Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1437

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 26 november 2025

De impact op de strafrechtsketen nadat het netwerk van het Openbaar Ministerie offline werd gehaald vanwege een Citrix-kwetsbaarheid, een cyberaanval bij het laboratorium Clinial Diagnostics waar honderdduizenden medische persoonsgegevens zijn gelekt en cyberspionagepogingen van Russische en Noord-Koreaanse staatshackers, tonen aan dat de toegenomen dreiging en digitale weerbaarheid nog niet in balans zijn.[1]

Daarmee is een versteviging van de inzet op de uitvoering van de Nederlandse Cybersecuritystrategie (NLCS) noodzakelijk. Dit wordt ook geconstateerd in het Cybersecuritybeeld Nederland (CSBN). In een sterk veranderende geopolitieke situatie nemen cyberdreigingen toe. Dit vereist permanente aandacht voor de weerbaarheid van de samenleving. Nederland moet weerbaarder worden tegen statelijke en niet-statelijke cyberactoren die het gemunt hebben op Nederland.

Digitale aanvallen kunnen ernstige consequenties hebben voor de continuïteit van organisaties en een grote impact hebben op onze samenleving. Het risico op een aanval kan niet weggenomen worden, maar kan met behulp van weerbaarheidsmaatregelen wel zoveel mogelijk worden verkleind. Nederlandse organisaties dienen de dreiging serieus te nemen en maatregelen te treffen om zich te beveiligen. Weerbaarheid tegen deze aanvallen gaat niet alleen om het inrichten van preventieve maatregelen en vroegtijdige detectie, maar ook om het snel kunnen handelen bij incidenten en het organiseren van herstelvermogen. Dit maakt dat bestuurders van zowel publieke als private organisaties een essentiële rol hebben te vervullen om cybersecurity risico's te beheersen en dat uitdragen zowel binnen als buiten hun organisatie.

Het kabinet neemt de risico's van digitalisering serieus en onderstreept de noodzaak om zich met urgentie in te blijven zetten op de uitvoering van de

[1] Kamerstuk 2024–2025, 29 628-1223; Kamerstuk 2024–2025, 32 761-330; Kamerstuk 2025–2026, 2025Z14918

kst-26643-1437
ISSN 0921 - 7371
's-Gravenhage 2025

NLCS, de implementatie van de herziene richtlijn Netwerk- en Informatiebeveiliging (NIS2) en de Cyber Resilience Act (CRA).

Tijdens de NAVO-top afgelopen juni is er door publieke en private organisaties hard gewerkt om adequaat te kunnen reageren op digitale dreiging. De integrale benadering en grootschalige voorbereiding heeft er mede voor gezorgd dat de top goed is verlopen. De paraatheid van alle organisaties symboliseert de extra inzet die nodig is om antwoord te geven op de toegenomen digitale dreiging. Het is daarom van belang gezamenlijk te blijven werken aan de uitvoering van de acties uit de NLCS om zo de weerbaarheid van Nederland te vergroten.

In deze brief neem ik u mee in de ontwikkelingen van de dreiging, de voortgang en de uitvoering van de NLCS en doen we een motie af. Daarnaast bied ik u namens het kabinet het CSBN 2025 en de voortgangsrapportage van het actieplan NLCS 2025 aan.

Nederlandse Cybersecuritystrategie 2022–2028

De NLCS is eind 2022 opgesteld en zet uiteen hoe de betrokken publieke, private en wetenschapspartijen in zes jaar werken naar een digitaal weerbaarder Nederland. Deze inzet is concreet gemaakt in een onderliggend actieplan. Dat actieplan wordt jaarlijks geactualiseerd en geeft inzicht in de onderliggende acties, verwachte doorlooptijd en verantwoordelijkheden. Op 8 februari 2024 is de nulmeting van de NLCS met de Kamer gedeeld.[2] Deze nulmeting maakt inzichtelijk wat de uitgangssituatie was voordat er met de uitvoering van de strategie werd gestart. Er is een tussentijdse evaluatie in 2026 en een eindevaluatie in 2028 voorzien. Daarnaast wordt de Kamer jaarlijks geïnformeerd over de voortgang van de acties middels de voortgangrapportages van de NLCS.

