraken tussen departementen, agentschappen en politie ("Tranche 1") om de ABRO toe te passen zijn vastgelegd in een Kaderbesluit.

Voor departementale implementatieteams komt een ABRO-handreiking beschikbaar. Voor de inkopende organisaties komt een ABRO-gids beschikbaar met praktische handvatten. Ook komt er een centraal portaal voor het indienen van ABRO aanvragen. Na afloop van het programma zal de verantwoordelijkheid voor actualisatie van het beveiligingsbeleid bij overheidsinkopen, interdepartementale coördinatie en toezicht op juiste toepassing van het beleid in de lijn belegd worden bij het ministerie van BZK.

[29] Non paper on CSA The Netherlands | Tweede Kamer der Staten-Generaal
[30] NSCIB: Netherlands scheme for Certification in the Area of IT Security en EUCC: EU Cybersecurity Certification Scheme on Common Criteria
[31] NBIV regeling

De Tweede Kamer is in maart 2025 geïnformeerd over de voortgang van het Programma ABRO.[32] Daarin is onder meer gemeld dat het streven is het regelgevings- en organisatorische kader van ABRO voor het zomerreces van 2025 af te ronden. Ook is aangegeven dat de eerste inkopende organisaties van tranche 1 naar verwachting vanaf de zomer van 2025 starten met het toepassen van ABRO. Dat is niet haalbaar gebleken. Voordat met de toepassing van ABRO kan worden begonnen, wordt een aantal consequenties van de invoering van ABRO nader onderzocht. Ook wordt bezien of inkopende organisaties uit de latere tranches met eveneens hoge risicoprofielen voor de nationale veiligheid, ABRO eerder dan gepland gaan invoeren. Er wordt momenteel toegewerkt naar 1 januari 2026 als start van de eerste tranche.

In opdracht van het ministerie van BZK heeft het Centrum voor Informatiebeveiliging en Privacy (CIP) een Inkoopeisen Cybersecurity Overheid (ICO) tool, de zogenaamde ICO-wizard, laten ontwikkelen die overheidsorganisaties ondersteunt bij de inkoop van ICT-producten en -diensten. De eerdere verkenning naar een wettelijke verplichting voor het toepassen van de ICO-eisen is losgelaten, omdat hiervoor geen draagvlak bleek. In de ICO-eisen is echter een duidelijke koppeling opgenomen met de BIO. Via die route bestaat er alsnog een verplichtend karakter, dat met behulp van de ICO-wizard inzichtelijk wordt gemaakt.

Doel 2: Nederland heeft een sterke cybersecuritykennis- en innovatieketen.

II.2.1: Veilige cryptografie

Op de uitvoering van de Nationale Cryptostrategie (NCS) zijn er afgelopen jaar meerdere stappen gezet. Zo is er een NCS governance model overeengekomen dat waarborgt dat de Staat als één opdrachtgever naar de cryptobedrijven optreedt. Daarnaast heeft TNO Vector een rapport uitgebracht dat dient als basis voor een nieuw samenwerkingsverband tussen de Rijksoverheid, Defensie, de AIVD en zeven cryptobedrijven waarin leveringszekerheid van cryptoproducten wordt geborgd.[33] Betrokken partijen hebben een intentieverklaring ondertekend en gaan samen een plan voor het nieuwe samenwerkingsverband uitwerken.

Binnen de NCS zijn twee nieuwe producten opgeleverd. Het gaat om een lijnvercijferaar en een switch waardoor randapparatuur zoals beeldscherm, muis en toetsenbord aan werkstations van verschillende rubriceringsniveaus kan worden gekoppeld. Binnen de NCS wordt verder gewerkt aan andere producten zoals bepaald door de werkgroep Roadmap van de Rijksoverheid. Om de Departementaal Vertrouwelijk (DepV) evaluatie capaciteit te verhogen zijn pilots gestart om deze evaluaties uit te besteden. De pilots zullen naar verwachting leiden tot het volledig kunnen uitbesteden van DepV evaluaties, onder toezicht van het Nationaal Bureau Verbindingsveiligheid van de AIVD. Hierdoor zal de lijst van DepV geëvalueerde middelen in en na 2026 versneld uitgebreid worden.

In het kader van strategische autonomie heeft de overheid belang genomen in Sentyron (voorheen FoxCrypto). Hiermee wordt de leveringszekerheid van cryptomiddelen voor de Staat verder vergroot en wordt een belangrijke stap gezet in de doelstelling een stabiel en betrouwbaar ecosysteem te bouwen van cryptobedrijven die middelen ontwikkelen en leveren voor de beveiliging van Staatsgeheimen. De Kamer is hierover geïnformeerd.[34]

De twee thematische routekaarten die onder regie van dcypher (nu NCC-NL) werden uitgevoerd, cryptocommunicatie en geautomatiseerd kwetsbaarhedenonderzoek, zijn in 2024 gestopt. De routekaart cryptocommunicatie bleek onvoldoende gedragen te worden door het bedrijfsleven en kennisinstellingen. Zowel cryptocommunicatie als AVR blijven belangrijke onderzoeksthema's voor EZ, en zijn onderwerpen die terug zullen komen in initiatieven vanuit de Nationale Technologiestrategie Cybersecurity Technologieën.

