Voortgangsrapportage 2026 Nederlandse Cybersecuritystrategie

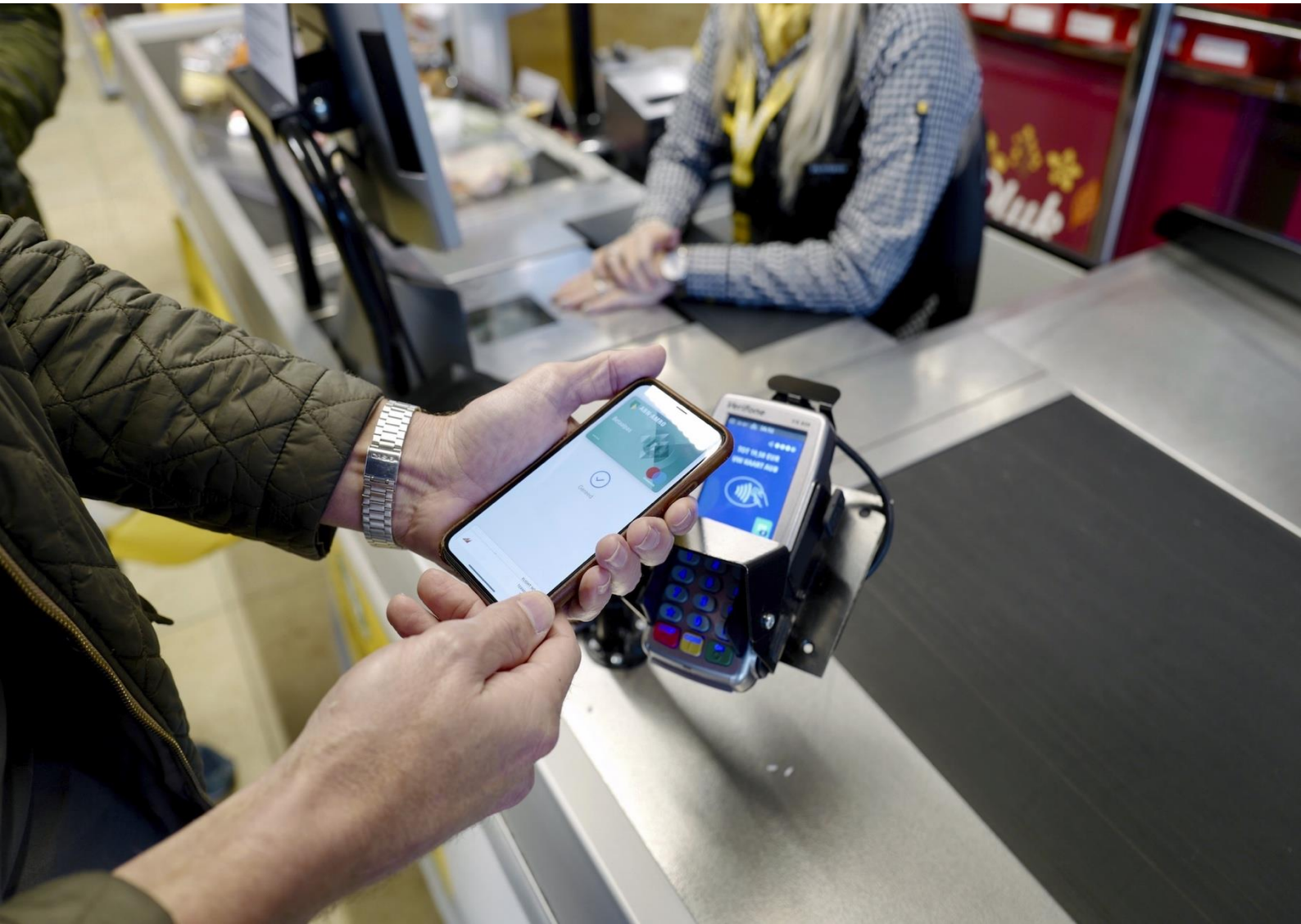


Foto omslag:

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 2026 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 Cyberbeveiligingswet en het CSIRT-stelsel *8*
De vernieuwde NCSC organisatie *8*
Cyclotron *8*
Caribisch deel van het Koninkrijk *8*

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

I.1.3: Uitbreiden schakelorganisaties binnen het CWN 9

I.1.4: Nationaal Detectie Netwerk 10

I.1.5: 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 kritieke infrastructuur 10

Meldplicht *10**Fout! Bladwijzer niet gedefinieerd.***
Samenhang sectorspecifieke wetgeving *10*
Voorlichtingscampagne Rijksoverheid *110*
Versterking aanpak Vitaal *110*

I.2.2: Digitale weerbaarheid MKB en bedrijfsleven 12

I.2.3: Digitale weerbaarheid onderwijs 12

I.2.4: Digitale weerbaarheid zorginstellingen 13

I.2.5: Digitale weerbaarheid sectoren infrastructuur en waterstaat 13

I.2.6: Digitale weerbaarheid Rijksoverheid 14

Versterking Security Operations Center (SOC)-stelsel Rijk (VSSR) *14*
Red Teaming bij de Rijksoverheid *14*
Ransomware ***Fout! Bladwijzer niet gedefinieerd.***
Verplichte basisopleiding digitale weerbaarheid *14*

I.2.7: Digitale weerbaarheid overheid 14

Digitale weerbaarheid gemeenten 14

Baseline Informatiebeveiliging Overheid (BIO) 14

I.2.8: Digitale weerbaarheid sectoren met operationele technologie- en procesautomatiseringssystemen 15

I.2.9: Zicht op digitale weerbaarheid van overheid en bedrijfsleven 15

Doel 3: Organisaties reageren, herstellen en leren snel en adequaat op en van cyberincidenten en –crises. 16

I.3.1: Incident- en crisispreparatie en I.3.2 oefenen 16

Pijler II
Veilige en innovatie digitale producten en diensten **18**

Doel 1: Digitale producten en diensten zijn veiliger 18

II.1.1: Europese wetgeving voor digitale producten en diensten 18

II.1.2: Toezicht en handhaving op digitale producten en diensten 18

II.1.3: Certificering en standaarden 19

II.1.4: Algemene beveiligingseisen rijksoverheid (ABRO) en overheidsinkoopbeleid 19

Doel 2: Nederland heeft een sterke cybersecuritykennis- en innovatieketen. 20

II.2.1: Veilige cryptografie 20

II.2.2: Nationale samenwerking kennis- en innovatie-onderzoekssamenwerking 21

II.2.3: Europese onderzoekssamenwerking en fondsen 21

Pijler III
Tegengaan van digitale dreigingen van staten en criminelen **23**

Doel 1: Nederland heeft zicht op digitale dreigingen van staten en criminelen. 23

III.1.1: Zicht op statelijke actoren 23

III.1.2: Onderzoeks- en opsporingscapaciteit cybercriminelen 23
III.1.3: Versterken diplomatiek netwerk 24

Doel 2: Nederland heeft grip op digitale dreigingen van staten en criminelen 25

III.2.1: Attributie en respons 25
III.2.2: Defensieve en offensieve cybercapaciteiten 25

Doel 3: Staten houden zich aan het normatief kader voor verantwoordelijk statelijk gedrag in de digitale ruimte 26

III.3.1: Normatief kader 26
III.3.2: Internet governance 26

Pijler IV
Cybersecurity arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers 30

Doel 1: Burgers zijn goed beschermd tegen digitale risico's 30

IV.1.1: Voorlichtingscampagnes 30
IV.1.2: Beveiligingsadvies burgers 30
IV.1.3: Betrouwbaarheid digitale overheidsvoorzieningen 31

Doel 2: Burgers reageren snel en adequaat op cyberincidenten 31

IV.2.1: Melding of aangifte doen van cybercrime fenomenen 31

Doel 3: Leerlingen krijgen onderwijs in digitale vaardigheden gericht op veiligheid 31

IV.3.1: Curriculum 31

Doel 4: De Nederlandse arbeidsmarkt kan voldoen aan de toenemende vraag naar cybersecurity-experts 31

IV.4.1: Cybersecurity arbeidsmarkt 31

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 Cyberbeveiligingswet en het CSIRT-stelsel

Afgelopen jaar zijn er grote stappen gezet in de herziening van het cybersecuritystelsel. Op 15 augustus 2026 trad de Cyberbeveiligingswet (Cbw) in werking. De Cbw is de Nederlandse uitwerking van de Europese NIS2-richtlijn, die zorgt voor een hoog, gelijkwaardig niveau van cyberbeveiliging binnen de EU. De Cbw stelt eisen aan de digitale weerbaarheid van ruim 8.000 organisaties die essentiële of belangrijke diensten verlenen.

Onder de Cbw en de NIS2-richtlijn moeten lidstaten Computer Security Incident Response Teams (CSIRT's) aanwijzen. Deze teams waarschuwen voor cyberrisico's en ondersteunen bij incidenten. Nederland richt dit CSIRT-stelsel in volgens het principe 'centraal, tenzij', conform het rapport "Een beleidskader voor het herinrichten van het stelsel met nationale en sectorale CSIRT's in Nederland".[1] Dit betekent dat het NCSC fungeert als de centrale, nationale CSIRT, aangevuld met erkende sectorale CSIRT's voor specifieke sectoren.

De vernieuwde NCSC organisatie

Per 1 januari 2026 zijn het Digital Trust Center (DTC) en het Cyber Security Incident Response Team for Digital Service Providers (CSIRT-DSP) geïntegreerd met het Nationaal Cyber Security Centrum (NCSC) tot één nationale cybersecurity-organisatie. Door de integratie van het DTC en het CSIRT-DSP met het NCSC, richt de dienstverlening van het NCSC zich niet langer alleen op de Rijksoverheid en kritieke sectoren, maar ook op het niet-kritieke bedrijfsleven inclusief het midden en klein bedrijf (mkb). Hiermee ontstaat er één duidelijk aanspreekpunt, snelle en gerichte informatiedeling, en toegang tot een uitgebreid netwerk van cyberexperts. Deze integratie is van groot belang om versnippering van taken en verantwoordelijkheden binnen het cybersecuritystelsel te verkleinen, de schaarse cybersecurity-expertise zo efficiënt mogelijk in te zetten, en hierdoor de cyberweerbaarheid in Nederland te vergroten.

Cyclotron

De huidige dreiging vraagt om vergaande publiek-private samenwerking. Het Programma Cyclotron verbindt publiek-private

[1] CSIRT-Stelsel - Een beleidskader voor het herinrichten van het stelsel met een nationale en sectorale CSIRT's in Nederland | Rijksoverheid.nl

partijen met een hoge cybersecurity volwassenheid en realiseert de uitwisseling van informatie over cyberdreiging en incidenten tussen deze partijen. Per 1 juli 2026 is de uitvoering van Cyclotron volledig ondergebracht bij het NCSC. Ter voorbereiding op deze transitie heeft het programmateam de aanbevelingen uit de Gateway Review van 2025[2] opgepakt en grotendeels geïmplementeerd. In deze review werd geconstateerd dat de samenwerking meer inhoudelijke sturing behoefde en dat de resultaten beter meetbaar en inzichtelijk moesten worden gemaakt. Daarnaast werd benadrukt dat publiek-private sturing op de samenwerking van belang is. Daarom zijn naar aanleiding van de review diverse verbetermaatregelen doorgevoerd. Zo is de governancestructuur herzien, waarbij de voormalige Governance Board en Stuurgroep zijn samengevoegd tot één publiek-private Regieraad. Deze Regieraad heeft als doel de strategische aansturing en besluitvorming binnen het programma te versterken. Daarnaast heeft het programmateam een dashboard ontwikkeld waarmee de voortgang en resultaten van het programma beter kunnen worden gemonitord en gerapporteerd.

Caribisch deel van het Koninkrijk

Ook is afgelopen rapportageperiode de samenwerking met het Caribisch deel van het Koninkrijk op het gebied van cybersecurity versterkt. Zo heeft er een onderzoek plaatsgevonden naar de aansluiting van het bestaande CSIRT-stelsel. Daarnaast is het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) gestart met een traject om samen met het Caribisch deel van het Koninkrijk invulling te geven aan de motie van de leden El Boujdaini en Kathmann om tot een concreet plan of een routekaart te komen voor een cybersecuritystelsel.

