Nationaal Coördinator Terrorismebestrijding
en Veiligheid
Ministerie van Justitie en Veiligheid



Actieprogramma toekomstbestendige digitale weerbaarheid

November 2026

Bijschrift omslag
Controlekamer van de Eemshavencentrale in Groningen.

Leeswijzer

De cyberdreiging wordt steeds complexer. Ontwikkelingen zoals een verharde geopolitieke arena en de opkomst van nieuwe technologieën, waaronder artificiële intelligentie (AI), vragen om extra aandacht en maatregelen gericht op onze digitale weerbaarheid. Het is niet langer de vraag óf, maar wanneer Nederland te maken krijgt met een maatschappij ontwrichtend cyberincident.

Het verhogen van de digitale weerbaarheid blijft dan ook een constante wedloop, waarbij onze digitale weerbaarheid niet op hetzelfde tempo meegroeit als de capaciteiten van kwaadwillenden. Het wordt voor individuen en (kleine) organisaties steeds lastiger om die complexiteit te overzien en volledig zelf in staat te zijn cyberdreigingen af te weren. Om hier effectief tegengewicht aan te bieden is het van cruciaal belang om, naast het bestaande actieplan NLCS, aanvullende stappen te nemen. Deze worden beschreven in voorliggend actieprogramma “Toekomstbestendige digitale weerbaarheid”.

Het actieprogramma is gestoeld op twee prioriteiten:
1. Weerbaarheid structureel versterken
2. Preventief én proactief

De snelheid van ontwikkelingen in het cybersecuritylandschap, vraagt om een slagvaardige en wendbare overheid die in nauwe verbinding staat met de wetenschap en het bedrijfsleven. Een sterk fundament is randvoorwaardelijk om met alle andere ambities aan de slag te gaan. Tegelijkertijd vraagt de snelheid van de dreiging om het doen van een stap naar voren. Daarom kiezen we er bewust voor om enerzijds in te zetten op maatregelen die de weerbaarheid structureel versterken en anderzijds maatregelen te nemen waardoor we naast preventief, juist ook proactief optreden. Zo bouwen we samen met de markt en de wetenschap aan een duurzame digitale weerbaarheid. Verder geeft dit actieprogramma bestuurders richting bij het prioriteren van de benodigde maatregelen om de digitale weerbaarheid tegen onder andere AI-dreigingen te verhogen. De uitvoering van het actieprogramma valt binnen de bestaande budgettaire kaders.

Het programma heeft een looptijd tot eind 2027 en loopt daarmee gelijk op met de totstandkoming van de nieuwe cybersecuritystrategie die wordt gepresenteerd in 2028. Bepaalde acties onder het actieprogramma leveren direct resultaat, andere acties zijn een verdieping of verbreding van lopende activiteiten en leveren voorbereidende bouwblokken op in aanloop naar de nieuwe strategie. Maar de wereld om ons heen staat niet stil. Wij dus ook niet. Het voorliggende actieprogramma is een belangrijke stap, maar gedurende de looptijd van het actieprogramma zal continu worden bekeken wat er aanvullend nodig is om onze digitale weerbaarheid blijvend te verhogen in het licht van de ontwikkelingen.

Daarbij is de uitdrukkelijke uitnodiging aan het bedrijfsleven en de wetenschap om hier gezamenlijk over na te denken en aanvullende gezamenlijke acties op te formuleren.

Het actieprogramma gaat daarmee noodzakelijkerwijs verder dan alleen inzicht hebben in risico’s en het mitigeren van de nieuwe cyberdreigingen. Een toekomstbestendige digitale weerbaarheid kan namelijk alleen ontstaan als er geïnvesteerd wordt in de héle basis van het ecosysteem: van kennisontwikkeling en innovatie, tot marktversterking. De samenhang met andere programma’s en initiatieven, zoals het programma Quantumveilige Cryptografie Rijk en de Nationale Technologie Strategie, is dan ook van groot belang om de digitale weerbaarheid van de Rijksoverheid en de samenleving te verhogen.

Weerbaarheid structureel versterken

Een essentiële stap voor het verhogen van de digitale weerbaarheid is het op orde hebben van de basis: organisaties dienen te beschikken over basiskennis, informatie, producten, en ervaring om cyberincidenten te voorkomen, te doorstaan en ervan te kunnen herstellen. Organisaties, waaronder Rijksoverheid en medeoverheden dienen bestaande wet- en regelgeving toe te passen en hieraan prioriteit te geven ter bescherming van de digitale overheid. Het Cybersecuritybeeld Nederland 2026 laat wederom zien dat hier nog niet door alle organisaties aan wordt voldaan. Daarnaast is gezien de snelheid en ontwikkelingen in het dreigingslandschap de huidige “basis op orde’’ niet altijd meer voldoende en zorgen we waar nodig voor een versnelling en aanscherping hierop. Daarom zetten we hier met prioriteit op in. Waar van toepassing gelden deze acties ook voor Caribisch Nederland.

