Ministerie van Justitie en Veiligheid

> Retouradres Postbus 16950 2500 BZ Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.rijksoverheid.nl/jenv

**Onze referentie**
8124184

**Bijlagen**
3

Datum 6 november 2026
Betreft Cybersecuritybeeld Nederland 2026 en Voortgang Nederlandse Cybersecuritystrategie

Nederland is één van de meest gedigitaliseerde landen ter wereld. Daardoor raakt de digitale dreiging onze hele samenleving. Het is niet langer de vraag óf, maar wanneer Nederland te maken krijgt met een maatschappij ontwrichtend cyberincident.

Persoonsgegevens die online worden gepubliceerd na een datadiefstal door cybercriminelen, overheidsorganisaties die worden gecompromitteerd en camera's langs militaire routes die worden gehackt. Wanneer digitale systemen uitvallen – of dat nu door een kwaadwillende cyberaanval is of door een niet-kwaadwillende storing – zijn de gevolgen onmiddellijk en ingrijpend. Omdat onze samenleving draait op de digitale infrastructuur, is de digitale weerbaarheid een kwestie die iedereen raakt.

Maar deze digitale weerbaarheid staat onder druk. Statelijke actoren en cybercriminelen die het op Nederland hebben gemunt, vallen de digitale infrastructuur voortdurend aan. Verschuivende en verhardende geopolitieke verhoudingen brengen statelijke actoren ertoe extra te investeren in hun cybercapaciteiten. Daarbij werken zij soms samen met cybercriminelen die op hun beurt ook steeds professioneler te werk gaan. Daarbovenop komt dat de ontwikkeling van artificiële intelligentie (AI) modellen een vlucht heeft genomen. AI wordt door kwaadwillenden gebruikt om de snelheid, schaal en efficiëntie van cyberaanvallen te vergroten. De verdere ontwikkeling van AI kan het dreigingslandschap de komende jaren drastisch veranderen.

Dit beeld wordt ondersteund door het Cybersecuritybeeld Nederland (CSBN) 2026, opgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Hoewel er door de overheid en het bedrijfsleven veel wordt gedaan om Nederland tegen de cyberdreiging te weren, groeit de weerbaarheid niet mee op het tempo dat nodig is om deze capaciteiten van kwaadwillenden bij te houden. Hierdoor ontstaat er een verdere scheefgroei tussen de cyberdreiging en de cyberweerbaarheid waar nu actie op nodig is. In het kader hiervan hebben de NCTV, het Nationaal Cyber Security Centrum (NCSC), de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- Veiligheidsdienst (MIVD), het Openbaar Ministerie (OM), CIO Rijk en de Politie op 24 september 2026 een statement gepubliceerd over de impact van AI op cybersecurity, en daarbij bestuurders opgeroepen om prioriteit te geven aan cybersecurity en hun verantwoordelijkheid hiervoor in te zetten.[1]

[1] AI versnelt en vergroot de dreiging: nu handelen noodzakelijk | Nationaal Coördinator Terrorismebestrijding en Veiligheid 2 oktober 2026

Ook op internationaal niveau neemt de aandacht voor het snel veranderende cyberdreigingslandschap toe. De Europese Commissie heeft onlangs een Actieplan voor Cybersecurity & AI gepubliceerd, voortbouwend op onder andere de EU AI verordening. Dit actieplan heeft als doel het veilige en verantwoorde gebruik van AI te ondersteunen en tegelijkertijd de cyberbeveiliging van Europa te versterken.

Met de implementatie van de Nederlandse Cybersecuritystrategie 2022-2028 (NLCS) en het onderliggende actieplan biedt het kabinet tegenwicht tegen deze ontwikkelingen. Maar dit is nog niet genoeg. Om het hoofd te kunnen bieden aan de huidige dreiging moeten we een extra stap zetten. Daarom heeft het kabinet een aanvullend actieprogramma 'Toekomstbestendige Digitale Weerbaarheid' opgesteld. Hierop geef ik in deze brief een toelichting.