II.2.2: Nationale samenwerking kennis- en innovatie-onderzoekssamenwerking

In het afgelopen jaar zijn verschillende workshops en sessies met andere departementen georganiseerd om de innovatiebehoeften vast te stellen. Deze sessies hebben onder andere geleid tot een concrete samenwerking tussen de ministeries van EZ en BZK, het NCSC en de AIVD voor de gezamenlijke financiering van een fundamenteel cybersecurity-innovatieonderzoek onder de Nationale Wetenschapsagenda programmalijn 2 (NWA lijn 2).

Het blijkt voor departementen en uitvoeringsorganisaties uitdagend om hun innovatiebehoeftes te duiden, zeker waar het gaat om lange-termijn behoeftes. Om deze reden is er door het ministerie van EZ gekozen om niet meer in te zetten op structurele inventarisatie van behoeftes, maar om departementen uit te nodigen om bij te dragen aan subsidieinstrumenten die door het ministerie van EZ worden

[32] Kamerstukken 2024-2025, 26643-1328
[33] Kamerstukken 2024-2025, 26643-1369
[34] Kamerstukken 2024-202530821-269

geïnitieerd. Het ministerie van EZ heeft voor dit proces een meerjarig plan opgezet dat andere departementen meer duidelijkheid geeft over de mogelijkheden en kaders, waardoor het gesprek gerichter gevoerd kan worden. Doordat het ministerie van EZ hierin het voortouw neemt wordt de drempel verlaagt voor andere departementen om aan te haken.

Het ministerie van EZ bouwt structureel aan ondersteuning van fundamenteel en toegepast onderzoek, praktijkgerichte samenwerking en innovatie bij mkb en start-ups. In 2025 zijn verschillende subsidies opengesteld. In samenwerking met NWO Regieorgaan SIA wordt in najaar 2025 een subsidie opengezet van minimaal €3,2 miljoen voor het opzetten van cybersecurity learning communities, waarin bedrijven en kennisinstellingen samenwerken om cybersecurity talent op te leiden. Daarnaast wordt via het Cyber Innovation Fund Nederland (CIF-NL) een subsidie instrument opengesteld ter waarde van €930.000 met focus op crypto-agility en AI-toepassingen, aan te vragen door innovatieve mkb. Via de NWA call Lijn 2 wordt aan onderzoeksinstellingen ruim €9 miljoen beschikbaar gesteld aan onderzoek naar digitaal weerbare ecosystemen.

Begin 2025 zijn twee Small Business Innovation Research (SBIR)-trajecten ter waarde van 3 miljoen uitgezet op het versterken van IT/OT security en autonome dreigingsinformatie. Tot medio 2024 is gewerkt via het Cybersecurity Innovatieprogramma CS4NL, waarmee ruim €20 miljoen is ingezet via diverse calls voor onderzoeksinstellingen en bedrijfsleven. Na afloop van CS4NL krijgt de samenwerking tussen het ministerie van EZ en de topsectoren vorm via de Actieagenda van de NTS Cybersecurity Technologie, die in het najaar van 2025 wordt gepresenteerd.

Het samenwerkingsplatform dcypher is in september 2025 samengevoegd met het Netherlands Cybersecurity Coordination Centre (NCC-NL). Daarmee krijgt NCC-NL, naast zijn Europese rol, ook een nationale taak als uitvoeringsplatform voor kennis- en innovatieontwikkeling op het gebied van cybersecurity. Deze stap is genomen om meer innovatie slagkracht te genereren, en nationale en internationale financiering beter op elkaar af te kunnen stemmen. De nieuwe NCC-NL organisatie is het centrale aanspreekpunt voor bedrijven, overheden en kennisinstellingen voor subsidiemogelijkheden in het cybersecurity innovatie domein, en ondersteunt de beleidsdoelen van het ministerie van EZ op gebied van talentontwikkeling, marktontwikkeling en publiek-private innovatie samenwerking.

Ook wordt de Cyber Innovation Hub (CIH) van Defensie verder versterkt en doordat het programma wordt doorontwikkeld naar een afdeling. De CIH streeft ernaar de reorganisatie medio 2026 te hebben afgerond. Een onderdeel van deze doorontwikkeling is een personele groei met onder andere een uitbreiding van cybersecurity specialisten. Het projectportfolio bestaat momenteel uit enige tientallen projecten met marktpartijen op het gebied van cyberveiligheid en digitale weerbaarheid. Naast testen en valideren in oefeningen, voert de CIH nu ook pilots uit waarbij innovaties in de praktijk worden beproefd.