Weerbaarheid structureel versterken

Verbeteren digitale weerbaarheid(Rijks)overheid

Versterken basisbeveiligingsniveau (Rijks)overheid

Doel: De digitale weerbaarheid van de Rijksoverheid is versterkt doordat het basisbeveiligingsniveau is aangescherpt en Rijksoverheidsorganisaties beveiligingsrisico’s aanpakken, adviezen van o.a. het Nationaal Cyber Security Centrum (NCSC) en inlichtingen- en veiligheidsdiensten snel opvolgen en noodzakelijke maatregelen implementeren.

Coördinatie: BZK.

Actie: We zorgen ervoor dat de aanwijsbevoegdheid van departementale CISO’s en CISO Rijk toereikend is en daarom brengen we waar nodig hier wijzigingen in aan. Om te bepalen waar dat nodig is, voeren we eerst een onderzoek uit naar de (on)mogelijkheden van de huidige aanwijsbevoegdheid.

Actie: We zorgen ervoor dat het basisbeveiligingsniveau van de (Rijks)overheid aansluit bij de verhoogde dreiging. Hiervoor evalueren we de beveiliging van de werkplekken van de Rijksoverheid en benutten we de uitkomsten bij de overheidsbrede herijking van de Baseline Informatiebeveiliging Overheid.

Actie: Met het instellen van regionale aanjaagteams worden medeoverheden hands-on ondersteund bij het sluitend krijgen van preventieve en nieuwe maatregelen ter versterking van de weerbaarheid tegen het verhoogde dreigingsniveau.

Actie: We zorgen ervoor dat bestuurders binnen de (Rijks)overheid de Cyberbeveiligingswet-bestuurdersopleiding in 2027 volgen.

Actie: We publiceren een routekaart om te komen tot een cybersecuritystelsel voor het Caribisch deel van het Koninkrijk dat zo veel mogelijk aansluit bij het niveau van digitale bescherming en weer-baarheid in Europees Nederland in aansluiting op de motie El Boujdaini/Kathmann[1] hierover. Deze routekaart dient als een bouwblok voor de nieuwe cybersecuritystrategie die wordt gepubliceerd in 2028.

1 Kamerstukken II 2025/26, 36764, nr 16

Logging, monitoring & Security Operations Center (SOC)-stelsel

Doel: Rijksorganisaties worden proactief ondersteund om de impact van dreigingen te verminderen.

Coördinatie: BZK en NSCSC.

Actie: We voeren een beoordeling van logging en monitoring uit op inhoud, bewaartermijn, en bewaarplek. In de monitoring wordt ervoor gezorgd dat kleine(re) signalen op aanvallen en breaches niet verloren gaan in filtering om cyberdreigingen vroegtijdig te ontdekken.

Actie: We zetten “assume breach” in binnen de red teaming-aanpak van de Rijksoverheid en vernieuwen doorlopend de aanpak op basis van bevindingen.

Actie: Het Versterkte SOC-Stelsel Rijk (VSSR) wordt structureel onderdeel van de taken van het NCSC in overleg met betrokken stakeholders.

Actie: Er wordt verkend hoe een federatief SOC-stelsel bij medeoverheden kan worden opgezet, met inachtneming van bestaande arrangementen en initiatieven, leidend tot een concreet plan van aanpak.

Actie: We stimuleren organisaties om een kwetsbaarheden assessment, inclusief de kwetsbaarheden die voortkomen vanuit AI, te doen op de software. Tegelijkertijd zetten we voor de Rijksoverheidsorganisaties hierin een eerste stap.

Leveranciersmanagement binnen de (Rijks)overheid

Doel: Digitale kwetsbaarheden en risico’s stoppen niet bij de organisatiegrenzen. De Rijksoverheid werkt samen met partners en leveranciers die hun risicobeheersing op orde hebben.

Coördinatie: BZK.

Actie: We zetten een Rijksbreed verbetertraject op, in samenhang met de Inkoopeisen Cybersecurity Overheid (ICO) en Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO), t.a.v. beoordeling externe en kritieke leveranciers, als onderdeel van de kerntaken, en hoe diep ketens geanalyseerd dienen te worden.