Namens het kabinet bied ik u hierbij het CSBN 2026, de Voortgangsrapportage NLCS 2026 en het aanvullend actieprogramma 'Toekomstbestendige Digitale Weerbaarheid' aan. Verder neem ik u in deze brief mee in de ontwikkelingen van de dreiging zoals beschreven in het CSBN, de voortgang en de uitvoering van de NLCS en worden er een aantal moties en toezeggingen afgedaan.

*Cybersecuritybeeld Nederland 2026*

Het CSBN 2026 laat zien dat de capaciteiten en activiteiten van statelijke actoren en cybercriminelen toenemen. Statelijke actoren zoals China, Rusland, Iran en Noord-Korea vergroten hun cybercapaciteiten als onderdeel van hybride en militaire conflictvoering. Nederlandse (overheids)organisaties, bedrijven en burgers zijn geregeld slachtoffer van hun aanvallen. Daarnaast is cybercriminaliteit inmiddels uitgegroeid tot een effectief georganiseerd ecosysteem, waarbij cybercriminelen zich in toenemende mate lijken te richten op het stelen van grote hoeveelheden data, om daarmee bedrijven en organisaties af te persen.

Dit CSBN laat voor het eerst zien dat cyberactoren AI aantoonbaar inzetten bij cyberaanvallen. AI vergroot de snelheid, schaal en efficiëntie van cyberaanvallen. De komende jaren zal AI het cyberlandschap ingrijpend veranderen en de dreiging verder versterken. Organisaties en bedrijven zijn volgens het CSBN onvoldoende voorbereid op deze technologische ontwikkelingen.

Hoewel er verschillende maatregelen worden genomen om Nederland tegen deze veranderende cyberdreiging te verdedigen, groeit de digitale weerbaarheid van Nederlandse organisaties en bedrijven niet in hetzelfde tempo mee. Hierdoor ontstaat verdere scheefgroei tussen de cyberdreiging en de digitale weerbaarheid. Dit vormt een ernstig risico voor de nationale veiligheid.

Wanneer AI alle onderdelen van cyberaanvallen verder automatiseert of zelfs autonoom uitvoert, worden cyberaanvallen nog sneller, grootschaliger en geavanceerder. Als de digitale weerbaarheid van Nederlandse (overheids)organisaties en bedrijven dan niet aanzienlijk verbetert, zal het aantal cyberincidenten de komende jaren fors toenemen. Dit zou met name een ongelijk speelveld vormen voor kleine organisaties en het midden- en kleinbedrijf (mkb).

*Actieprogramma Toekomstbestendige Digitale Weerbaarheid*

Er is nú actie nodig om tegenwicht te bieden aan deze alarmerende ontwikkelingen. De implementatie van de NLCS is én blijft een belangrijke basis voor het versterken van onze digitale weerbaarheid. Maar het is niet langer genoeg: de veranderende dreiging vraagt om stap naar voren en om een aanpassing aan de nieuwe realiteit. 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. De ingrijpende veranderingen in het cybersecuritylandschap vragen om een intensivering van de huidige aanpak. Daarom presenteert het kabinet het actieprogramma 'Toekomstbestendige Digitale Weerbaarheid'.

Het doel van dit actieprogramma is om te voorkomen dat onze digitale weerbaarheid achterblijft bij de dreigingen die in hoog tempo op ons afkomen. Dit doen we door aan de slag te gaan met het verhogen van de weerbaarheid van nú, maar ook door te bouwen aan een stevig fundament voor de toekomst. De ontwikkelingen in het cyberdreigingslandschap vragen namelijk om een weerbaarheid die niet alleen bestand is tegen de dreigingen van vandaag, maar ook kan meegroeien met die van morgen.

Hierbij leggen we de focus op twee prioriteiten: de weerbaarheid structureel versterken en maatregelen waardoor we preventief én proactief kunnen optreden. De prioriteiten in het actieprogramma zijn niet één-op-één te herleiden tot een specifieke pijler, maar juist pijleroverstijgend: ze raken meerdere onderdelen van de NLCS tegelijk en worden integraal benaderd. Het actieprogramma gaat daarmee noodzakelijkerwijs verder dan alleen het voorkomen van de nieuwe cyberdreigingen.