II.2.3: Europese onderzoekssamenwerking en fondsen

Sinds de oprichting in 2023 heeft NCC-NL actief gecommuniceerd over Europese financieringsmogelijkheden en matchmaking gefaciliteerd voor consortia via het Europese netwerk. Zo ondersteunt het NCC-NL Nederlandse partijen bij het benutten van EU-subsidies en coördineert de Nederlandse inbreng richting het Europese Cybersecurity Competence Centrum (ECCC). Het NCC-NL onderhoudt bijvoorbeeld een ‘funding portal’ dat informatie over financieringsmogelijkheden geeft en publiceert regelmatig nieuwsbrieven.

Via het CIF-NL is een eerste subsidieregeling opengesteld, waarvoor €930.000 beschikbaar was. Deze subsidie is bedoeld om Nederlandse cybersecurity innovatieprojecten bij het mkb te stimuleren. In het najaar van 2025 volgt een nieuwe CIF-NL-call.

Het ECCC zal vanaf 2025 verantwoordelijkheid dragen voor de subsidieprogramma’s van Digital Europe en Horizon Europe voor specifiek de Cybersecurity werkprogramma’s met een looptijd van 2025-2027. Hierbij vormen belangrijke documenten, zoals de Strategische Agenda van het ECCC, de basis voor deze werkprogramma’s. Nederland heeft een sleutelrol gespeeld bij de totstandkoming van deze Strategische Agenda. De behoeftes worden meegenomen naar het ECCC om de Nederlandse prioritaire innovatiethema’s zo goed mogelijk te vertegenwoordigen bij de totstandkoming van de cybersecurity werkprogramma’s van Digital Europe en Horizon Europe.

Luchthavens proberen zich niet meer enkel te onderscheiden met service en aanbod.
Ook digitalisering en data zijn terreinen waarop ze
zich snel ontwikkelen. Zowel voor passagiers- als goederenverkeer betekent dit ook dat de afhankelijkheid en mogelijke kwetsbaarheid groeit.

Pijler III

Tegengaan van digitale dreigingen van staten en criminelen

Doel 1: Nederland heeft zicht op digitale dreigingen van staten en criminelen.

III.1.1: Zicht op statelijke actoren

De Inlichtingen- en Veiligheidsdiensten delen structureel producten zoals inlichtingenberichten, cyberadviezen en risicoanalyses met de verschillende afnemers. Daarnaast treden de diensten waar mogelijk naar buiten over cyberaanvallen. Zo hebben de AIVD en MIVD middels inlichtingenonderzoek in 2025 een nieuwe Russische cyberactor onderkend en publiekelijk geattribueerd. Aanleiding voor het onderzoek was een cyberaanval bij de politie in september 2024. De actor voert sinds tenminste 2024 cyberaanvallen uit tegen westerse overheden, bedrijven en andere organisaties. Zeer waarschijnlijk zijn ook Nederlandse organisaties getroffen, die hierover in een eerder stadium geïnformeerd zijn. Vanuit het belang van het verhogen van de weerbaarheid, wil het kabinet publieke en private organisaties in staat stellen om mitigerende maatregelen te kunnen treffen. De diensten publiceerden daarom een technisch rapport met de belangrijkste aspecten van de werkwijze van de actor. Met deze publieke attributie wordt invulling gegeven aan de motie Erkens om indien mogelijk vaker cyberaanvallen en bijbehorende technische werkwijzen openbaar te maken om het bewustzijn en de weerbaarheid in Nederland op het gebied van cyberveiligheid te vergroten.[35]

De Tijdelijke wet Cyberoperaties (de Tijdelijke wet), om de AIVD en de MIVD grotere slagvaardigheid bij deze onderzoeken te geven is op 1 juli 2024 in werking getreden en daarmee afgerond. De CTIVD heeft aangegeven vanwege huisvestingsproblemen en het daaruit volgende capaciteitsgebrek beperkt toezicht te kunnen houden op de Tijdelijke Wet, waardoor er momenteel maar beperkt toepassing gegeven is aan de Tijdelijke wet. Vanaf maart 2025 is de CTIVD verhuisd naar hun tijdelijke huisvestingslocatie en is de personeelswerving geïntensiveerd. Sindsdien zijn de gesprekken geïntensiveerd om zo snel mogelijk naar volledige toepassing van de Tijdelijke wet toe te groeien. Uitgangspunt is en blijft volledige toepassing van de Tijdelijke wet, onder het noodzakelijke onafhankelijke toezicht van de CTIVD, op een zo'n kort mogelijke termijn. Over de inwerkingtreding en gebruik van de Tijdelijke wet zijn meerdere Kamerbrieven gestuurd.[36]

III.1.2: Onderzoeks- en opsporingscapaciteit cybercriminelen

[35] Kamerstukken II 2024-25, nr.46
[36] Kamerstukken II 2023-24, nr. 43, 44

Bestrijding van cybercriminaliteit is een doorlopende actie van de politie en het Openbaar Ministerie (OM). Dit is geborgd in de doelstellingen van de Veiligheidsagenda. Over de voortgang is gerapporteerd via het Jaarverslag Politie en Kamerbrieven over de integrale aanpak cybercrime.[37] Hieronder een overzicht van lopende acties:

- In 2023 en 2024 vonden diverse strafrechtelijke interventies plaats, waaronder het neerhalen van botnets (Operation Endgame), aanpak van DDoS-for-hire diensten (Operation PowerOFF)[38], en het ontmantelen van onder andere Anyproxy (Operation Moonlander) en infostealers (Operation Magnus). Ook heeft er een veroordeling plaatsgevonden voor een bulletproof hoster. Daarnaast werd voor €41 miljoen aan cryptovaluta in beslag genomen en voerde een gezamenlijke operatie, gecoördineerd door Europol en Eurojust, acties uit tegen het pro-Russische cybercrimenetwerk NoName057(16) met steun van meerdere landen en organisaties.
- Eind juni 2024 zijn op Nederlands initiatief de eerste cybercriminelen op de Europese sanctielijst geplaatst. Daardoor mogen zij de EU niet meer inreizen, mogen bedrijven in de EU geen zaken meer met hen doen en worden hun tegoeden bevroren. Dat heeft onder andere gevolgen voor de Europese hosting sector, omdat er geen diensten geleverd mogen worden aan cybercriminelen die misbruik willen maken van de Europese digitale infrastructuur.
- In publiek-private samenwerking toont het project Melissa meerwaarde bij de aanpak van ransomware, onder meer bij het onderzoek Operation Endgame en een onderzoek naar een Counter Anti Virus dienst. Drie nieuwe convenantpartners sloten zich aan en Universiteit Leiden evalueerde het project, wat waardevolle inzichten opleverde voor toekomstige publiek-private samenwerkingen.
- Het Ministerie van JenV heeft samen met politie en OM een verkenning uitgevoerd naar oplossingen voor bad hosting en resellers. Een mogelijke maatregel is bijvoorbeeld de wettelijke verankering van het Know Your Customer-principe.
- Daarnaast is door de Politie en het OM geïnvesteerd in samenwerking met ACM, toezichthouder op de naleving van verplichtingen uit de Digitale Dienstenverordening. Verplichtingen waar hostingproviders aan dienen te voldoen zijn onder andere het inrichten van een meldmisbruikprocedure en respons op notice and take down (NTD)-verzoeken.
- Politie en OM werken samen met publieke en private partners voortdurend aan nieuwe verstoringsmaatregelen en daderpreventie interventies. Doelen zijn afschrikking, gedragsbeïnvloeding en verstoring van criminele processen. Voorbeelden hiervan zijn Hack_Right, re_B00TCMP, advertentiecampagnes en vroegsignalering.

Kennisuitwisseling en samenwerking

Binnen het OM wordt op dit moment gewerkt aan de realisatie van het opleidingsplan gericht op het versterken van de basiskennis op het gebied van cybercrime en gedigitaliseerde criminaliteit binnen de gehele organisatie.

In algemene zin wil het OM zaken sneller afdoen. Het OM onderzoekt op dit moment of dit ook mogelijk is voor cyberzaken. Dit bevindt zich in een onderzoeksfase. Hierbij wordt onder andere gekeken naar de haalbaarheid en de impact van een versnelde afdoening van cyberzaken.

III.1.3: Versterken diplomatiek netwerk

Naast de reguliere individuele kennisontwikkeling die door het jaar heen plaatsvindt, organiseert het Ministerie van Buitenlandse Zaken (BZ) verdiepingsdagen voor de diplomaten die belast zijn met de dossiers cyber- en economische veiligheid om zo de kennis en kunde van onze diplomatieke inzet nog verder te versterken. Tevens zorgt het ministerie van BZ ervoor dat cybersecurity meer verankerd wordt in de reguliere Nederlandse diplomatieke inzet en contacten, waardoor de bredere veiligheidssamenwerking kan worden bevorderd.

Het ministerie van BZ heeft zich in samenwerking met interdepartementale partners afgelopen jaar actief ingezet om gedeelde situationele beelden te bespreken in EU- en NAVO-verband. Het verspreiden van deze informatie heeft tot nieuwe gezamenlijke verklaringen en sancties geleid. Zo zijn er het afgelopen jaar onder andere sancties aangenomen tegen drie Russische individuen die in opdracht van de Russische militaire inlichtingendienst cyberaanvallen uitvoerde op de Estse overheid. Andere voorbeelden richten zich bijvoorbeeld op deelname aan conferenties, zoals de NATO Cyber Defence

[37] Jaarverslag Politie 2024 en Kamerstukken 2024-2025, 29911-474 en 26643-1357

[38] In Operation PowerOFF werden naast internationale takedowns ook waarschuwingsberichten, stopgesprekken en huiszoekingen ingezet. De politie zette honeypot-DDoS-sites op, gepromoot via Google Ads, die bezoekers directconfronteerden met een waarschuwingsbericht. Onderzoek van Cambridge University laat voorzichtige positieve gedragsveranderingen zien in DDoS-communities.

