Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

26 643 Informatie- en communicatietechnologie (ICT)

30 821 Nationale Veiligheid

Nr. 1440 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 8 december 2025

Digitale processen vormen het zenuwstelsel van de maatschappij, en beveiliging hiervan binnen de vitale infrastructuur is daarom onlosmakelijk verbonden met de nationale veiligheid. Een wezenlijke ontwikkeling die onze samenleving raakt is dat Nederland steeds vaker wordt geconfronteerd met cyberaanvallen op vitale processen door zowel statelijke als criminele actoren. Naar verwachting zal de cyberdreiging de komende jaren aanhouden omdat het voor landen relatief makkelijk is om een (nieuw) digitaal aanvalsprogramma op te zetten en dergelijke aanvallen steeds moeilijker herleidbaar zijn tot de aanvaller.[1, 2] Deze ontwikkelingen passen in een dreigingslandschap dat steeds diverser en onvoorspelbaarder wordt.[3]

Uw Kamer heeft terecht aandacht voor de digitale weerbaarheid van de vitale infrastructuur. Zo wordt in de moties Rajkowski (VVD) c.s. verzocht in kaart te brengen in hoeverre (analoge) terugvalopties nodig zijn voor het versterken van onze digitale weerbaarheid[4] en een scan te maken van apparatuur of programmatuur van organisaties uit landen met een tegen Nederland gerichte offensieve cyberagenda die aanwezig is binnen (de kernsystemen van) de vitale sector.[5] Daarnaast vraagt uw Kamer met de motie Chakor c.s. aandacht voor het ontwikkelen van plannen met overheden en vitale sectoren om essentiële dienstverlening bij grootschalige digitale storingen in stand te houden.[6] In deze brief zet ik uiteen op welke wijze invulling is gegeven aan deze drie moties.

---

[1] Cybersecuritybeeld Nederland 2025 (NCTV), november 2025.
[2] Openbaar jaarverslag van de AIVD over het jaar 2024, april 2025; Openbaar jaarverslag van de MIVD over het jaar 2024, april 2025.
[3] Idem.
[4] Kamerstukken II 2022/23, 26 643, nr. 1048.
[5] Kamerstukken II 2022/23, 26 643, nr. 830.
[6] Kamerstukken II 2024/25, 26 643, nr. 1256.

kst-26643-1440
ISSN 0921 - 7371
's-Gravenhage 2025

Wetgeving ter versterking van (digitale) weerbaarheid

Veel van ons leven en werk speelt zich af in de digitale wereld. Omdat de digitale veiligheid van onze samenleving en economie steeds vaker onder druk staat, heeft de Europese Unie (EU) de «Network and Information Security Directive» (NIS2) ingevoerd. De NIS2-richtlijn wordt momenteel door alle betrokken departementen omgezet in de nationale Cyberbeveiligingswet (Cbw). Op het moment dat de Cbw wordt geïmplementeerd, vervangt deze de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni) voor digitale dienstverleners. Tegelijkertijd loopt ook de implementatie van de «Critical Entities Resilience Directive» (CER), die wordt omgezet in de nationale Wet weerbaarheid kritieke entiteiten (Wwke). Hiermee wordt de huidige beleidsmatige Aanpak vitaal wettelijk verankerd om de weerbaarheid van de kritieke infrastructuur *all hazard* te verhogen.

Deze richtlijnen verplichten lidstaten om kritieke, essentiële en belangrijke entiteiten te ondersteunen bij het versterken van hun weerbaarheid tegen zowel fysieke als digitale risico's. Zo schrijft de NIS2-richtlijn voor dat essentiële en belangrijke entiteiten ondersteund worden met advies en bijstand in geval van een digitale hack of cyberincident door een CSIRT (Computer Security Incident Response Team). De CER-richtlijn schrijft voor dat de overheid elke vier jaar per sector een sectorale risicobeoordeling uitvoert en deze deelt met de aangewezen kritieke entiteiten binnen die sector. De overheid kan verdere ondersteuning bieden in de vorm van informatie-uitwisseling, handreikingen en instrumenten ter verhoging van de weerbaarheid, zoals bijvoorbeeld voor het uitvoeren van een risicobeoordeling of op het gebied van veilig ondernemen.