Verder heeft in april 2026 het NCSC op Aruba in het kader van Opleiden, Trainen, en Oefenen, lokale experts van verschillende publieke en private organisaties opgeleid in de methodiek van het MASKeR traject.[3] Deze experts zijn direct ingezet als begeleider van verschillende groepen tijdens verschillende MASKeR sessies op het eiland.

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

Het Cyberweerbaarheidsnetwerk (CWN), als opvolger van het LDS, is een publiek-private samenwerking binnen het Koninkrijk der Nederlanden, gericht op het samenbrengen van overheid en bedrijfsleven om de digitale weerbaarheid te vergroten en incidenten aan te pakken. In deze rapportageperiode zijn concrete stappen gezet in de opbouw van het CWN. Met de publicatie van het CWN Bouwplan is de Toekomstvisie Cyberweerbaarheidsnetwerk vertaald naar een uitvoeringsagenda welke nu actief wordt gerealiseerd.[4]

Er zijn vier werkgroepen bestaande uit publieke en private organisaties (netwerkpartners) die het CWN Bouwplan nu tot uitvoering brengen. Het gaat hierbij om de volgende vier CWN-functies: Informatiedeling (waaronder ook 'Doelwit en Slachtoffer Notificatie'), Incidentafhandeling, Kennisuitwisseling en 'Opleiden, Trainen, Oefenen'. Het netwerk omvat inmiddels 106 deelnemende organisaties. Daarnaast loopt er een bredere inventarisatie van overige potentiële netwerkpartners en is er een wervingsplan vormgegeven. Het NCSC Community platform is geïdentificeerd als centraal samenwerkingsplatform voor het netwerk en wordt met de werkgroepen verder doorontwikkeld om kennisuitwisseling te faciliteren binnen het CWN.

Omdat het cybersecuritylandschap mede door de komst van de nieuwe Cbw is veranderd en dit niet eerder is gevisualiseerd, heeft de NCTV samen met de wetenschap, publieke en private partners het Nederlandse cybersecurity landschap in kaart gebracht. Hierbij was het doel om een gedeeld begrip van het landschap en helderheid over rollen en relaties te creëren. Daarnaast ondersteunt de visualisatie in verdere beleidsontwikkeling, toezicht en uitvoering. De focus lag bij de ontwikkeling op pijlers één (versterken van digitale weerbaarheid) en drie (tegengaan van cyberdreigingen) van de NLCS. De visualisaties worden dit jaar nog opgeleverd.

I.1.3: Uitbreiden schakelorganisaties binnen het CWN

De uitbreiding van schakelorganisaties[5] binnen het CWN is noodzakelijk om digitale dreigingsinformatie sneller en gerichter door te geleiden naar het bedrijfsleven en organisaties. In het Caribisch gebied ondersteunt het NCSC het opzetten van een lokale ISAC op Bonaire, door het delen van kennis, ervaringen en kennisproducten over het opzetten van een ISAC.

[2] Gateway Reviewrapport Programma Cyclotron | Rijksoverheid.nl
[3] MASKeR methode | Versterken weerbaarheid
[4] Bouwplan Cyberweerbaarheidsnetwerk | NCSC
[5] Schakelorganisaties zijn 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.

I.1.4: Nationaal Detectie Netwerk (NDN)

Publiek-private informatiedeling is cruciaal om cyberdreigingen in een vroeg stadium te analyseren en te ontdekken. Daarom zijn er het afgelopen jaar op dit gebied stappen gezet. Via het Nationaal Detectie Netwerk (NDN) werken overheidsorganisaties en bedrijven samen om geavanceerde digitale aanvallen eerder en beter waar te nemen. Hiermee wordt kennisdeling tussen aangesloten partijen versterkt. Daarnaast is het momenteel voor de volledige Cbw-doelgroep mogelijk om dreigingsinformatie in te zien in een open standaard via MijnNCSC.

I.1.5: Slachtoffernotificatie

Dankzij een wijziging in 2025 van het Besluit politiegegevens[6] kan de politie nu structureel informatie delen met het NCSC voor deze slachtoffer- en doelwitnotificaties. Om tot een internationaal systeem te komen van slachtoffernotificatie heeft de Nederlandse politie vanuit de EU via het EU Internal Security Fund (ISF) een bijdrage ontvangen om 'Check je hack', 'No More Leaks' en het nog te ontwikkelen 'protect your password' ook in andere landen te introduceren, zodat steeds meer landen en haar burgers kunnen worden gewaarschuwd voor diefstal en handel van hun gebruikersgegevens.

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 kritieke infrastructuur

Voor de digitale veiligheid van Nederland is de inzet van alle bedrijven en organisaties noodzakelijk, niet alleen vanwege de continuïteit van de eigen dienstverlening maar ook vanwege de mogelijk bredere negatieve effecten voor afnemers, toeleveranciers of anderen. De Cyberbeveiligingsweg (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke), die respectievelijk de NIS2-richtlijn en de CER-richtlijn van de EU implementeren, zijn op 15 augustus 2026[7] in werking zijn getreden. Ook de onderliggende amvb's, het Cyberbeveiligingsbesluit en het Besluit weerbaarheid kritieke entiteiten zijn sinds die dag van kracht, net als de onderliggende ministeriële regelingen van de verschillende ministeries. Deze wetgeving vormt een belangrijk juridisch fundament voor het versterken van de digitale en fysieke weerbaarheid tegen de toenemende dreigingen. Hiermee is actie I.2.1.1 van de NLCS gerealiseerd.

De cyberbeveiliging en fysieke bescherming van onze kritieke infrastructuur zijn onlosmakelijk met elkaar verbonden en dienen integraal benaderd te worden. Het uitgangspunt bij implementatie van de NIS2-richtlijn en de CER-richtlijn is dat beide wetten zoveel mogelijk op elkaar aansluiten. Daarom is aangestuurd op uniformiteit en complementariteit bij bijvoorbeeld de verplichtingen onder de zorgplicht en de meldplicht. Kritieke entiteiten die zijn aangewezen onder de Wwke zijn van rechtswege essentiële entiteiten onder de Cbw en zullen daarom ook onder de Cbw maatregelen moeten nemen ter bescherming van hun netwerk- en informatiesystemen.

Om te voorkomen dat entiteiten met (dubbele) administratieve lasten te maken krijgen die verder gaan dan nodig is om de doelstellingen van de Wwke en de Cbw te verwezenlijken, werken de bevoegde autoriteiten onder de Wwke en de Cbw nauw samen en wisselen noodzakelijke informatie uit. Om deze samenwerking te bevorderen is er een samenwerkingsprotocol opgesteld met afspraken die de toezichthouders hebben gemaakt over onder meer de afstemming van toezichtactiviteiten, de uitwisseling van informatie en de overige onderlinge samenwerking.[8]

De samenhang tussen het fysieke en digitale domein komt ook naar voren bij het uitvoeren van een risicobeoordeling door de kritieke entiteiten, een belangrijk onderdeel van de Wwke. Op basis van deze risicobeoordelingen moeten kritieke entiteiten maatregelen nemen om de weerbaarheid van hun organisatie te verhogen. In beginsel is deze risicobeoordeling vormvrij en kan deze aansluiten op documenten waarin andere risicoanalyses zijn opgenomen, zoals die voor de Cbw. Dit zorgt niet alleen voor meer samenhang tussen de fysieke beschermings- en cyberbeveiligingsmaatregelen, maar kan ook dubbele lasten voorkomen bij entiteiten.

Meldplicht

Een onderdeel van de Cbw en Wwke is het inrichten van een meldportaal waarmee meldingen laagdrempelig en gelijktijdig kunnen worden gedaan. Door het NCSC is één centraal meldportaal ingericht op mijn.ncsc.nl. Hierdoor is het voor entiteiten mogelijk om in één portaal de op grond van de Cbw en de Wwke verplichte melding van significante incidenten te doen bij het betreffende CSIRT en de bevoegde toezichthouder. Verder is het centraal meldportaal van het NCSC zo ingericht, dat ook meldingen onder de Digital Operational Resilience Act (DORA) en de Network Code on Cybersecurity (NCCS) in dit meldportaal kunnen worden gedaan. Tot slot is het uitgangspunt dat het

[6] wetten.nl - Regeling - Besluit politiegegevens - BWBR0023086
[7] Staatsblad 2026, 188 | Overheid.nl > Officiële bekendmakingen Staatsblad 2026, 188 | Overheid.nl > Officiële bekendmakingen
[8] https://zoek.officielebekendmakingen.nl/stcrt-2026-29343.html

meldportaal op een lastenluwe manier is ingericht en dat waar mogelijk de meldcriteria op elkaar zijn afgestemd. Dit alles draagt eraan bij dat de lasten voor bedrijven zoveel mogelijk worden beperkt. Hiermee is actie I.2.1.5 van het NLCS-actieplan gerealiseerd.

Voor het maken van een verplichte melding van een significant incident onder de Cbw gelden drempelwaarden. Iedere vakminister heeft voor de sectoren waar zij verantwoordelijk voor zijn drempelwaarden vastgesteld. Op deze manier sluiten de drempelwaarden goed aan bij het specifieke karakter van de sector. Deze drempelwaarden zijn tot stand gekomen in overleg met de sector en de toezichthoudende instanties.

Samenhang sectorspecifieke wetgeving

De DORA en de NCCS zijn sectorspecifieke wetgeving om de digitale weerbaarheid te verhogen van respectievelijk de financiële sector en de elektriciteitssector. Om de lasten voor bedrijven zoveel mogelijk te beperken, is de NIS2-richtlijn in nauwe samenhang geïmplementeerd met deze Europese verordeningen. Voor de onder de DORA vallende entiteiten en onderwerpen geldt de DORA als lex specialis ten opzichte van de NIS2-richtlijn. Dit betekent dat, voor zover de DORA specifieke regels bevat over dezelfde onderwerpen, deze regels voorgaan boven de overeenkomstige bepalingen van de NIS2-richtlijn.

Zo regelt de DORA dat de daarin bedoelde toezichthoudende autoriteiten kunnen samenwerken met instanties uit de Cbw en met hen informatie kunnen uitwisselen. In de Cbw wordt andersom geregeld dat de in deze wet bedoelde instanties, zoals CSIRT's met de in de DORA bedoelde toezichthoudende instanties samenwerken en aan hen informatie kunnen verstrekken.

Voorlichtingscampagne Rijksoverheid

Voorafgaand aan de inwerkingtreding van de Cbw is gedurende langere tijd actief gecommuniceerd om organisaties te stimuleren zich hierop voor te bereiden. Ter ondersteuning van de implementatie zijn diverse praktische hulpmiddelen, handreikingen en kennisproducten ontwikkeld.[9] Zo heeft de Rijksinspectie Digitale Infrastructuur (RDI) onder meer de NIS2-Zelfevaluatietool en de NIS2-Quickscan beschikbaar gesteld.[10] Daarnaast hebben de Auditdienst Rijk (ADR) en NOREA, in opdracht van het Ministerie van BZK, het NIS2 Control Framework ontwikkeld.[11] Dit biedt organisaties en IT-auditors een praktisch hulpmiddel om inzicht te krijgen in de maatregelen die nodig zijn om te voldoen aan de zorgplicht uit de Cbw, het Cyberbeveiligingsbesluit (Cbb) en andere mogelijk relevante sectorale normen en regelgeving, zoals de BIO2 en de DORA.

Daarnaast hebben de NCTV en het NCSC een brede campagne uitgevoerd om organisaties en overheden actief te informeren. Vakdepartementen hebben deze communicatie aangevuld met een sectorspecifieke aanpak, in nauwe samenwerking met brancheorganisaties, die een belangrijke rol spelen in het breed verspreiden van informatie binnen de sectoren. Sinds november 2025 organiseren de NCTV en het NCSC daarnaast webinars waarin organisaties uitleg krijgen over de beschikbare hulptools en de praktische uitvoering van de nieuwe verplichtingen. Na de inwerkingtreding van de Cbw is met deze campagne doorgegaan, om organisaties zo goed als mogelijk te ondersteunen. De communicatie is daarbij niet alleen gericht op bewustwording, maar vooral op het ondersteunen van organisaties bij de naleving en praktische uitvoering van de Cbw.