Pledge Conference en de NAVO Cyber Champions Top. Dit is een jaarlijkse door de NAVO ondersteunde bijeenkomst met NAVO landen en de Indo-Pacific Partners die dient als platform voor het uitwisselen van informatie en ervaringen. Het gezamenlijke inzicht en de samenwerking hierop zijn cruciaal om tijdig en effectief te kunnen handelen bij digitale dreigingen. Ook heeft Nederland rondom de publicatie omtrent de Russische cyberactor Laundry Bear gedetailleerde info met EU- en NAVO-partners gedeeld.

Het NCSC heeft in 2025 meerdere trajecten in het kader van het internationale cybercapaciteitsopbouwprogramma (CCB) afgerond. Dit programma versterkt de cyberweerbaarheid van partnerlanden, draagt bij aan een veiliger wereldwijd digitaal ecosysteem en bevordert strategische allianties. Het programma loopt tot eind 2025, met focus op de Westelijke Balkan, de Indo-Pacific, Oost-Europa en Zuidelijk Afrika. Voor 2026 e.v. wordt bezien op wat voor manier het programma kan worden voortgezet.

Doel 2: Nederland heeft grip op digitale dreigingen van staten en criminelen

III.2.1: Attributie en respons

Vanwege de Nederlandse capaciteit en expertise op het onderwerp vervult Nederland binnen de EU een voorbeeldfunctie, bijvoorbeeld bij de aanscherping van de EU cyber diplomacy toolbox.[39] Het is positief te zien dat mede door Nederlandse inzet bespreking van de cyberdreiging in EU-verband hoger op de agenda is gekomen, en dat de dreigingen in meer detail worden besproken. Kleinere gelegenheidscoalities spelen in die inzet een belangrijke rol. In mei 2025 publiceerde Tsjechië een attributie aan China met betrekking tot APT 31.[40] Mede door Nederlandse inzet werden door EU en NAVO steunverklaringen uitgebracht. Die boodschap werd ook door het ministerie van BZ afgegeven. In gemeenschappelijk verband met partners blijft het ministerie van BZ investeren in versterking van het responsinstrumentarium, zowel nationaal als via EU en NAVO. Dit gaat met kleine stapjes. Op nationaal niveau is het afgelopen jaar frequenter gebruik gemaakt van technical advisories.[41]

III.2.2: Effectieve cybercapaciteiten

Actieve cyberverdediging

Nederland moet zich in een dreigings- en conflictscenario actief digitaal kunnen verdedigen en in staat zijn om te interveniëren als de dreiging daarom vraagt. Ter versterking van het instrumentarium voor actieve cyberverdediging is onder coördinatie van de NCTV in 2025 een verkenning uitgevoerd naar de mogelijkheden van actieve cyberverdedigingsmaatregelen. Volgend op deze verkenning wordt vanaf eind 2025 door de NCTV, samen met betrokken departementen en diensten, geïnventariseerd hoe actieve cyberverdedigingsmaatregelen kunnen worden vormgegeven, waarna gestart zal worden met de implementatie van maatregelen.

Cybercapaciteiten Defensie

Defensie heeft de afgelopen jaren geïnvesteerd in haar cybercapaciteiten en blijft dat de komende jaren doen om permanent en proactief tegendruk te kunnen geven aan agressieve cyberactoren. De nieuwe Defensie Cyberstrategie, gepubliceerd op 3 oktober 2025, scherpt de cybertaken van Defensie aan en geeft op basis daarvan richting aan de wijze waarop Defensie haar cybercapaciteiten moet, wil en kan inzetten in de huidige omstandigheden.[42] Defensie heeft drie taken in het cyberdomein, namelijk:

1. Eigen cyberveiligheid in alle omstandigheden
2. Het uitvoeren van militaire cyberoperaties
3. Rol Defensie bij de Cyberweerbaarheid van het Koninkrijk en bondgenoten

Cybercapaciteiten die raken aan de NLCS zijn:

- Verbeteren van de cyberveiligheid van Defensiesystemen en –netwerken;
- verhogen van de bewustwording en het trainen van personeel op het gebied van cyberveiligheid;
- doorontwikkelen van capaciteiten voor militaire cyberoperaties om Nederland te beschermen en bondgenoten te steunen;

---

39 Cyber Blueprint - Draft Council Recommendation | Shaping Europe's digital future

40 MFA TSJ: Statement by the Government of the Czech Republic | Ministry of Foreign Affairs of the Czech Republic
NUKIB (NCSC TSJ) National Cyber and Information Security Agency - The Czech Government Has Publicly Attributed Cyberattacks to China: Actor APT31 Linked to the Chinese Ministry of State Security Has Targeted the Infrastructure of the Czech Ministry of Foreign Affairs
EU: Cyber: Statement by the High Representative on behalf of the European Union on malicious behaviour in cyberspace against Czechia - Consilium
NAVO: NATO - News: Statement of solidarity by the North Atlantic Council concerning the malicious cyber activities against the Czech Republic, 28-May.-2025

41 Zie bijvoorbeeld: State-Sponsored Russian Media Leverages en Publicatie van AIVD en MIVD over Laundry Bear | Nieuwsbericht | Nationaal Cyber Security Centrum

42 Kamerstukken 2024-2025, 26643-1422

- de samenwerking blijven zoeken met andere departementen, private partijen, kennisinstellingen en bondgenoten op het gebied van cyberveiligheid;
- uitbreiden bijstandsconstructies om andere organisaties te kunnen helpen bij grootschalige incidenten, onder andere via het Nationaal Respons Netwerk (NRN) en Multidisciplinaire Cyber Teams (MDCT's);
- werken aan een het beter benutten van de capaciteiten van cyberreservisten.