Cybersecuritybeeld Nederland 2025

Het CSBN 2025 schetst dat de digitale dreiging onverminderd hoog is en dat het dreigingslandschap steeds diverser en onvoorspelbaarder wordt. Er is sprake van een wereldwijde toename in offensieve cybercapaciteiten, net als een toename in risicobereidheid van staatsgesteunde groeperingen. Criminele, statelijke én staatsgesteunde actoren begeven zich op het digitale strijdtoneel, ontwikkelen cybercapaciteiten en zetten deze in. Bovendien vermengen statelijke actoren zich met niet-statelijke actoren of organisaties. Dit leidt tot een diffuus dreigingsbeeld, waarbij scheidslijnen tussen typen actoren vervagen. Ook statelijke actoren die eerder geen (offensief) cyberprogramma hadden, ontwikkelen deze. Deze ontwikkelingen hangen samen met de huidige geopolitieke verharding.

Kwaadwillende actoren hebben een doorlopende interesse in het compromitteren van (organisaties in) vitale sectoren en het stimuleren van maatschappelijke onrust, bijvoorbeeld door het uitvoeren van DDoS-aanvallen. Daarnaast illustreert de campagne van Salt Typhoon, die resulteerde in vergaande compromittatie van de Amerikaanse telecomsector en waarbij enkele kleinere Nederlandse Internet Service- en Hosting providers ook doelwit waren, dat de dreiging richting vitale sectoren reëel is.

Digitale processen vormen het zenuwstelsel van de Nederlandse maatschappij, en voor vele hiervan zijn wij afhankelijk van buitenlandse, niet-Europese, partijen. Zulke digitale afhankelijkheden kunnen risicovol worden als gevolg van geopolitieke ontwikkelingen. Digitale veiligheid is

[2] Kamerstukken II, 2023–2024 26 643, nr. 1128

dan ook zeker niet alleen een onderwerp voor technici, maar moet juist met oog voor de geopolitieke context worden benaderd. Geopolitiek en de invloed daarvan op digitale veiligheid moet dan ook nu onderwerp van gesprek zijn op de bestuurstafel.

Uit het in het CSBN opgenomen Jaarbeeld blijkt dat er in de afgelopen rapportageperiode geen cyberincidenten zijn geweest die hebben geleid tot maatschappelijke ontwrichting. Wel hebben incidenten bij onder andere het OM en Clinical Diagnostics laten zien wat de impact van cyberincidenten kan zijn op de samenleving, én hoezeer de samenleving leunt op de beschikbaarheid van digitale diensten. Daarnaast is gebleken dat aanvallen in veel gevallen konden plaatsvinden omdat de digitale basisprincipes zoals opgesteld door het NCSC en het DTC niet voldoende waren toegepast. Daaronder valt ook het bestaan van kwetsbare systemen die niet (tijdig) zijn gepatcht. De aandacht voor het treffen van basismaatregelen dient niet te verslappen en blijft een sleutel om de digitale weerbaarheid en veerkracht te verhogen. Juist nu er sprake is van toenemende complexiteit in het dreigingsbeeld, vormen de basisprincipes voor digitale weerbaarheid effectieve barrière voor vele verschillende aanvallen en kwaadwillenden.

Voortgangsrapportage 2025

De Cyberbeveiligingswet

De Cyberbeveiligingswet (Cbw) is onderdeel van de Nederlandse implementatie van de Europese NIS2-richtlijn. De Cbw gaat naar verwachting een stevige impuls geven aan de versterking van de digitale weerbaarheid van Nederland door organisaties op wie de wet van toepassing is, te verplichten cyberbeveiligingsmaatregelen te treffen en ernstige incidenten te melden. Op 2 juni jl. zijn het wetsvoorstel en op 30 juni jl. het bijbehorende conceptbesluit met de Tweede Kamer gedeeld. De inwerkingtreding wordt verwacht in het tweede kwartaal van 2026.[3] In 2024 en 2025 heeft een consultatie plaatsgevonden over het concept van de Cbw en het bijbehorende Cyberbeveiligingsbesluit.

Wet weerbaarheid kritieke entiteiten

Ook voor de Wet weerbaarheid kritieke entiteiten (Wwke) en het bijbehorende besluit zijn organisaties in 2024 en 2025 geconsulteerd. De Wwke heeft als doel om de weerbaarheid te verhogen van organisaties die essentiële diensten verlenen in Nederland. De Wwke sluit inhoudelijk goed aan op de Cbw en vormt de Nederlandse uitwerking van de Europese *Critical Entities Resilience* (CER-) richtlijn. Het wetsvoorstel is op 2 juni aangeboden aan de Tweede Kamer en het conceptbesluit volgde op 30 juni. Afhankelijk van de parlementaire behandeling treedt de wet- en regelgeving naar verwachting in werking in Q2 2026. De rijksoverheid roept organisaties op zich op zowel de implementatie van de Cbw als de Wwke zich tijdig voor te bereiden en waar mogelijk reeds maatregelen te treffen gezien de noodzaak om de weerbaarheid te verhogen.