Actie: In elke bestuurslaag wordt binnen één jaar minimaal één pilot uitgevoerd waarin bestuurders en inkopers bij de inkoop van ICT (en AI-tools) inzicht krijgen in afhankelijkheden, AI-gerelateerde dreigingen, alternatieven en exitmogelijkheden. De pilots leiden tot een praktische handreiking, die overheidsbreed beschikbaar wordt gesteld.

Verbeteren digitale weerbaarheid bedrijfsleven

Organisaties in publiek/privaat collectief helpen om de basis op orde te krijgen

Doel: De effectiviteit van de advisering richting organisaties gaat omhoog, zodat organisaties hun basismaatregelen op orde kunnen brengen en hierdoor digitaal weerbaarder worden.

Coördinatie: NCTV, EZK, NCSC en de inlichtingen- en veiligheidsdiensten.

Actie: De basismaatregelen van het NCSC worden getoetst aan het huidige dreigingsbeeld en krijgen waar nodig een update. Hierbij wordt concreet de invloed van AI meegenomen.

Actie: We nemen gericht actie om ervoor te zorgen dat basismaatregelen worden doorgevoerd bij kritieke, belangrijke en essentiële entiteiten. Een eerste stap hierin is het uitvoeren van een onderzoek naar de oorzaken van het achterblijven van de basismaatregelen, zodat we organisaties hierin effectiever kunnen ondersteunen.

Actie: De inlichten- en veiligheidsdiensten en het NCSC vertalen hun informatie sneller naar publiekelijk deelbare technische advisories met handelingsperspectief. Daarbij gaan we in gesprek met gebruikers hoe we deze advisories nog effectiever kunnen maken.

Het midden- en kleinbedrijf (mkb) beter voorbereiden op incidenten.

Doel: Het mkb en kleine organisaties zijn beter voorbereid op incidenten. Doordat de kennis van deze organisaties over cyberdreigingen is verhoogd, zijn zij beter voorbereid op incidenten en hebben zij meer inzicht in handelingsopties.
De functionaliteiten en faciliterende rol van intermediaire organisaties worden hiervoor ingezet.

Coördinatie: EZK en NCSC.

Actie: We versterken het Cyberweerbaarheidsnetwerk (CWN) door in te zetten op een centraal laagdrempelig punt ingericht voor mkb’ers met informatie bij en ter voorbereiding op incidenten, inclusief handelingskaders, informatie-uitwisselingmogelijkheden, en oefenformats. IT-dienstverleners, die voor mkb’ers het eerste aanspreekpunt bij een incident zijn, worden hier ook bij betrokken. Het centrale punt richt zich inhoudelijk vooral op de actuele dreigingen.

Actie: We zorgen met een nieuwe openstelling van de subsidieregeling “Versterken Cyberweerbaarheid” dat bestaande intermediaire netwerken die werken, goed worden geborgd door onder andere verdere verdieping en verbreding en daarbij goed kunnen aansluiten op de functionaliteiten van het CWN.

Gecoördineerde crisispreparatie

(Herijkte) inventarisatie en afwegingskader van incidentresponse (IR) capaciteit en afspraken met de private sector voor IR ondersteuning

Doel: Nederland bereidt zich voor op een (potentieel) toenemend aantal cyberincidenten dat gelijktijdig plaatsvindt. De AI-dreiging vergroot de kans op meerdere vergelijkbare incidenten tegelijkertijd of een verergering van de effecten van een enkel incident. De incident respons capaciteit kan hierdoor onder druk komen te staan. Deze acties dragen bij aan het in kaart brengen van de nodige capaciteit (zowel kwantitatief als kwalitatief) en de mogelijkheden voor tijdelijke bijstand van partners, om hier vervolgens afspraken over te kunnen maken.

Coördinatie: NCTV, BZK en NCSC

Actie: Om inzicht te verkrijgen in de benodigde en beschikbare incidentrespons capaciteit en expertise bij de Rijksoverheid ten tijde van één of meerdere gelijktijdige cyberincidenten voeren we een inventarisatie uit.

Actie: We richten een efficiëntere incidentresponse in, met aandacht voor schaarste en inzet van capaciteit en ontwikkeling van de juiste kennis en tooling. Ten behoeve hiervan worden afspraken gemaakt over de uitwisseling en samenwerking van personeel inclusief een onderzoek de randvoorwaarden. Dit doen we onder andere voor de uitwisseling en samenwerking van personeel tussen het NCSC, de inlichtingen- en veiligheidsdiensten, Defensie en de politie en de rol van het Nationaal Reponse Netwerk (NRN) en het Joint SOC-stelsel. Bij het maken van afspraken wordt aangesloten bij het Rijksbrede wegingskader schaarste.