De personele gereedheid is verder vergroot via opleiding, training en oefening, waardoor de medewerkers van Defensie beter in staat zijn om te reageren op cyberdreigingen. In de Defensiebegroting 2023 is verwoord dat Defensie haar cybercapaciteit met onder meer 400 Fte's gaat versterken. Het is de bedoeling dat dit in vier jaar wordt gerealiseerd. In de periode 2024-2025 is dit volgens plan verlopen. Ook in de komende jaren zal Defensie blijven investeren in de personele en technische capaciteit. Verder draagt een bestaand IT-programma van Defensie zorg voor de benodigde technische hulpmiddelen.

Pilot Anti Phishing Shield

In de zomer van 2025 is een pilot gestart om de inzet van een Anti Phishing Shield (APS) te onderzoeken. Dit is een systeem dat internetgebruikers herleidt naar een waarschuwingspagina in het geval zij een malafide website dreigen te bezoeken. Het doel van de pilot is de effectiviteit van het APS in kaart brengen. De pilot wordt uitgevoerd door het Nationaal Cyber Security Center in samenwerking met KPN. De pilot sluit aan bij de maatregelen die KPN al neemt binnen de bestaande, versterkte beveiliging voor KPN-klanten. De pilot wordt De pilot wordt op een later moment mogelijk uitgebreid met meerdere partijen uit de telecomsector. De pilot duurt zes maanden. De pilot wordt tussentijds en na afloop geëvalueerd.

Doel 3: Staten houden zich aan het normatief kader voor verantwoordelijk statelijk gedrag in de digitale ruimte

III.3.1: Normatief kader

Het normatief kader voor verantwoordelijk statelijk gedrag is in 2015 opgesteld en in 2021 door alle VN-lidstaten bekrachtigd in de Algemene Vergadering van de VN. Belangrijk onderdeel van het kader is de afspraak dat internationaal recht van toepassing is op de digitale ruimte. Nederland zette zich samen met gelijkgezinde landen actief in via interventies in de VN Eerste Commissie en bilaterale gesprekken voor de totstandkoming van het Program of Action ter opvolging van de huidige Open Ended Working Group on Cyber (OEWG). Ook draagt Nederland bij aan de uitwerking en promotie van het Program of Action via een project met het EU Institute for Security Studies en heeft zitting in het steering board. De slotonderhandelingen van de OEWG hebben plaatsgevonden in juli 2025 waarin consensus is bereikt over het nieuwe VN-mechanisme op cyber.

III.3.2: Internet governance

In 2025 worden de afspraken die tijdens World Summit on the Information Society van de VN in 2005 zijn gemaakt in een zogeheten 'WSIS+20 review' herzien. Onderdeel hiervan is het bereiken van overeenstemming voor een nieuw mandaat van het jaarlijkse Internet Governance Forum (IGF) en behoud van het multi-stakeholdermodel voor internet governance. De inzet van onder andere Nederland heeft geresulteerd in de VN-brede erkenning dat internet governance mondiaal en multi-stakeholder moet blijven, met de volledige betrokkenheid van overheden, de private sector, maatschappelijk middenveld, internationale organisaties, academische en technische gemeenschappen en andere stakeholders. Met een brede Nederlandse delegatie van diverse stakeholdergroepen is deel genomen aan het IGF 2025 in Noorwegen. Dit jaar was naast de ministeries van EZ en BZ ook JenV aanwezig bij het IGF.

Onder Nederlands voorzitterschap heeft de Freedom Online Coalition (FOC) in oktober 2024 een Joint Statement uitgebracht over de interactie tussen mensenrechten en technische standaarden.[43]Tijdens de World Telecommunications Standardization Assembly (WTSA) van de International Telecommunications Union (ITU) in New Delhi, India, en in een bijdrage aan de Telecommunications Standardisation Advisory Group (TSAG) heeft Nederland samen met Tsjechië en andere Europese lidstaten, ook om acties gevraagd die tot doel hebben de impact van de door de ITU ontwikkelde standaarden op de bescherming van mensenrechten te evalueren. Hierbij is afgesproken dat de ITU voorafgaand aan de volgende vergadering van TSAG, begin 2026, rapporteert over welke acties de organisatie heeft ondernomen. Mede op basis van dit rapport wordt de Nederlandse inzet in de ITU verder vormgeven.