[3] MJenV zegt toe in antwoord op de Motie Six-Dijkstra tijdens het tweeminutendebat Datalek Politie uit december 2024 dat in de voortgangsrapportage wordt meegenomen wat de verantwoordelijkheid is van het NCSC in de nieuwe situatie (Cbw) als het gaat om logging of adviezen aan andere overheidsorganisaties. Wegens de inwerkingtreding van de Cbw in Q2 2026 wordt deze motie in de voortgangsrapportage van 2026 afgedaan.

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 loopt er onder coördinatie van de Nationaal Coördinator Terrorismebestrijding en Veiligheid een verkenning naar de mogelijkheden van actieve cyberverdedigingsmaatregelen. Op basis van de uitkomsten van de verkenning zullen verschillende beleidsopties worden uitgewerkt.

Landelijk Crisisplan Digitaal

De implementatie van de Cbw en de stelselwijzigingen die als gevolg hiervan plaatsvinden, hebben een belangrijke uitwerking op het Landelijk Crisisplan Digitaal (LCP-D). Zo breidt de doelgroep van het Nationaal Cyber Security Centrum (NCSC) fors uit naar alle Nederlandse organisaties en samen met de andere sectorale CSIRTS ook diens ondersteuning. Om die reden is besloten om in 2026, na inwerkingtreding van de Cbw, een geüpdatete versie van het LCP-D te publiceren. Verschillende publieke en private stakeholders en partners op het vlak van (digitale) crisisbeheersing en de lessen van de afgelopen NAVO-top worden nauw bij de aankomende update betrokken. Het afgelopen jaar hebben er verschillende oefeningen plaatsgevonden waarin de aansluiting van het LCP-D op de departementale crisisplannen werd getest. Zo werd door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties het afgelopen jaar de 6e editie van de Overheidsbrede Cyberoefening georganiseerd. Ook namen vrijwel alle departementen van de rijksoverheid in 2025 deel aan de Crisis Management Exercise (CMX) van de NAVO. Deelname aan dergelijke internationale oefeningen blijft een belangrijke prioriteit voor Nederland. Ook op lokaal niveau werd er door gemeentelijke organisaties gewerkt aan lokale digitale crisisplannen. Deze sluiten steeds beter aan het op LCP-D en worden blijvend doorontwikkeld.

De integratie van NCSC, DTC en CSIRT-DSP

De integratie van het NCSC, Digital Trust Center (DTC) en Computer Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP) verloopt volgens planning. Naast de integratie verkent het kabinet de mogelijkheden voor het fysiek samenbrengen van publiek en private partijen middels het House of Cyber. Fysieke nabijheid heeft een positieve impact op de digitale weerbaarheid doordat informatie, expertise en elkaars netwerk gemakkelijker gedeeld kunnen worden. De verkenning naar het samenwerkingsverband in het fysieke House of Cyber is inmiddels afgerond en momenteel lopen de gesprekken over een mogelijke locatie.

Het Cyberweerbaarheidsnetwerk

Volgend op de versterking van publiek-private samenwerking is het bouwplan voor het Cyberweerbaarheidsnetwerk (CWN) op 10 september opgeleverd.[4] Dit bouwplan geeft concrete invulling aan de implementatie van de Toekomstvisie Cyberweerbaarheidsnetwerk, de doorontwikkeling van het Landelijk Dekkend Stelsel (LDS).[5]

[4] Bouwplan Cyberweerbaarheidsnetwerk | Publicatie | Nationaal Cyber Security Centrum
[5] Toekomstvisie cyberweerbaarheidsnetwerk

Bestuurlijk convenant digitale veiligheid gemeenten

Om digitale dreiging bij gemeenten beter aan te pakken is in december 2022 het Bestuurlijk convenant digitale veiligheid gemeenten gepubliceerd.[6] Doel is, om meer aandacht te geven aan het lokale perspectief op digitale veiligheid en enkele fundamentele uitdagingen gezamenlijk op te pakken, zoals een betere informatiepositie voor gemeenten en duidelijke afspraken over de verantwoordelijkheden en bevoegdheden van het lokaal bestuur op digitale veiligheid van de gemeente en in de gemeente. Een rapport met aanbevelingen voor de uitwerking van het Bestuurlijk Convenant Digitale Veiligheid Gemeenten en het Rijk wordt naar verwachting eind 2025 met uw Kamer gedeeld.