Organisaties die onder deze wetgeving vallen, zullen wettelijk worden verplicht om (significante) incidenten die hun essentiële dienstverdeling aanzienlijk verstoren te melden bij de bevoegde autoriteit en in het geval van de Cbw ook bij het betreffende CSIRT. Naast deze meldplicht schrijven deze wetten ook voor dat organisaties op basis van een zorgplicht passende en evenredige maatregelen moeten nemen om de beveiliging van hun netwerk- en informatiesystemen en fysieke omgeving te waarborgen. Onder meer redundantie, zoals het in kaart brengen van (analoge) terugvalopties, en cascade-effecten zijn een inherent onderdeel van de risicobeoordeling die kritieke, essentiële en belangrijke entiteiten moeten uitvoeren. Aansluitend worden de risico-mitigerende maatregelen getoetst op hun effectiviteit en waar nodig bijgesteld. Het onafhankelijke toezicht op de naleving van deze wetten heeft onder meer expliciet aandacht voor ketenafhankelijkheden, crisisplanvorming en (digitale) weerbaarheidsmaatregelen.

Met de inwerkingtreding van de Cbw worden essentiële en belangrijke entiteiten op basis van de zorgplicht ook wettelijk verplicht om beleid vast te stellen voor het borgen van hun bedrijfscontinuïteit. Hierbij moeten in ieder geval processen en procedures worden opgesteld voor het herstellen van netwerk- en informatiesystemen én voor het periodiek verifiëren van de betrouwbaarheid van back-ups van software en gegevens. In het verlengde daarvan dienen voornoemde entiteiten zowel een bedrijfscontinuïteitsplan en een herstelplan te hebben die zij periodiek moeten testen. Op deze wijze kunnen zij controleren of het plan nog steeds werkt en actueel is. Hierdoor kan de impact van een toekomstig incident op de dienstverlening – zoals uitval van digitale processen – worden geminimaliseerd en kan de dienstverlening zo spoedig mogelijk worden hersteld en hervat.

Met bovenstaande verplichtingen, volgend uit de inwerkingtreding van de Cbw en Wwke, en de aanvullende inzet in het kader van de maatschappe-

lijke weerbaarheid tegen hybride en militaire dreigingen beschouw ik de motie Chakor c.s., die verzocht om plannen te ontwikkelen met overheden en vitale sectoren om essentiële dienstverlening in geval van grootschalige digitale storing zo veel mogelijk in stand te houden, en de motie Rajkowski, c.s., die verzocht om in kaart te brengen in hoeverre (analoge) terugvalopties nodig zijn voor het versterken van onze digitale weerbaarheid en om dit te betrekken bij de Aanpak vitaal, als afgedaan.

Apparatuur uit landen met een offensieve cyberagenda tegen Nederland

Zoals beschreven in het Cyber Security Beeld Nederland 2025[7], het Dreigingsbeeld Statelijke Actoren[8] en jaarverslagen van de Inlichtingen- en Veiligheidsdiensten intensiveren meer statelijke actoren hun activiteiten en verbreden ze hun capaciteiten voor de behartiging van hun geopolitieke belangen. Het demissionaire kabinet is, net als uw Kamer, doordrongen van de risico's en dreigingen die uitgaan van landen met een tegen Nederland gerichte offensieve cyberagenda en onderstreept dan ook de aandacht die de motie Rajkowski c.s. voor dit onderwerp vraagt. Zoals in de Kamerbrief over het overzicht van overheids-ICT van de Rijksoverheid uit 12 maart jl. toegelicht, brengt het opstellen van een rijksbreed overzicht van alle ICT-assests, naast juridische en praktische beperkingen, ook veiligheidsrisico's met zich mee.[9] Het uitvoeren van een integrale scan op de aanwezigheid van apparatuur en programmatuur uit landen met een offensief cyberagenda in vitale overheids- en private sectoren wordt dus niet als haalbaar en wenselijk beschouwd.