Na een succesvolle campagne, met steun van de Europese Commissie en lidstaten, is Nederland in oktober 2025 herkozen als één van de vijf vice-voorzitters van de Government Advisory Committee in ICANN, de non-profit organisatie belast met de wereldwijde coördinatie van het domeinnaamsysteem.

[43] Joint statement

Toenemende digitalisering biedt het onderwijs veel kansen, bijvoorbeeld door het aanbieden van online colleges en voor het ontsluiten van kennis. Tegelijkertijd brengt deze grotere afhankelijkheid van technologie risico's met zich mee. Verschillende universiteiten zijn de laatste jaren doelwit van ransomware geweest.

Pijler IV

Cybersecurity arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers

Doel 1: Burgers zijn goed beschermd tegen digitale risico's

IV.1.1: Voorlichtingscampagnes

Er lopen inmiddels drie verschillende publiekcampagnes, opgezet in afstemming tussen de ministeries Binnenlandse Zaken en Koninkrijksrelaties (BZK), EZ en JenV. De campagnes 'Laat je niet interneppen' (JenV & BZK); 'Dubbel beveiligd is dubbel zo veilig' (JenV); en 'Doe je updates' (EZ) zijn in 2025 voorgezet. Op basis van een campagne-effectonderzoek worden de campagnes geactualiseerd om de doelgroepen zo gericht mogelijk te bereiken.

Er is naast deze publiekscampagnes aandacht besteed aan het aanbieden van handelingsperspectieven om slachtofferschap te voorkomen. Van alle campagnes zijn toolkits beschikbaar die vrij kunnen worden gebruikt door andere partijen om de campagnes te ondersteunen, waaronder gemeenten.

Ook hebben de drie ministeries in de Overkoepelende Rijksbrede Cybercrime Aanpak (ORCA) periodiek overleg om de campagnes op elkaar af te stemmen en zullen ze deze samenwerking voortzetten tot (tenminste) 2030.

Sinds 2020 zijn in het kader van de City Deal Lokale Weerbaarheid Cybercrime innovatieve projecten ontwikkeld voor de jeugd, het midden- en kleinbedrijf, senioren en laaggeletterden. De City Deal loopt eind 2025 af, daarom zijn de interventies waar mogelijk ondergebracht bij partners van de City Deal. Het doel hiervan is om alle succesvolle interventies blijvend beschikbaar te maken en verder te verspreiden.[44]

Daarnaast wordt het jaarlijkse bewustzijnsonderzoek Alert Online uitgevoerd.[45] Hier worden kennis, houding en gedrag op het gebied van digitale weerbaarheid geanalyseerd. Over de jaren heen is het beeld wat betreft cybercrime is stabiel: zo blijft phishing de meest voorkomende vorm van cybercrime. De resultaten van het onderzoek worden traditioneel tijdens de kick of van de cybersecurity maand oktober gepresenteerd.

IV.1.2: Beveiligingsadvies burgers

Op de publiek-private website veiliginternetten.nl vinden circa 1.5 miljoen burgers per jaar informatie en advies over hoe ze zich online kunnen beschermen. Veiliginternetten.nl is ook dé centrale plek waar de cybersecurity publiekscampagnes van de overheid naartoe leiden. Op basis van onderzoek hoe de website meer kan voldoen aan de gebruiksvriendelijkheid voor

[44] Voor een overzicht van de interventies, zie City Deal Lokale Weerbaarheid Cybercrime
[45] Cybersecurity onderzoek Alert Online 2025

burgers heeft de website in 2024 een nieuwe *look & feel* gekregen.

IV.1.3: Betrouwbaarheid digitale overheidsvoorzieningen

De overheid zet in op een uniforme domeinnaamextensie, zodat burgers gemakkelijk kunnen herkennen of zij online echt te maken hebben met een overheid of niet. Dit helpt online fraude als phishing tegen te gaan. Op dit moment loopt een impactanalyse naar de haalbaarheid en betaalbaarheid van invoering van een uniforme domeinnaamextensie zoals overheid.nl of gov.nl voor overheidswebsites, te beginnen binnen een beperkte scope. Afronding van het onderzoek wordt op zijn vroegst eind 2025 verwacht. Deze actie is onderdeel geworden van het Nationaal Actieplan Webbeleid dat op 1 juli 2025 is gedeeld met de Tweede Kamer. [46]

Het Register Internetdomeinen Overheid is eind 2023 in een eerste versie live gegaan. In dit register kunnen burgers bij twijfel checken of een website of emailadres bij een overheidsorganisatie hoort. Op dit moment zijn de websites van de Rijksoverheid vindbaar in het register. Medeoverheden zijn in de gelegenheid om aan te sluiten, momenteel loopt dit proces.

Doel 2: Burgers reageren snel en adequaat op cyberincidenten

IV.2.1: Melding of aangifte doen van cybercrime fenomenen

De online aangiftemogelijkheid voor ransomware voor burgers ontwikkeld door de politie is sinds begin 2024 live. Naar verwachting is het later dit jaar mogelijk voor bedrijven om gebruik te maken van de online aangiftemogelijkheid voor ransomware.

