Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

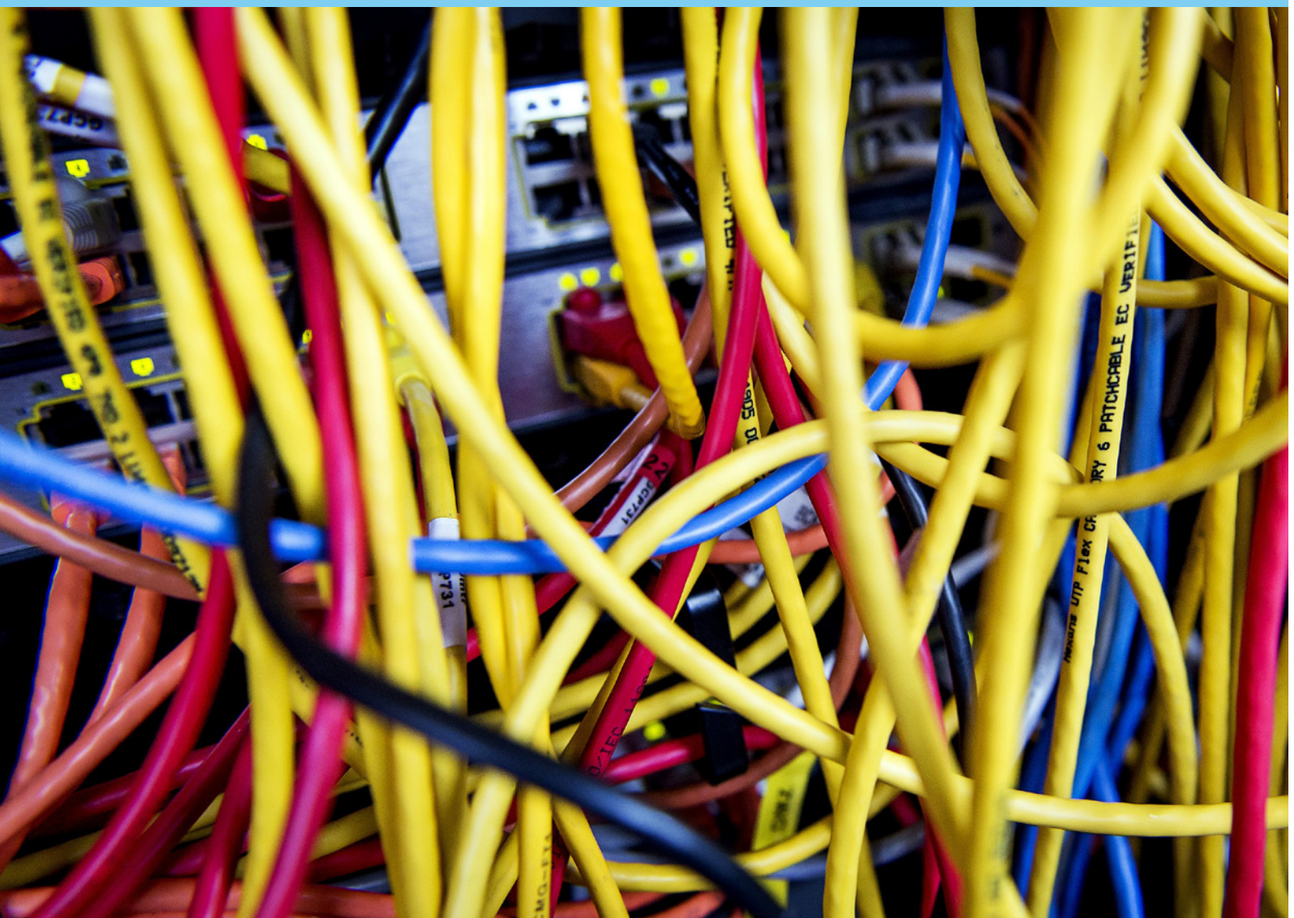
Cybersecuritybeeld Nederland 2025

Riskante mix in een onvoorspelbare wereld

Inhoudsopgave

Coverbeeld: Europa, en daarmee Nederland, is voor vele verschillende digitale processen en diensten afhankelijk van aanbieders uit andere, veelal niet-Europese, landen. Digitale afhankelijkheden die eerder niet als risicovol zijn beoordeeld kunnen dat later alsnog worden, bijvoorbeeld vanwege geopolitieke ontwikkelingen.

Er is een grote verscheidenheid van aanvallen, cybercapaciteiten nemen toe en vermenging tussen actoren vindt plaats. Geopolitieke onvoorspelbaarheid vertaalt zich naar het digitale domein. Het digitale dreigingslandschap wordt hierdoor in toenemende mate complex.



Riskante mix in een onvoorspelbare wereld

Het digitale dreigingslandschap wordt steeds diverser en onvoorspelbaarder. Er is een grote verscheidenheid aan aanvallen door statelijke actoren, cybercriminelen en andere kwaadwillenden. Daarnaast vertaalt geopolitieke onvoorspelbaarheid zich naar het digitale domein. Statelijke actoren zetten cyberprogramma's op of breiden die uit met de inzet van niet-statelijke actoren of private organisaties. Ook kunnen veranderende geopolitieke verhoudingen ervoor zorgen dat digitale afhankelijkheden risicovol worden, terwijl ze dat eerder niet waren. Verder kunnen kwaadwillenden generatieve AI inzetten, waardoor zij aanvallen eenvoudiger en op grotere schaal kunnen uitvoeren.

AI deze ontwikkelingen vinden gelijktijdig en in samenhang met elkaar plaats, waardoor het dreigingslandschap in toenemende mate complex wordt. Het op niveau krijgen en houden van digitale weerbaarheid wordt zeker niet eenvoudiger, maar hoeft in de basis niet dermate complex te zijn. Zo vormen de vijf basisprincipes van digitale weerbaarheid een effectieve barrière tegen een groot gedeelte van cyberaanvallen. Digitale veiligheid is al langer niet enkel een vraagstuk voor technische experts. Zeker voor niet-digitale factoren zoals geopolitiek geldt dat dit juist een vraagstuk is, of moet zijn, dat op de bestuurstafel ligt.

Grote verscheidenheid aan incidenten illustreert divers en onvoorspelbaar dreigingslandschap

Het digitale dreigingslandschap wordt steeds diverser, onvoorspelbaarder en complexer. Dat blijkt onder andere uit de grote verscheidenheid aan incidenten die zich deze rapportageperiode hebben voorgedaan. Daarbij is sprake van een variëteit aan aanvallers, methoden, doelwitten en motieven. Zo waren meerdere Nederlandse en buitenlandse organisaties doelwit van de Chinese statelijke actor Salt Typhoon, voerde de Russische actor Laundry Bear een cyberaanval uit op de Nationale Politie, maakten Noord-Koreaanse hackers digitale valuta buit bij onder andere Nederlandse organisaties en werd Nederland voor het eerst slachtoffer van cybersabotage door een Russische staatsgesteunde groepering. Ook cybercriminelen voerden doorlopend aanvallen uit. Zo werden bij een laboratorium gevoelige persoonsgegevens en patiëntdata van bijna 1 miljoen personen gestolen door cybercriminelen. Daarnaast voerden pro-Russische hacktivisten – in veel gevallen staatsgesteund – verschillende DDoS-campagnes

uit op Nederlandse websites, onder andere tijdens de NAVO-top die in juni 2025 plaatsvond.

Ook werd eens te meer duidelijk dat cyberincidenten door kunnen werken op het fysieke domein. Zo kregen hackers toegang tot Citrix Netscaler-systemen van het Openbaar Ministerie (OM) via een kwetsbaarheid. Het OM besloot na vaststelling van de hack hun systemen te ontkoppelen van het internet, wat zorgde voor hinder in de strafketen en de dagelijkse werkzaamheden. Het incident bij het OM is daarnaast illustratief voor de onverminderd hoge interesse die kwaadwillenden hebben in edge devices.[1] Zowel statelijke als criminele actoren vallen deze systemen veelvuldig en in toenemende mate aan om aangrenzende netwerken binnen te dringen.

Alhoewel incidenten in Nederland deze rapportageperiode niet hebben geleid tot maatschappelijke ontwrichting of significante impact op de nationale veiligheid, hadden verschillende incidenten wel die potentie. Meer dan in voorgaande jaren is ook in Nederland gebleken dat de impact van cyberincidenten verder gaat dan het digitale domein en dat digitale processen, dagelijkse werkzaamheden en persoonlijke levens hierdoor worden geraakt. Het illustreert dan ook hoe afhankelijk ons land is van digitale processen en dat dat ons kwetsbaar maakt.

Geopolitieke onvoorspelbaarheid brengt risico's met zich mee voor digitale veiligheid

Internationale betrekkingen worden onvoorspelbaarder en dat heeft impact op digitale veiligheid. Zo kunnen verslechterende verhoudingen het aantrekkelijker maken voor statelijke actoren om cyberaanvallen in te zetten, omdat die goedkoop en schaalbaar zijn en bovendien omdat betrokkenheid valt te ontkennen. Dat leidt ertoe dat steeds meer landen cyberprogramma's optuigen of uitbreiden, en dat landen niet-statelijke actoren of private organisaties inzetten voor (onderdelen van) het uitvoeren van cyberaanvallen. Zo blijkt uit onderzoek van de AIVD en MIVD dat alle door hen onderzochte pro-Russische hacktivistische groeperingen in zekere mate gesteund worden door de Russische overheid. Voor China geldt dat er een nauwe verwevenheid bestaat tussen inlichtingen- en veiligheidsdiensten, kennisinstellingen en bedrijven. Chinese bedrijven leveren bijvoorbeeld aanvalsinfrastructuur of malware, en kennisinstellingen doen onderzoek naar kwetsbaarheden in edge devices. Hierdoor zijn Chinese actoren structureel succesvol in het hacken van onder meer westerse overheden en bedrijven.

Dezelfde geopolitieke onvoorspelbaarheid leidt ertoe dat digitale afhankelijkheden risicovol kunnen worden terwijl ze dat eerder niet waren. Nederland is, net als andere landen, voor vele digitale processen en diensten afhankelijk van aanbieders uit andere landen, waaronder de Verenigde Staten. Wet- en regelgeving van dergelijke landen kan extraterritoriaal doorwerken en keuzes van die landen kunnen dus impact hebben op Nederland, ook wanneer deze niet direct tegen Nederland zijn gericht. Dit brengt onzekerheden met zich mee. Het is daarom van belang om afhankelijkheden doorlopend te beoordelen op potentiële risico's en, waar mogelijk, digitale en niet-digitale terugvalopties in te richten.

Geopolitieke ontwikkelingen, en met name de huidige onvoorspelbaarheid daarvan, leiden op verschillende manieren tot een ondoorzichtig en onvoorspelbaar dreigingslandschap. Daarbij dient ook in overweging te worden genomen dat dit plaatsvindt in een tijd waarin technologische ontwikkelingen elkaar in rap tempo opvolgen. Zo ontwikkelt generatieve Artificial Intelligence (AI) zich razendsnel en kunnen kwaadwillende actoren dit inzetten om aanvallen eenvoudiger en op grotere schaal uit te voeren – ook wanneer zij minder geavanceerd zijn.

Telecomsector illustratief voor samenkomen dreigingen, risico's en afwegingen

Een sector waarbinnen de vele risico's, dreigingen en afwegingen samenkomen, is de telecomsector. De impact die een succesvolle aanval op de telecomsector kan hebben is groot, onder andere omdat vele andere sectoren afhankelijk zijn van het functioneren van telecommunicatie. Door die afhankelijkheid kan een incident in de telecomsector al snel verstrekkende gevolgen hebben voor andere (vitale) sectoren. Alhoewel alle vitale sectoren interessante doelwitten vormen voor kwaadwillenden, heeft de telecomsector doorlopend hun aandacht. Zo kan de sector aantrekkelijk zijn voor het uitvoeren van spionage; hacks op telecommunicatieproviders behoren volgens de AIVD tot de meest waardevolle inlichtingenposities voor statelijke actoren. Ook sabotage kan een doel zijn, waarbij dat ook gericht kan zijn tegen (specifieke) afnemers die gebruik maken van het netwerk. Daarnaast is voor criminelen de sector interessant, vooral vanwege de grote hoeveelheden persoonsgegevens die daarbinnen worden verwerkt.

De telecomsector voert continu een balanceeract uit tussen veiligheid en toegankelijkheid van de diensten die het levert. Om gebruikers communicatiediensten aan te kunnen bieden, moet namelijk toegang worden verleend tot het netwerk. Daardoor worden miljoenen gebruikers aan het netwerk gekoppeld, wat een zekere mate van openheid vereist die kan schuren met digitale veiligheid.

Dat de dreiging richting de telecomsector reëel is en welke impact een succesvolle aanval kan hebben, werd duidelijk door de wereldwijde aanvalscampagne van cyberactor Salt Typhoon. De hackers drongen diep door in de infrastructuur van Amerikaanse telecomnetwerken en verkregen volgens media toegang tot privécommunicatie van onder andere de Amerikaanse president en vicepresident. Ook in Nederland was een aantal kleinere internet service- en hosting providers doelwit van Salt Typhoon.

Alhoewel de verschillende dreigingen, risico's en afwegingen die samenkomen in de telecomsector niet enkel voorbehouden zijn aan die sector, illustreert het de complexiteit van het huidige dreigingslandschap en de noodzaak van het maken van doorlopende risicoafwegingen.

Basisprincipes verhogen weerbaarheid tegen complex dreigingslandschap

De conclusie dat dreigingen onvoorspelbaarder en complexer worden, betekent niet per definitie dat het verdedigen daartegen dat ook wordt. Veel digitale incidenten vinden namelijk hun oorzaak in het niet op orde hebben van 'digitale basishygiëne'. De digitale basisprincipes, zoals opgesteld door het NCSC en DTC, vormen nog altijd een efficiënte verdediging tegen een groot gedeelte van cyberaanvallen. Voor een gemiddelde organisatie geldt dan ook: fixeer niet op het complexe dreigingslandschap, maar weer je daar in eerste instantie tegen met de basisprincipes. Een belangrijk onderdeel van die basisprincipes is het voorbereiden op incidenten, waarbij het gaat om de veerkracht en het herstelvermogen wanneer een incident zich heeft voorgedaan.

Meerdere incidenten bij Nederlandse slachtoffers tonen aan dat de cybersecuritymaatregelen bij veel organisaties binnen de Rijksoverheid al langere tijd ontoereikend zijn. Ondanks de diverse projecten en verbetertrajecten van de Rijksoverheid ten aanzien van cybersecurity zijn deze organisaties vaak niet in staat om aanvallen zelfstandig te detecteren en mitigeren. Veel overheidsorganisaties voldoen niet aan de informatiebeveiligingsrichtlijnen die de Rijksoverheid zelf voorschrijft. Het gebrek aan cybersecurity zorgt bovendien voor een vals gevoel van veiligheid; het is simpelweg onmogelijk om te concluderen dat overheidsorganisaties op dit moment niet zijn gecompromitteerd. De mate van weerbaarheid verschilt van organisatie tot organisatie en van sector tot sector. Te concluderen valt wel dat de Rijksoverheid nog stappen te zetten heeft op dit gebied. Het gaat daarbij ook om het adequaat inrichten van terugvalopties in het geval van uitval of verstoring van digitale processen. Daarnaast blijkt dat de afhankelijkheid van externe digitale dienstverleners en de mogelijke risico's die daaruit voortkomen niet voldoende worden afgewogen. De huidige geopolitieke onvoorspelbaarheid kan die risico's (verder) vergroten.