Versterking aanpak Vitaal

De Aanpak Vitaal vormde jarenlang het beleidskader voor het beschermen van vitale processen in Nederland. Met de inwerkingtreding van de Wwke heeft er een overgang plaatsgevonden van de beleidsmatige Aanpak Vitaal naar een stelsel met een stevige juridische basis. Onder deze Aanpak vitaal vond er al een nauwe samenwerking plaats tussen publieke en private partijen ten behoeve van de bescherming van de kritieke infrastructuur. Ook werden er onder deze aanpak aanbieders van kritieke infrastructuur aangewezen door verantwoordelijke ministeries en namen deze aanbieders maatregelen om de risico's voor hun kritieke infrastructuur te mitigeren.

De Aanpak Vitaal wordt grotendeels vervangen met de inwerkingtreding van de Wwke, maar de doelstellingen uit de Aanpak vitaal en de wet sluiten inhoudelijk op elkaar aan. Voor de entiteiten die onder de wet vallen zal de Aanpak vitaal overgaan naar het nieuwe wettelijke kader. De instrumenten uit de Aanpak vitaal zijn zo doorontwikkeld om aan te sluiten bij de verplichtingen uit de wet. Zo is de nieuwe risicobeoordeling, die verantwoordelijke vakministers moeten uitvoeren onder de wet, een doorontwikkeling van de huidige vitaal beoordeling en weerbaarheidsanalyse uit de Aanpak vitaal.

Het veranderende (cyber)dreigingslandschap vraagt om een integrale, adaptieve en richtinggevende aanpak om risico's binnen onze kritieke infrastructuur het hoofd te blijven bieden. De risicobeoordelingen die de vakdepartementen én de kritieke entiteiten onder de Wwke moeten uitvoeren vormen daarbij een belangrijk fundament. In deze risicobeoordelingen worden de relevante dreigingen die de dienstverlening kunnen verstoren afgewogen, waaronder ook nieuw optredende dreigingen. De risicobeoordelingen worden periodiek uitgevoerd, maar dienen eerder te worden herzien indien hiertoe aanleiding bestaat, bijvoorbeeld bij een veranderd dreigingsbeeld.

De Rijksoverheid ondersteunt kritieke entiteiten bij het verhogen van hun weerbaarheid. Die ondersteuning kan bestaan uit

[9] https://www.ncsc.nl/cyberbeveiligingswet-nis2/zorgplicht
[10] NIS2 Zelfevaluatie NL en NIS2 Quickscan.
[11] Cbw (NIS2) Control Framework | Auditdienst Rijk.

informatie-uitwisseling, bijvoorbeeld over nieuwe relevante dreigingen, en het bieden van methodieken en weerbaarheid-verhogende instrumenten. In aanloop naar de inwerkingtreding van de Wwke is er actief ingezet op communicatie richting organisaties die onder de wet zullen vallen. Het doel hiervan is om organisaties in een vroegtijdig stadium bewust te maken van de komst van de Wwke, de mogelijke aanwijzing als kritieke entiteit en wettelijke verplichtingen die daaruit voortvloeien, zoals het uitvoeren van een risicobeoordeling. Daarnaast zijn in aanloop naar de wet samen met de verantwoordelijke vakministers diverse contactmomenten met de relevante sectoren georganiseerd om hen te informeren over de komst van de wet. Ook hebben de verantwoordelijke vakministers in hun reguliere contact met huidige vitale aanbieders deze gewezen op een mogelijke aanwijzing als kritieke entiteit onder de Wwke.

I.2.2: Digitale weerbaarheid MKB en bedrijfsleven

Het vernieuwde NCSC is er voor álle organisaties in Nederland, dus ook voor alle mkb'ers. Hier is de dienstverlening van het vernieuwde NCSC op aangepast. Er is in de aanloop naar de integratie zorgvuldig gekeken naar de dienstverlening die door partijen is aangeboden en hoe deze in het vernieuwde NCSC een plek konden krijgen. Daarbij is er oog voor de verschillen in behoeften van de doelgroepen en is gekeken naar verschillende producten en diensten waarop doelgroepen op een voor hen passende wijze kunnen worden bereikt. Het mkb is daarbinnen een belangrijke doelgroep. Het Ministerie van Economische Zaken en Klimaat (EZK) blijft als verantwoordelijke voor het uitvoeren van de Wet bevordering digitale weerbaarheid bedrijven (Wbdwb) voor het mkb betrokken bij het NCSC en zal ook vanuit die rol toezien op dit belang.

Het vernieuwde NCSC gaat door met stimuleren van het gebruik van risicoscans en de opvolging van concrete beveiligingsadviezen en handelingsperspectieven binnen alle doelgroepen van het vernieuwde NCSC inclusief het mkb. Via verschillende (ondernemers)verhalen uit de praktijk blijft het NCSC via onder andere haar website het belang van digitale weerbaarheid en de aanbevolen tools op een herkenbare manier onder de aandacht brengen.

Verder blijft EZK ook in 2026 via de subsidieregeling 'Mijn Cyberweerbare Zaak' voor micro- en kleine ondernemingen een financiële compensatie beschikbaar stellen voor de aanschaf en implementatie van één of meerdere belangrijke cyberweerbaarheidsmaatregelen. De meeste aanvragen in het afgelopen jaar waren op het gebied van veilige netwerktoegang en het instellen en testen van back-ups.

I.2.3: Digitale weerbaarheid onderwijs

Afgelopen rapportageperiode is vol ingezet op het verbeteren van het bewustzijn van digitale risico's en maatregelen in de onderwijssector. Zo is het normenkader informatiebeveiliging en privacy voor het primair en voortgezet onderwijs uit actie I.2.3.1 ontwikkeld door Kennisnet. De implementatie loopt momenteel. Als onderdeel van de vervolgacties is er binnen de onderwijssector een website ontworpen over het groeipad normenkader.[12] Het bereik van de website en het groeipad worden gemonitord. Daarnaast is het CERT voor het funderend onderwijs, het School-CERT, volledig operationeel. Stapsgewijs sluiten er steeds meer scholen aan die dreigingsinformatie ontvangen en hulp krijgen als ze te maken krijgen met een cyberincident.

Zoals elk jaar is het onderwerp informatiebeveiliging en privacy opgenomen als maatschappelijk thema in het bestuursverslag. Daarmee zijn scholen verplicht om verantwoording af te leggen over welke acties ze hebben ondernomen op het gebied van de borging van informatiebeveiliging en privacy. De Inspectie van het Onderwijs heeft in een gepubliceerde monitor een analyse gedaan van de jaarverslagen.[13] Actie I.2.3.2 is daarmee gerealiseerd.

Daarnaast zijn in 2025 de meeste instellingen in het mbo, hbo en wo extern geaudit. Het sectorbeeld digitale veiligheid in het vervolgonderwijs wordt continu bijgewerkt. Actuele dreigingen en kwetsbaarheden worden actief gedeeld in een besloten omgeving van coöperatie SURF. Ook hebben scholen in het funderend onderwijs deelgenomen aan Deep Dives, en diensten als 'CISO-as-a-Service' afgenomen van het programma Digitaal Veilig Onderwijs.

Ook is er continue ingezet op verschillende bewustwordingscampagnes voor studenten, medewerkers en bestuurders (inclusief Raden van Toezicht), en is bewustwording verhoogd door deelname aan oefeningen en weerbaarheidstesten.

In het mbo zijn er nu op vrijwel alle instellingen awareness-programma's opgezet. SURF heeft het informatiepunt cybersaveyourself.nl opgezet, gericht op docenten, studenten en de security en privacy professionals binnen de school. In de jaarlijkse benchmark informatiebeveiliging en privacy (IBP) is het thema 'governance op cybersecurity en inbedding in de organisatie' vanaf 2025 regulier opgenomen. Instellingen in het hoger onderwijs houden om het jaar een awareness-meting. Daarnaast zijn er ook weer jaarlijkse cybercrisisoefeningen georganiseerd door de sector. Doordat bestuurlijke afspraken met de mbo-instellingen zijn verlengd tot 2027 blijft de inzet op cyberbeveiliging voor het komende jaar geborgd. Met

[12] Groeipad - Normenkader informatiebeveiliging en privacy voor het onderwijs
[13] Monitor digitale weerbaarheid en veiligheid 2025 | Inspectie van het onderwijs

bovenstaande activiteiten zijn acties I.2.3.3 en I.2.3.4 feitelijk afgerond. Veel activiteiten en acties gericht op bewustwording lopen door.

Tot slot 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, besloten om de bekostigde hogescholen en universiteiten onder toepassing van de Cbw te brengen.[14] Dit besluit wordt in nauw overleg met de betrokken stakeholders nader uitgewerkt. De Minister van Onderwijs, Cultuur en Wetenschap heeft de Kamer op 25 juni jl. over de laatste stand van zaken geïnformeerd.[15]

I.2.4: Digitale weerbaarheid zorginstellingen

Ook in de zorgsector zijn stappen gezet om de digitale weerbaarheid te bevorderen. In het kader van het project risicogestuurde aanpak worden zorgsectoren stapsgewijs aangesloten bij Z-CERT. Daarnaast is het zorgveld in deze rapportageperiode geconfronteerd met twee grote incidenten: de hack bij het laboratorium Clinical Diagnostics en de hack bij softwareleverancier voor de zorg ChipSoft. Bij deze incidenten traden bestaande crisisplannen en -structuren van het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) in werking. De incidenten worden geëvalueerd en geconstateerde verbeterpunten zijn input voor het verbeteren van het crisismanagement van VWS.

Op het gebied van preventie en detectie (actie I.2.4.5) heeft Z-CERT in 2026 ondersteund bij 11 oefeningen die met name waren gericht op het functioneren van de crisisorganisatie ten tijde van een cyberincident en om te ervaren hoe compleet de crisisplannen zijn in geval van een dergelijk scenario. Ook zijn er 6 laagdrempeliger technische tests uitgevoerd waarbij de systeembeheerders van zorginstellingen worden meegenomen in de manier van denken van een ethisch hacker om de deelnemers kennis en expertise bij te brengen over cybersecurity. Verder heeft Z-CERT een dag georganiseerd waarbij geholpen wordt met de actuele dreigingen en kwetsbaarheden in kaart te brengen, om daarmee de juiste (vervolg)test in te kopen en prioriteiten te stellen aan de juiste onderwerpen.

Daarnaast is het bereik van het programma informatieveilig gedrag in de zorg (actie I.2.4.4) wederom gegroeid. Om het bereik te vergroten zijn er verschillende webinars georganiseerd waarmee er op een laagdrempelige kennisoverdracht gerealiseerd. Verder zijn er externe evenementen georganiseerd, (kennis) producten opgeleverd en podcast afleveringen gemaakt om bewustwording te creëren bij de specifieke doelgroep van zorgbestuurders.

Ter bevordering van de informatiebeveiliging is in maart 2026 de Risicotool NEN7510 gerealiseerd. Deze tool ondersteunt zorgorganisaties bij het uitvoeren van de verplichte risicoanalyse zoals voorgeschreven in NEN 7510. Met de oplevering van deze tool zijn alle doelen binnen actie I.2.4.1 gerealiseerd.

I.2.5: Digitale weerbaarheid sectoren infrastructuur en waterstaat

Er is deze rapportageperiode verder gewerkt aan de digitale weerbaarheid van sectoren die onder de systeemverantwoordelijkheid van het Ministerie van Infrastructuur en Waterstaat (IenW) vallen. Dit gebeurt via de IenW brede Cyberweerbaarheidsprogrammering. Deze programmering dient ter ondersteuning voor entiteiten die onder de scope van de Cbw vallen. Een belangrijk aandachtspunt hierbij is operationele technologie (OT), dat een centrale rol speelt in met name vitale processen die onder systeemverantwoordelijkheid van het IenW vallen. Deze OT-systemen kennen vaak een langere levensduur, beperkte aanpasbaarheid en andere beveiligingsprioriteiten dan IT systemen, waardoor OT zorgt voor extra uitdagingen in het versterken van de cyberweerbaarheid. Hiertoe zijn het afgelopen jaar onder andere producten opgeleverd rondom het risicobeheer van cyberrisico's in OT, het grip krijgen op risico's in de leverancierskeketen en trainingen om de kennis over OT binnen entiteiten te vergroten.

