Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

26 643 Informatie- en communicatietechnologie (ICT)

30 821 Nationale Veiligheid

Nr. 1444

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 11 december 2025

Tijdens de Regeling van Werkzaamheden op 24 september 2024 heeft het lid Paternotte (D66) verzocht om middels een brief inzicht te geven in het overheidsbeleid met betrekking tot de gevaren die de afhankelijkheid van elektronica voor onze samenleving kan opleveren. Deze brief richt zich allereerst op de gevaren van elektronica als potentieel middel voor terroristische aanslagen, waarbij de verschillende risico's die elektronica met zich meebrengt worden geschetst, gevolgd door een uiteenzetting van de aanpak om deze risico's te beheersen. Vervolgens zal ook het beleid rondom de weerbaarheid van digitale (vitale) infrastructuur worden uitgelicht.

Elektronische hardware(componenten) als explosief

Elektronica is onmiskenbaar een integraal onderdeel van ons dagelijks leven. Van telecominfrastructuren tot consumentenelektronica zoals telefoons, laptops, elektrische fietsen en video-deurbellen. Deze apparaten zijn onlosmakelijk verbonden met onze moderne samenleving. Maar juist doordat we steeds meer afhankelijk zijn van deze technologie, ontstaan er ook risico's die we niet mogen negeren. De veelvuldigheid aan elektronische apparaten in ons dagelijks leven kunnen kwetsbaarheden bevatten die kwaadwillenden in staat stellen gegevens te onderscheppen, kritieke systemen te manipuleren of de functionaliteiten van deze apparatuur in te zetten als aanslagmiddel. Een zorgwekkend fenomeen blijft het gebruik van elektronische componenten of hardware voor het op afstand activeren van explosieven. Hiermee kunnen explosies worden veroorzaakt zonder dat de dader fysiek aanwezig hoeft te zijn bij het doelwit, mits er elektrische stroom beschikbaar is – via een batterij of netspanning. In dergelijke gevallen kan elektronische aansturing leiden tot de ontsteking van opzettelijk geplaatste explosieven. Een voorbeeld hiervan was de aanslag op een vliegtuig van Daallo Airlines in 2016, waarbij een laptop als explosief werd gebruikt. Meer recent, in september 2024, werden in Libanon piepers en portofoons gebruikt om explosies te initiëren. Deze

kst-26643-1444
ISSN 0921 - 7371
's-Gravenhage 2025

incidenten onderstrepen de dreiging die kan uitgaan van alledaagse elektronische apparaten.

Het op grote schaal manipuleren van elektronische apparaten om deze op een gecontroleerd moment te laten ontsteken, vergt een langdurige voorbereiding en gedegen kennis en kunde. Daarbij is het noodzakelijk om over voldoende financiële middelen en contacten te bezitten. Deze (logistieke) voorwaarden maken dat een soortgelijke aanval, waarin op grote schaal gemanipuleerde elektronica gecontroleerd wordt ingezet als aanslagmiddel, een lage mate van waarschijnlijkheid betreft. Dit neemt niet weg dat mijn ministerie en alle betrokken veiligheidspartners voortdurend alert zijn op de reële dreiging die uitgaat van elektronica als wapen in onze samenleving, en oog blijven houden voor technologische ontwikkelingen en trends. Op basis hiervan bouwen we daar waar mogelijk tijdig barrières in, zoals het verbeteren van wetshandhaving en beleid, en het verhogen van (de zichtbaarheid van) beveiligingsmaatregelen om de risico's te mitigeren.

Aanpak

Om de kans op gemanipuleerde hardware tegen te gaan, werken we in Nederland risicogestuurd. We zetten continue in op het verbeteren van detectiemethoden, die gericht zijn op het herkennen van verdachte elektronische componenten en/of hardware door onder andere het versterken van de samenwerking én uitwisseling van informatie tussen veiligheidsdiensten en overige (publieke, private en technologische) ketenpartners maakt hier onderdeel van uit. Dagelijks passeren duizenden elektronische apparaten de Nederlandse grens, waardoor een 100% controle niet realiseerbaar is. Wel worden op basis van risico-indicatoren veel controles voor goederen van buiten de Europese Unie door de Douane uitgevoerd. Daarnaast kunnen steekproeven plaatsvinden van zowel binnen als buiten de EU. Ook logistieke vervoerbedrijven hebben een rol in het controleren van (verboden) goederen. Gezien de aanzienlijke stroom aan (elektronische) goederen die Nederland binnenkomen, is het van groot belang om te beschikken over betrouwbare en actuele informatie. Ketenpartners, zoals de Nationale Politie en de Douane, richten zich daarom actief op het verzamelen en delen van relevante informatie zodat risicovolle hardware tijdig onderschept kan worden.