Uit voorgaande teksten blijkt dat niet alle factoren die digitale veiligheid beïnvloeden digitaal van aard zijn. Zo hebben geopolitieke ontwikkelingen geen digitale component, maar beïnvloeden ze digitale veiligheid wel. Dat betekent dat digitale veiligheid al lang niet meer alleen een opgave is voor technische experts. Het is ook, of misschien juist, een vraagstuk voor bestuurders om die niet-digitale factoren onderdeel te laten zijn van een continue en doorlopende risicoafweging.

1 Edge devices bevinden zich aan de rand van het netwerk en bestaan uit (beveiligings)producten zoals firewalls, VPN-servers, en routers.

Clinical Diagnostics (Eurofins) maakte in augustus bekend dat er gevoelige patiëntendata is gestolen van zorgverleners die onderzoek hebben laten verrichten bij het laboratorium. Dit zou zijn gebeurd bij een ransomware-aanval in juli. Bevolkingsonderzoek Nederland informeerde 941.000 personen dat hun data (mogelijk) is gestolen bij de aanval.

1 Jaarbeeld

Hoewel nuances veranderen, hebben er geen grote verschuivingen plaatsgevonden in het dreigingsbeeld. Er is sprake van een grote verscheidenheid aan typen incidenten, oorzaken, aanvallers en mate van impact. Zowel statelijke actoren als cybercriminelen voeren cyberaanvallen uit op Nederlandse doelen en/of raken Nederlandse belangen. Hierbij zijn edge devices blijvend interessant voor kwaadwillende actoren, wat onder andere geïllustreerd wordt door het incident bij het Openbaar Ministerie. Ook blijft er sprake van verstoringen die worden veroorzaakt door DDoS-aanvallen. Zo waren websites/applicaties van bijvoorbeeld DigiD verschillende keren niet of beperkt bereikbaar. Daarnaast zijn er met regelmaat cybersecurityincidenten bij toeleveranciers/dienstverleners die leiden tot datalekken bij afnemers. Een voorbeeld hiervan is de ransomware-aanval op een laboratorium waarbij gevoelige data werd gestolen van diverse zorgverleners en hun patiënten. Verder vond in 2025 de NAVO-top plaats in Nederland. Alhoewel geopolitieke evenementen een aantrekkelijk doelwit zijn voor kwaadwillenden, zagen we tijdens de NAVO-top geen cyberincidenten die leidden tot verstoring van de top of maatschappelijke ontwrichting.

Naast cyberaanvallen zijn er opnieuw tal van voorbeelden van storingen als gevolg van niet moedwillig handelen. Meer dan eens waren softwarefouten de oorzaak van verstoringen.

Verscheidenheid incidenten illustreert diffuus dreigingsbeeld

Verstoring van diensten door DDoS-aanvallen

De afgelopen rapportageperiode zorgden meerdere DDoS-aanvallen voor (tijdelijke) verstoringen van diensten. Zo vonden van januari tot en met maart 2025 vier aanvallen plaats waardoor DigiD een uur of langer niet beschikbaar was. Daardoor waren ook aanverwante diensten beperkt beschikbaar en konden gebruikers tijdelijk niet inloggen. Een DDoS-aanval is laagdrempelig in te zetten en organisaties kunnen zich relatief goed weerbaar maken tegen dit type aanval. Over het algemeen is de impact van DDoS-aanvallen dan ook beperkt en wordt slechts de beschikbaarheid van digitale processen tijdelijk aangetast. In geval van de aanvallen op DigiD begin dit jaar stelde Logius, beheerder van DigiD, dat het om een ander kaliber DDoS-aanvallen ging. De aanvallen wisten zich volgens Logius sneller aan te passen aan de defensieve inspanningen.[1] Daarnaast stelde Logius dat het niet met zekerheid kon aangeven of er meer DDoS-aanvallen op DigiD plaatsvonden dan

voorheen. Mogelijk dat het type aanval zichtbaarder is voor gebruikers omdat de aanvallen een belangrijk proces raakten. Ook later in het jaar zorgden DDoS-aanvallen op DigiD voor verstoringen. Andere aanvallen die voor verstoring van dienstverlening zorgden waren de aanvallen op Adyen, SURF en websites van de Nederlandse overheid. Bij Adyen ontstonden betalingsproblemen in (online) winkels en horeca. Het is niet bekend wie verantwoordelijk is voor de aanvallen op DigiD en Adyen. Door DDoS-aanvallen op SURF kampten onderwijsinstellingen en ziekenhuizen met (internet)verstoringen, het is onbekend wie er achter de aanvallen zit. Tot slot waren Nederlandse overheidswebsites tijdelijk uit de lucht door DDoS-aanvallen, hiervoor waren pro-Russische hackers verantwoordelijk.

Minimaal 121 unieke Nederlandse ransomware-incidenten in 2024

In 2024 hebben het NCSC, de Politie, het Openbaar Ministerie, Cyberveilig Nederland en cybersecuritybedrijven maandelijks informatie over ransomware-incidenten uitgewisseld in het kader van project Melissa (zie Bijlage 2). Uit die gegevens blijkt dat er in 2024 minimaal 121 unieke ransomware-incidenten in Nederland zijn geweest. 76 van deze incidenten zijn bekend via aangiften en 20 via incident response bedrijven. Daarbovenop is bij 25 van de unieke incidenten sprake van overlap - dit betreft incidenten die zowel uit de maandelijkse uitvraag als uit de aangifte data van de politie naar voren zijn gekomen. Over 2023 bleek nog uit project Melissa dat er sprake was van minimaal 147 unieke ransomware-aanvallen. Opgemerkt moet worden dat uitgegaan wordt van de initiële ransomware-aanval. Een aanval op een aanbieder met tientallen klanten die ook slachtoffer worden van dezelfde aanval, telt dus als 1 aanval. Uit een analyse van de ransomware-aanvallen in 2024 blijkt dat cybercriminelen geen nieuwe technieken gebruiken om ransomware in te zetten. Zo verkrijgen criminelen nog steeds het vaakst via kwetsbaarheden in software en via accountovername toegang.[2] In 2024 ontving de Autoriteit Persoonsgegevens 1.430 unieke datalekmeldingen van cyberaanvallen, waarvan het er 853 heeft onderzocht. Van de onderzochte aanvallen ging het in 112 gevallen (13 procent) om ransomware. Bij minimaal 53 procent van die ransomware-aanvallen werd data gestolen.[3]

Spionage en (voorbereidingshandelingen voor) sabotage door statelijke actoren, onder andere in Nederland

De AIVD en MIVD stellen dat Rusland, China, Iran en Noord-Korea offensieve cyberprogramma's hebben die zijn gericht tegen de Nederlandse belangen en waarmee zij onder andere spioneren, beïnvloeden en saboteren. Sabotage heeft in potentie de grootste impact op de Nederlandse samenleving.[4] Ook andere dan de hierboven genoemde landen investeren in cyberprogramma's. Alhoewel offensieve cyberprogramma's van andere landen niet specifiek tegen Nederland gericht hoeven te zijn, kan dat in de toekomst wel veranderen. Hierdoor kunnen Nederlandse belangen worden geraakt of kan bijvoorbeeld de Nederlandse digitale infrastructuur worden misbruikt en ingezet bij aanvallen op andere doelwitten.[5]

Grote cybersecuritybedrijven publiceerden deze rapportageperiode meerdere keren over wereldwijde cybercampagnes van statelijke actoren. Daarbij waren ook Nederlandse slachtoffers te onderkennen. Zo verscheen in de media dat de Universiteit Delft (onsuccesvol) was aangevallen door Salt Typhoon. Bevestigd kan worden dat de universiteit is gescand, maar dat er geen sprake was van een aanval. CrowdStrike berichtte deze rapportageperiode dat Noord-Koreaanse hackers ook cyberaanvallen hebben uitgevoerd op Nederlandse organisaties.

Verder werd de politie in september 2024 slachtoffer van een cyberaanval. Bij deze aanval maakten kwaadwillenden werkgerelateerde contactgegevens buit van politiemedewerkers. De diensten en politie hebben niet kunnen vaststellen dat andere gegevens zijn buitgemaakt. Deze aanval werd in mei 2025 door de Nederlandse inlichtingendiensten geattribueerd aan een tot dan toe onbekende, zeer waarschijnlijk Russische staatsgesteunde cyberactor. Naast de Nationale Politie zou de groep, Laundry Bear genoemd, ook andere Nederlandse organisaties hebben aangevallen als onderdeel van een wereldwijde campagne. Daarnaast waarschuwde de MIVD in mei 2025 voor een spionagecampagne van APT28[II], deze zou spionageoperaties hebben uitgevoerd tegen Oekraïne en NAVO-landen. De Nederlandse krijgsmacht, ministeries en het bedrijfsleven zijn direct en indirect doelwit geweest van deze cyberspionagepogingen. Verder stelde de MIVD dat in 2024 Nederland voor het eerst slachtoffer was van moedwillige cybersabotage door een Russische staatsgesteunde groepering. Deze cybersabotageaanval was gericht op het digitale bedieningssysteem van een openbare faciliteit.[6]

Incidenten bij toeleveranciers leiden tot datalekken, illustreren kwetsbaarheid toeleveringsketen

Een cyberincident bij een toeleverancier of dienstverlener kan verstrekkende gevolgen hebben voor organisaties binnen dezelfde keten, waaronder klanten van het bedrijf. Dit werd deze periode bijvoorbeeld geïllustreerd door een cyberaanval op een toeleverancier van verschillende gemeenten. Dit zorgde bij onder meer de gemeente Dinkelland, Tubbergen en Amersfoort voor datalekken. Daarnaast leidde een ransomware-aanval op een Nederlands laboratorium tot het lekken van zeer gevoelige gegevens van honderdduizenden patiënten. Deze data was afkomstig van diverse zorgverleners die werk hadden laten verrichten door het laboratorium.

II De afkorting APT staat voor Advanced Persistent Threat: een voortdurende dreiging van een geavanceerde tegenstander, zoals statelijke actoren of cybercriminelen. Een APT verschilt van andere digitale dreigingsactoren door de mate van capaciteiten, de (lange) tijdsinvestering, het motief, de vasthoudendheid en soms ook de gekozen methoden van de aanvaller. Unieke APT's worden binnen de cybersecuritywereld vaak aangeduid met een naam. Dit kan zijn APT gevolgd door een nummer, maar ook code namen zoals Fancy Bear of Forest Blizzard.

NAVO-Top in Nederland: incidenten binnen verwachting, geen significante impact

Op 24 en 25 juni 2025 vond de NAVO-top plaats in Den Haag. De top trok tientallen wereldleiders, ministers en duizenden delegatieleden en kreeg wereldwijde aandacht. Dergelijke geopolitieke evenementen zijn een aantrekkelijk doelwit voor kwaadwillenden. Hoewel tijdens de top enkele storingen zich voordeden in de transport- en telecomsector, hadden deze volgens betrokken partijen geen cybersecuritycomponent. De media besteedden aandacht aan een DDoS-campagne door pro-Russische hackers gericht op Nederlandse organisaties, maar de daadwerkelijke impact hiervan was zeer beperkt.

Het NCSC stelde samen met partners vooraf scenario's op. Deze maakten een goede voorbereiding op voorstelbare incidenten mogelijk en zorgden ervoor dat tijdens de NAVO-top eventuele incidenten daartegen afgezet werden en de waarschijnlijkheid kon worden ingeschat. Alle incidenten pasten in de vooraf geschetste scenario's. Wel laat de aandacht voor een dergelijk evenement zien dat zelfs de kleinste, vaker voorkomende verstoringen meteen vol in de schijnwerpers staan. Dit kan de gepercipieerde aanwezigheid van de dreiging vergroten en de beeldvorming vertroebelen.

Om goed voorbereid te zijn is er voorafgaand aan, tijdens en rondom de NAVO-top ingezet op verschillende aspecten van digitale weerbaarheid. Daarbij was ook veel aandacht voor niet-technische maatregelen, zoals publiek-private samenwerking. Alles met als doel om niet alleen de NAVO-top veilig te houden, maar ook daarna de vruchten ervan te kunnen plukken.

Processen ontregeld door softwarefouten en verouderde hardware

In juli 2024 rolde CrowdStrike een software update uit waarna Windows-systemen offline gingen en een 'blue screen of death' toonden. Hierdoor kwamen hele systemen plat te liggen en kampten (vitale) organisaties wereldwijd met problemen. Een maand later zorgde een softwarefout in een standaard netwerkonderdeel van het Defensienetwerk NAFIN voor een grootschalige storing in Nederland, waarbij processen van allerlei overheidsinstanties en Eindhoven Airport werden verstoord. De NAFIN- en CrowdStrike-storingen waren zichtbaar wegens hun grote impact, maar ook op kleinere schaal werden deze rapportageperiode processen ontregeld door storingen. Het Arnhemse ziekenhuis Rijnstate zag zich genoodzaakt planbare zorg af te zeggen nadat een software update ertoe leidde dat medewerkers geen gegevens meer konden verwerken in het patiëntendossier. Het Openbaar Ministerie haalde in maart zelfs tijdelijk ict-systemen offline wegens een 'hardnekkige storing'. Hoewel de exacte oorzaak van de storing niet bekend is gemaakt, gaf het OM aan vaker met storingen te kampen, (mede) door verouderde infrastructuur.

Cyberaanvallen raken alle lagen van de samenleving, grote incidenten tonen kwetsbaarheid

Edge devices onverminderd aantrekkelijk voor kwaadwillende actoren

In het CSBN 2024 is gesteld dat kwaadwillenden in toenemende mate edge devices aanvallen. Deze rapportageperiode laat zien dat deze apparaten onverminderd interessant zijn als doelwit voor kwaadwillende actoren. Een Nederlands incident dat dit illustreert is het misbruik van kwetsbaarheden in Citrix waarvoor het NCSC in juli (opnieuw) waarschuwde. Hieraan gerelateerd was het incident bij het Openbaar Ministerie (OM) in juli 2025. Het OM besloot vanwege de kwetsbaarheden om alle systemen van het internet te ontkoppelen, waardoor het voor haar werkzaamheden over moest op noodprocessen. Dit had impact op de strafrechtketen, waarbij advocaten aangaven hun werk niet goed te kunnen doen. In sommige zaken leidde de ontkoppeling direct tot vertraging. In augustus 2025 bevestigde het OM dat onbevoegden via een kwetsbaarheid toegang hebben verkregen tot de systemen. Het is niet bekend of hierbij data is gestolen of gemanipuleerd. Het NCSC stelde dat ook een aantal andere Nederlandse organisaties succesvol zijn aangevallen en dat één van de kwetsbaarheden al ruim voor publieke bekendmaking werd misbruikt.