Gezien de actuele cyberdreiging, ook richting de vitale infrastructuur, zet IenW zich in om de kennisproducten rondom cyberrisico's in OT in haar IenW brede cyberweerbaarheidsprogrammering door te ontwikkelen en in het verlengde daarvan een rol op zich te nemen als centrale kennismakelaar die kennis deelt, normen stelt, innovatie stimuleert, en als loket kan fungeren voor bijbehorende IenW diensten en andere essentiële en belangrijke entiteiten binnen de vitale sectoren van het Ministerie van IenW. Hierbij zal actief samenwerking worden gezocht met het NCSC, de RDI, kennisinstituten, brancheverenigingen en entiteiten zelf. Daarmee is actie I.2.5.1 herijkt.

Verder heeft IenW het CERT Watermanagement (CERT-WM) officieel aangewezen als sectoraal CSIRT voor de waterschappen. Daarmee fungeert het als cruciale schakelorganisatie om de digitale weerbaarheid van de watersector te versterken. CERT-

[14] Kamerstuk 31288, nr. 1189 | Overheid.nl > Officiële bekendmakingen
[15] Kamerstuk 26643, nr. 1535 | Overheid.nl > Officiële bekendmakingen

WM is goed bekend met de structuren van en processen binnen de watersector.

I.2.6: Digitale weerbaarheid Rijksoverheid

De digitale weerbaarheid van de (Rijks)overheid is van essentieel belang voor het digitaal veiliger maken van Nederland. Burgers en bedrijven moeten er immers op kunnen vertrouwen dat de (Rijks)overheid betrouwbaar haar taken uitvoert en zorgvuldig omgaat met hun (persoons)gegevens. De ambitie op het gebied van de digitale weerbaarheid van de Rijksoverheid is eerder uiteengezet in de I-strategie Rijk en de bijbehorende routekaart. Omdat de I-strategie in 2025 is geëindigd is de digitale weerbaarheid voor de overheid – voor alle overheidslagen – één van de prioriteiten geworden onder de Nederlandse Digitaliseringsstrategie (NDS)[16] , die in juli 2025 is vastgesteld in de ministerraad. In de NDS zijn de ambities voor digitale weerbaarheid vastgelegd in de vorm van 6 thema's, versnellers genoemd. De uitvoering van deze versnellers valt onder de verantwoordelijkheid van de Staatssecretaris van EZK. Over de voortgang op de NDS over het eerste jaar wordt de Tweede Kamer naar verwachting in Q4 van 2026 geïnformeerd. Een aantal trajecten voor 2026 worden uitgelicht, hiervan zijn Federatief SOC stelsel (doorontwikkeling VSSR) en Quantumveilige cryptografie onderdeel van de NDS.

Versterking Security Operations Center (SOC)-stelsel Rijk (VSSR)

De VSSR richt zich op het versterken van en ondersteunen bij het inrichten van Security Operations Centers (SOC's) bij rijksoverheidsorganisaties door het ontwikkelen van generieke aanpakken en kennisproducten. Formeel is VSSR per 1 januari 2026 overgedragen aan het NCSC. De doorontwikkeling van VSSR is onderdeel van de NDS.

Red Teaming bij de Rijksoverheid

Om de feitelijke digitale veiligheid van kerntaken van de Rijksoverheid te testen past de Rijksoverheid Red Teaming testen toe via de TIBER-aanpak. Hierbij voeren red teams (die bestaan uit ethisch hackers) op dreiging gebaseerde testaanvallen uit. Zo wordt inzichtelijk waar de organisatie kwetsbaar is voor echte aanvallers. Op basis van de uitkomsten verbetert de Rijksoverheid haar verdediging tegen aanvallen door criminelen en statelijke actoren. Ook in deze NLCS-voortgangsperiode zijn er weer testen afgerond en bevinden zich verschillende testen in diverse fases van uitvoering. De uitkomsten hiervan zijn onderdeel van gesprek op het SG-overleg.

Ransomware

Het doel van het ransomware project is om overheidsorganisaties te helpen zich te wapenen tegen (de gevolgen van) aanvallen met ransomware. De kaders van de ransomware managementgame zijn vastgesteld en zijn bekend gemaakt onder meer via de website van het Centrum voor Informatiebeveiliging en Privacy.[17] De ransomware managementgame is een serious game en geeft inzicht in hoe om te gaan met ransomware aanvallen en crisisbeheersing in het algemeen. Deze game heeft in 2025 circa 600 deelnemers gehad over de hele overheid en wordt in samenwerking met het Centrum voor Informatiebeveiliging en Privacy (CIP) en Radio aangeboden. De game wordt in de komende jaren verder doorontwikkeld en ook zullen de kaders geëvalueerd en bijgesteld worden.

Verplichte basisopleiding digitale weerbaarheid

In januari 2024 is in beleid vastgelegd dat alle medewerkers van de Rijksoverheid verplicht zijn een basisopleiding digitale weerbaarheid te volgen. Om dit zo eenvoudig mogelijk te maken, is er centraal een e-learning ontwikkeld die via het eigen leerplatform kan worden aangeboden. Sommige rijksorganisaties hadden ook al een eigen opleiding.

I.2.7: Digitale weerbaarheid overheid

Digitale Weerbaarheid Gemeenten

Ook gemeenten krijgen steeds vaker te maken met digitale dreigingen en cyberaanvallen. Het Bestuurlijk Convenant Digitale Veiligheid Gemeenten is in 2022 opgesteld om deze risico's het hoofd te bieden. Afgelopen rapportageperiode is in het kader van dit Convenant het onderzoek Cyberweerbaarheid binnen gemeentegrenzen "uitwerking Bestuurlijk Convenant Digitale Veiligheid" uitgevoerd. Het onderzoeksrapport is verschenen in de zomer van 2025 en is in december 2025, samen met een beleidsreactie, aan de Tweede Kamer aangeboden.[18]

In 2026 is een nieuwe programmamanager aangesteld om de uitvoering van het Bestuurlijk Convenant Digitale Veiligheid Gemeenten verder vorm te geven. Daarbij is de nadruk gelegd op concrete uitvoering en versterkte interbestuurlijke samenwerking. Deze aanpak richt zich op het bezien wat nodig is om de interbestuurlijke samenwerking op dit thema structureel te borgen, voorbij de looptijd van het convenant.

[16] Nederlandse Digitaliseringsstrategie (NDS) - Digitale Overheid
[17] Kennisproducten Ransomware en Datadiefstal - cip-overheid: https://www.cip-overheid.nl/producten-en-diensten/kennisproducten-ransomware-en-datadiefstal
[18] Kamerstuk 26643, nr. 1447 | Overheid.nl > Officiële bekendmakingen

Conform de motie-El Boujdaini is de informatiepositie van burgemeesters en voorzitters van veiligheidsregio's bij cyberincidenten met gevolgen voor de openbare orde als prioritair thema binnen het programma opgepakt.

Inmiddels is een belangrijke stap gezet. In nauwe samenwerking met de gemeente Den Haag, de VNG, de veiligheidsregio's en het Platform Cyberburgemeesters is de behoefte om de melding van een significant cyberincident ook beschikbaar te maken voor de burgemeester helder naar voren gebracht, zodat hij/zij zelf de mogelijke gevolgen voor de openbare orde en veiligheid kan inschatten en zo nodig actie kan ondernemen. De vervolgstap is een gezamenlijke verkenning.

Verder is de doorontwikkeling van de verantwoordingssystematiek voor informatieveiligheid van gemeenten, ook wel Eenduidige Normatiek Single Information Audit (ENSIA), in 2026 voortgezet. Verantwoording vanuit de gemeenten over de Cbw zal via ENSIA verlopen en er wordt gekeken naar verdere harmonisatie en uitbreiding van ENSIA in de toekomst. Ook is in 2026 gestart met het opnieuw aanbesteden van de ENSIA tooling.

Baseline Informatiebeveiliging Overheid (BIO)

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen. In maart 2026 is de BIO 2 versie 1.3 in de Staatscourant gepubliceerd.[19] Deze wordt niet via de Wet Digitale Overheid (WDO) maar via de Cyberbeveiligingsregeling sector Overheid (Cbro) als onderdeel van de zorgplicht onder de Cbw verplicht. BZK werkt samen met het CIP en alle betrokken partijen verder aan de doorontwikkeling van de BIO2. Naar verwachting volgt een nieuwe versie in vierde kwartaal van 2027.

De uitvoering van het ondersteuningsprogramma BIO is gecontinueerd in 2026. Er is onder meer gewerkt aan een CISO toolbox, een volwassenheidsmodel, het meer betrekken van bestuurders bij informatiebeveiliging en een campagne rond continuïteitsmanagement. Tevens is BZK gestart met een verkenning naar de bruikbaarheid van de BIO2 als normenkader in het Caribisch deel van het Koninkrijk.

De service Informatiebeveiliging en Privacy van het CIP is gecontinueerd in 2026. Het CIP verzorgt de website bio-overheid.nl als informatiepunt voor alle overheidsorganisaties en behandelt vragen via de BIO-mailbox. Zij verbinden bovendien vraag en aanbod binnen de community van overheidsorganisaties om onderlinge kennisdeling te bevorderen. Ook worden er informatiebeveiliging en privacy themasessies georganiseerd om kennis te delen op de thema's die dit jaar relevant zijn.

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

De IACS (Industrial Automation and Control Systems) Coalitie is een samenwerkingsverband dat de digitale weerbaarheid van industriële en operationele automatiseringssystemen versterkt. Het doel van de IACS is om de ontwikkelingen en activiteiten op dit vakgebied te volgen, te bundelen, er richting aan te geven en de kennis hierover vanuit het collectief te delen met anderen. Door de samenwerking van diverse overheidsorganisaties is dit collectief een krachtig orgaan voor zowel publieke als private organisaties om de digitale weerbaarheid van het IACS-landschap te verhogen. IenW neemt deel aan de IACS Coalitie en levert ook bijdragen aan de acties die voortkomen uit deze coalitie gericht op OT, waaronder initiatieven die kritieke sectoren moet helpen om cyberdreigingen binnen OT sneller te kunnen detecteren.

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

Om zicht te creëren op de digitale weerbaarheid van overheid en bedrijfsleven zijn het afgelopen jaar een aantal initiatieven uitgewerkt.

De eerste pilots met betrekking tot een IT-verslag en IT-auditverklaring hebben inmiddels plaatsgevonden. BZK werkt aan het organiseren van aanvullende pilots waarbij lessen uit deze eerdere pilots worden meegenomen. Daarnaast sluit BZK aan bij de regieraad voor het International Digital Reporting Standards (IDRS) van ECP Platform voor de Informatiesamenleving om de standaard verder te ontwikkelen. Tenslotte voert BZK in opdracht van de Tweede Kamer[20] een verkenning uit naar de mogelijke invoering van een dergelijk verslag voor de Rijksoverheid. De Tweede Kamer wordt naar verwachting voor het einde van het jaar nader geïnformeerd over uitkomsten van deze verkenning.

Om de beleidsinitiatieven op het terrein van digitale weerbaarheid te kunnen evalueren onderzocht RAND Europe in opdracht van het WODC of, en zo ja hoe, de digitale weerbaarheid van Nederlandse organisaties meetbaar kan worden gemaakt.[21] De uitkomsten van het onderzoek bieden aanknopingspunten en uitgangspunten voor het verder verkrijgen van inzicht in het

[19] Staatscourant 2026, 7416 | Overheid.nl > Officiële bekendmakingen
[20] Kamerstukken II 2024/25, 26643, nr. 1342
[21] Kamerstukken II 2025/26, 26642, nr. 1454

meetbaar maken van digitale weerbaarheid. Het rapport zal nationaal en waar mogelijk internationaal onder de aandacht worden gebracht om elkaar in staat te stellen te leren van elkaars inzichten.