Een weerbare digitale samenleving kan namelijk alleen ontstaan als geïnvesteerd wordt in de héle basis van het ecosysteem. Cyberdreigingen houden zich niet aan organisatiegrenzen, sectoren of landsgrenzen. Cybersecurity is een gezamenlijke verantwoordelijkheid, waarbij samenwerking tussen overheid, bedrijfsleven en wetenschap cruciaal is om de dreiging het hoofd te bieden.

*Voortgang Nederlandse Cybersecuritystrategie in 2026*
De NLCS blijft daarbij het fundament bieden om onze digitale weerbaarheid te versterken. Het afgelopen jaar zijn er dan ook belangrijke stappen gezet om de NLCS te implementeren. In de Voortgangsrapportage NLCS ga ik namens het kabinet uitgebreider in op de concrete stappen die er in de afgelopen rapportageperiode zijn gezet. Graag licht ik in deze brief een paar belangrijke mijlpalen van de rapportage uit.

Met de inwerkingtreding van de Cyberbeveiligingswet (Cbw) en de Wet Weerbaarheid Kritieke Entiteiten (Wwke) op 15 augustus 2026 heeft Nederland een belangrijke stap gezet in het versterken van de digitale en fysieke weerbaarheid van organisaties tegen toenemende dreigingen. Met de Cbw zijn ruim 8.000 organisaties in Nederland verplicht om passende en evenredige technische-, beveiligings- en organisatorische maatregelen te treffen ten aanzien van hun netwerk- en informatiesystemen. Een andere belangrijke stap die is gezet ten behoeve van de digitale weerbaarheid van de Rijksoverheid is de invoering de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO). De ABRO-eisen gelden vanaf 1 januari 2026 en zijn er voor bedrijven die voor de rijksoverheid en de politie een opdracht uitvoeren met risico's voor de nationale veiligheid. Hiermee worden deze risico's, zoals cyberaanvallen, verkleind.

Daarnaast wil ik u informeren over een aanvulling op datgene wat in de memorie van toelichting bij het voorstel voor de Cbw[2] is opgemerkt over de wijze waarop in de praktijk de taken van de bevoegde autoriteit in relatie tot de meldplicht in de Cyberbeveiligingswet worden uitgeoefend. Op grond van artikel 25 van de Cbw zijn essentiële entiteiten en belangrijke entiteiten verplicht om significante incidenten te melden bij zowel hun Computer Incident Response Team (CSIRT) als bij hun bevoegde autoriteit. De bevoegde autoriteit betreft de toezichthoudende instantie én de vakminister. Voor het doen van deze verplichte meldingen is een centraal meldportaal ingericht dat wordt beheerd door het NCSC. In de memorie van toelichting van de Cbw is toegelicht dat (alleen) de toezichthoudende instantie van het ministerie geacht wordt de wettelijke taken van de bevoegde autoriteit, waaronder het in ontvangst nemen van verplichte meldingen, in de praktijk uit te oefenen. Als gevolg hiervan ontvingen alleen het betreffende CSIRT én de toezichthoudende instantie de verplichte meldingen en was de hiervan deel uitmakende informatie ('meldingsinformatie') niet direct beschikbaar voor de betreffende vakminister. Echter geldt dat de bovengenoemde wettelijke taken van de bevoegde autoriteit in de praktijk ook, naast de toezichthoudende instantie, worden uitgeoefend door het vakdepartement ("vakminister") én dat ten behoeve daarvan verplichte meldingen daarom eveneens bij het vakdepartement moeten worden gedaan. De vakministers hebben daarnaast meldingsinformatie nodig om beleidskeuzes te maken ten behoeve van de sector waarvoor zij beleidsverantwoordelijke zijn om zo de gevolgen van het incident zo snel mogelijk te kunnen beperken. Het bovenstaande is inmiddels ingeregeld in het centrale meldportaal, waardoor verplichte meldingen van entiteiten, zonder extra benodigde handelingen voor die entiteiten, ook voor het vakdepartement ("vakminister") direct beschikbaar wordt.