Doel 3: Leerlingen krijgen onderwijs in digitale vaardigheden gericht op veiligheid

IV.3.1: Curriculum

Stichting Leerplan Ontwikkeling (SLO) heeft in 2025 de kerndoelen voor basisvaardigheden voor het primair onderwijs en het voortgezet onderwijs aangescherpt en in een wetsvoorstel aan de Tweede Kamer voorgelegd. Digitale vaardigheden maken onderdeel uit van deze kerndoelen. In juni 2025 is een vooronderzoek naar digitale geletterdheid afgerond en een adviesrapport gepubliceerd.[47] Het voornemen is de wetswijziging kerndoelen in het najaar van 2025 aan de Kamer te zenden ter behandeling. De implementatie wordt verwacht in 2027.

Daarnaast is het schooljaar 2024-2025 het voorlaatste jaar dat scholen de Subsidie Verbetering Basisvaardigheden kunnen aanvragen, in het kader van het Masterplan Basisvaardigheden. Het Expertisepunt Digitale Geletterdheid wordt nu doorontwikkeld om beter aan te sluiten bij de behoeften van onderwijsprofessionals

Doel 4: De Nederlandse arbeidsmarkt kan voldoen aan de toenemende vraag naar cybersecurity-experts

IV.4.1: Cybersecurity arbeidsmarkt

Het ministerie van OCW investeert structureel in hbo-opleidingen in de bètatechniek, waar cybersecurityopleidingen ook onderdeel van zijn. Een tussenevaluatie vindt plaats in het najaar 2025.

OCW werkt ook aan de doorontwikkeling van het Leven-Lang-Ontwikkelen-beleid (LLO), met als doel om- en bijscholingstrajecten in samenwerking met de beroepspraktijk kunnen aan te bieden. Er is een verkenning gestart naar de mogelijkheid en wenselijkheid van het wettelijk verankeren van de LLO-opdracht voor publieke instellingen, de resultaten hiervan worden in het najaar van 2025 verwacht. De subsidies van de LLO-Katalysator (een groeifondsproject) zijn gericht op de grondstoffen- en energietransitie. Voor zover bekend zijn er geen aanvragen ingediend voor cybersecurity. De subsidieronde loopt tot 2026, hierna wordt de subsidie mogelijk verbreed naar andere sectoren.

Er worden binnen het sectorplan Bèta (Informatica) verschillende posities voor onderzoek en onderwijs met een focus op cybersecurity gefinancierd. De eerste tussentijdse evaluatie geeft een positieve indruk. Onder andere het Twente

[46] Kamerstuk, 2024-2025, 2025-0000351913
[47] Adviesrapport vooronderzoek digitale geletterdheid

University Centre for Cyber Security Research heeft met de gelden een stevige impuls gekregen.

De acties uit de Onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity, opgeleverd in 2024, hebben in 2025 vervolg gekregen: [48]

- De informatie die is voortgekomen uit het onderzoek zal online worden ontsloten en worden bijgehouden in de vorm van netwerkkaarten en dashboards. Eén van de acties is om het bestaande arbeidsmarktdashboard ICT uit te breiden met inzichten in de (regionale) tekorten van cybersecurity specialisten, zodat zij gerichter kunnen worden ingezet.
- Om praktijkgericht onderzoek naar het versterken van de samenwerking tussen kennisinstellingen en het bedrijfsleven te kunnen uitvoeren wordt een NWO subsidiecall uitgezet. Dit moet leiden tot verbeterde aansluiting tussen de vraag van de arbeidsmarkt en het aanbod van het onderwijs, het opleiden van studenten via onderwijsinstellingen en via het bedrijfsleven en het betrekken van de arbeidsmarkt bij onderwijsvorming. Dit instrument wordt geopend in het najaar van 2025, en kent een budget van €2.5 miljoen.
- Binnen de Human Capital Agenda ICT zijn er door de taskforce HCA Cyber vier werktafels geformuleerd: carrièrepaden, coördinatie van vraag en aanbod, beroep en aantrekkelijkheid, en regionale en sectorale samenwerking. In deze werktafels zijn partijen uit onderwijs, overheid, onderzoek en arbeidsmarkt vertegenwoordigd. Tevens heeft in augustus 2025 de Nationale Cyber Security Summer School (NCS3) plaats gevonden, onder organisatie van dcypher (nu NCC-NL). In zomer 2026 wordt een nieuwe editie van de NCS gehouden.
- Daarnaast wordt in het najaar 2025 door EZ in samenwerking met NWO Regieorgaan SIA een subsidie instrument opengezet van minimaal €3,2 miljoen. Deze call biedt het winnende consortium financiële middelen om cybersecurity learning communities op te zetten waarin bedrijven en kennisinstellingen samenwerken om cybersecurity talent op te leiden.

[48] Onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity

Uitgave
Nationaal Coördinator
Terrorismebestrijding
en Veiligheid (NCTV)
Postbus 20301, 2500 EH Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5050

Meer informatie
www.nctv.nl
info@nctv.minjenv.nl

November 2025