Cyberaanvallen op telecomsector illustreren interesse kwaadwillenden in vitale infrastructuur

Cyberaanvallen, door zowel statelijke actoren als cybercriminelen, raken alle lagen van de samenleving waaronder ook de vitale infrastructuur. In het CSBN 2024 werd al beschreven dat er uiteenlopende cyberaanvallen hadden plaatsgevonden, waarbij organisaties in vitale sectoren in westerse landen werden geraakt. Ook deze rapportageperiode zijn door zowel cybersecuritybedrijven als overheden aanvallen waargenomen die de aanhoudende interesse in de vitale infrastructuur illustreren. Zo zijn er de afgelopen periode wereldwijd verschillende aanvallen op de telecomsector waargenomen. Sommige van die aanvallen waren van langdurige aard en toonden aan dat kwaadwillenden zich al geruime tijd in de systemen bevonden. Een voorbeeld hiervan zijn de aanvallen van de Chinese hackersgroep Salt Typhoon op (voornamelijk) telecombedrijven waarbij in Amerika grote providers langdurig waren gecompromitteerd (zie Hoofdstuk 3 voor een verdieping). In Nederland compromitteerde de groep routers van kleinere internet service- en hosting providers, voor

zover bekend zijn de hackers daar niet doorgedrongen in de interne netwerken. De telecomsector is voor statelijke actoren een interessant doelwit vanwege onder meer de hoeveelheid (gevoelige) data (zie Hoofdstuk 3). Daarnaast voeren ook cybercriminelen aanvallen uit op die sector. Zo claimde een nieuwe ransomwaregroep een aanval op het Amerikaanse telecombedrijf WideOpenWest. Daarbij zouden de criminelen niet alleen controle hebben verkregen over kritische systemen maar ook data hebben gestolen. Ook in Europa zijn voorbeelden van cyberincidenten bij telecombedrijven. Zo meldde zowel Orange als Bouygues (beide Frankrijk) slachtoffer te zijn geworden van cyberaanvallen. Verdere details over de aanvallen zijn niet bekend, het is daarom onduidelijk wie erachter zit en wat de motieven waren.

Grootste cryptodiefstal ooit door naar verluidt Noord-Koreaanse staatshackers

Noord-Korea is een statelijke actor wiens offensieve cyberprogramma gericht is op zowel spionage als financieel gewin. Met regelmaat vinden incidenten plaats waarbij Noord-Koreaanse actoren financieel gemotiveerde aanvallen uitvoeren. Met de buitgemaakte winst probeert Noord-Korea de opgelegde sancties te omzeilen en het regime in stand te houden. Hierbij worden ook Nederlandse slachtoffers gemaakt. Een geliefd doelwit zijn cryptobeurzen en bedrijven in die sector, welke uiteraard niet alleen worden aangevallen door staatshackers maar ook doelwit zijn van cybercriminelen. Opvallend deze periode was de cyberaanval op ByBit. Daarbij maakte, naar verluidt Noord-Koreaanse, (staats)hackers bijna 1,5 miljard dollar aan digitale valuta buit. Dit is tot op heden de grootste cryptodiefstal ooit.

Internationale acties tegen kwaadwillenden en hun infrastructuur

Internationale operaties verstoren cybercriminele infrastructuur

Deze rapportageperiode vonden meerdere grootschalige internationale operaties plaats, waarbij opsporingsinstanties wereldwijd criminele infrastructuur verstoorden. In 2025 werd opnieuw Operation Endgame uitgevoerd.[7] Tijdens deze gecoördineerde internationale operatie van opsporingsautoriteiten werden meerdere botnets[III] ontmanteld die werden gebruikt voor grootschalige cybercriminaliteit. Meer dan 300 servers werden wereldwijd offline gehaald, waarvan 60 servers zich in Nederland bevonden. Daarnaast richtte Operation Magnus, aangestuurd door de Nederlandse politie en het OM, zich op het ontmantelen van infostealers.[8] Dit is malware die gevoelige informatie, zoals inloggegevens, van slachtoffers buitmaakt. Binnen Operation PowerOFF, waarvan onder andere de Nederlandse politie en het OM coördinatoren waren, werden aanbieders en gebruikers van DDoS-for-hire diensten aangepakt.[9] Ook werd onder Operation Moonlander proxydienst Anyproxy offline gehaald.[10] Dit platform werd door cybercriminelen gebruikt voor onder andere phishing, ransomware-aanvallen en datadiefstal. Een deel van de Anyproxy-infrastructuur werd in Nederland gehost. Tot slot werd in een internationale, door de Nederlandse politie en het OM gecoördineerde, operatie met Amerika en Finland een zogenoemde Counter Antivirus (CAV)-dienst uit de lucht gehaald.[11] Met een CAV-dienst kunnen ontwikkelaars van malware testen of hun malware gedetecteerd wordt door verschillende antivirusprogramma's. De dienst die uit de lucht werd gehaald is AVCheck, een van de grootste CAV-diensten die internationaal gebruikt werd door cybercriminelen.

Nederland vervult belangrijke rol binnen internationale samenwerking en zet in op informatiedeling en daderpreventie

Nederland draagt actief bij aan internationale samenwerking tegen cyberdreigingen. De Nederlandse FIOD, het Duitse BKA, Europol en cybersecuritybedrijf zeroShadow haalden in 2025 een servernetwerk in Duitsland, dat werd gebruikt voor het witwassen van door Noord-Korea gestolen cryptovaluta, offline. Daarbij werd €34 miljoen aan cryptovaluta inbeslaggenomen.[12]

De Nederlandse overheid werkt samen met publieke en private organisaties, in zowel nationaal als internationaal verband, onder andere om informatiedeling te bevorderen. Het samenwerkingsverband Melissa richt zich op de bestrijding van ransomware-aanvallen door technische, juridische en operationele kennis en middelen te bundelen, te delen en om te zetten in gezamenlijke acties. De partners van het samenwerkingsverband hebben een bijdrage geleverd aan operatie Endgame en het onderzoek naar een CAV-dienst.

De Nederlandse politie investeert in samenwerking met publieke en private partners op het gebied van daderpreventie[IV]. Ook worden buitenlandse politieorganisaties gestimuleerd om zich bezig te houden met daderpreventie; vanuit de Nederlandse politie is het internationale daderpreventie cybercrime netwerk (InterCOP) gelanceerd.[13] Dit is een samenwerkingsverband dat inmiddels uit 37 landen bestaat. Binnen het onderzoek naar een CAV-dienst zijn door de Nederlandse politie brede interventies ingezet. Zo is er een nep login-pagina online gezet, met als doel om gebruikers van AVCheck aan te spreken, te waarschuwen en af te schrikken. Binnen eerdergenoemde operaties Endgame en PowerOFF is ook ingezet op alternatieve interventies met een verstorende en/of afschrikkende werking.

III De term botnet (afkomstig van 'robot network') wordt gebruikt voor een verzameling van computers waarop malware is geïnstalleerd zonder dat de eigenaren zich daarvan bewust zijn. Deze geïnfecteerde computers (bots) vormen een netwerk en worden centraal aangestuurd via een server. Een botnet kan bijvoorbeeld worden gebruikt om ongewenste e-mail (spam) door te sturen of DDoS-aanvallen uit te voeren.

IV Daderpreventie ziet toe op (1) het afschrikken van potentiële daders en (2) het trachten hen bij te sturen naar positieve en legale keuzes.

Individuen en groepen gearresteerd, veroordeeld en/of op sanctielijst

In deze rapportageperiode zijn meerdere individuen en groepen gesanctioneerd, veroordeeld en/of gearresteerd. In het kader van Operation Endgame zijn twintig cybercriminelen toegevoegd aan de lijst van Europe's Most Wanted Fugitives.[14] In het kader van Operation Magnus heeft de Verenigde Staten een beheerder van een infostealer in staat van beschuldiging gesteld en heeft de Belgische politie twee personen aangehouden.[15] Ook is een internationale operatie uitgevoerd, gecoördineerd door Europol en Eurojust, tegen zowel de daders als de onderliggende infrastructuur van de pro-Russische hackersgroep NoName057(16). NoName057(16) heeft in de afgelopen jaren veel digitale aanvallen uitgevoerd op landen die steun bieden aan Oekraïne, waaronder Nederland. Twee mensen zijn gearresteerd, er zijn voor acht personen arrestatiebevelen uitgevaardigd en ruim duizend aanhangers van de groep hebben bericht gekregen dat justitie ze in het vizier heeft. Meer dan honderd servers waarmee de groep DDoS aanvallen uitvoerde zijn offline gehaald.[16] Desondanks blijft NoName057(16) actief. De groep heeft nieuwe allianties gesloten met andere pro-Russische hackers en blijft doorgaan met hun aanvallen, onder andere gericht op politieke partijen, overheden, vervoersbedrijven en politie in verschillende Europese landen.[17]

Deze rapportageperiode vond voor het eerst in Nederland een veroordeling van een hostingprovider plaats, omdat die zich schuldig maakte aan het faciliteren van een botnet.[18] [19] De servers zijn in beslaggenomen en vernietigd.

In het verlengde daarvan hebben de politie en het OM geïnvesteerd in het opbouwen van de samenwerking met de Autoriteit Consument en Markt (ACM). De ACM is aangewezen als toezichthouder voor de naleving van de verplichtingen die volgen uit de digitale dienstenverordening. Verplichtingen voor hostingproviders die volgen uit de verordening gaan bijvoorbeeld over het tijdig en adequaat reageren op bevelen en Notice and Takedown-verzoeken. Zulke verplichtingen gelden voor alle hostingproviders binnen de Europese Unie (EU). De politie, het OM en de ACM zullen nauw samenwerken in de aanpak van bad hosting. Dit geldt ook voor de Autoriteit online Terroristische en Kinderpornografisch Materiaal (ATKM), waarmee zal worden samengewerkt om bad hosting aan te pakken.

Zoals in het CSBN 2024 vermeld, zijn eind juni 2024 op initiatief van Nederland voor het eerst twee cybercriminelen op de Europese sanctielijst geplaatst. Recentelijk heeft de EU deze sancties met drie jaar verlengd.[20] De EU plaatste in december 2024 de Russische staatshackersgroep GRU 29155[V] op de sanctielijst. De MIVD waarschuwde in september 2024 nog voor activiteiten van deze eenheid, welke zouden zijn gericht op het in beeld krijgen en verstoren van de westerse hulp aan Oekraïne.[21] Op 27 januari 2025 werden nog eens drie Russische individuen die deel uitmaken van GRU 29155 toegevoegd aan de EU sanctielijst, wegens hun betrokkenheid bij cyberaanvallen op Estland.[22] [23]

In 2025 heeft de EU wegens het mogelijk maken van "destabiliserende activiteiten" tegen de EU sancties opgelegd aan webhostingprovider Stark Industries en aan de twee personen die het bedrijf leiden. Hierdoor is ook PQ Hosting indirect gesanctioneerd.[24] Door deze sancties mogen de personen de EU niet meer inreizen, hun tegoeden worden bevroren en burgers en bedrijven in de EU mogen geen zaken meer doen met de gesanctioneerde bedrijven en personen. Dit is een belangrijke stap naar een veiliger cyberdomein.

V De GRU, ook wel afgekort als GROe, is de Russische militaire inlichtingendienst. 29155 verwijst naar een specifieke eenheid binnen die organisatie.

2024

Juli 2024

Binnenland

- Onder meer vliegverkeer en gezondheidszorg ontregeld door wereldwijde computerstoring als gevolg van foutieve update

Buitenland

- Russische staatshackers voeren cyberaanvallen uit op Olympische Spelen

Augustus 2024

Binnenland

- Overheidsdiensten en vliegverkeer Eindhoven verstoord door softwarefout op netwerk Defensie

September 2024

Binnenland

- Gegevens politiemedewerkers buitgemaakt bij cyberaanval door Russische zeer waarschijnlijk staatsgesteunde cyberactor
- Bedrijfsgegevens gestolen bij Fortinet na cyberaanval

Oktober 2024

Binnenland

- Nederlandse overheidswebsites tijdelijk uit de lucht door DDoS-aanvallen van pro-Russische hackers
- Afspraken afgezegd door storing bij diverse Gelderse gemeenten na software-update
- Kritieke kwetsbaarheid in Fortimanager wereldwijd misbruikt
- Data gestolen bij phishingaanval op gemeente Velsen
- Duizenden e-mailadressen op straat door hack bij medewerker van Combinatie Jeugdzorg

Buitenland

- Websites vitale infrastructuur en overheid Cyprus tijdelijk verstoord door gecoördineerde cyberaanvallen van pro-Palestijnse groeperingen
- Europese zorginstanties aangevallen met ransomware
- Europese overheden en militaire organisaties zijn doelwit geweest van Russische phishingaanvallen

November 2024

Binnenland

- Data gestolen na grootschalig misbruik van kritieke kwetsbaarheid in Cleo file transfer software
- Data gestolen bij Ahold Delhaize na ransomware-aanval

Buitenland

- Verstoring processen Duitse apotheekgroothandel door ransomware-aanval

December 2024

Binnenland

- Data gemeenten gelekt na cyberaanval op softwareleverancier

Buitenland

- 680 gigabyte aan data gestolen bij Blue Yonder door ransomwaregroep
- Amerikaanse telecominfrastructuur gecompromitteerd door Chinese hackers
- Klanten Deens waterzuiveringsbedrijf zonder water door cybersabotage van pro-Russische hackers

2025

Januari 2025

Binnenland

- Communicatieproblemen bij hulpdiensten door urenlange landelijke storing C2000-systeem
- Geen onderwijs en tentamens uitgesteld na cyberaanval op TU Eindhoven
- DigiD niet bereikbaar door storing, veroorzaakt door DDoS-aanval
- Drie dagen op rij (internet)storingen bij onderwijsinstellingen en ziekenhuizen, veroorzaakt door DDoS-aanvallen
- Patiënten afgebeld en operaties uitgesteld door computerstoring in Rijnstate
- Persoonsgegevens van 2.200 gebruikers gelekt na aanval op website raad van Almere
- Ambassades in Europese landen, waaronder in Nederland, aangevallen door vermoedelijk Russische hackers

Buitenland

- Locatiegegevens van mogelijk miljoenen mensen gelekt na hack bij datahandelaar
- Data gestolen bij ransomware-aanval op Italiaans ziekenhuis, maar systemen niet versleuteld

Februari 2025

Binnenland

- Paragon spyware ingezet tegen Europese WhatsApp-gebruikers, ook tegen Nederlandse nummers
- Politienummer 0900-8844 tijdelijk niet bereikbaar door een storing

Buitenland

- Systemen Canadese telecombedrijven gecompromitteerd

Maart 2025

Binnenland

- DigiD slecht bereikbaar wegens terugkerende DDoS-aanvallen
- Strafzittingen ondervinden hinder na herstelwerkzaamheden storing OM
- Nederlandse bedrijven aangevallen door Noord-Koreaanse hackers

Buitenland

- 1,5 miljard dollar aan crypto gestolen door Noord-Koreaanse hackers

April 2025

Binnenland

- DigiD beperkt beschikbaar door DDoS-aanvallen
- Datalek bij ministeries door foutief uploaden documenten, impact onduidelijk
- Betalingsproblemen door DDoS-aanvallen op Adyen
- Ruim vijftig Nederlandse websites korte tijd moeilijk bereikbaar door DDoS-aanvallen

Buitenland

- Waalse overheid koppelt zichzelf los van het internet na gerichte cyberaanval
- APT29 voert phishing-aanvallen uit op de diplomatieke entiteiten in Europa
- Waterstroom Noorse dam aangepast door pro-Russische hackers

Mei 2025

Binnenland

- Nederland (in)direct doelwit van cyberspionagepogingen door Russische staatshackers

Buitenland

- Lege schappen bij Britse supermarkten na cyberaanval

Juni 2025

Binnenland

- Nederlandse organisaties doelwit van DDoS-aanvallen, impact beperkt
- Internationaal Strafhof slachtoffer van cyberaanval

Juli 2025

Binnenland

- Strafrechtsketen verstoord nadat netwerk OM offline werd gehaald vanwege Citrix-kwetsbaarheid
- Wereldwijd organisaties gecompromitteerd via kwetsbaarheid in SharePoint, ook Nederlandse organisaties geraakt

Buitenland

- Verstoring van diensten voor Franse klanten Orange na cyberaanval
- Landelijke uitval 4G- en 5G-netwerk in Luxemburg na cyberaanval
- Data gestolen van Orange België na cyberaanval

Augustus 2025

Binnenland

- Gevoelige data burgers gelekt na ransomware-aanval op laboratorium
- Werkzaamheden instanties Caribische eilanden verstoord door cyberincidenten
- Data KLM gestolen nadat aanvallers toegang wisten te krijgen tot platform externe partij
- Routers Internet Service - en Hosting providers gecompromitteerd door Salt Typhoon

Buitenland

- Gegevens 6,4 miljoen klanten van Franse Bouygues Telecom gestolen bij cyberaanval
- Data van diverse grote bedrijven gestolen na aanvallen op CRM-systemen
- Data gestolen en bedrijfsactiviteiten verstoord na cyberaanval op telecombedrijf Colt
- Grootschalige datadiefstal uit Salesforce-omgevingen na inbraak bij Salesloft Drift
- Productie en dienstverlening Jaguar Land Rover wekenlang verstoord door cyberaanval

Opvallende incidenten Nederland

Juli 2024

Onder meer vliegverkeer en gezondheidszorg ontregeld door wereldwijde computerstoring als gevolg van foutieve update
Op 19 juli introduceerde CrowdStrike een software-update die ervoor zorgde dat er wereldwijd zo'n 8,5 miljoen Windowssystemen onbruikbaar werden.[25] De fout zorgde voor 'Blue Screens of Death' op Windowssystemen.[26] Dit zorgde wereldwijd voor grote problemen, zo ook in Nederland. Schiphol annuleerde vluchten en in sommige ziekenhuizen werd de zorg afgeschaald. Ook delen van de overheid werden geraakt. Zo ondervonden het ministerie van Buitenlandse Zaken en het UWV hinder van de storing.[27] [28] Hoewel een deel van de bedrijven na het uitvoeren van de arbeidsintensieve workaround relatief snel weer online was, ondervond een deel van de CrowdStrike-klanten ook na een paar dagen nog problemen.