Actie: We voeren gesprekken met private partijen over samenwerkingsafspraken met betrekking tot incidentondersteuning tijdens cyberincidenten- en crisis en brengen de randvoorwaarden en afwegingskaders voor de ondersteuning van private partijen in kaart.



Preventief én proactief

Preventief én proactief

De huidige dreiging vraagt om een aanpak waarbij we niet alleen afwachtend zijn, maar ook zelf actief stappen ondernemen om de impact van de dreiging te beperken. Door een stap naar voren te zetten beschermen we, waar mogelijk, organisaties voordat de dreiging hen bereikt.

Om voorbereid te zijn op het nu én de toekomst werken we ook aan investeringen en onderzoek waarmee we de kennis en capaciteiten in Nederland op het gebied van AI voor cyber opbouwen, en zorgen we voor digitale producten die beter ‘cybersecure by design en default’ zijn. Hiermee zorgen we ervoor dat we niet achter raken en voorbereid zijn op wat op ons afkomt. Dit kan alleen door nauwe samenwerking tussen overheid, markt, wetenschap en innovatiepartijen: samen begrijpen hoe de wereld verandert en welke kennis en nieuwe technologie noodzakelijk zijn, en het aansterken van de markt zodat er daadwerkelijk adequate producten beschikbaar komen.

Verkleinen aanvalsoppervlak

Ontwikkelen scanplatform	
Doel: Dreigingen worden proactief aangepakt door het aanvalsoppervlak (de te beschermen doelgroepen en netwerken) van Nederland in kaart te brengen en organisaties actief te notificeren bij gevonden kwetsbaarheden. **Coördinatie:** NCTV en NCSC.	**Actie:** We stellen het NCSC in staat om een eigen (netwerk) scanplatform te ontwikkelen om kwetsbaarheden te ontdekken, waarbij wordt gezorgd voor aansluiting met doelwit- en slachtoffernotificatie op de genormaliseerde scandata. Als eerste stap verkennen we wat er nodig is om dit platform te realiseren.

Versneld (en waar mogelijk geautomatiseerd) patchen

Doel: Organisaties (zowel overheden als bedrijven) zijn voorbereid op de afnemende beschikbare tijd om te patchen als gevolg van het groeiende tempo van cyberaanvallen door onder andere AI.

Coördinatie: BZK, EZK, NCTV en NCSC.

Actie: We stimuleren organisaties om adviezen van het NCSC over nieuwe ontwikkelingen, bijvoorbeeld rondom nieuwe technologieën zoals AI, op te nemen in de beveiligingsmaatregelen.

Actie: We brengen in kaart wat er op technische en organisatorisch vlak nodig is om geautomatiseerd te kunnen patchen en wat daarbij de randvoorwaarden en risico's zijn. Daarbij sluiten we zo veel mogelijk aan bij verplichtingen over patchen in de Cyber Resilience Act, de Cyberbeveiligingswet en de ABRO.

Uitbreiden en doorontwikkeling actieve cyberverdediging

Doel: We beschermen internetgebruikers door hen te herleiden naar een waarschuwingspagina in het geval zij een malafide website dreigen te bezoeken. Daarnaast hebben we zicht op digitale dreiging en nemen deze waar mogelijk preventief weg bij overheden, kritieke infrastructuur, topsectoren en ABDO/ABRO partijen.

Coördinatie: NCTV.

Actie: We breiden het aantal deelnemers van het Anti Phishing Shield (APS) uit. We zetten een nader onderzoek op naar andere mogelijkheden die APS kan bieden om proactief de weerbaarheid van Nederland tegen online dreigingen te vergroten.

Actie: Om preventie en monitoring schaalbaar te krijgen werken we aan het kunnen aanbieden van protective DNS (Protective Domain Name Service) aan doelgroepen van het NCSC, het Ministerie van Defensie, en het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties. Hiervoor nemen we de eerste stap in de ontwikkeling van protective DNS.

Inspelen op nieuwe technologie

Strafbaarstelling malafide AI-modellen

Doel: We hebben inzicht in wettelijke mogelijkheden om op te treden tegen ontwikkelaars en verspreiders van malafide AI-tools en nemen afhankelijk van de bevindingen eventueel aanvullende maatregelen.

Coördinatie: JenV en OM.