Via het Centrum voor Informatiebeveiliging en Privacy (CIP) heeft BZK in 2026 een bijdrage gedaan aan de Stichting Internet Cleanup Foundation (ICF) voor het onderhoud en de verdere ontwikkeling van de site Basisbeveiliging.nl. Op deze wijze wordt voorkomen dat de getoonde informatie op de website veroudert of onvoldoende aansluit bij de werkpraktijk. De website is belangrijk, omdat overheidsorganisaties zich kunnen spiegelen aan andere overheidsorganisaties en geeft een prikkel om concrete verbeteringen aan te brengen in de beveiliging.

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

Zowel nationaal als internationaal wordt er hard gewerkt aan incident- en crisispreparatie. Dit gebeurt onder andere door middel van (inter)nationale oefeningen. Op nationaal vlak werd vanuit de landelijke werkgroep cyber in 2026 een tabletop excercise georganiseerd om de leerpunten uit ISIDOOR IV en incidenten te beoefenen. Verschillende veiligheidsregio's, Knooppunt Coördinatie Regio's-Rijk (KCR2) en de NCTV namen hieraan deel. Daarnaast vonden er verschillende sectoralen oefeningen plaats binnen de onderwijs- en zorgsector.

In het najaar van 2026 organiseert BZK voor de achtste keer het Overheidsbreed Cyberprogramma. Het programma zal bestaan uit de jaarlijkse Overheidsbrede Cyberoefening, webinars, een masterclass en bestuurlijke interviews. Deelnemers van de cyberoefening kunnen op drie manieren meedoen: vooraf mee-oefenen, live mee-oefenen in de 'Greenroom' of (via de livestream) meekijken met de centrale oefentafel.

Het Overheidsbreed cyberprogramma is daarnaast in 2025 uitgebreid naar het Caribisch deel van het Koninkrijk. In dat kader wordt tijdens de BQ cybersecurity convention op Bonaire een cyber table-top verzorgd en worden voor dit deel van het Koninkrijk ook bestuurlijke interviews en webinars georganiseerd. De digitale weerbaarheid van het Caribisch deel van het Koninkrijk staat tijdens de BQ conferentie centraal. De conferentie heeft als doel om alle belangrijke spelers in de cybersecurity community bij elkaar te brengen. Deze cyber table-top heeft op 29 oktober jl. wederom plaatsgevonden.

Verder blijven cyberoefeningen bij Defensie, zowel nationaal als met (inter)nationale partners, een belangrijk aandachtspunt. Bovendien wordt er gewerkt aan een betere coördinatie van cyberoefeningen binnen Defensie en aan de integratie van cyber in multidomein-oefeningen. Hierdoor kunnen de cyberentiteiten binnen Defensie ook mee oefenen in bestaande Defensiebrede oefeningen. Daarnaast bereiden verschillende departementen zich voor op de deelname aan de CMX'27, de NAVO Crisis Management Exercise. Digitale weerbaarheid vormt een belangrijk aandachtspunt binnen deze oefening.

Daarnaast is er in 2026 door Nederland deelgenomen aan verschillende internationale oefeningen waaronder Cyber Europe en BlueOlex, waarin er met de EU-cybercrisismanagementmechanisme werd geoefend. Ook nam Nederland deel aan de NAVO-oefening Locked Shields waarin het volledige spectrum van defensieve cyberactiviteiten werd beoefend. Aan deze oefening namen 4000 deelnemers deel uit 40 landen. In november en december van dit jaar nemen het NCSC en de NCTV samen met Defensie, de Koninklijke Marechaussee, de watermanagementsector en luchthavens deel aan de Cyber Coalition oefening van de NAVO. Ook deelname aan PACE staat gepland voor dit jaar.

Tot slot werken we aan actualisatie van onze nationale crisisplannen, door in de aankomende update van het Landelijk Crisisplan Digitaal (LCP-D) de meest actuele versie van het nationale cybercrisisstelsel op te nemen. De implementatie van de Cbw en de stelselwijzigingen die als gevolg hiervan plaatsvinden hebben hier een belangrijke uitwerking op. Om dit goed te laten landen wordt in 2027 aan de actualisatie van het LCP-D gewerkt.

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

Cyber Resilience Act (CRA)

Het toewerken naar een veilige en innovatieve digitale economie draagt bij aan de digitale veiligheid en het verdienvermogen van Nederland. Een belangrijk Europese wet in dit kader is de Cyber Resilience Act (CRA), die eind 2024 is gepubliceerd. In de CRA worden essentiële eisen aan de cybersecurity van producten met digitale elementen (hardware, en software en elementen) gesteld die fabrikanten, importeurs en distributeurs vanaf 11 december 2027 in de EU op de markt aanbieden. Hiermee verschuift de verantwoordelijkheid voor de digitale veiligheid van een product van de eindgebruiker naar de fabrikant. Dit draagt bij aan zowel de doelstellingen uit pijler II, namelijk veilige producten, als de doelstelling uit pijler IV van de NLCS over het verhogen van de digitale weerbaarheid van burgers.

De uitvoeringswet die het toezicht vastlegt is in december 2025 aangeboden aan de Tweede Kamer en is daar in september 2026 behandeld. De uitvoeringswet regelt onder andere het toezicht en de handhaving van de CRA door de RDI. Ook worden zij aangewezen als autoriteit die verantwoordelijk is voor de procedure om conformiteitsbeoordelingsinstanties te beoordelen, aan te melden en te monitoren. Fabrikanten van belangrijke of kritieke producten moeten onder de CRA langs een aangemelde conformiteitsbeoordelingsinstantie om hun product te laten beoordelen, alvorens zij hun product op de markt mogen aanbieden. In september 2026 is de meldplicht van de CRA ingegaan en worden fabrikanten geacht om bij uitgebuite kwetsbaarheden en ernstige incidenten een melding te maken bij het NCSC. Daarnaast worden er nog standaarden ter ondersteuning van de CRA uitgewerkt en heeft de Europese Commissie in augustus 2026 richtsnoeren gepubliceerd ter ondersteuning van de implementatie. Ter ondersteuning van het mkb wordt er een nationaal communicatiekanaal en een testomgeving voor regelgeving (‘regulatory sandbox’) ingeregeld.

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

Effectief toezicht en handhaving op digitale producten en diensten zorgt ervoor dat cybersecurity risico’s beperkt worden en regels daadwerkelijk worden nageleefd. Sinds 1 augustus 2025 zijn de cybersecurity eisen op draadloos verbonden apparaten die onder de Radioapparatuurrichtlijn (RED 3.3)[22] vallen van toepassing. De RDI houdt toezicht op de toepassing van deze eisen. Vanaf december 2027 vervangt en verbreedt de CRA de eisen voor draadloos verbonden apparaten in de RED. Daarmee is actie II.

[22] RED 3.3 voor radioapparatuur | Rijksinspectie Digitale Infrastructuur (RDI)

1.1.2 afgerond en loopt deze over in het toezicht en de handhaving van de RDI op de CRA.

II.1.3: Certificering en standaarden

Op Europees niveau spelen verschillende certificeringsinitiatieven. In 2025 is het eerste Europese certificeringsschema, het EU Cybersecurity Certification Scheme on Common Criteria (EUCC), opgeleverd en geïmplementeerd. Het EUCC-schema controleert aan de hand van de Common Criteria-standaard of een ICT-product aan bepaalde beveiligingseisen voldoet. In Nederland is de ministeriële regeling inzake EUCC vastgesteld en goedgekeurd door de Ministerraad, waarmee het schema nationaal is geoperationaliseerd. Inmiddels hebben meerdere partijen aanvragen ingediend bij de RDI om gecertificeerd te worden.

Het Europees Certificeringsschema voor Clouddiensten (EUCS) is medio 2025 opgeleverd, maar vervolgens door de Europese Commissie aangehouden in het licht van de herziening van de EU Cybersecurity Act (CSA). De Commissie heeft in het voorjaar van 2026 heeft haar voorstel voor de herziene CSA ("CSA2") gepresenteerd. Dit voorstel bevat naast een herzien Europees kader voor cybersecuritycertificering onder meer nieuwe bepalingen over de beveiliging van ICT-toeleverancier sketens (supply chain security). De onderhandelingen over CSA2 vinden momenteel plaats in de Raad. Na vaststelling van de posities van de Raad en het Europees Parlement kunnen de triloogonderhandelingen over de definitieve verordening van start gaan.

De CSA-certificeringssystemen spelen een rol in een toenemend aantal Europese wetten en hebben daarmee een ondersteunend belang voor het Nederlandse bedrijfsleven om in de Europese markt te opereren. De RDI neemt actief deel aan de Europese werkgroep die zich richt op de beveiliging van digitale producten door middel van toezicht in het kader van de CSA. Ter bevordering van de bewustwording en ter ondersteuning van de implementatie van certificeringsschema's in het kader van de CSA, heeft de RDI meerdere overlegtafels en informatieve bijeenkomsten georganiseerd, zoals webinars en toespraken op congressen.

Daarnaast wordt momenteel gewerkt aan de ontwikkeling van het European Union Managed Security Services (EUMSS) -schema. Naar verwachting zal dit certificeringsschema eind 2026 worden opgeleverd.

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

Algemene beveiligingseisen Rijksoverheid (ABRO)

Ter bescherming van de nationale veiligheid zijn er extra beveiligingseisen opgesteld voor bedrijven die overheidsopdrachten uitvoeren met risico's voor de nationale veiligheid. Dat zijn de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO).[23] Vanaf 1 januari 2026 gelden de ABRO voor bedrijven die voor de rijksoverheid en politie een opdracht uitvoeren met risico's voor de nationale veiligheid. De invoering gaat in verschillende tranches, waarbij de opdrachtgevers van inkopende organisaties (in tranche 1 zijn dat de politie, ministeries, hun diensten en agentschappen) de ABRO uiterlijk 31 december 2027 toepassen op inkoopopdrachten die de nationale veiligheid raken.[24] De inkopende organisaties implementeren de toepassing van de ABRO binnen hun interne inkoopketens en zorgen voor integratie in hun beleid, inkoop- en aanbestedingsprocedures, en contractvorming. Zij blijven verantwoordelijk voor risicomanagement en de acceptatie van eventuele restrisico's met betrekking tot de bijzondere opdracht en de uiteindelijke inkoop hiervan. Het programma ABRO is inmiddels omgedoopt tot programma "Veilig inkopen".

Er wordt onderzocht welke juridische mogelijkheden bestaan of nodig zijn om het toepassen van de ABRO door inkopende organisaties in de opvolgende tranches te borgen. Het gaat hierbij onder meer om de zelfstandige bestuursorganen, decentrale overheden en nader vast te stellen organisaties in kritieke sectoren, alsmede enkele sui generis organisaties. Deze organisaties vallen niet allemaal onder de werking van het regelgevend kader dat voor ABRO in tranche 1 is gecreëerd.[25]

Met het bedrijfsleven worden vraag- en antwoordsessies gehouden over de ABRO. In samenwerking met VNO NCW MKB Nederland is een mkb-panelgesprek gehouden met een tiental bedrijven over de ABRO. De Kamer wordt daarover in de 3e Voortgangsrapportage Veilig inkopen geïnformeerd, welke in het 3e kwartaal van 2026 wordt aangeboden.

Ten behoeve van de implementatie richt het programma zich op dit moment vooral op de speerpunten Kennisontwikkeling, Ontwikkelen van hulpmiddelen en Voortgangsmonitoring. Samen met de Universiteit Utrecht wordt een serie van masterclasses Veilig Inkopen & Aanbesteden georganiseerd. Daarnaast heeft het Ministerie van BZK aan PIANOo de opdracht gegeven voor het organiseren van kennissessies op het gebied van veilig inkopen. Deze zijn gericht op bredere kennisdeling over veilig inkopen en

[23] Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO)
[24] Invoeringsdatum en geplande invoering ABRO door inkopende organisaties in tranche 1 | Rijksoverheid.nl
[25] ABRO kaderbesluit rijksdienst

sluiten aan op het bestaande PIANOo-aanbod. Het programma Veilig Inkopen heeft recent voorbeeldteksten voor inkoopdocumenten gepubliceerd die inkopende organisaties kunnen gebruiken om in een inkooptraject juridisch houdbaar aan te geven dat ABRO van toepassing is op een opdracht, en wat dit betekent voor het inkoopproces.