Verder wordt in het CSBN geschetst dat met name voor mkb'ers het op peil brengen en houden van de cyberweerbaarheid een uitdaging is. Inzet op publiek-private samenwerking is daarom essentieel. 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. Hiermee is het vernieuwde NCSC er voor álle organisaties in Nederland, en dus ook voor het mkb. Zij kunnen nu informatie, tools en adviezen ontvangen van het NCSC om hiermee hun digitale weerbaarheid te verhogen. Verder werken in het Cyberweerbaarheidsnetwerk (CWN) overheidsinstanties, vitale bedrijven en sectorpartijen, waaronder kleine organisaties, samen zodat zij dreigingen beter kunnen zien én sneller kunnen reageren.

Tot slot is er in het CSBN aandacht voor de impact van datadiefstal door cybercriminelen. Voor de voortgang op de integrale aanpak op cybercrime verwijs ik u graag naar de Kamerbrief van 9 september jl.[3]

*Cyber Security Raad*
De Cyber Security Raad (CSR) heeft als taak het kabinet te adviseren over de uitvoering en uitwerking van de NLCS. De raad constateert dat het cybersecuritystelsel gedurende de looptijd van de NLCS aanzienlijk is versterkt. Met nieuwe wet- en regelgeving zijn

[2] Kamerstukken II, 2024/2025, 36764, nr. 3
[3] Kamerstukken II, 2026/2027, 26643, nr. 1555.

bovendien belangrijke stappen gezet om zowel de cybersecurity van organisaties als de digitale veiligheid van producten en diensten te vergroten. Tegelijkertijd constateert de raad dat het huidige strategische kader onvoldoende inzicht biedt in de resultaten van de ingezette acties en in de prioritering daarvan.

Daarnaast stelt de CSR de vraag of een langdurig strategisch kader voor het Nederlandse cybersecuritybeleid nog volstaat in een wereld die wordt gekenmerkt door een steeds onvoorspelbaarder dreigingslandschap en snelle technologische ontwikkelingen. De leden wijzen daarbij in het bijzonder op ontwikkelingen op het gebied van AI, de inzet van cyberaanvallen als onderdeel van hybride oorlogsvoering, toenemende strategische afhankelijkheden en de noodzaak van technologische autonomie. Ook benadrukt de CSR terecht het belang van publiek-private samenwerkingen en het gebruik van wetenschappelijke kennis. Een nauwere koppeling tussen onderzoek, beleid en operationele praktijk is essentieel voor het behalen van de doelstellingen uit het actieplan.
Het kabinet deelt de zorgen van de CSR. Hoewel de NLCS een belangrijke basis vormt voor het Nederlandse cybersecuritybeleid, vraagt de ontwikkeling naar een complexer en onvoorspelbaarder dreigingslandschap om versterking en wendbaarheid. Het actieprogramma 'Toekomstbestendige Digitale Weerbaarheid' is daarin een belangrijke eerste stap.

*Moties en toezeggingen*
Onderstaande moties en toezegging worden middels deze Kamerbrief en de voortgangsrapportage NLCS 2026 afgedaan.