Inwerkingtreding Algemene Beveiligingseisen Rijksoverheidsopdrachten (ABRO)

De Tweede Kamer is in maart 2025 geïnformeerd over de voortgang van het Programma ABRO.[7] Het streven om het de regelgevings- en organisatorische kader van ABRO voor het zomerreces 2025 af te ronden is niet haalbaar gebleken. De Kamer wordt hierover middels deze brief geïnformeerd. Er wordt momenteel toegewerkt naar 1 januari 2026 als introductiedatum.

Defensie Cyberstrategie

De nieuwe Defensie Cyberstrategie, gepubliceerd op 3 oktober 2025, geeft richting aan de wijze waarop Defensie haar cybercapaciteiten wil inzetten tegen cyberdreigingen tegen Nederland en bondgenoten.[8] Synergie tussen de taken en middelen van Defensie en die van andere overheden, private partijen en bondgenoten in het cyberdomein is daarbij essentieel. Naast de eigen taken van Defensie in het cyberdomein, geeft deze strategie ook nadere invulling aan de rol van Defensie binnen de NLCS.

Cybersecurity Raad

De Cyber Security Raad (CSR) heeft als taak het kabinet te adviseren over de uitvoering en uitwerking van de NLCS en heeft dit ook gedaan met betrekking tot de voorliggende voortgangsrapportage. De CSR ziet dat de doelen en de strategie van het actieplan breed worden gedragen. Wel vragen sommige leden om een herijking waarbij de leden wijzen op recente ontwikkelingen, bijvoorbeeld op geopolitiek terrein. De CSR noemt hierbij digitale autonomie als prioriteit. Terecht wijst de CSR daarnaast op het belang van publiek-private samenwerking en de raad beveelt aan om private en wetenschappelijke partijen structureel te betrekken bij de strategie en te sturen op meer samenwerking. Een uitwerking hiervan is het CWN, waar verschillende private en wetenschappelijke partijen direct bij betrokken zijn. De CSR stelt voor om kaders en afspraken helder neer te zetten en ook vanuit de nieuwe fusieorganisatie van het NCSC, het DTC en het CSIRT-DSP aandacht te houden voor cyberweerbaarheid van het midden- en kleinbedrijf. Ook vraagt de CSR aandacht voor versterking van de digitale infrastructuur, met name op de gebieden van ketenafhankelijkheden, de robuustheid van onderliggende netwerken en de beperkte zichtbaarheid op digitale risico's bij toeleveranciers. Het vergroten van weerbaarheid op systeemniveau vraagt om structurele betrokkenheid van aanbieders en beheerders van die infrastructuur. De leden noemen ook de gevolgen van nieuwe technologische

[6] Bestuurlijk convenant digitale veiligheid gemeenten
[7] Kamerstukken 2024–2025, 26 643-1328
[8] Kamerstukken 2024–2025, 26 643-1422

ontwikkelingen en geven prioriteit aan de kennisopbouw over cyberaanvallen met kunstmatige intelligentie (AI).

Samenhangend Inspectiebeeld cybersecurity vitale processen 2024

Het Samenhangend Inspectiebeeld (SIB) werd jaarlijks opgesteld door de toezichthouders van de Wet beveiliging netwerk- en informatiesystemen (Wbni) en beschrijft de staat van de cybersecurity van vitale aanbieders en vitale processen. De toezichthouders zien ruimte voor verbetering op het gebied van risicomanagement op bestuursniveau, want met name door de komst van de CER en de NIS2 is meer toekomstgerichte samenwerking tussen toezichthouders nodig. Gelet hierop is er een noodzaak om de governance rondom samenwerking te versterken. Daarom is recentelijk het «directeurenoverleg toezicht digitale weerbaarheid» opgericht. Dit gremium fungeert als opdrachtgever van de werkgroep «samenwerkend toezicht digitale weerbaarheid». Met de inrichting van deze samenwerkingsvormen streven de toezichthouders naar effectief en efficiënt toezicht en een zo laag mogelijke gezamenlijke werklast voor organisaties die onder toezicht staan. Gelet op de aandacht voor de herinrichting van de governancestructuur is besloten de publicatie van het SIB voor twee jaar te pauzeren.

Overige moties en toezeggingen

Motie Six-Dijkstra en Postma

Motie 30 821, nr. 288 van de leden Six-Dijkstra en Postma verzoekt de regering om in wetgeving, bijvoorbeeld binnen de Aanpak vitaal, expliciet op te nemen dat zonnepanelen, omvormers, laadpalen, warmtepompen en vergelijkbare (consumenten)apparatuur niet doorleveranciers uit het buitenland aan- en uitgezet mogen kunnen worden.