Inkoopeisen Cybersecurity Overheid (ICO)

Digitale risico's ontwikkelen zich steeds vaker in toeleveringsketens en gedeelde digitale ecosystemen. Daarom wordt door BZK in samenwerking met de VNG verkend hoe beter overheidsbreed inzicht kan worden verkregen in gedeelde digitale afhankelijkheden, leverancierscconcentraties en keten- en concentratierisico's die individuele organisaties niet zelfstandig kunnen overzien. In dat kader wordt onderzocht hoe signalen, analyses en inzichten uit organisaties op federatieve wijze kunnen worden verbonden, zonder verantwoordelijkheden te centraliseren. Deze verkenning, bekend als ICO 2.0, geeft een ontwikkelrichting voor inkoopeisen ten aanzien van cybersecurity (ICO). Deze uitwerking is in 2026 verder vormgegeven. Op dit moment loopt de voorbereiding voor besluitvorming over deze ontwikkelrichting met als doel om overheidsbreed afspraken te maken over de gekozen richting.

Ondertussen wordt, naar aanleiding van de Cbw tevens verkend hoe de bestaande ICO kunnen worden doorontwikkeld naar een bredere lifecyclegerichte aanpak voor leveranciersmanagement. Doel is organisaties beter te ondersteunen bij het identificeren, afwegen en beheersen van risico's gedurende de volledige levenscyclus van digitale afhankelijkheden, waaronder continuïteit, leveranciersrisico's, ketenafhankelijkheden, restrisico's en exitmogelijkheden. Deze ontwikkelrichting is in 2026 inhoudelijk verder uitgewerkt, mede op basis van gesprekken met betrokkenen vanuit inkoop, beleid en uitvoering. De uitkomsten worden momenteel verwerkt in de verdere ontwikkeling van ICO 1.5 en in samenhang met ICO 2.0 in de praktijk en bestuurlijk getoetst. Op basis daarvan wordt bepaald welke vervolgstappen en structurele borging nodig zijn. Uw Kamer wordt over de uitkomsten en vervolgstappen geïnformeerd.

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

II.2.1: Veilige cryptografie

Het is essentieel dat de ontwikkeling en toepassing van Nederlandse kennis en kunde op het gebied van cybersecurity continu worden versterkt, zodat we nu en in de toekomst maatregelen kunnen nemen tegen digitale dreigingen. Om de Rijksoverheid te verzekeren van goede en duurzame informatiebeveiligingsmiddelen voor de middellange (drie jaar) en lange termijn (vijf jaar en verder) is de Nationale Cryptostrategie (NCS) in het leven geroepen. In het kader van de Nationale Crypto Strategie (NCS) zijn er afgelopen jaren meerdere stappen gezet op verschillende facetten. Met betrekking tot het rijksbreed en eensgezind opdrachtgeverschap is een NCS-governance model overeengekomen dat waarborgt dat de Staat als één opdrachtgever richting de cryptobedrijven optreedt. De belangrijkste stakeholders hierbij zijn het Ministerie van Defensie, de AIVD en CIO-Rijk. Door dit governance model kunnen het Rijk en Defensie op basis van één gecombineerde behoeftestelling cryptomiddelen door de crypto-industrie laten ontwikkelen. Naar verwachting wordt vóór eind 2026 het eerste NCS strategische samenwerkingscontract afgesloten met een cryptobedrijf waarbij de Staat als één opdrachtgever optreedt.

Verder ondersteunt TNO sinds 2024 de NCS als (proces)adviseur bij de realisatie van de NCS-doelstellingen[26]. Centraal staat daarbij de ontwikkeling van een nieuwe marktbenadering als alternatief voor traditionele aanbestedingen, gericht op het creëren van een stabiel ecosysteem dat langdurige leveringszekerheid van cryptomiddelen voor het Rijk en Defensie waarborgt. De cryptobedrijven zijn actief betrokken bij deze aanpak, waardoor tevens draagvlak binnen de sector wordt gecreëerd. Op basis hiervan heeft TNO-adviezen uitgebracht over de implementatie van eerder aanbevolen verandermaatregelen. In juni 2026 is TNO gestart met de laatste fase van de opdracht, gericht op het operationaliseren van deze implementatieadviezen, met als hoofdonderwerp de inrichting en werking van de NCS-governance structuur. Deze werkzaamheden zullen naar verwachting begin 2027 worden afgerond. Daarmee wordt een belangrijke stap gezet richting versterkte strategische autonomie van de Staat op het gebied van de levering van cryptomiddelen voor de beveiliging van staatsgeheimen.

In 2026 zal het dossier NCS worden overgedragen aan EZK, onder de verantwoordelijkheid van de staatssecretaris voor Digitale Economie en Soevereiniteit. EZK heeft aangegeven prioriteit te willen geven aan kennisopbouw, innovatie en versterking van de Nederlandse cryptosector, met als doel zowel de digitale weerbaarheid als de economische waardecreatie voor Nederland te vergroten[27]. EZK ziet hiervoor een belangrijke rol weggelegd binnen de bredere cybersecurity-ambities en de nationale technologieagenda (NTA). De overdracht van het dossier draagt daarmee bij aan de verdere verankering van de NCS binnen het rijksbrede beleid voor digitale soevereiniteit, innovatie en strategische autonomie. BZK en Defensie blijven nauw samenwerken om de overheidsbehoefte in te brengen in het ecosysteem.

[26] Een nieuw samenwerkingsmodel voor de Nationale Crypto Strategie
[27] Zie bijvoorbeeld: Strategische inzet digitalisering | Tweede Kamer der Staten-Generaal

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

Sinds de start van de NLCS zijn verschillende initiatieven gestart om de interdepartementale kennis- en innovatiebehoefte vast te stellen. 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 EZK gekozen om niet meer in te zetten op een jaarlijkse inventarisatie van behoeftes zoals beschreven in actie II.2.2.1, maar om departementen uit te nodigen om bij te dragen aan subsidie-instrumenten die EZK initieert. Zo kunnen departementen per mogelijkheid naar wens bijgedragen aan de keuze van onderwerpen voor cybersecurityinnovatie, en aan de keuze of er ingezet wordt op fundamenteel of toegepast onderzoek. Dit proces heeft de afgelopen NLCS-periode geleid tot meer onderling begrip van behoeftes, en tot daadwerkelijke interdepartementale financiering van innovatie calls. Een mooi voorbeeld daarvan is de financiering van de NWA call Weerbare Digitale Ecosystemen (2026) waar EZK, JenV en BZK gezamenlijk financieel bijdragen, en met NWO de inhoudelijke doelstelling afgestemd hebben.

Defensie heeft afgelopen jaar haar innovatieportfolio uitgebreid. Het portfolio bestaat uit projecten met marktpartijen op het gebied van cyber en digitale weerbaarheid, waarbij marktrijpe innovaties worden beproefd in de operationele omgeving van Defensie. De landelijke positie in cybersecurity kennis- en innovatienetwerken is verder versterkt. Zo is eind 2025 de denktank "Forward Thinkers" opgericht, waarin per kwartaal met vooruitstrevende denkers uit de markt wordt gekeken naar ontwikkelingen op onder andere het gebied van cybersecurity en de betekenis daarvan voor Defensie. Daarnaast draagt de Cyber Innovation Hub (CIH) bij aan het ecosysteem door samenwerking met marktpartijen, kennisinstellingen en collega-innovatieorganisaties en door actieve kennisdeling via evenementen en publicaties. Een voorbeeld hiervan is SIGMA Experience Lab, waarin de CIH met deze partijen werkt aan een gezamenlijke experimenteeromgeving voor het ontwikkelen en beproeven van nieuwe technologieën en concepten.

II.2.3: Europese onderzoekssamenwerking en fondsen

Op Europees niveau lopen initiatieven ter versterking van de cybersecuritysector. Het Europese Cybersecurity Competence Centrum (ECCC) draagt de verantwoordelijkheid voor de invulling van het Cybersecurity werkprogramma 2025-2027 van Digital Europe. Hierbij vormen belangrijke documenten, zoals de Strategische Agenda van het ECCC, de basis voor deze werkprogramma's. Nederland heeft een sleutelrol gehad bij de totstandkoming van deze Strategische Agenda en daarmee zijn Nederlandse prioritaire onderwerpen zoals Post-Quantum Cryptografie en talentontwikkeling goed behartigd in de calls.

Tevens wordt actief met publieke en private partners de cybersecurity kennis- en innovatiebehoefte opgehaald. Dat gebeurt bijvoorbeeld binnen de NTS Actieagenda Cybersecurity Technologieën en lopende innovatieprogramma's. Deze inzichten worden door EZK ingebracht bij uitvragen vanuit de EU, bijvoorbeeld bij de vorming van de nieuwe werkprogramma's van Digital Europe en Horizon Europe door het ECCC, en de inhoudelijke opbouw van het European Competitiveness Fund (ECF), zodat de Nederlandse behoeften zo goed mogelijk worden vertegenwoordigd.

Organisaties uit de Nederlandse cybersecuritysector (waaronder het voormalige dcypher-netwerk) worden ondersteund via het Nationaal Coördinatie Centrum (NCC-NL) in de voorbereiding en uitvoering van projecten uit Europese initiatieven en fondsen zoals Digital Europe en Horizon Europe. Via verschillende kanalen wordt de doelgroep geïnformeerd over openstaande Europese calls, bijvoorbeeld via een nieuwsbrief en de NCC-NL funding portal. NCC-NL ondersteunt Nederlandse partijen bij het participeren in subsidietrajecten, door bijvoorbeeld partners te vinden voor consortia, en feedback te geven op voorstellen. Daarnaast heeft NCC-NL het 'Cyber Innovation Fund (CIF-NL) opgezet waarin met EZK en EU Digital Europe financiering aan het mkb aangeboden wordt voor cybersecurity innovatie trajecten. CIF-NL heeft in 2026 haar tweede openstelling gehad en zal naar verwachting 60+ bedrijven voorzien van financiering.

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 AIVD en MIVD blijven investeren in de onderzoekscapaciteit. Ondanks deze investeringen staan we voor een steeds grotere uitdaging ten aanzien van de dreigingen. De AIVD en MIVD hebben dit jaar veel stappen gezet in het vertalen van unieke inlichtingen naar specifiek handelingsperspectief. Onder andere door, indien mogelijk, vaker naar buiten te treden, bijvoorbeeld doormiddel van het uitbrengen van weerbaarheid verhogende en openbaar toegankelijke cyberadviezen met technisch handelingsperspectief. Hiermee wordt de weerbaarheid tegen malicieuze cyberoperaties vergroot inclusief het bewustzijn van dit soort operaties. Een voorbeeld hiervan is het cyberadvies over phishing via chatapps Signal en Whatsapp dat is uitgebracht op 9 maart jl.

Hoewel de Tijdelijke wet Cyberoperaties (de Tijdelijke wet) op 1 juli 2024 volledig in werking is getreden, heeft de commissie van toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD) eerder laten weten, wegens huisvestingsproblematiek, slechts beperkt bindend toezicht te kunnen houden. Om die reden kon de wet nog niet volledig toegepast worden door de diensten. De CTIVD heeft laten weten dat zij sinds 1 oktober 2025 klaar is voor een zo goed mogelijke uitvoering van de Tijdelijke wet. De MIVD en AIVD hebben in de verrichte invoeringstoets van de Tijdelijke wet[28] aangegeven dat er tot nu toe positieve ervaringen zijn opgedaan met de toepassing van de wet, zoals inzetmogelijkheden op kabelinterceptie en de regeling rondom de verlenging van de eindtermijn van bulkdatasets. Ook zijn een aantal knelpunten gesignaleerd. Deze aspecten en ervaringen worden meegenomen in het wetstraject voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv). Hiermee wordt ingezet op een toekomstbestendige en uitvoerbare wet die de benodigde operationele slagkracht en wendbaarheid biedt.