Actie: Ondersteunend aan een effectieve aanpak van AI-modellen stelt het OM een rapport op waarin de huidige interventiemogelijkheden zijn uitgewerkt en wat daarin op dit moment mogelijk ontbreekt om effectief op te treden tegen ontwikkelaars van malafide AI-modellen. Op basis van de bevindingen wordt vervolgens bepaald of aanvullende maatregelen nodig zijn om via het strafrecht een effectieve aanpak te kunnen formuleren.

Intensivering migratie quantumveilige cryptografie

Doel: Cryptografie is een fundament van onze digitale infrastructuur. Het is zaak dat we hierop kunnen vertrouwen. Door de komst van de quantumcomputer komt dit in het geding. Dit levert risico's op voor informatiebeveiliging en bedrijfscontinuïteit. Daarom moeten we ons voorbereiden op de migratie naar quantumveilige cryptografie en publiek-private samenwerking op dit thema versterken.

Coördinatie: EZK.

Actie: We maken quantum technologie en het risico daarvan op cryptografische informatiebescherming een focuspunt in het CWN en in de publiek-private samenwerking. Hiertoe wordt afgestemd met het programma Quantumveilige Cryptografie NL (EZK).

Versterken publiek-private samenwerking, innovatie en markt

Inzetten op eigen AI-capaciteit

Doel: In publiek-private partnerschappen wordt (waar mogelijk praktijkgericht) eigen Nederlandse kennis en vaardigheid van AI-technologie voor cybersecurity doeleinden opgebouwd, waarbij de neutraliteit tussen overheid en markt wordt gewaarborgd zodat publieke en private inzet elkaar versterken.

Actie: We houden Nederland onder de motorkap veilig door het starten van een verkenning naar een publiek-privaatplatform in de vorm van een digitale "AI-wasstraat". Indien deze verkenning een positief resultaat kent, zal het NCSC in staat worden gesteld om deze AI-wasstraat samen met publieke en private partners, zoals Digital Holland, de Prometheus werkgroep en betrokken departementen, op te zetten.

Coördinatie: NCSC en EZK.

Actie: We verkennen de mogelijke oprichting van een Nederlands AI-Veiligheidsinstituut[2], waarbij de focus ligt op de impact van AI op cybersecurity en de nationale veiligheid. Hierbij wordt rekening gehouden met bestaande instituten, zowel Europees als nationaal, die de overheid en private partijen al van advies en expertise voorzien op het gebied van AI.

Coördinatie: EZK, BZK en NCTV.

2 Bijvoorbeeld naar voorbeeld van reeds bestaande Europese AI Security Institutes

Versnellen “House of Cyber”

Doel: Door samen te werken in een “House of Cyber”, zowel in de koude, lauwe als warme fase, kunnen incidenten en dreigingen beter worden aangepakt en gaan we efficiënter en effectiever om met de beperkte cybercapaciteit. Het House of Cyber zorgt daarmee voor het bij elkaar brengen van publieke en private partijen in het cyberecosysteem, waar nodig fysiek.

Coördinatie: NCSC.

Actie: We werken versneld aan de totstandkoming van het “House of Cyber”: een publiek-private samenwerking waar het NCSC samen met publieke operationele en private partijen 24/7 werkt aan de digitale weerbaarheid van Nederland.

Signalerings- en foresighting team op het snijvlak van AI en Cybersecurity

Doel: We hebben structureel zicht op de veranderingen op het gebied van AI in het cybersecuritylandschap. Deze inzichten gebruiken we voor bruikbare advisering naar overheid, innovatie en bedrijfsleven.

Coördinatie: NCTV, EZK, BZK en NCSC in samenwerking met betrokken departementen en TNO.

Actie: We voeren een verkenning uit naar het uitbouwen van een breed gedragen, publiek-private werkgroep die ‘horizon scanning’ en foresighting kan uitvoeren op het snijvlak van AI en Cybersecurity. Bij voldoende draagvlak en deelneming wordt gedurende een afgesproken periode een proefproject uitgevoerd en geëvalueerd.

Cybersecurity Incubator Netwerk

Doel: We versterken de innovatiemogelijkheden voor startende bedrijven in de cybersecuritysector en dragen bij aan de ontwikkeling van business skills op de cybersecuritymarkt.

Coördinatie: EZK in samenwerking met Yes!Delft, ROMs, regionale cybersecurity innovatie coalities (Zuid-Holland, Brabant) en Digital Holland (Actieagenda Cybersecurity Technologieën).

Actie: We richten een Nationaal Cybersecurity Incubator Netwerk op met specifieke aandacht voor AI-technologie in cybersecurity. In de looptijd van het actieprogramma wordt een nationale kerngroep geformeerd en een opbouwprogramma gelanceerd.

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

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

november 2026