Digitale sabotage

Het is naast het manipuleren van de elektronische hardware ook mogelijk om middels digitale sabotage software en/of hardware te verstoren, beschadigen of vernietigen, met fysieke consequenties tot gevolg[1]. De digitalisering van de samenleving zorgt voor veel onderlinge afhankelijkheden. Door toenemende verwevenheid van digitale en fysieke processen kunnen de gevolgen van een sabotage groot zijn. Zeker wanneer de sabotage gericht zou zijn op vitale processen kan dit gevolgen hebben voor het ongestoord functioneren van de economie en maatschappij en daarmee in het uiterste geval een bedreiging vormen voor de nationale veiligheid.

De digitale dreiging is permanent en neemt eerder toe dan af, met alle mogelijke gevolgen van dien[2]. Daar komt bij dat de digitale ruimte – het complexe samenspel van onderling verweven digitale processen, gebruikmakend van netwerken, ICT-systemen en operationele technologieën – continu in beweging is, waardoor er doorlopend nieuwe risico's

[1] Cybersecuritybeeld Nederland 2024
[2] Dreigingsbeeld Statelijke Actoren 2 en Cybersecuritybeeld Nederland 2024

kunnen ontstaan. Dit vraagt om een doorlopende inspanning om de weerbaarheid tegen sabotagedreigingen te verhogen. Daarom werken overheden, bedrijven, organisaties en inlichtingen- en veiligheidsdiensten voortdurend nauw samen aan de weerbaarheid tegen dergelijke dreigingen, onder andere binnen de uitvoering van de Nederlandse Cybersecuritystrategie en de aanpak vitaal[3].

Aanpak

Onder de Nederlandse Cybersecuritystrategie[4] wordt gewerkt aan het verhogen van de digitale weerbaarheid en het tegengaan van digitale dreigingen van statelijke actoren en criminelen. Hierbinnen is er onder andere aandacht voor risico's die eventueel voort kunnen komen uit de aanwezigheid van apparatuur en software uit landen met een offensief cyberprogramma gericht tegen Nederlandse belangen. Het inzichtelijk maken van afhankelijkheden van toeleveranciers uit het buitenland heeft de prioriteit binnen het Rijk maar ook bij vitale aanbieders. Dit doen we met de versteviging van risicomanagement onder andere binnen de (inkoop)keten.[5]

Daarnaast speelt de overheid een actieve rol in het verhogen van de cyberweerbaarheid door het vaststellen van wet- en regelgeving zoals de Wet beveiliging netwerk- en informatiesystemen (Wbni). Met deze wet worden aangewezen organisaties verplicht om passende digitale beveiligingsmaatregelen te nemen. Als door een incident de gevolgen voor de continuïteit van een dienstverlening een sectorspecifieke drempelwaarde overschrijden, is een aangewezen organisatie verplicht het incident te melden bij het Nationaal Cyber Security Centrum (NCSC). Momenteel wordt er gewerkt aan de opvolger van de Wbni: de Cyberbeveiligingswet[6]. Met deze wet worden ruim 7000 extra organisaties in Nederland verplicht tot het nemen van beveiligingsmaatregelen en het doen van meldingen van incidenten. Met de Cyberbeveiligingswet zullen organisaties die onder de wet komen te vallen ook verplicht rekening moeten houden met risico's die voort kunnen komen uit de toeleverancierskete. Tenslotte ondersteunt het NCSC alle organisaties in Nederland met advies om de digitale weerbaarheid te versterken, onder andere door informatiedeling over kwetsbaarheden en dreigingen.

Tot slot hecht ik eraan aan te geven dat technologische ontwikkelingen en elektronica ook kansen bieden voor de bevordering voor de nationale veiligheid. Technologieën kunnen bijdragen aan het versterken van capaciteiten om onze samenleving weerbaarder te maken. Digitalisering, data science en Artificial Intelligence bieden bijvoorbeeld de mogelijkheid om dreigingen sneller te identificeren, de afhankelijkheid van menselijke waarneming te verminderen, grote hoeveelheden data te analyseren en de communicatie tussen betrokkenen te verbeteren.

De Minister van Justitie en Veiligheid,
F. van Oosten

---

[3] Kamerstukken II 2023/24. 30 821, nr. 203
[4] Nederlandse Cybersecuritystrategie 2022–2028
[5] Voortgangsrapportage 2024 Nederlandse Cybersecuritystrategie
[6] Cyberbeveiligingswet | Overheid.nl | Wetgevingskalender