Een tijdsgewricht van toegenomen, complexere en diffusere dreigingen voor nationale veiligheid vraagt ook om diensten die effectief kunnen reageren op geopolitieke en technologische ontwikkelingen, zonder afbreuk te doen aan fundamentele waarborgen zoals onafhankelijk toezicht. Tegen die achtergrond wordt ook gekeken naar het actualiseren van benodigde grondslagen voor samenwerking met buitenlandse partners-medeoverheden, kennisinstellingen en bedrijven.

III.1.2: Onderzoeks- en opsporingscapaciteit cybercriminelen

De politie en het OM hebben dit jaar weer een groot aantal onderzoeken en interventies uitgevoerd, onder andere in het

[28] Kamerstukken II 2025/26 36 263, nr. 46

kader van de International operatie Endgame. Verantwoording hierover vindt plaats via de gebruikelijke kanalen, waaronder het jaarverslag van de Politie. Daarnaast is de Kamer geïnformeerd over de voortgang middels de Kamerbrief integrale aanpak cybercrime.[29]

Daarnaast is er op 3 september 2026 weer een cybercrimebeeld Nederland opgeleverd.[30] De beelden in het veiligheidsbeeld geven richting aan de keuze van de politie en het OM voor de fenomenen waarop wordt ingezet en de onderzoeken die worden geprioriteerd.

Binnen het OM is er een brede behoefte aan kennisuitwisseling en opleidingen op het gebied van cybercrime en gedigitaliseerde criminaliteit. Deze behoefte strekt zich uit van algemene kennis tot de specifieke expertise die is vereist voor cyberdeskundigen. Om deze kennis te versterken wordt er op dit moment intern bij het OM breed ingezet op het vergroten van kennis en kunde door leertrajecten die door specialisten worden gegeven en door kennispagina's up-to-date te houden.

Verder wordt de bestaande samenwerking tussen de KMar en politie in het cyberdomein verder versterkt op verschillende niveaus. Dit gebeurt zowel op het gebied van informatie- en kennisdeling, op operationeel niveau binnen Team DIGIT, op tactisch vlak als op strategisch niveau in de samenwerking op cyberstrategieën. Samenwerking en kennisdeling blijven gezien de complexiteit en snelheid van het domein van groot belang voor beide partijen. Daarom blijft het verdiepen en versterken van de samenwerking een continu aandachtspunt. Zo is het afgelopen jaar ingezet op structurele kennisdeling, heeft de Kmar bijgedragen aan de nieuwe strategie voor online criminaliteit van de politie en heeft de politie ondersteund in de totstandkoming van een KMar-plan voor de oprichting van een team om cybercriminaliteit tegen te gaan.

Om hier verder vorm aan te geven werkt de KMar aan een eigen interne cyberstrategie waarin Samenwerking één de vijf fundamentele thema's is om richting te geven aan de ontwikkeling en inzet van cyber. Het ontwikkelen en onderhouden van duurzame samenwerkingsrelaties binnen het cyberdomein en het effectief uitwisselen van kennis, informatie en expertise met partners zijn twee van de doelen die uitgewerkt worden binnen dit thema van de KMar-strategie. Uitwerking van de strategie langs deze lijnen zal de samenwerking tussen KMar en politie in de komende jaren verder vormgeven en kracht bijzetten.

III.1.3: Versterken diplomatiek netwerk

Om in te kunnen spelen op relevante cyberontwikkelingen in derde landen is het ook van belang dat de cyberkennis en capaciteit van Nederlandse vertegenwoordigingen in het buitenland verder wordt versterkt. Een uitbreiding van het cyberdiplomatennetwerk heeft grotendeels plaatsgevonden in 2023. Nadien waren er 34 functies op ambassades, consulaten en permanente vertegenwoordigen die geheel of gedeeltelijk waren gewijd aan cyber- en digitaliseringsvraagstukken. Deze ontwikkelingen dragen bij aan actie III.1.3.1 en III.1.3.2. In het kader van de taakstelling op het overheidsapparaat is ervoor gekozen een aantal van die functies op te heffen dan wel anders in te richten. Op de prioritaire posten in Europa, Noord-Amerika en de Indo-Pacific is de inzet ongewijzigd gebleven. Ook rapporteren posten frequenter over ontwikkelingen in derde landen die behulpzaam kunnen zijn bij de beleidsbepaling in Nederland op gebied van het tegengaan van statelijke en niet-statelijke dreigingen. Ook dragen posten actief bij aan het onder de aandacht brengen van relevante Nederlandse beleidsstukken en publicaties.

Het Ministerie van Buitenlandse Zaken (BZ) heeft zich afgelopen jaar in nauwe samenwerking met interdepartementale partners, wederom actief ingezet om het gedeelde situationele beeld van digitale dreigingen in EU- en NAVO-verband verder te versterken. Deze inzet bestond onder andere uit het verzorgen van meer technische en beleidsmatige briefings en Nederlandse best practices te delen. Daarbij is ook bij concrete casussen gedetailleerde informatie met EU en NAVO landen uitgewisseld, waarmee de basis is gelegd voor meer gezamenlijke duiding en vervolgacties.

In 2026 voert NCSC-NL het Cyber Capacity Building (CCB)-programma volledig zelfstandig uit, op basis van het vernieuwde convenant. De overeengekomen activiteiten voor 2026 sluiten direct aan bij de doelstellingen van de internationale cyberstrategie, met name op het gebied van internationale capaciteitsopbouw en normstelling. In 2026 zijn een CCB-training in Wenen (in opdracht van BZ en in samenwerking met de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE)) en een CCB-training Montenegro (in opdracht van BZ en in samenwerking met Western Balkans Cyber Capacity Centre (WB3C) gerealiseerd.

Daarnaast heeft in 2026 het NCSC niet alleen bestaande CCB-missies uitgevoerd, maar ook de CIIP- en OT-trainingsmodules doorontwikkeld in samenwerking met Clingendael, inclusief Train-the-Trainer-programma's. Hiermee wordt structurele kennisoverdracht gewaarborgd en is er een flexibele pool van

[29] Voortgangsbrief integrale aanpak cybercrime | Tweede Kamer der Staten-Generaal
[30] Het Cybercrimebeeld Nederland (CCBN) 2026

minimaal 10 gecertificeerde trainers per module gevormd, die intern binnen NCSC-NL zijn geïntegreerd. Dit versterkt de eigen capaciteit en zorgt voor schaalbaarheid in de uitvoering. Daarnaast zijn in 2026 twee internationale outreachactiviteiten gerealiseerd en worden er momenteel twee nieuwe trainingen voorbereid.

Verder biedt internationale samenwerking – bijvoorbeeld met de EU en de NAVO – aan Defensie een waardevolle springplank voor innovatie op cybergebied en voor het opzetten van gezamenlijke cybercapaciteiten. Het PESCO-project 'Cyber and Information Domain Coordination Center' (CIDCC) gaat over in het EU Cyber Defence Coordination Centre (EUCDCC), waarmee de coördinerende rol van Europa binnen cyber wordt versterkt. Zo wordt onder andere gewerkt aan de uitwisseling van Cyber Rapid Response Teams tussen deelnemende landen. Defensie draagt hier actief bij aan de uitwisseling van informatie en de coördinatie van cybercapaciteiten. Zoals genoemd onder actie 1.3.2 wordt de interne coördinatie op deelname aan oefeningen verbeterd.

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

III.2.1: Attributie en respons

Samen met partners blijft BZ investeren in versterking van het respons en attributie instrumentarium, zowel nationaal als via de EU en de NAVO. BZ heeft in samenwerking met de betrokken departementen actief gewerkt aan het adresseren van de dreiging door diplomatieke attributies en bewustwording via het co-sponsoren (medeondertekenen) van verschillende Cyber Security Advisories (CSA's) of door het eigenstandig uitbrengen van Nederlandse CSA's, zoals bijvoorbeeld het cyberadvies van de AIVD en MIVD over het gebruik van Signal en WhatsApp, gepubliceerd op 9 maart jl.[31]

Daarnaast blijft Nederland een voortrekkersrol spelen bij de totstandkoming van sancties tegen kwaadwillende cyberactoren. De EU nam op 13 juli van dit jaar het grootste pakket aan sancties tot nu toe onder het EU Cyber Sanctie Regime. In de begeleidende EU 27-verklaring attribueerde de EU een aantal specifieke cyberoperaties aan de FSB.[32] Nederland zette zich er vooral voor in om het sanctie instrument in te zetten tegen cybercriminelen wier activiteiten een bedreiging vormen voor de veiligheid van Nederland en rest van de EU.[33]

Statelijke actoren vergroten hun cybercapaciteiten ten behoeve van hun geopolitieke agenda. Om hier tegenwicht aan te bieden, gaat BZ van een reactieve, naar een proactieve omgang met cyberdreigingen. Daarbij hoort ook het acteren op zelfgekozen manieren en momenten. De beschikbare instrumenten (inlichtingen, diplomatiek, militair, weerbaarheid en steun aan derde landen) worden doelgerichter en meer geïntegreerd ingezet. Daarbij gaat aandacht uit naar patronen van dreiging in plaats van specifieke incidenten. Hiermee is de actie III.2.1.1 herijkt.

III.2.2: Defensieve en offensieve cybercapaciteiten

Defensie investeert in haar cybercapaciteiten en haar (inter)nationale positie in het cyberdomein, onder andere via de Defensie Cyberstrategie 2025[34] en de Defensienota 2026.[35] Dit stelt Defensie in staat verder bij te dragen aan de digitale bescherming van het Koninkrijk en bondgenoten, inclusief Defensietoeleveranciers en kritieke sectoren. Ook wordt geïnvesteerd in kennisontwikkeling, innovatie en opleidingen. Met de maatregelen en investeringen zorgt Defensie ervoor dat het cyberdomein zich blijft doorontwikkelen, dat Cyber Rapid Respnse Teams (CRRT's) en Cyber Mission Teams (CMT's) verder worden ontwikkeld als structureel beschikbare en schaalbare capaciteit, en dat de personele gereedheid via opleiding, training en realistische oefeningen continu wordt vergroot. De CRRT's en CMT's vormen een capaciteit voor cyberbijstand. Deze bijstandsconstructies gaan echter verder dan alleen cyber. Dit kan ook inzet op andere dimensies behelzen, zoals het inzetten van fysieke bewaking en beveiliging of bijdragen ter voorkoming en beperking van calamiteiten, ook in geval van grootschalige cyberincidenten.

Op het vlak van cyber werkt Defensie verder aan de mogelijkheden om bij ernstige cybercalamiteiten ondersteuning en militaire steun te kunnen verlenen. In de Defensie Cyberstrategie 2025 is nader beschreven hoe Defensie daarbij kan aansluiten op de nationale crisisbeheersingsstructuur en, waar van toepassing, internationale coördinatiemechanismen. Daarbij is het NLD JFC aangewezen voor de beoordeling van nationale en internationale cybersteunverzoeken en het DCC voor de aansturing van de daaruit voortvloeiende cyberinzet.

[31] Cyberadvies. Phishing via chatapps Signal en WhatsApp | AIVD
[32] Cyber / Russia: Statement by the High Representative on behalf of the European Union denouncing Russia's malicious cyber ecosystem targeting the EU, its member states and international partners - Consilium
[33] EU sanctioneert voor het eerst cybercriminele kopstukken | Nieuwsbericht | Rijksoverheid.nl
[34] Defensie Cyberstrategie 2025 | Rijksoverheid.nl
[35] Defensienota 2026 | Defensie.nl

Binnen Defensie wordt daarnaast gewerkt aan de verdere samenhang tussen de betrokken rollen, verantwoordelijkheden, mandaten en cybercapaciteiten. Eventuele inzet vindt plaats in afstemming met de bestaande interdepartementale overleg- en crisisstructuren.