- Motie 36 764, nr. 16 van de leden El Boujdaini (D66) en Kathmann (PRO) waarin het kabinet wordt verzocht aan een concreet plan of een routekaart te werken 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 weerbaarheid in Europees Nederland, en dit samen met het Caribisch deel te doen. Het kabinet hecht waarde aan een goede aansluiting van het Caribisch deel van het Koninkrijk op de NLCS. Daarom wordt in de opvolger van de huidige NLCS expliciet aandacht besteed aan de BES-eilanden. De CAS-eilanden ontwikkelen hun eigen strategie. In voorbereiding hierop wordt in het najaar van 2026 een meerdaagse Caribische cybersecuritystelsel bijeenkomst met regionale stakeholders georganiseerd om te komen tot een concreet plan of een gedragen roadmap met inachtneming van de Caribische context. Het inventariseren van de benodigde centrale en structurele financiering ten behoeve van het opzetten en onderhouden van dit stelsel, is onderdeel van de routekaart. Hiermee beschouw ik deze motie als afgedaan.
- Motie 36 764, nr. 17 van het lid Zwinkels (CDA) waarin de regering wordt verzocht in kaart te brengen hoe de uitwisseling van dreigingsinformatie en geleerde lessen binnen ketens kan worden versterkt, in het bijzonder zodat ook kleinere bedrijven daarvan beter kunnen profiteren, en Motie 26 643, Nr. 1341 van de leden Michon-Derksen en Kathmann (PRO) waarin de regering wordt verzocht om een zichtbaar en benaderbaar loket over cybersecurity te borgen

voor mkb ondernemers. Zoals uitgebreider beschreven op pagina 2 en 7 van de voortgangsrapportage is met de integratie van het NCSC met het DTC en het CSIRT-DSP de dienstverlening van het NCSC gericht op alle organisaties in Nederland waaronder het mkb. Hiermee is één duidelijk aanspreekpunt, snelle en gerichte informatiedeling, en toegang tot een uitgebreid netwerk van cyberexperts tot stand gekomen waarbij zorgvuldig is gekeken naar de behoefte van verschillende doelgroepen waaronder het mkb. Daarnaast wordt door organisaties binnen het Cyberweerbaarheidsnetwerk informatie en kennis met elkaar uitgewisseld om samen sterker te staan tegen de dreiging. Ook voor kleinere organisaties is hierin een rol weggelegd. Hiermee beschouw ik deze beide moties als afgedaan.

- Motie 36 764, nr. 19 van de leden Kathmann (PRO) en Dassen (VOLT) waarin de regering wordt verzocht om één centraal meldportaal in te richten voor organisaties en zich in te spannen om hier, naast de meldingen die volgen uit de Cbw en de Wwke, ook zoveel mogelijk andere soorten meldingen in te kunnen maken. Op dit moment is het mogelijk om via MijnNCSC portaal meldingen op basis van wetgeving te doen: Cbw, Wwke, Digital Operational Resilience Act (DORA), CRA,  Netcode. Daarmee is het voor cybersecuritywetgeving mogelijk voor organisaties om te melden via één meldportaal. Hiermee beschouw ik deze motie als afgedaan.
- Motie 36 945, Nr. 12 van het lid El Boujdaini waarin de regering wordt verzocht om de Kamer uiterlijk voor het einde van 2026 een plan van aanpak te sturen waarin uiteen wordt gezet welke stappen het kabinet zet om de relatief dalende cyberweerbaarheid van Nederland te verbeteren en op welke wijze inzet op de legacyvernieuwing hieraan bijdraagt. Hierin is de toezegging TZ202606-161 aan het lid El Boujdaini meegenomen. Recente inspanningen hebben ertoe geleid dat Nederland is gestegen tot de 19e plek in de NCSI index. Daarnaast is er, zoals beschreven in deze kamerbrief, een actieprogramma opgesteld om de cyberweerbaarheid van Nederland verder te verhogen. Hiermee beschouw ik deze motie als afgedaan.
- Motie 36 084, Nr. 10 van het lid Leijten (SP) waarin de regering wordt verzocht bij de evaluatie van de wet (Wbni) en/of het wegingskader specifiek aandacht te besteden aan toezicht op het delen van de gegevens, de verwerking en het bewaren daarvan. Met de komst van de Cbw is er geen evaluatie meer gedaan van de Wbni. Het ‘toezicht op het delen van de gegevens, de verwerking en het bewaren daarvan’ wordt daarom meegenomen in de evaluatie die twee jaar na inwerkingtreding van de Cbw zal plaatsvinden. Hiermee beschouw ik deze motie als afgedaan.

De Minister van Justitie en Veiligheid,

D.M. van Weel

**Datum**
6 november 2026