Augustus 2024

Overheidsdiensten en vliegverkeer Eindhoven verstoord door softwarefout op netwerk Defensie
Eind augustus kampten hulpdiensten en diverse overheidsinstellingen met een IT-storing. De oorzaak van de problemen lag in de toegangsverlening tot het zogenoemde Netherlands Armed Forces Integrated Network (NAFIN). Hulpdiensten hadden hierdoor problemen met hun communicatie- en alarmeringssysteem, waardoor ze onderling moeilijker konden communiceren. Ambtenaren van diverse ministeries konden niet inloggen op werksystemen. Ook Eindhoven Airport ondervond hinder vanwege het gebruik van datzelfde netwerk. Daar konden vliegtuigen niet opstijgen of landen. Er kwamen ook berichten van diverse gemeenten waarbij de dienstverlening was verstoord. Zo konden er geen rijbewijzen en paspoorten worden afgegeven. Ook DigiD werd geraakt door de storing.[29] NAFIN is een zwaarbeveiligd netwerk dat onder meer Defensielocaties met elkaar verbindt en ook wordt gebruikt bij datacenters van verschillende ministeries en politiebureaus. Door een fout in de software ontstond een probleem in de tijdsynchronisatie op het netwerk.[30] Uit de evaluatie van de storing blijkt dat er onvoldoende aandacht is geweest voor cyberrisico's en de bredere maatschappelijke impact.[31]

September 2024

Gegevens politiemedewerkers buitgemaakt bij cyberaanval door Russische zeer waarschijnlijk staatsgesteunde cyberactor
Eind september werd de politie slachtoffer van een hack waarbij contactgegevens van politiemedewerkers zijn buitgemaakt. Hierbij verkregen hackers de gegevens van alle politiemedewerkers via de global address list. In sommige gevallen werden ook privégegevens buitgemaakt.[32] Er is gebruikgemaakt van een zogenoemde 'pass-the-cookie-aanval'.[VI] In mei 2025 maakten de inlichtingendiensten bekend dat een Russische zeer waarschijnlijk staatsgesteunde cyberactor, welke Laundry Bear wordt genoemd, verantwoordelijk was voor de aanval. Naast de aanval op de Nationale Politie werden wereldwijd ook andere organisaties door de groep aangevallen, waaronder in Nederland.[33]

Bedrijfsgegevens gestolen bij Fortinet na cyberaanval
Fortinet heeft bevestigd dat het slachtoffer is geworden van een cyberaanval waarbij de hacker claimt klant- en bedrijfsgegevens te hebben gestolen. Volgens de aanvaller is er 440GB aan gegevens buitgemaakt, welke van een Microsoft Azure SharePoint-server gestolen zouden zijn. De crimineel zou losgeld van Fortinet hebben geëist, maar dat heeft het bedrijf niet betaald. Het bedrijf stelde wel dat het incident minder dan 0,3% van het klantenbestand heeft getroffen en dat het niet heeft geleid tot kwaadaardige activiteiten gericht op klanten.[34] Uit onderzoek van het NCSC blijkt dat de impact voor Nederland beperkt is.[35]

Oktober 2024

Nederlandse overheidswebsites tijdelijk uit de lucht door DDoS-aanvallen van pro-Russische hackers
Verschillende Nederlandse overheidswebsites zijn tijdelijk onbereikbaar geweest door een DDoS-aanval. Deze aanval werd opgeëist door een pro-Russische hacktivistische groep.[36]

Afspraken afgezegd door storing bij diverse Gelderse gemeenten na software-update
Door een grote technische storing konden inwoners van Nijmegen, Beuningen, Berg en Dal, Wijchen, Druten en Heumen tijdelijk niet terecht bij hun gemeenten. Alle afspraken werden afgezegd. De storing werd veroorzaakt door een update van authenticatie software, een hack is volgens de gemeenten uitgesloten.[37]

Kritieke kwetsbaarheid in Fortimanager wereldwijd misbruikt
Een kritieke kwetsbaarheid in de managementtool Fortimanager van Fortinet is wereldwijd misbruikt. Bij het misbruik zouden voornamelijk configuratie-bestanden zijn buitgemaakt die onder andere gehashte wachtwoorden van gebruikers bevatten.[38] Daarnaast vond het misbruik al plaats sinds juni 2024, voordat er een patch beschikbaar was. Uit onderzoek van het NCSC bleek dat er ook kwetsbare systemen in Nederland vanaf het internet bereikbaar waren. De desbetreffende organisaties zijn door het NCSC en sectorale samenwerkingspartners geïnformeerd.

Data gestolen bij phishingaanval op gemeente Velsen
De gemeente Velsen is slachtoffer geworden van een phishingaanval. De phishingmail in kwestie werd verstuurd vanuit een bekende, vertrouwde organisatie, waardoor deze werd geopend door een medewerker van de gemeente. Daardoor zijn mailadressen van 327 Velsenaren gestolen, ook zijn enkele interne adressen en telefoonnummers buitgemaakt.[39]

Duizenden e-mailadressen op straat door hack bij medewerker van Combinatie Jeugdzorg
Een hacker heeft duizenden e-mailadressen buitgemaakt van zorginstellingen en andere bedrijven waarmee de Eindhovense organisatie Combinatie Jeugdzorg zakendoet. Ook zijn er e-mailadressen van cliënten gelekt. Volgens Combinatie Jeugdzorg gaat het alleen om e-mailadressen en voor zover bekend niet om andere persoonlijke informatie. Wie verantwoordelijk is voor de hack is onbekend.[40]

November 2024

Data gestolen na grootschalig misbruik van kritieke kwetsbaarheid in Cleo file transfer software
Kwetsbaarheden in de Cleo file transfer software zijn uitgebuit door kwaadwillenden. De cybercriminele groep Clop zou verantwoordelijk zijn voor het misbruik en heeft daarmee data gestolen van tientallen organisaties.[41] De criminelen wisten ook data te stelen bij het Nederlandse Centric. Volgens het bedrijf hebben de criminelen toegang verkregen tot een testserver waar privacygevoelige data van 1 klant op stond.[42] Het zou gaan om de data van 24 (oud-)inwoners van de gemeente Amersfoort.[43]

Data gestolen bij Ahold Delhaize na ransomware-aanval
Een hackerscollectief claimt dat het een ransomware-aanval heeft uitgevoerd op Ahold Delhaize. Er zou daarbij 6 terabyte aan data zijn gestolen.[44] Hoewel in eerste instantie werd gesteld dat het om Amerikaanse gegevens zou gaan, bleek in een later stadium dat er mogelijk ook gegevens van Nederlandse (voormalig) medewerkers zijn buitgemaakt.[45] Het zou volgens latere berichtgeving gaan om persoonsgegevens van in totaal 2,2 miljoen mensen.[46]

December 2024

Data gemeenten gelekt na cyberaanval op softwareleverancier
Diverse gemeenten maakten bekend dat persoonsgegevens van hun inwoners waren gelekt. De gegevens zijn buitgemaakt bij een aanval op een externe leverancier. Het zou gaan om een ransomware-aanval. In geval van gemeente Amersfoort lekten er gegevens van 100.000 (voormalig) inwoners.[47] Van de gemeente Arnhem lekte data van tientallen inwoners. [48] Daarnaast maakten de gemeenten Tubbergen en Dinkelland melding van een datalek, hiervan is onbekend hoeveel personen zijn geraakt.[49]

VI Bij een pass-the-cookie aanval stelen hackers sessiecookies om accounts over te nemen.

Januari 2025

Communicatieproblemen bij hulpdiensten door urenlange landelijke storing C2000-systeem
Tijdens de jaarwisseling had het C2000-systeem urenlang storing. De storing betrof het EOCS, waarmee centralisten op de meldkamer kunnen spreken met hulpverleners op straat. Door de beschikbaarheid van het back-upsysteem konden centralisten wel met hulpverleners op straat blijven communiceren. Agenten zeiden hier echter over dat het back-upsysteem praktisch onbruikbaar was en dat communiceren erg moeilijk was.[50] Naast dat C2000 haperde, werkte ook de noodknop op portofoons van politieagenten niet goed.[51]

Geen onderwijs en tentamens uitgesteld na cyberaanval op TU Eindhoven
Begin januari werd de TU Eindhoven (TU/e) slachtoffer van een cyberaanval. Hierop werden systemen een week lang offline gehaald, waardoor er geen onderwijsactiviteiten mogelijk waren. Tentamens werden daarom uitgesteld.[52] Onderzoek naar de aanval is door TU/e publiek gemaakt en hieruit blijkt dat aanvallers al 5 dagen op het netwerk aanwezig waren en misbruik hebben gemaakt door met gelekte accountgegevens in te loggen via de VPN-verbinding.[53]

DigiD niet bereikbaar door storing, veroorzaakt door DDoS-aanval
Deze maand was DigiD verschillende dagen tijdelijk niet bereikbaar door DDoS-aanvallen.[54] Er zijn geen verdere details over de aanvallen bekend gemaakt.

Drie dagen op rij (internet)storingen bij onderwijsinstellingen en ziekenhuizen, veroorzaakt door DDoS-aanvallen
Drie dagen op rij waren er (internet)storingen bij onderwijsinstellingen en ziekenhuizen als het gevolg van DDoS-aanvallen op SURF. Hierdoor hadden onderwijsinstellingen in heel Nederland last van trage of geen internetverbindingen.[55] Ook verschillende ziekenhuizen ondervonden hinder door de DDoS-aanvallen.[56]

Patiënten afgebeld en operaties uitgesteld door computerstoring in Rijnstate
Door een computerstoring werden op 14 januari in drie vestigingen van het Rijnstate ziekenhuis alle afspraken, geplande operaties en onderzoeken geschrapt. Medewerkers konden geen nieuwe gegevens opslaan in de elektronische patiëntendossiers, daarop werd besloten om alle planbare zorg af te zeggen. Het probleem zou zijn ontstaan na het uitvoeren van updates.[57]

Persoonsgegevens van 2.200 gebruikers gelekt na aanval op website raad van Almere
De persoonsgegevens van 2.200 gebruikers van raadvanalmere.nl zijn gelekt. Dit gebeurde na een aanval op de website, die daarna offline is gehaald. Er zouden namen, e-mailadressen en soms telefoonnummers en gegevens over de wijk waar mensen wonen zijn gelekt.[58]

Ambassades in Europese landen, waaronder in Nederland, aangevallen door vermoedelijk Russische hackers
Onderzoekers van Bitdefender hebben waargenomen dat vermoedelijk Russische hackers een digitale spionagecampagne uitvoerden. Hierbij zouden ambassades in verschillende Europese landen zijn aangevallen, waaronder in Nederland, Duitsland en Roemenië.[59]

Februari 2025

Paragon spyware ingezet tegen Europese WhatsApp-gebruikers, ook tegen Nederlandse nummers
Italiaanse autoriteiten hebben verklaard dat zeven WhatsApp-gebruikers met een Italiaans telefoonnummer zijn aangevallen met de Paragon spyware. Daarnaast zouden gebruikers uit meer dan een dozijn andere Europese landen zijn aangevallen met de commerciele spyware. Hiertussen zaten onder andere Nederlandse, Duitse en Belgische nummers. Dit suggereert dat zij uit deze landen komen, maar de identiteit van de gebruikers is niet bekend gemaakt. Ook is niet duidelijk om hoeveel Nederlandse nummers het gaat. Het is onbekend of de aanvallen met de spyware succesvol waren.[60] WhatsApp stelde dat er bij deze campagne zo'n 90 gebruikers zijn aangevallen, waaronder journalisten.[61]

Politienummer 0900-8844 tijdelijk niet bereikbaar door een storing
Het landelijke politienummer 0900-8844 is op 25 februari tijdelijk niet bereikbaar geweest vanwege een storing. Voor niet-spoedeisende zaken werd een alternatief nummer ingesteld. Het noodnummer was wel bereikbaar. De oorzaak van de storing is niet bekend gemaakt.[62]

Maart 2025

DigiD slecht bereikbaar wegens terugkerende DDoS-aanvallen
Verspreid over de maand kampte DigiD meerdere keren met storingen door terugkerende DDoS-aanvallen.[63] DigiD, DigiD Machtigen, BSN, Digipoort en MijnOverheid waren hierdoor beperkt beschikbaar.[64] Logius weet de verstoringen aan slimmere DDoS-aanvallen.[65]

Strafzittingen ondervinden hinder na herstelwerkzaamheden storing OM
Eind maart koppelde het Openbaar Ministerie de volledige ict-omgeving tijdelijk af van het internet. In eerste instantie was de oorzaak niet duidelijk, later bleek het te gaan om een 'hardnekkige verstoring'. Tijdens de herstelwerkzaamheden konden werknemers niet inloggen en ondervonden strafzittingen hinder. Sommige zittingen konden niet doorgaan of moesten worden verplaatst.[66]

Nederlandse bedrijven aangevallen door Noord-Koreaanse hackers
Uit een rapportage van CrowdStrike blijkt dat Famous Chollima, een hackersgroep uit Noord Korea, ook Nederlandse bedrijven aanvalt.[67] Om welke bedrijven het gaat is niet bekend gemaakt, maar CrowdStrike stelt dat het vooral gaat om bedrijven in de techsector. CrowdStrike heeft in 2024 meer dan 300 incidenten door deze groep waargenomen. 40 procent daarvan had te maken met een insider threat. Er is niet bekend hoeveel van deze incidenten in Nederland hebben plaatsgevonden, het overgrote deel van de aanvallen richtte zich op de VS.