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 begin 2026 een verkenning opgeleverd naar de mogelijkheden van actieve cyberverdedigingsmaatregelen. De resultaten van deze verkenning bieden een vertrekpunt voor het ontwikkelen van beleid voor een Nederlandse actieve cyberverdedigingsaanpak. Volgend op deze verkenning is vanaf halverwege 2026 door de NCTV, samen met betrokken departementen en diensten, geïnventariseerd hoe actieve cyberverdedigingsmaatregelen kunnen worden vormgegeven, waarna gestart zal worden met de implementatie van nieuwe maatregelen of versterking van maatregelen die reeds worden uitgevoerd. Een voorbeeld van actieve cyberverdediging is het Anti Phishing Shield (APS).[36]

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

III.3.1: Normatief kader

Het NLCS benadrukt het belang van internationale afspraken om de dreiging van destabiliserende cyberaanvallen het hoofd te bieden. 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. Het eindrapport van de Open Ended Working Group on Cyber (OEWG), waar de multilaterale onderhandelingen plaatsvonden, is aangenomen op 11 juli 2025. Hierbij heeft Nederland zich hardgemaakt voor de erkenning en bescherming van de publieke kern van het internet, alsmede voor het belang van de positie van internationaal humanitair recht binnen het normatieve kader. Daarmee is actie III.3.1.1 afgerond.

Daarnaast is in 2025 de OEWG formeel overgegaan in de UN Global Mechanism on Cyber. Mede door Nederlandse inzet is het 'Programme of Action', een centraal document in de strategiebepaling voor de EU, de basis geweest voor de permanente structuur van het mechanisme, ondanks tegenstand van landen die het normatief kader voor verantwoord statelijk gedrag binnen het cyberdomein proberen te ondermijnen. In zowel de Eerste Commissie als binnen het nieuwe VN Mechanisme maakt Nederland zich hard voor de implementatie van het normatieve kader (inclusief de 11 niet bindende vrijwillige normen voor verantwoord statelijk gedrag in het cyberdomein) en staat Nederland voor een actiegericht proces om uit te diepen hoe de toepassing van het internationaal recht binnen het cyberdomein kan worden bevorderd. De nieuw opgezette regelmatige werkgroepen bieden het mechanisme een versterkt platform voor praktische samenwerking, om cyberdreigingen te bestrijden en verantwoord statelijk gedrag in het cyberdomein verder te implementeren. Hiermee wordt de vrijwillige naleving van het normatieve kader voor verantwoord statelijk gedrag binnen het cyberdomein verder versterkt.

III.3.2: Internet governance

Nederland zet zich zowel nationaal als internationaal in voor een vrij, open, veilig en betrouwbaar internet. Zo is in nauwe samenwerking met ECP Platform voor de Informatiesamenleving is op 2 november 2026 opnieuw het Nederlandse Internet Governance Forum (NLIGF) georganiseerd. Het NLIGF brengt de Nederlandse stakeholders bij elkaar en vormt tevens de opmaat voor de Nederlandse deelname aan het wereldwijde multi-stakeholder platform IGF, wat in december in Nairobi plaats zal vinden.

Verder hebben het Ministerie van EZK en de RDI samen een dialoog opgezet met de Nederlandse deelnemers aan de Internet Engineering Task Force (IETF). Deze organisatie ontwikkelt de wereldwijd gebruikte standaarden die de publieke kern van het internet vormgeven. Met het bij elkaar brengen van de Nederlandse stakeholders wordt het momentum van de inzet vergroot en de aandacht voor het sociaal-economisch belang van een wereldwijd verbonden open, vrij en veilig internet versterkt.

Ook heeft Nederland, samen met het Verenigd Koninkrijk en Frankrijk, een aantal tekstvoorstellen voorbereid die namens een groot aantal Europese landen in november 2026 zullen worden ingebracht tijdens de Plenipoteniary Conference van de ITU (International Telecommunications Union) in November 2026. Deze voorstellen zien toe op de rol van ITU in het beheer en standaardisatie van het internet en hebben tot doel de multistakeholder methode van internet governance te beschermen en te versterken.

Tenslotte blijft Nederland zich, als vicevoorzitter van de Government Advisory Committee (GAC) van de Internet Cooperation for Assigned Names and Numbers (ICANN), inzetten voor een effectieve en efficiënte dialoog om het beleid rondom het beheer van het wereldwijde domeinnaamsystem (DNS) te

[36] Voortgangsbrief integrale aanpak cybercrime | Tweede Kamer der Staten-Generaal

verbeteren. Onder Nederlandse initiatief is o.a. overgegaan tot het oprichten van een werkgroep in de GAC die via capaciteitsopbouw deelname van overheidspartijen aan het internationale debat versterkt.

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

Het is belangrijk dat burgers bewust zijn van de digitale risico's. Om dit te bewerkstelligen, liepen er deze rapportageperiode verschillende publiekscampagnes, opgezet in samenwerking tussen de ministeries BZK, EZK en JenV, waaronder de campagnes 'Laat je niet interneppen' (JenV & BZK); 'Dubbel beveiligd is dubbel zo veilig' (JenV); De campagne 'Doe je updates' (EZK) is in 2025 gestopt.[37]

Om de weerbaarheid van de jeugd, het midden- en kleinbedrijf, senioren en laaggeletterden tegen cybercrime verder te verbeteren is daarnaast in 2023 is de City Deal Lokale Weerbaarheid Cybercrime met twee jaar verlengd, tot 2025. Op 31 december 2025 werd de City Deal afgesloten. Daarmee is de innovatiefase van deze actielijn afgerond. De projecten uit de City Deal zijn afgerond en beoordeeld, waarvan in totaal 35 succesvolle interventies zijn geborgd. Het Centrum voor Criminaliteitspreventie en Veiligheid verspreidt de succesvolle interventies onder gemeenten en andere partners. De verantwoording van de City Deal vindt nog plaats. BZK en JenV hebben in 2026 een vervolgaanpak gefinancierd en zijn voornemens om dit de komende jaren ook te blijven doen. Zo vormen de resultaten van de City Deal de basis van de verdere versterking van de lokale weerbaarheid in Nederland.[38]

Daarnaast wordt het jaarlijkse bewustzijn onderzoek Alert Online uitgevoerd.[39] Tot aan vorig jaar werden hiervoor kennis, houding en gedrag op het gebied van digitale weerbaarheid geanalyseerd, naast de informatiebehoeften op dit gebied, de verschillen tussen doelgroepen, en veranderingen hierin na verloop van tijd. In 2026 ligt de nadruk echter op een aantal gedragingen. Op basis hiervan kunnen volgende campagnes en activiteiten beter en gerichter worden ingestoken. De resultaten worden jaarlijks tijdens de start van de cybersecurity maand oktober gepresenteerd.

IV.1.2: Beveiligingsadvies burgers

Door het Centrum voor Criminaliteitspreventie en Veiligheid is een gratis ondersteuningstool voor onder meer Informatiepunten Digitale Overheid en bibliotheekmedewerkers ontwikkeld.[40] De tool biedt medewerkers van helpdesks en steunpunten inzicht in hulp en ondersteuningsmogelijkheden op gebied van digitale weerbaarheid. Dit najaar wordt onderzocht of de tool voldoende meerwaarde biedt om deze te continueren in de komende jaren.

[37] Zoals beschreven in *IV.1.2: Beveiligingsadvies burgers* blijft de informatie over het veilig gebruik van slimme apparaten wel beschikbaar op veiliginternetten.nl.
[38] Voor het slotstuk van de City Deal Lokale Weerbaarheid Cybercrime, zie: City Deal Lokale Weerbaarheid Cybercrime
[39] Voor meer informatie, zie: Alert Online - Alert Online
[40] De Tool Cyberweerbaarheid is beschikbaar via: Cyberweerbaarheid - Het CCV

Op basis van jaarlijks gebruikersonderzoek wordt de website veiliginternetten.nl continu doorontwikkeld en verbreed. Op veiliginternetten.nl vinden circa 1.5 miljoen burgers per jaar informatie en advies over hoe ze zich online kunnen beschermen. Het is ook hét centrale informatiepunt waar de cybersecurity publiekscampagnes van de overheid naartoe leiden. Daarnaast wordt dit platform verbreedt naar het Caribisch deel van het Koninkrijk en zal daarbij de regionale context en taal (Papiaments en Engels) centraal staan in de aangeboden informatie en adviezen.

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. De impactanalyse naar de haalbaarheid en betaalbaarheid van invoering van een uniforme domeinnaamextensie zoals overheid.nl of gov.nl voor overheidswebsites is gedeeld met de Tweede Kamer[41]. De impactanalyse vormt input voor vervolgbesluitvorming door de adviesraden van de overheid op gebied van IT en Communicatie. Voor het einde van 2026 zal hierover een update worden gegeven aan de Tweede Kamer via de verzamelbrief digitalisering.

Zoals eerder gerapporteerd, is het Register Internetdomeinen Overheid (RIO) is eind 2023 live gegaan. Op dit moment wordt gewerkt aan een technisch voorstel om uitwisseling van domeinen en domeinnaamregistratiegegevens tussen verschillende registers te vergemakkelijken om afronding van het RIO als de officiële bron van domeinregistraties van de overheid te versnellen. Deze actie is onderdeel geworden van het Nationaal Actieplan Webbeleid[42] dat op 1 juli 2025 is gedeeld met de Tweede Kamer. Op dit moment wordt gewerkt aan een technisch voorstel voor data-uitwisseling voor verdere doorontwikkeling van het RIO, bedoeld om aansluiting met het register te vergemakkelijken en bespoedigen.

Doel 2: Burgers reageren snel en adequaat op cyberincidenten

IV.2.1: Melding of aangifte doen van cybercrime fenomenen

In navolging van de digitale mogelijkheid voor burgers om aangifte te doen van ransomware, is dit sinds dit jaar ook mogelijk voor bedrijven. Dit kan via politie.nl onder ‘aangifte en melding doen’. Dit maakt onderdeel uit van de afspraken in de veiligheidsagenda. De verantwoording vindt plaats via de gebruikelijke kanalen, waaronder het jaarverslag van de politie.

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

IV.3.1: Curriculum

Het wetsvoorstel Wet herziening wettelijke grondslagen kerndoelen is op 9 december 2025 aangenomen. De inwerkingtreding wordt verwacht in 2027. De kerndoelen digitale geletterdheid gaan ook in op veiligheid, privacy en participeren in een gedigitaliseerde wereld.

De Subsidie Verbetering Basisvaardigheden wordt vanaf januari 2027 vervangen door structurele bekostiging voor de verbetering van de basisvaardigheden. Deze structurele financiering is voor alle scholen in het primair, voortgezet en (voortgezet) speciaal onderwijs. Het Expertisepunt Digitale Geletterdheid wordt sinds april 2026 bestuurd door Kennisnet, Beeld & Geluid en de KB.

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

IV.4.1: Cybersecurity arbeidsmarkt

De Nederlandse arbeidsmarkt is volop in beweging, er is brede krapte en vaardigheid en kennis eisen veranderen snel. Het kabinet heeft op basis van adviezen van onder meer Mario Draghi, Peter Wennink, de Sociaal-Economische Raad (SER) en de Staatscommissie Demografische Ontwikkelingen 2050 gekozen voor een gerichte aanpak op vier domeinen waar de grootste economische kansen voor Nederland liggen. Cybersecurity is hierin een doorsnijdend thema dat raakvlakken heeft met alle vier de domeinen. De vraag naar gekwalificeerd talent is in al deze sectoren groot, wat heeft geleid tot de ontwikkeling van de Talentstrategie door de ministeries OCW, EZK en SZW.[43]

Daarnaast werken de ministeries OCW, EZK en SZW sinds 2024 gezamenlijk aan het Actieplan Groene en Digitale Banen (hierna AGDB).[44] Dit is de overkoepelende paraplu waarbinnen

[41] *Kamerstukken II* 2025/26, 26643, nr. 1521
[42] Nieuw actieplan om het aantal overheidswebsites te verminderen | Rijksoverheid.nl
[43] Kabinet lanceert Talentstrategie voor toekomstige welvaart | Rijksoverheid.nl
[44] Actieplan Groene en Digitale Banen | Bedrijvenbeleid in beeld

werkgevers, werknemers, onderwijsinstellingen en de overheid met elkaar samenwerken met het doel om meer dan 1 miljoen digitaal geschoolden in 2030 te realiseren en de technische- en digitale arbeidsmarkt te versterken. Binnen het AGDB werken de ministeries van OCW, EZK en SZW verder aan verschillende initiatieven om cybersecuritytalent te ontwikkelen en beschikbaar te maken.

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
@nctv_nl

Oktober 2026