In antwoord hierop informeer ik u dat onder de huidige Aanpak vitaal vitale aanbieders verplicht zijn om een breed scala aan risico's af te wegen in hun risicobeoordeling, waaronder mogelijke gevolgen van het aan- en uitzetten van zonne-omvormers.[9] Vitale aanbieders die actief zijn in de elektriciteitssector, gebruikmaken van omvormers en onder de Wbni vallen, zijn verplicht beveiligingsmaatregelen te nemen. De Rijksdienst Digitale Infrastructuur (RDI) houdt hier toezicht op.

In 2026 worden deze wettelijke verplichtingen uitgebreid middels de Cbw en de Wwke, waarin aanzienlijk zwaardere beveiligingseisen worden gesteld dan in de Wbni. Samen met mijn collega's van Klimaat en Groene Groei en Economische Zaken hebben wij uitvoerig contact met bedrijven over de uitvoering van deze toekomstige wetgeving. Bedrijven die onder de nieuwe wetgeving komen te vallen, moeten op basis van een risico gebaseerde aanpak zorgdragen voor de beveiliging van hun netwerk- en informatiesystemen. Bij het overwegen van passende maatregelen zijn bedrijven verplicht om rekening te houden met de specifieke kwetsbaarheden van hun rechtstreekse leveranciers en dienstverleners en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners. Daarnaast is het voornemen om in de lagere regelgeving onder Cbw en Wwke een bevoegdheid voor de vakministers op te nemen om in het kader van de zorgplicht in bepaalde gevallen, en als laatste redmiddel, bedrijven te kunnen verplichten specifieke producten en diensten van leveranciers te weren.

[9] Kamerstukken II 2022/23, 30 821, nr. 178.

Voor mogelijke cyberrisico's van zonne-omvormers zijn er verder additionele wetgevingstrajecten die gericht zijn op de fabrikanten van hard- en software. Voor digitale producten op de Europese markt introduceren de gedelegeerde handeling onder de radioapparatuurrichtlijn (RED3.3def) en de CRA cybersecurityeisen waaraan deze producten moeten voldoen. Vanaf augustus 2025 is de RED3.3def van kracht met eisen voor alle draadloos verbonden apparaten, waaronder zonnepaneelomvormers. Vanaf december 2027 is de CRA van kracht met eisen voor alle producten met digitale elementen (hardware- en softwareproducten), waaronder zowel consumentenapparatuur en -software, als digitale producten voor industriële en operationele toepassingen vallen.

Fabrikanten, importeurs en distributeurs mogen op grond van deze productregelgeving alleen producten op de EU-markt aanbieden die passende beveiligingsmaatregelen bevatten. Deze maatregelen hebben onder meer betrekking op ongeautoriseerde toegang. Producten moeten passend beveiligd zijn tegen hacken.

Op de Europese markt is het verboden om (heimelijk) functionaliteit in te bouwen (zowel software en hardware) die niet in de technische documentatie is beschreven. Het is verboden om producten aan te bieden die «verstopte» functionaliteiten bevatten om apparaten op afstand aan of uit te zetten. Deze eisen gelden ook voor producten die afkomstig zijn van een fabrikant die buiten de EU is gevestigd, zodra deze producten op de Europese markt worden aangeboden.

De RDI houdt toezicht op deze wettelijke verplichtingen. De RDI onderzoekt onder meer op basis van steekproeven in testlaboratoria of de producten overeenkomen met de technische documentatie en of de producten de nodige cybersecuritymaatregelen bevatten. Vooruitlopend op de inwerkingtreding van deze cybersecurityproducteisen heeft de RDI in 2023 een rapport gepubliceerd over zonnepaneelomvormers waarin fabrikanten op deze aankomende verplichtingen worden gewezen.[10]

Ik beschouw deze motie hiermee als afgedaan.

Tot slot

In het huidige dreigingslandschap is het verhogen van de weerbaarheid in het digitale domein essentieel. Het is van belang dat bestuurders van grote publieke en private organisaties zorg dragen voor hun cyberweerbaarheid. Een goede stap is het zorgen voor implementatie van de vijf basisprincipes van het NCSC: zorg voor een risicobeoordeling, bevorder veilig gedrag, bescherm systemen, applicaties en apparaten, beheer toegang tot data en diensten, en zorg voor een gedegen voorbereiding op incidenten.

De Minister van Justitie en Veiligheid,
F. van Oosten

[10] Rapport RDI