April 2025

DigiD beperkt beschikbaar door DDoS-aanvallen
De diensten van DigiD waren opnieuw beperkt beschikbaar door DDoS-aanvallen. Het is onbekend wie verantwoordelijk is voor de aanvallen.[68]

Datalek bij ministeries door foutief uploaden documenten, impact onduidelijk
Ministeries in Den Haag zijn getroffen door een datalek. Het probleem ontstond in interne processen van ministeries toen de betreffende metadata bij de omzetting van documenten naar een publicatieformat niet goed worden opgeschoond. Hierdoor konden persoonlijke gegevens van ambtenaren worden achterhaald.[69]

Betalingsproblemen door DDoS-aanvallen op Adyen
Betaalbedrijf Adyen is getroffen door meerdere DDoS-aanvallen, waardoor klanten hadden van betalingsproblemen in (online) winkels en horeca.[70]

Ruim vijftig Nederlandse websites korte tijd moeilijk bereikbaar door DDoS-aanvallen
Eind april kampten zeker 57 verschillende Nederlandse websites met problemen nadat zij te maken kregen met DDoS-aanvallen. Onder meer de sites van de gemeenten Apeldoorn, Nijmegen, Breda en Tilburg waren korte tijd onbereikbaar. De aanvallen werden geclaimd door pro-Russische hackers. Zij hadden het voornamelijk voorzien op overheidswebsites, maar ook websites van onder meer het GVB, Arriva en NRC werden getroffen.[71]

Mei 2025

Nederland (in)direct doelwit van cyberspionagepogingen door Russische staatshackers
Uit onderzoek van meerdere partijen, waaronder de MIVD, blijkt dat Russische staatshackers (bekend als APT28) cyberaanvallen hebben uitgevoerd tegen Oekraïne en NAVO-landen. Ook de Nederlandse krijgsmacht, ministeries en het bedrijfsleven zijn direct en indirect doelwit geweest van deze cyberspionagepogingen. Het doel van de aanvallen is onder meer het in beeld krijgen en verstoren van de westerse (militaire) steun aan Oekraïne.[72]

Juni 2025

Nederlandse organisaties doelwit van DDoS-aanvallen, impact beperkt
In aanloop naar de NAVO-top zijn een tiental organisaties in Nederland het doelwit geworden van DDoS-aanvallen. [73] De geraakte organisaties waren voornamelijk publieke organisaties die een rol hadden rondom de NAVO-top. Onder de getroffen organisaties zijn het NAVO-hoofdkantoor in Nederland en Notubiz. Die laatste levert het Raadsinformatiesysteem, een dienst waarmee gemeenten en provincies officiële berichten publiceren. Hierdoor waren pagina's met raads- en statenstukken op verschillende sites van gemeenten en provincies slechter bereikbaar dan normaal.[74] Een aantal van de aanvallen is opgeëist door de pro-Russische hackersgroep NoName057(16).

Internationaal Strafhof slachtoffer van cyberaanval
Het Internationaal Strafhof (ICC) is eind juli doelwit geweest van een 'geavanceerde en gerichte' cyberaanval. Het ICC heeft niet bekend gemaakt of er gevoelige informatie is gestolen en wie er achter de aanval zit, maar had de aanval volgens eigen zeggen op tijd gestopt.[75]

Juli 2025

Strafrechtsketen verstoord nadat netwerk OM offline werd gehaald vanwege Citrix-kwetsbaarheid
Op donderdag 17 juli ontkoppelde het Openbaar Ministerie de systemen van het internet, naar aanleiding van een waarschuwing over kwetsbaarheden in Citrix NetScaler.[76] Hierdoor moest het OM overstappen op noodprocedures om werkzaamheden door te kunnen laten gaan. Dit zorgde voor hinder in de strafrechtketen, waarbij in sommige zaken ook direct vertraging ontstond.[77] Begin augustus sloot het OM systemen stapsgewijs weer aan op het internet. Uit het onderzoek bleek dat onbevoegden toegang hebben verkregen tot de Citrix NetScaler-systemen van het OM. Er is tot op heden niet vastgesteld dat er gegevens zijn gemanipuleerd of weggehaald.[78] Het NCSC stelde dat meerdere kritieke Nederlandse organisaties succesvol zijn aangevallen via een van de Citrix-kwetsbaarheden en dat één van de kwetsbaarheden al ruim voor publieke bekendmaking werd misbruikt.[79] Ook bij de Dienst Justitiële inrichtingen vond onderzoek plaats naar aanleiding van misbruik van de kwetsbaarheden.[80]

Wereldwijd organisaties gecompromitteerd via kwetsbaarheid in SharePoint, ook Nederlandse organisaties geraakt
Kritieke kwetsbaarheden in Microsoft SharePoint zijn misbruikt door statelijke actoren en voor ransomware-aanvallen.[81] Bij meerdere Nederlandse en buitenlandse organisaties zijn kwetsbare systemen aangetroffen. Als een systeem kwetsbaar blijkt, betekent dat niet direct dat er misbruik heeft plaatsgevonden.[82] Media berichtten dat honderden servers door aanvallers zijn gecompromitteerd. Vier procent van de infecties werd in Nederland waargenomen.[83]

Augustus 2025

Gevoelige data burgers gelekt na ransomware-aanval op laboratorium
Nadat Bevolkingsonderzoek Nederland melding maakte van een datalek, maakte Clinical Diagnostics (Eurofins) in augustus bekend dat er gevoelige patiëntendata is gestolen van zorgverleners die onderzoek hebben laten verrichten bij het laboratorium. Dit zou zijn gebeurd bij een ransomware-aanval in juli. Bevolkingsonderzoek Nederland informeerde 941.000 personen dat hun data (mogelijk) is gestolen bij de aanval. Het datalek gaat echter verder dan alleen die organisatie. Ook patiëntgegevens van onderzoeken die voor andere zorginstellingen zoals ziekenhuizen en huisartsen zijn uitgevoerd zijn door de aanval geraakt.[84] Cybercriminelen claimden 300GB aan data te hebben gestolen, waarvan een deel online verscheen. Uit een analyse van RTL bleek dat het gaat om namen, woonadressen en geboortedata van patiënten, hun burgerservicenummers en informatie over en uitslagen van het onderzoek. Ook zijn er adviezen naar aanleiding van onderzoeken buitgemaakt. Tussen de gegevens zit ook data van politici, gedetineerden en tbs'ers en vrouwen die wonen in blijf-van-mijn-lijfhuizen.[85] Hackersgroep eiste losgeld en zou anders de gestolen gegevens publiceren. Later werd nogmaals losgeld geëist met de bedreiging om alle buitgemaakte data te publiceren omdat de organisatie zich niet aan de afspraken zou hebben gehouden, maar later werd dit weer ingetrokken.[86] Clinical Diagnostics zou in eerste instantie losgeld hebben betaald om te voorkomen dat meer data wordt gelekt door de criminelen. Hoeveel er zou zijn betaald, is niet bekend.[87] Op het moment van schrijven zijn de onderzoeken naar modus operandi en oorzaken nog gaande.

Werkzaamheden instanties Caribische eilanden verstoord door cyberincidenten
Diverse organisaties in het Caribische deel van het Koninkrijk zijn geraakt door cyberincidenten waardoor werkzaamheden werden verstoord. Zo was onder meer de Belastingdienst van Curaçao slachtoffer van ransomware. Na het ontdekken van de hack is een van de systemen offline gehaald. Bij het Hof van Justitie, dat op alle zes eilanden actief is, is malafide software in het IT-systeem gevonden. Daarom is het computersysteem offline gehaald.[88]

Data KLM gestolen nadat aanvallers toegang wisten te krijgen tot platform externe partij
Aanvallers hebben data gestolen bij KLM, bestaande uit mogelijk naam en contactgegevens. De aanvallers wisten toegang te krijgen tot een niet gespecificeerd 'extern platform', dat de luchtvaartmaatschappij voor de klantenservice gebruikt. Vermoedelijk gaat het hier om het Salesforce platform. Hoeveel klanten zijn geraakt is niet bekend gemaakt.[89]

Routers Internet Service - en Hosting providers gecompromitteerd door Salt Typhoon
Uit onderzoek van de AIVD en MIVD blijkt dat Chinese hackers toegang hadden tot routers van kleinere Nederlandse Internet Service - en Hosting providers. Voor zover bekend zijn de hackers niet verder doorgedrongen in de interne netwerken. De aanvallen zijn toegeschreven aan de groep die Salt Typhoon wordt genoemd en zijn onderdeel van een grootschalige wereldwijde campagne. De grote telecomproviders in Nederland zijn niet geraakt.[90]

Opvallende incidenten in buitenland

Juli 2024

Russische staatshackers voeren cyberaanvallen uit op Olympische Spelen
Volgens het Franse ministerie van Buitenlandse Zaken zit de Russische militaire inlichtingendienst achter een reeks cyberaanvallen in Frankrijk, waaronder een aanval op een sportorganisatie die betrokken was bij de organisatie van de Olympische en Paralympische Spelen van 2024. APT28 wordt hiervoor verantwoordelijk gehouden. Ook verschillende ministeries, bedrijven in de defensie-industrie en organisaties in de financiële sector zouden het doelwit van de Russische hackers zijn geweest.[91]

Oktober 2024

Websites vitale infrastructuur en overheid Cyprus tijdelijk verstoord door gecoördineerde cyberaanvallen van pro-Palestijnse groeperingen
Vitale infrastructuur en overheidswebsites in Cyprus zijn doelwit geweest van een reeks gecoördineerde cyberaanvallen die werd opgeëist door verschillende pro-Palestijnse hackersgroepen, waaronder LulzSec Black.[92] De meeste aanvallen waren volgens de autoriteiten niet succesvol. De beoogde organisaties, waaronder banken, luchthavens en overheidswebsites werden slechts tijdelijk verstoord. Er werden verschillende aanvalstechnieken gezien, waaronder DDoS-aanvallen. De operatie zou zijn uitgevoerd als reactie op de steun van Cyprus aan Israël.

Europese zorginstanties aangevallen met ransomware
Volgens Orange Cyberdefense zijn Europese zorginstanties tussen juni en oktober 2024 via een kwetsbaarheid in gateways van securitybedrijf CheckPoint aangevallen met ransomware.[93] Hoeveel en welke zorginstanties zijn getroffen en wat de impact van de aanvallen is, laat Orange Cyberdefense niet weten.

Europese overheden en militaire organisaties zijn doelwit geweest van Russische phishingaanvallen
Europese overheden en militaire organisaties zijn het doelwit geweest van phishingaanvallen, die door Google worden toegeschreven aan een aan Rusland gelieerde actor, gevolgd als UNC5837. De campagne maakte gebruik van ondertekende .rdp-bestandsbijlagen om Remote Desktop Protocol (RDP)-verbindingen tot stand te brengen vanaf de computers van de slachtoffers. [94]

November 2024

Verstoring processen Duitse apotheekgroothandel door ransomware-aanval
De Duitse apotheekgroothandel AEP is getroffen door een ransomware-aanval, waarmee een deel van hun IT-systeem is versleuteld.[95] Zodra de aanval werd opgemerkt, zijn alle externe verbindingen afgesloten en zijn alle getroffen IT-systemen uitgeschakeld. Daardoor konden klanten geen bestellingen plaatsen en konden apotheken beperkt worden bevoorraad. AEP zou meer dan 6000 apotheken als klant hebben. AEP was door de aanval telefonisch niet bereikbaar, en zeer gelimiteerd te bereiken via e-mail.

December 2024

680 gigabyte aan data gestolen bij Blue Yonder door ransomwaregroep
De ransomwaregroep Termite heeft verantwoordelijkheid geclaimd voor een aanval op softwarebedrijf Blue Yonder.[96] De Software-as-a-Service (SaaS) provider heeft meer dan 3000 klanten, waaronder Microsoft, Renault, Lenovo, Procter & Gamble en Carlsberg. Ook in Nederland heeft het bedrijf klanten, waaronder Jumbo en Hema.[97] Klanten in verschillende landen ervaarden de gevolgen van dit incident, maar het leidde niet tot grote verstoringen. Bedrijven hadden vooral problemen met hun betalings- en planningssystemen. Klanten en werknemers van de Jumbo en Hema ondervonden geen hinder. Blue Yonder heeft niet bekend gemaakt hoeveel klanten precies geraakt zijn door de aanval. Naar eigen zeggen zou Termite zo'n 680 gigabyte (GB) aan data hebben gestolen, waaronder documenten, mailinglijsten, databasedumps en verzekeringsdocumenten.

December 2024

Amerikaanse telecominfrastructuur gecompromitteerd door Chinese hackers
Chinese hackers van de groep Salt Typhoon hebben minimaal een jaar lang toegang gehad tot de netwerken van diverse telecomproviders.[98] Volgens de Amerikaanse autoriteiten zou het gaan om meerdere Amerikaanse telecombedrijven, waaronder T-Mobile, Verizon, AT&T en Lumen Technologies. [99] De hackers zouden zo bij gespreksgegevens van prominente politici zijn gekomen.[100] CISA en de FBI hebben bevestigd dat de hackers toegang hebben gehad tot de privécommunicatie van een 'gelimiteerd aantal' mensen. Daarnaast stellen media op basis van anonieme bronnen dat de hackers toegang hebben gehad tot het afluisterplatform van de Amerikaanse overheid en hebben ze verzoekgegevens van wethandhavingsinstanties en telefoongesprekken van klanten gestolen.[101] De campagne zou mogelijk al 1 tot 2 jaar lopen. Er is niet met zekerheid gezegd dat de hackers verwijderd zijn uit het systeem.

Klanten Deens waterzuiveringsbedrijf zonder water door cybersabotage van pro-Russische hackers
Volgens Denemarken hebben pro-Russische hackers eind december 2024 een Deens waterzuiveringsbedrijf aangevallen, met als gevolg dat klanten een aantal uur zonder water zaten. Een van de pijpleidingen is gebarsten door een verhoogde waterdruk.[102]

Januari 2025

Locatiegegevens van mogelijk miljoenen mensen gelekt na hack bij datahandelaar
Na een hack bij Gravy Analytics, een commerciële datahandelaar, is mogelijk van miljoenen mensen de locatiegegevens gelekt.[103] Gravy Analytics ontdekte dat iemand door middel van een 'gestolen key' toegang zou hebben gekregen tot de cloud-omgeving. Online claimde iemand bij de inbraak een dataset van zeventien terabyte (TB) aan data te hebben gestolen. In de dataset zouden locatiegegevens van gebruikers van honderden populaire apps (zoals Candy Crush, FlightRadar, Grindr en Tinder) zijn verzameld. De hacker dreigde de data openbaar te maken als het bedrijf het gevraagde losgeld niet zou betalen.

Data gestolen bij ransomware-aanval op Italiaans ziekenhuis, maar systemen niet versleuteld
Een Italiaans ziekenhuis is doelwit geworden van een ransomware-aanval, door een kwetsbaarheid in de firewall, waarbij persoonlijke gegevens van patiënten en personeel zijn buitgemaakt.[104] Via de gecompromitteerde firewall wisten de aanvallers 'domain credentials' te verkrijgen, waarmee ze toegang kregen tot de fileserver. Hier bleken gezondheidsgegevens op te staan, hoewel de server alleen bedoeld was voor administratieve doeleinden. Het bleef bij datadiefstal, de ransomware werd uiteindelijk niet ingeschakeld.