Het demissionaire kabinet investeert doorlopend in bewustwording, kennisopbouw, en handelingsperspectief ter versterking van digitale en fysieke weerbaarheid. Het in kaart brengen en beheersen van risico's in de toeleverancierssketen is namelijk van groot belang voor het digitaal veilig functioneren van publieke en private organisaties. Daarom hebben de AIVD, CIO Rijk, het NCSC en de NCTV gezamenlijk de handreiking *«Cybercheck: ook jij hebt supply chain risicos!»* gepubliceerd.[10] Deze handreiking biedt organisaties en bedrijven handvatten om te inventariseren of de inzet van een bepaald product of dienst afkomstig uit een land met een offensief cyberprogramma mogelijk tot een verhoogd beveiligingsrisico leidt. Daarnaast heb ik TNO verzocht een zelfscantool te ontwikkelen waarmee vitale aanbieders een risicoafweging kunnen maken van hardware en software ten aanzien van operationele technologie van leveranciers uit risicolanden. De inzichten uit bovengenoemde handreiking en de zelfscantool zijn verspreid en worden geïncorporeerd in de risicobeoordelingen die op grond van de Cbw en Wwke moeten worden uitgevoerd door kritieke entiteiten.

Daarnaast zal in het licht van het huidige dreigingsbeeld de uitwerking van de algemene zorgplicht van de Cbw en de Wwke de mogelijkheid bevatten om als uiterste redmiddel een entiteit de verplichting op te leggen om bepaalde producten of diensten van specifieke leveranciers te weren indien de nationale veiligheid in het geding is.Het zal hierbij gaan om leveranciers die zelf de intentie hebben om de beveiliging van de netwerk- en informatiesystemen van de entiteiten aan te tasten of om incidenten bij die entiteiten te veroorzaken, of leveranciers die nauwe banden hebben met of onder invloed van een dergelijke partij zijn. Van

---

[7] Cybersecuritybeeld Nederland 2025 (NCTV), november 2025.
[8] Dreigingsbeeld Statelijke Actoren 3 (AIVD, MIVD, NCTV), juli 2025.
[9] Kamerstuk 2025/26, 26 643, nr. 1314.
[10] NCSC, Cybercheck: ook jij hebt supply chain risico's! | Publicatie | Nationaal Cyber Security Centrum, 18 april 2024.

nauwe banden of invloed kan bijvoorbeeld sprake zijn indien de leverancier afkomstig is, of onder controle staat van een partij, uit een land met wetgeving die particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder staatsorganen die zijn belast met een inlichtingen- of militaire taak.

Met bovengenoemde inzet heeft het demissionaire kabinet invulling gegeven aan de moties van Rajkowski c.s. die verzocht een scan uit te voeren naar de aanwezigheid van apparatuur en programmatuur uit landen met een tegen Nederland gerichte offensieve cyberagenda in kernsystemen van vitale sectoren.[11] Over het deel van de motie van Rajkowski (VVD) c.s. dat oproept om een scan te maken over hoe apparatuur en programmatuur van organisaties uit landen met een tegen Nederland gerichte offensieve cyberagenda geweerd kan worden uit aanbestedingen van de Rijksoverheid is uw Kamer op 17 april 2023 geïnformeerd[12].

Tot slot

Het geheel aan maatregelen dat hierboven staat beschreven, kan niet los van elkaar worden gezien en is onderdeel van de bredere inzet ter bescherming van de vitale infrastructuur. Door veiligheidswaarborgen juridisch te verankeren en ons beleid doorlopend aan te passen aan het actuele dreigingslandschap neemt het demissionaire kabinet noodzakelijke stappen om de nationale veiligheid te beschermen. In de Kamerbrief over de voortgang van de NLCS is uw Kamer dit najaar nader geïnformeerd over digitale weerbaarheid en de verdere versterking van de vitale infrastructuur.[13]

De Minister van Justitie en Veiligheid,
F. van Oosten

[11] Kamerstukken II 2023/24, 30 821, nr. 203.
[12] Kamerstukken II 2022/23, 26 643, nr. 1007.
[13] Kamerstukken II 2025/26, 26 643, nr. 1437.