Februari 2025

Systemen Canadese telecombedrijven gecompromitteerd
Het Canadese Centrum voor Cybersecurity meldde dat er in februari bij meerdere Canadese telecommunicatiebedrijven activiteit van kwaadwillenden is geweest, specifiek van de Chinese cyberactor Salt Typhoon. De Canadese overheid meldde dat de systemen zijn gecompromitteerd via een bekende Cisco-kwetsbaarheid. Om welke telecommunicatiebedrijven het precies gaat werd niet gespecificeerd.[105]

Maart 2025

1,5 miljard dollar aan crypto gestolen door Noord-Koreaanse hackers
Bij een hack op de cryptobeurs Bybit is bijna 1,5 miljard dollar aan digitale munten gestolen. Dit maakt het de grootste cryptodiefstal ooit. De aanval is door verschillende onderzoekers en de Amerikaanse autoriteiten toegeschreven aan Noord-Koreaanse hackers.[106] Experts van verschillende bedrijven stelden al snel dat de Lazarus-hackers minstens 300 miljoen dollar wit hebben weten te wassen.[107]

April 2025

Waalse overheid koppelt zichzelf los van het internet na gerichte cyberaanval
De Waalse overheid heeft zichzelf van het internet losgekoppeld nadat ze een grootschalige "gesofisticeerde en gerichte inbraak" hadden vastgesteld in het IT-systeem.[108] De aanvaller, een onbekende partij, zou zich hebben gericht op een kwetsbare plek in de systemen van de Waalse overheid. Om te voorkomen dat de aanval tot (verdere) impact zou leiden, is besloten om de systemen los te koppelen van het internet, waardoor meerdere administratieve diensten offline waren.

APT29 voert phishing-aanvallen uit op de diplomatieke entiteiten in Europa
De Russische hackersgroep APT29 heeft volgens cybersecuritybedrijf Checkpoint een maandenlange phishing-campagne uitgevoerd tegen Europese diplomatieke entiteiten, waarbij nep-uitnodigingen voor wijnproeverijen en diners van een Europees ministerie van Buitenlandse Zaken werden verstuurd.[109] De campagne lijkt te zijn gefocust op Europese diplomatieke entiteiten, inclusief ambassades van niet-Europese landen welke zich in Europa bevinden.

Waterstroom Noorse dam aangepast door pro-Russische hackers
Pro-Russische hackers zitten volgens de Noorse autoriteiten waarschijnlijk achter de vermoedelijke sabotage bij een dam in het Noorse Bremanger. Bij die sabotage-aanval werd de waterstroom beïnvloed. De hackers kregen toegang tot een digitaal systeem dat op afstand een van de kleppen van de dam bestuurt en openden deze om de waterstroom te vergroten. De klep stond ongeveer vier uur open en in totaal liepen er miljoenen liters water weg, maar dit vormde geen gevaar voor de omgeving.[110]

Mei 2025

Lege schappen bij Britse supermarkten na cyberaanval
Bij het Britse Co-op zijn delen van de IT-systemen offline gehaald toen een ransomware-aanval werd gedetecteerd. De supermarktketen meldde dat de hackpoging hun dienstverlening heeft verstoord, de aanval zorgde onder meer voor lege schappen in de winkels.[111] Voordat de systemen van Co-op Group werden versleuteld met ransomware, wisten de aanvallers de gegevens van 6,5 miljoen klanten te bemachtigen.[112] De aanval op Co-op was onderdeel van een bredere aanvalscampagne op de Britse retailsector, zo werden ook Marks & Spencer en Harrods slachtoffer van cyberaanvallen. Volgens het Britse Cyber Security Monitoring Centre zit de financieel gemotiveerde cyberactor Scattered Spider[VII] achter de aanvallen.[113] De groep staat bekend om telefonische phishingaanvallen (vishing genoemd) waarbij zij zich voordoen als IT-medewerkers.[114]

Juli 2025

Verstoring van diensten voor Franse klanten Orange na cyberaanval
Orange, een van de grootste mobiele dienstverleners in zowel Europa als Afrika, maakte bekend dat het een cyberaanval had ontdekt die een van zijn interne systemen trof. Het bedrijf heeft gelijk maatregelen getroffen, waaronder het isoleren van systemen. Dit heeft geleid tot verstoring van bepaalde diensten en beheerplatforms ivoor een aantal van hun zakelijke klanten en voor een aantal consumentendiensten in voornamelijk Frankrijk.[115] Criminelen achter de WarLock-ransomware zouden bij de aanval ook data hebben gestolen.[116]

Landelijke uitval 4G- en 5G-netwerk in Luxemburg na cyberaanval
Op 23 juli waren de mobiele 4G- en 5G-netwerken van Luxemburg meer dan drie uur onbereikbaar. Grote delen van de bevolking konden de hulpdiensten niet bellen omdat het 2G-noodsysteem overbelast raakte. Ook internettoegang en elektronisch bankieren waren niet mogelijk. Volgens overheidsverklaringen aan het parlement van het land werd de uitval veroorzaakt door een cyberaanval. Deze aanval zou opzettelijk verstorend zijn geweest en niet een poging om het telecomnetwerk te compromitteren.[117]

VII In media zijn berichten verschenen over de campagnes van de financieel gemotiveerde groepen Scattered Spider en ShinyHunters. Sommige media suggereren dat er op zijn minst overlap zit tussen de groepen.

Juli 2025

Data gestolen van Orange België na cyberaanval
Telecomprovider Orange Belgium is eind juli het slachtoffer geworden van een cyberaanval. Volgens de provider hebben onbevoegden ingebroken in 'een van de IT-systemen'. De hackers zouden toegang hebben verkregen tot 850.000 klantaccounts waardoor onder meer namen, telefoonnummers, simkaartnummers en PUK-codes zijn gelekt.[118]

Augustus 2025

Gegevens 6,4 miljoen klanten van Franse Bouygues Telecom gestolen bij cyberaanval
Bouygues, een grote Franse telecomprovider, meldde dat het op 4 augustus een cyberaanval heeft gedetecteerd. Bij de aanval zouden gegevens van 6,4 miljoen klanten zijn gestolen. Het gaat onder meer om contactgegevens, bedrijfsgegevens en IBAN-nummers.[119]

Data van diverse grote bedrijven gestolen na aanvallen op CRM-systemen
In juli en augustus meldden diverse bedrijven datalekken nadat aanvallers toegang wisten te krijgen tot Customer Relationship Management (CRM)-systemen van de betreffende bedrijven. Daar waar bekend, ging het meer dan eens specifiek om SalesForce. Een van de bedrijven was Google. Deze gaf aan dat hun SalesForce omgeving was gecompromitteerd na telefonische phishing (vishing). Bij de aanval zou data van potentiële Google Ads-klanten zijn gestolen.[120] Daarnaast maakte Cisco bekend dat aanvallers persoonlijke gegevens van gebruikers van cisco.com had buitgemaakt. Ook daarbij wist een aanvaller via vishing toegang te krijgen tot een niet nader genoemd third-party CRM-systeem.[121] Aanvallen op SalesForce CRM-systemen zijn gelinkt aan de financieel gemotiveerde ShinyHunters[VIII] groep.[122]

Data gestolen en bedrijfsactiviteiten verstoord na cyberaanval op telecombedrijf Colt
Het Britse telecommunicatiebedrijf Colt Technology Services kampte begin augustus met een cyberaanval die heeft geleid tot een meerdaagse uitval van een aantal bedrijfsactiviteiten. De criminelen achter de WarLock-ransomware hebben de aanval geclaimd en boden gestolen data te koop aan.[123]

Grootschalige datadiefstal uit Salesforce-omgevingen na inbraak bij Salesloft Drift
Onderzoekers hebben een grootschalige campagne ontdekt waarbij hackers, door Google gevolgd als UNC6395, systematisch grote hoeveelheden gegevens van zakelijke SalesForce-instanties exporteerden. De aanvallers maakten geen gebruik van een kwetsbaarheid in het SalesForce-platform, maar raakten binnen op SalesForce-systemen via Salesloft Drift. Dat is een integratie voor SalesForce, ontwikkeld door een derde partij. Met de cyberaanval op Drift wisten criminelen Open Authorization- en refreshtokens voor integratie in het Salesforce-ecosysteem te stelen, waarmee zij vervolgens toegang konden krijgen tot SalesFocre-data van klanten.[124] Obsidian stelde dat meer dan 700 bedrijven zijn geraakt.[125] Bevestigd is dat de hackers onder meer bij de securitybedrijven Zscaler, Palo Alto en CloudFlare data wisten te stelen.[126] [127]

Productie en dienstverlening Jaguar Land Rover wekenlang verstoord door cyberaanval
Het Britse bedrijf Jaguar Land Rover (JLR) maakte bekend hun systemen proactief uit te hebben geschakeld naar aanleiding van een cyberincident.[128] Hierdoor werd onder andere de productie wekenlang stil gelegd en kregen werknemers de instructie thuis te blijven. Op 10 september gaf JLR aan dat sommige data waarschijnlijk was geraakt, maar verdere details werden niet gegeven.[129] De BBC stelde dat de aanval is geclaimd in een Telegramkanaal dat Scattered Lasus$ Hunters heet en dat de hackers losgeld zouden eisen.[130]

VIII In media zijn berichten verschenen over campagnes van de financieel gemotiveerde groepen Scattered Spider en ShinyHunters. Sommige media suggereren dat er op zijn minst overlap zit tussen de groepen.

Begin januari werd de TU Eindhoven (TU/e) slachtoffer van een cyberaanval. Hierop werden systemen een week lang offline gehaald, waardoor er geen onderwijsactiviteiten mogelijk waren. Uit onderzoek van de TU/e blijkt dat aanvallers met gelekte accountgegevens wisten in te loggen via de VPN-verbinding.

2 Steeds complexer dreigingsbeeld door toenemende cybercapaciteiten wereldwijd

Landen zijn meer en meer bereid hun macht te gebruiken om hun geopolitieke belangen te behartigen. Deze ontwikkelingen leiden wereldwijd tot een verdere vergroting van cybercapaciteiten. Staten zetten staatsgesteunde groeperingen zoals 'hacktivistische' collectieven in. Ook worden private bedrijven en organisaties ingezet om ondersteuning te bieden aan statelijke cyberaanvallen. Verder ontwikkelen meer landen offensieve cyberprogramma's. Deze vermenging en proliferatie leiden in toenemende mate tot verdere complexiteit en een onvoorspelbaar dreigingsbeeld.

Statelijke cybercapaciteiten nemen toe en vermengen met niet-statelijke organisaties

Statelijke actoren zetten cyberaanvallen in om hun politieke, militaire en/of economische doelen te bereiken. Door een offensief cyberprogramma op te zetten, kunnen statelijke actoren (heimelijk) hun belangen behartigen zonder dat ze de juridische drempel[IX] van gewapend conflict over gaan. Steeds meer landen raken betrokken bij een wedloop om kennis, technologie, wapens, grondstofmonopolies en economische voorsprong, die bepalend kan zijn voor de machtsbalans in de wereld.[131] De wereld is steeds openlijker in conflict en er is sprake van een turbulente tijd waarin internationale betrekkingen onvoorspelbaarder worden.[132] [133] De machtsbalans in de wereld verandert en landen zijn steeds meer bereid om macht te gebruiken om hun eigen belangen te verdedigen.[134] Dergelijke geopolitieke ontwikkelingen kunnen wereldwijd leiden tot een verdere toename en inzet van cybercapaciteiten.

Sommige statelijke actoren voeren niet enkel zelf cyberaanvallen uit, maar maken vernuftig gebruik van bestaande of nieuwe collectieven of organisaties. In sommige gevallen gaat het om zogeheten staatsgesteunde groeperingen. Staatsgesteunde groeperingen zijn groeperingen die niet primair onderdeel uitmaken van staatsstructuren, zoals hacktivisten of

IX Dat wil zeggen: onder de drempel van wat in het algemeen onder internationaal recht als 'gewapend conflict' wordt gekwalificeerd.

cybercriminelen. Deze groepen kunnen echter wel worden gedoogd, gesteund of aangestuurd door statelijke actoren. Er zijn verschillende redenen voor staten om staatsgesteunde groeperingen in te zetten. Een belangrijke reden is het kunnen ontkennen van betrokkenheid. Zelfs wanneer er bewijs lijkt te zijn dat een staat verantwoordelijk is voor een cyberaanval, kan deze de schuld afschuiven op een andere groep die officieel geen onderdeel uitmaakt van staatsstructuren. Door die vermenging betekent dit dat een strikt onderscheid in bijvoorbeeld technieken of doelwitten niet valt te maken per type actor. De inzet van staatsgesteunde groeperingen brengt risico's met zich mee (zie kader hieronder).

Risico's van staatsgesteunde groeperingen in het dreigingslandschap

- Staatsgesteunde groeperingen kunnen toegang krijgen tot bijvoorbeeld meer middelen vanuit een statelijke actor. Hierdoor kunnen capaciteiten toenemen.
- Als niet bekend is dat een groepering staatsgesteund is, kan de dreiging afkomstig van de groep structureel te laag worden ingeschat omdat niet bekend is over welke capaciteiten of intenties zij beschikken.
- Staatsgesteunde groeperingen zijn zich over het algemeen minder bewust van potentiële risico's, wat kan leiden tot grote of onvoorziene impact of escalatie.

Pro-Russische hacktivisten zijn verlengde van de Russische overheid

Een voorbeeld van een staat die veelvuldig gebruikmaakt van staatsgesteunde groeperingen is Rusland. De inzet van de Russische dreiging uit zich via een diffuus, opportunistisch en onvoorspelbaar samenspel van Russische overheidsentiteiten (waaronder de inlichtingen- en veiligheidsdiensten), een diverse groep Russische of pro-Russische individuen, organisaties en netwerken in zowel Rusland als het Westen. Die worden ingezet of bieden zich actief aan voor het verrichten van vaak lucratieve activiteiten.[135] Volgens de MIVD en AIVD nam het aantal hackerscollectieven dat aan het Russische regime te koppelen is de afgelopen twee jaar toe en bovendien zijn de groepen steeds diverser.

Sommige staatsgesteunde groeperingen handelen wel in het belang van het Russische regime, maar opereren ogenschijnlijk op eigen initiatief. Dit geldt in het bijzonder voor pro-Russische hacktivisten. Lange tijd beoordeelden de diensten de dreiging die uitgaat van pro-Russische hacktivisten als niet hoog. Deze groeperingen hebben in het eerste jaar van de Russische oorlog tegen Oekraïne laagdrempelige cybercampagnes uitgevoerd die naar inschatting van de MIVD en AIVD zeer waarschijnlijk geen dreiging vormden voor de nationale veiligheid van Nederland. In het tweede jaar van de oorlog bleek dat verschillende groeperingen aan de technische capaciteit werkten of erover beschikten en bereid waren om impactvolle cyberoperaties uit te voeren. Sinds eind 2023 zien de MIVD en AIVD dat de risicobereidheid van deze groeperingen toeneemt wanneer het gaat om het ontplooien van offensieve cybercapaciteiten tegen westerse landen. Ook stellen de diensten vast dat alle door hen onderzochte pro-Russische hacktivistische groeperingen banden onderhouden met de Russische overheid, waaronder de Russische inlichtingen- en veiligheidsdiensten. Volgens onderzoek van Pointer bleek dit onder andere het geval te zijn voor de Russische hacktivistische groep NoName057(16), welke hulp ontvangt van een Russisch staatscensuurbureau dat onder toezicht staat van het Kremlin.[136] Ook voor de cyberactor Laundry Bear, welke in 2025 als nieuwe cyberactor werd onthuld door de diensten, geldt dat deze zeer waarschijnlijk staatsgesteund is.[137] De groep was onder andere verantwoordelijk voor een hack op de Nederlandse politie (zie Jaarbeeld). Opvallend aan de groep is dat deze, vergeleken met sommige andere Russische actoren, zeer succesvol is.[138]

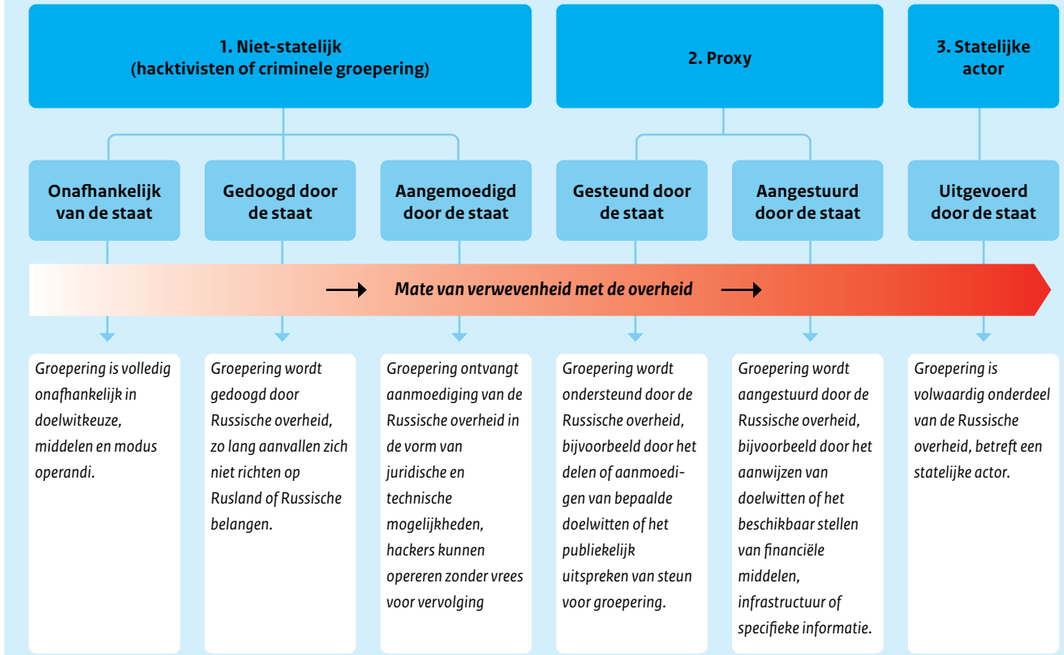
De steun die deze groeperingen ontvangen van de Russische overheid varieert. Dat betekent dat dergelijke groeperingen op een spectrum kunnen worden gezien, waarbij die groepen ook kunnen verplaatsen binnen het spectrum. De AIVD en MIVD hebben een visuele weergave van dit spectrum gecreëerd (zie volgende pagina).

Het feit dat pro-Russische hacktivisten in de praktijk gezien moeten worden als een verlengstuk van de Russische overheid of de Russische inlichtingen- en veiligheidsdiensten, betekent dat de dreiging vanuit deze groep ook groter is. Als deze hacktivisten bijvoorbeeld toegang hebben tot technische kennis van een statelijke actor, verhoogt dat hun capaciteiten en daarmee de potentiële impact van cyberaanvallen aanzienlijk. Dat betekent dat de dreiging voor Nederland vanuit hacktivisten mogelijk groter is dan eerder werd aangenomen.

Chinese bedrijven en kennisinstellingen ondersteunen Chinese statelijke cyberprogramma

China maakt in toenemende mate gebruik van organisaties die geen onderdeel uitmaken van het staatsapparaat. Zo stellen de AIVD en MIVD dat het Chinese cyberecosysteem wordt gekenmerkt door nauwe verwevenheid tussen inlichtingen- en veiligheidsdiensten, kennisinstellingen en bedrijven. In de afgelopen rapportageperiode werd voor het eerst bekend dat een middelgroot beursgenoteerd Chinees bedrijf direct betrokken is geweest bij het uitvoeren van cyberoperaties. Voorheen waren weliswaar diverse andere Chinese bedrijven geïdentificeerd die zelf offensieve cyberoperaties uitvoeren, maar daarbij ging het om frontorganisaties van Chinese inlichtingen- en veiligheidsdiensten of relatief kleine en obscure bedrijven. Met betrekking tot grote en middelgrote Chinese bedrijven was tot dusverre slechts waargenomen dat deze enkel ondersteuning leveren, zoals training, research & development of het leveren van aanvalsinfrastructuur, malware en exploits voor (on)bekende kwetsbaarheden. Ook worden Chinese statelijke actoren ondersteund door grootschalige Chinese onderzoeksprogramma's om kwetsbaarheden in edge devices te identificeren. Hierdoor zijn deze actoren structureel succesvol in het hacken van onder meer westerse overheden en bedrijven. Toenemende aandacht voor deze modus operandi leidt nog niet tot een afname van deze dreiging. Volgens de MIVD kunnen kwetsbaarheden in edge devices worden uitgebuit binnen enkele uren of dagen nadat deze bekend worden gemaakt.[139] Dat geeft (potentiële) slachtoffers zeer kort de tijd om eventuele patches voor de kwetsbaarheden te installeren voordat deze mogelijk worden misbruikt.

Figuur 1 Mate van verwevenheid met de overheid



Noord-Koreaanse staatshackers hebben vaak financieel motief en vallen cryptosector aan

Noord-Korea is een voorbeeld van een statelijke actor die technieken en aanvallen inzet die normaliter worden geassocieerd met niet-statelijke actoren. Alhoewel een gedeelte van Noord-Koreaanse cyberaanvallen gericht is op spionage, is een groot deel van de aanvallen ook gericht op financieel gewin. Een financieel motief wordt over het algemeen geassocieerd met criminele cyberactoren. Daarbij is de cryptosector een gelief doelwit, waar dit jaar door naar verluidt Noord-Koreaanse hackers bijna 1,5 miljard dollar aan digitale valuta werd buitgemaakt (zie Jaarbeeld). Ook zet het land Noord-Koreaanse freelance IT'ers in. Zij laten zich in het buitenland onder valse identiteit inhuren bij bedrijven om op die manier geld te verdienen voor het regime, onder andere door data of cryptovaluta te ontvreemden.[140] Daarnaast vergrootte Noord-Korea het afgelopen jaar de toch al zeer geavanceerde mogelijkheden om cyberaanvallen uit te voeren.[141] Het is al langer bekend dat Noord-Koreaanse cyberactoren cryptovaluta stelen om zo het regime te financieren. Maar het blijft noemenswaardig dat dit de enige statelijke actor met een dermate ontwikkeld offensief cyberprogramma is, die de capaciteiten op zulke grote schaal inzet voor financieel gewin. Het illustreert bovendien dat de afbakening tussen verschillende actoren en motieven niet zwart-wit is, maar dat die in elkaar kunnen overlopen.

Voorbereidingen voor digitale sabotage door Rusland en China waargenomen, tot dusver geen aanvallen met ontwrichtende impact

In de afgelopen rapportageperiode is gebleken dat zowel Rusland als China voorbereidingshandelingen voor digitale sabotage hebben ondernomen. Deze handelingen hebben tot op heden geen ontwrichtende impact gehad in Nederland.

De MIVD stelt dat Rusland inmiddels een grotere risicobereidheid toont, die zich manifesteert via meer brutale, agressieve of provocatieve activiteiten in zowel het fysieke als het cyberdomein.[142] In Nederland hebben de AIVD en de MIVD cyberoperaties en voorbereidende handelingen onderkend die mogelijk tot sabotage hadden kunnen leiden. Ook was Nederland in 2024 voor

het eerst slachtoffer van moedwillige cybersabotage door een Russische staatsgesteunde groepering.[143]

Ook Chinese hackersgroepen hebben stappen gezet die wijzen op voorbereidingshandelingen voor sabotage. In de VS hebben twee groepen, Volt Typhoon en Salt Typhoon, zich de afgelopen jaren diepgaand weten in te nestelen in verschillende onderdelen van de Amerikaanse vitale infrastructuur (zie Jaarbeeld en Hoofdstuk 3). De stappen in de cybercampagnes van de twee groepen kunnen wijzen op voorbereidingshandelingen voor digitale sabotage. Dat illustreert dat er sprake is van een brede Chinese cyberdreiging die zich, in tegenstelling tot wat lang het beeld was van Chinese dreiging, niet enkel richt op economische spionage. Zo kan er sprake zijn van niet-economische spionage. Dergelijke voorbereidingshandelingen kunnen ook toekomstgericht zijn: door zich in te nestelen in vitale infrastructuur kan later, bijvoorbeeld ten tijde van een conflict, gebruik worden gemaakt van deze positie voor sabotage. China ziet waarschijnlijk de VS als primaire tegenstrever in het cyberdomein, maar het land kan haar aanzienlijke cybersabotagecapaciteiten in de toekomst ook inzetten tegen Europese doelen.[144]

Onvoorspelbaar dreigingslandschap door verdere toename aantal landen met offensieve cyberprogramma's

In 2024 constateerde de AIVD een verdere toename van het aantal landen dat offensieve cyberprogramma's ontwikkelt. Over de afgelopen drie jaar genomen gaat het om een scherpe stijging.[145] Die ontwikkeling is niet los te zien van de toenemende geopolitieke verharding in een wereld die steeds openlijker in conflict is. En hoewel de aanvallen van nieuwe cyberactoren tot dusver zelden of niet tegen Nederland waren gericht, bedreigen ze wel de digitale veiligheid van partners, bondgenoten, de EU en de NAVO.[146] Digitale processen zijn immers niet aan landsgrenzen gebonden, maar zijn juist in hoge mate met elkaar verweven en van elkaar afhankelijk. Een aanval op een digitaal proces in een ander land kan dus doorwerken en zo ook Nederland(se belangen) raken. Daarnaast leidt de opkomst van nieuwe statelijke cyberactoren tot een onvoorspelbaarder cyberlandschap in het algemeen, waarbij grip krijgen en houden op de dreiging steeds complexer wordt.[147]

Daarnaast blijkt uit mediapublicaties dat een uiteenlopende en grote groep van statelijke actoren spyware koopt.[148] Aangezien commerciële spyware beschikbaar is voor statelijke actoren met voldoende financiële middelen, is het een toegankelijke manier om over offensieve cybercapaciteiten te beschikken. Hiervoor hoeft de actor geen technische kennis te bezitten of een uitgebreid inlichtingenapparaat op te zetten. Door de introductie van commerciële spyware, ontwikkeld door private bedrijven, is het monopolie van overheden op hoogwaardige offensieve cybercapaciteiten voorbij. Hiermee neemt de kans op cyberproliferatie toe.

Complex en onvoorspelbaar dreigingsbeeld vraagt om brede notie weerbaarheid

De ontwikkelingen beschreven in dit hoofdstuk zorgen ieder op zichzelf voor een complex dreigingslandschap, dat bovendien onvoorspelbaar is. Er is sprake van proliferatie van cybercapaciteiten van in ieder geval Rusland, China en Noord-Korea. Rusland ziet zichzelf in een breder conflict met het westen en heeft minstens één keer (een poging tot) cybersabotage in Nederland uitgevoerd. China maakt gebruik van het bredere cyberecosysteem en is zo onder andere in staat om kwetsbaarheden razendsnel uit te buiten, wat de kans verkleint dat organisaties een patch op tijd installeren. Daarnaast voeren Chinese actoren (voorbereidingshandelingen voor) sabotage uit in andere delen van de wereld, wat ook mogelijk richting Europa kan plaatsvinden. Noord-Korea vergroot de mogelijkheden om cyberaanvallen uit te voeren en steelt steeds grotere bedragen aan cryptovaluta, die onder andere worden gebruikt om het regime te financieren. Naast statelijke actoren waarvan bekend is dat die een offensief cyberprogramma hebben, tuigen ook andere landen deze op. Daarvoor kopen sommige landen commerciële spyware in. Statelijke actoren zetten niet-statelijke actoren of organisaties in, waardoor de scheidslijn daartussen vervaagt. Daarnaast zorgt vermenging van actoren ook voor vermenging of vertroebeling van motieven, zoals geïllustreerd door Noord-Korea. Bovendien is gebleken dat voor sommige (statelijke of staatsgesteunde) actoren de risicobereidheid toeneemt om offensieve cybercapaciteiten tegen het westen te ontplooien.

Al deze ontwikkelingen vinden tegelijkertijd en in toenemende mate plaats. Dat leidt tot een dreigingslandschap dat in hoge mate ondoorzichtig en onvoorspelbaar is. Ondanks die complexiteit vormen de digitale basisprincipes nog altijd een zeer effectieve barrière tegen vele soorten cyberaanvallen. Het is daarnaast ook cruciaal voor organisaties hun weerbaarheid zo in te richten dat deze niet enkel gericht is op het voorkomen van incidenten, maar ook op veerkracht en andere onderdelen van weerbaarheid. Dat omvat onder andere het ontdekken van cyberincidenten, en wanneer deze zich voordoen het beperken van schade, het eenvoudiger maken van herstel en voorhanden hebben van terugvalopties of -procedures.

De impact die een succesvolle aanval op de telecomsector kan hebben is groot, onder andere omdat vele andere sectoren afhankelijk zijn van het functioneren van telecommunicatie.

3 Dreiging telecomsector reëel, ook Nederland doelwit

Er is al jaren terecht aandacht voor de weerbaarheid van de vitale infrastructuur. De continuïteit van een vitaal proces als telecommunicatie is immers van groot belang voor het functioneren van onze samenleving. Incidenten in de Amerikaanse telecomsector laten zien dat de dreiging zich manifesteert. Ook Nederland was doelwit in deze spionagecampagne van Salt Typhoon, maar ondervond hier geen impact van. De sector is om verschillende redenen interessant voor actoren en is daarom ook een mogelijk doelwit. Alhoewel grote incidenten in Nederland tot nu toe zijn uitgebleven en de weerbaarheid binnen de sector robuust is, laten grote incidenten als in de VS zien dat er continu aandacht moet blijven voor de weerbaarheid en de ontwikkelende dreiging.

Incidenten in de VS laten zien dat dreiging richting de telecomsector reëel is

Salt Typhoon valt telecomsector VS aan, ook Nederland doelwit

Een grootschalige en vergaande cybercampagne in de Verenigde Staten laat zien dat de dreiging richting de telecomsector reëel is. In oktober 2024 kwam aan het licht dat ten minste negen Amerikaanse telecombedrijven waren getroffen door een campagne uitgevoerd door een Chinese APT, genaamd Salt Typhoon.[149] De cyberactor wist bij verschillende telecommunicatiebedrijven binnen te dringen met behulp van gestolen inloggegevens en door misbruik te maken van kwetsbaarheden in edge devices, waarvan sommige al langer bekend waren.[150] Hoelang de actor precies in de systemen heeft gezeten is onbekend. In initiële berichtgeving werd beschreven dat de actor al sinds maart 2024 in de systemen zat, maar volgens andere Amerikaanse berichtgeving startte de campagne al in 2021.[151] [152] Daarnaast wist de cyberactor tot diep in de infrastructuur van het Amerikaanse telecomnetwerk te dringen. Verschillende Amerikaanse media berichtten dat de hackers gespreksgegevens en privécommunicatie wisten te stelen van onder andere huidige Amerikaanse president Trump en vicepresident Vance.[153] Aanvullend zou de groep toegang hebben gehad tot het afluisterplatform van de Amerikaanse overheid om Chinese agenten te identificeren die onder surveillance stonden.[154] [155] Tot op heden is niet bekend gemaakt of de Chinese hackersgroep volledig uit de systemen is verwijderd. De campagne van Salt Typhoon[X] werd door een senator in de VS uitgeroepen tot "de ergste telecomhack uit de Amerikaanse geschiedenis".[156] Ook een aantal kleine Nederlandse kleinere internet service- en hosting providers was doelwit van Salt Typhoon.[157] [158] In augustus 2025 meldden de

X Cyberactor Salt Typhoon is volgens het Amerikaanse Cyber Infrastructure and Security Agency (CISA) een Chinese staats-gesteunde hackersgroep.

AIVD en de MIVD dat toegang was verkregen tot routers van deze aanbieders, maar dat de aanvallers voor zover bekend niet verder zijn doorgedrongen in de interne netwerken. Een mogelijke verklaring daarvoor is dat de Nederlandse doelwitten niet dezelfde mate van aandacht kregen van de hackers. De FBI heeft aangegeven dat Salt Typhoon meer dan 200 bedrijven in 80 landen heeft aangevallen.[159]

De situatie in de VS is niet één-op-één te vertalen naar de situatie in Nederland. De infrastructuur van de telecomsector in de VS is, in tegenstelling tot veel Europese landen en zeker tot Nederland, verouderd en is volgens de voorzitter van de Senaatscommissie van inlichtingen opgemaakt uit een "brei van aan elkaar geplakte netwerken".[160] De aan elkaar geplakte netwerken zijn zo verouderd dat ze niet altijd goed kunnen worden gepatcht, waardoor kwetsbaarheden niet worden opgelost en kwetsbaarheden blijven bestaan of andere ingewikkelde mitigerende maatregelen getroffen moeten worden.[161] De campagne in de VS laat zien hoe diep en hoe breed de actor zich heeft weten te verspreiden in en over de telecomnetwerken, en dat er grote interesse is bij statelijke actoren om bij telecomnetwerken binnen te dringen. Hoewel de Nederlandse situatie niet overeenkomt met de situatie in de VS, kennen ook vitale sectoren in Nederland risico's door een grote afhankelijkheid van buitenlandse leveranciers en een toenemende complexiteit van de infrastructuur.

Dat de dreiging aanhoudend en reëel is, is gebleken uit de Salt Typhoon campagne. Bovendien lijkt dezelfde cyberactor zich te richten op meerdere telecomproviders en ook op andere vitale infrastructuur, en breidt de actor zich uit naar andere landen. Zo kondigde het Amerikaanse satellietbedrijf Viasat in juni 2025 aan dat ze gehackt waren door Salt Typhoon, waarbij weinig details zijn vrijgegeven over de omvang van de hack.[162] Het satellietbedrijf levert satellietbreedbanddiensten aan overheden over de hele wereld en aan klanten in de luchtvaart, defensie, energie, scheepvaart en zakelijke sector. Daarnaast publiceerde het Canadese Cybersecurity Agentschap dat een Canadees telecombedrijf ook slachtoffer is geweest van een cyberaanval, hoogstwaarschijnlijk door Salt Typhoon.[163] [164] Ook in Europa zijn het afgelopen jaar meerdere cyberaanvallen geweest op de telecomsector, zoals ook terug te lezen in het Jaarbeeld. Het Deense Cybersecurity Agentschap (CFCS) waarschuwde al voor verhoogde interesse van statelijke actoren in de Europese telecomsector. In maart 2025 verhoogde het CFCS dan ook de dreiging richting de Deense telecomsector van "gemiddeld" naar "hoog".[165] Het Franse Agentschap voor Veiligheid en Informatiesystemen (ANSSI) schrijft over aanvallen op de telecomsector in het jaarrapport.[166] Het ANSSI beschrijft onder andere dat telecombedrijven aanhoudend worden aangevallen voor spionagedoeleinden en raadde entiteiten binnen de telecomsector aan om rekening te houden met een blijvende dreiging richting dit type infrastructuur.[167][168]

Alle vitale sectoren potentieel interessante doelwitten, kenmerkende eigenschappen telecomsector

Alle vitale sectoren[XI] kunnen aantrekkelijke doelwitten vormen voor kwaadwillende actoren, zoals in eerdere CSBN's beschreven. Binnen vitale processen worden diensten en processen aangeboden die het fundament vormen waarop de Nederlandse samenleving draait. Daarom is continuïteit van groot belang; langdurige uitval of verstoring kan ver doorwerken en grote maatschappelijke gevolgen hebben.[169] Interesse van kwaadwillenden in vitale sectoren, en bij uitstek de telecomsector, wordt vergroot door kenmerkende eigenschappen, die van invloed zijn op de algehele weerbaarheid, en door het potentieel gewin dat in de sector te behalen valt. Een gerichte recente aanvalscampagne op de telecomsector in de VS heeft bovendien laten zien dat deze interesse en de al langer bekende dreiging richting de telecomsector reëel is. De kenmerkende eigenschappen van de telecomsector hebben betrekking op de functie van de sector, de inherente verbondenheid met de buitenwereld en gebruikers en concurrentie tussen aanbieders binnen deze vitale sector.

De telecomsector omvat alle openbare communicatiediensten, waaronder mobiele- en vaste diensten en netwerken, satellietverbinding en zeekabels. De cruciale rol van de telecomsector is het mogelijk maken van communicatie tussen bedrijven, overheden en burgers door toegang te geven tot de digitale wereld.[170] Een onderscheidende eigenschap van de telecomsector is dat veel andere (vitale) sectoren afhankelijk zijn van de sector. Denk bijvoorbeeld aan de financiële sector, waarbij voor het doen van de vele miljoenen betalingen de infrastructuur van de telecomsector noodzakelijk is, of de logistieke sector, waar telecominfrastructuur cruciaal is voor bijvoorbeeld voorraadbeheer en de toeleverketen.[171]

Een andere kenmerkende eigenschap van de telecomsector is de balanceeract die de sector uitvoert tussen veiligheid en de toegankelijkheid van de dienst. Om gebruikers communicatiediensten aan te kunnen bieden moet hen toegang verleend worden tot het netwerk. Doordat er miljoenen gebruikers aan het netwerk verbonden zijn, vaak met meerdere en verschillende soorten apparaten, wordt ook automatisch het aanvalsoppervlak van de netwerken en daarmee de hele sector vergroot. De manier waarop de sector de dienst aan moet bieden, creëert dus ook noodzakelijk een groter aanvalsoppervlak waar de sector aanvullende maatregelen op moet treffen. Doordat de telecominfrastructuur volledig verbonden is met de buitenwereld, zijn beveiligingsmaatregelen, die voor andere bedrijven wel te implementeren zijn, niet altijd toepasbaar binnen de telecomsector. De netwerken verwerken zeer gevoelige gegevens van gebruikers. Grote incidenten kunnen daarom grote uiteenlopende impact hebben. Grootschalige uitval binnen de telecomsector kan ook voor cascade effecten zorgen binnen andere vitale sectoren, die ook gebruikmaken van de netwerken en waarvoor niet altijd een terugvalopties ingeregeld zijn, wat uiteindelijk ook kan leiden tot maatschappelijke ontwrichting. De afgelopen jaren zijn er gelukkig geen incidenten geweest die dergelijke impact hebben gehad.

Telecomsector interessant doelwit voor kwaadwillende actoren, succesvolle aanvallen hebben potentieel grote impact

Voor zowel criminele als statelijke actoren is de telecomsector onder andere interessant omdat de sector enorme hoeveelheden persoonsgegevens verwerkt, waaronder gespreksgegevens, locatiegegevens, klantgegevens en internetverkeer.[172] Toegang tot deze gegevens kan door statelijke actoren misbruikt worden om personen te volgen, te monitoren en te beïnvloeden, zoals leden van de diasporagemeenschappen, activisten of dissidenten. De sector is ook interessant voor statelijke actoren, vanwege de opties voor spionage.[173] Hacks op telecommunicatieproviders behoren volgens de AIVD tot de meest waardevolle inlichtingenposities voor statelijke actoren.[174] Daarom wordt onder andere het gebruik van IT-producten en -diensten uit landen waarvan is vastgesteld dat ze een offensief cyberprogramma tegen Nederlandse belangen voeren in kritieke onderdelen van het telecomnetwerk als onwenselijk gezien.[175] Door spionage kan data worden verworven en kan (technische) kennis worden opgedaan over de infrastructuur. Deze kennis kan enerzijds een spionagedoel dienen, maar kan anderzijds ook gebruikt worden als verkenning van de netwerken. Een verkenning kan onderdeel zijn van (voorbereidingshandelingen voor latere) sabotage. Voorbereidingshandelingen stellen actoren in staat om sabotageacties met weinig tot geen waarschuwing uit te voeren.[176] Bij sabotage van de telecomsector hoeft de sector zelf niet per se het doelwit te zijn, maar kunnen sabotageacties ook gericht zijn tegen (specifieke) afnemers die gebruik maken van het netwerk of op bredere maatschappelijke ontwrichting. Zo wist in 2023 een Russische APT het netwerk van de Oekraïense netwerkprovider Kyivstar plat te leggen, waardoor miljoenen gebruikers dagenlang geen toegang hadden tot hun mobiele netwerk.[177] Ook het uitvoeren van DDoS-aanvallen heeft effect op telecomnetwerken, omdat het aanvalsverkeer gebruikt maakt van de infrastructuur van deze netwerken, ook wanneer de telecomaanbieder zelf geen doelwit is. Voor cybercriminelen zijn vooral de grote hoeveelheden persoonsgegevens die in de sector worden verwerkt interessant. De gegevens kunnen worden gestolen en doorverkocht, of ze kunnen worden gebruikt (als opstap) voor een toekomstige aanval. Zoals voor alle vitale sectoren geldt, is de telecomsector een interessant doelwit voor cybercriminelen omdat continuïteit van groot belang is. Hoewel het belang van continuïteit voor alle vitale sectoren geldt, geldt voor de telecomsector dat er niet altijd een analoge en openbaar toegankelijke terugvaloptie is. Wanneer de financiële sector bijvoorbeeld is aangevallen en pinbetalingen niet meer mogelijk zijn, kan deels, hoe ingewikkeld ook, teruggevallen worden op betalingen met contant geld. Voor de telecomsector is er geen analoge, grootschalige en openbaar toegankelijke terugvaloptie.

Weerbaarheid telecomsector in Nederland robuust, succesvolle aanvallen niet ondenkbaar

Weerbaarheid is het kunnen voorkomen van incidenten door (relevante) risico's tot een aanvaardbaar niveau te reduceren, het kunnen beperken van schade en het kunnen herstellen na het voordoen van een incident.[178] Er wordt continu aan verschillende maatregelen gewerkt om vitale processen te beschermen en om de weerbaarheid van vitale sectoren te vergroten.[179] Sommige weerbaarheidsmaatregelen die effect hebben op de telecomsector zijn of worden wettelijk verankerd in de nationale wetgeving, zoals in de Telecommunicatiewet en de aankomende Cyberbeveiligingswet (Cbw), de implementatie van de Network and Information Security Directive (NIS2-richtlijn).[180]

Er worden grote inspanningen geleverd om de weerbaarheid binnen de telecomsector te vergroten en de weerbaarheid van de Nederlandse telecomsector is robuust.[181] Wel blijven er altijd uitdagingen bestaan. Net als in veel andere landen is in Nederland de telecomsector wettelijk verplicht om voorzieningen in te bouwen waarmee in opdracht van het Openbaar Ministerie (OM) of inlichtingendiensten verkeer afgetapt mag worden (lawful intercept). Deze voorzieningen moeten voldoen aan strenge beveiligingseisen, omdat het staatsgeheime of strafrechtelijke informatie kan bevatten.[182] Uit een onderzoek van de Rijksinspectie Digitale Infrastructuur (RDI) bij providers KPN (2022) en Vodafone (2024) bleek echter dat de beveiliging van het aftapsysteem op enkele onderdelen niet aan de wettelijke eisen voldeed.[183] [184] Beide providers losten de tekortkomingen volledig op na het onderzoek. We kunnen hieruit niet concluderen dat een geavanceerde aanvalscampagne zoals in de VS ook in Nederland succesvol zal zijn. Het onderzoek van de AIVD en MIVD laat echter zien dat ook Nederlandse bedrijven slachtoffer kunnen worden van een dergelijke aanvalscampagne.[185] Het illustreert de aanhoudende en dynamische dreiging, en bovendien het belang van het doorlopend op orde houden van de digitale weerbaarheid in de telecomsector maar ook in andere vitale sectoren.

XI In Nederland zijn de volgende sectoren als vitaal aangemerkt: energie, telecommunicatie, transport, drinkwater, water, chemie, nucleair, financiën, overheid, openbare orde en veiligheid en defensie.

De Zr.Ms. Van Amstel escorteert het Russische fregat Admiral Grigorovich op de Noordzee. Dat gebeurt om ze af te schrikken zodat ze geen sabotage- en spionageactiviteiten uitvoeren.

4 Geopolitieke ontwikkelingen leggen afhankelijkheden nadrukkelijk bloot

Europa, en daarmee Nederland, is voor vele verschillende digitale processen en diensten afhankelijk van aanbieders uit andere, veelal niet-Europese, landen. Zo zijn publieke organisaties in allerlei sectoren in toenemende mate afhankelijk van diensten van enkele grote technologiebedrijven in de VS. Digitale afhankelijkheden die eerder niet als risicovol zijn beoordeeld kunnen dat later alsnog worden, bijvoorbeeld vanwege geopolitieke ontwikkelingen. In die context is het van belang dat potentiële risico's van digitale afhankelijkheden in kaart worden gebracht om de weerbaarheid te kunnen verhogen.

Digitale afhankelijkheden kunnen risico's met zich meebrengen

Nederland is, net als de meeste andere landen, afhankelijk van andere landen en buitenlandse bedrijven. Die afhankelijkheid geldt onder andere voor vele digitale diensten en processen. Wederzijdse afhankelijkheden kunnen positieve gevolgen hebben, zoals ruimte voor specialisatie en het stimuleren van innovatie.[186] Wat betreft digitale technologie staat de Europese positie echter in toenemende mate onder druk.[187] Zo kromp het wereldwijde marktaandeel van Europese bedrijven van 22 procent in 2013 naar 11 procent in 2022.[188] Daaruit volgt dat Europa, en dus Nederland, in toenemende mate afhankelijk is van niet-Europese bedrijven voor digitale technologie. Dat kan risico's met zich meebrengen. Zo geldt dat de nationale veiligheid onder druk kan komen te staan door het gebruik van geïmporteerde technologie die bedrijven of statelijke actoren toegang geeft tot gevoelige informatie en processen. Ook als de vitale digitale processen van de overheid verstoord raken, bestaat het risico dat overheidsprocessen en bedrijfsvoering tot stilstand komen, waardoor het functioneren van de democratische rechtsstaat en de publieke dienstverlening van de overheid in gevaar komt.[189] Verder kunnen (digitale) afhankelijkheden worden ingezet als strategisch of economisch drukmiddel. Economische beïnvloeding voor geopolitieke doeleinden wordt in toenemende mate toegepast door economische grootmachten en ook Europese lidstaten kunnen hier het doelwit van zijn. In dat kader zouden ook knelpunten in de digitale toeleveringsketens actief door staten kunnen worden ingezet als (geo)politiek drukmiddel.[190]

In de huidige geopolitieke context moeten we er rekening mee houden dat landen scherper hun eigen belangen afwegen, waardoor Nederland geconfronteerd kan worden met afhankelijkheden die als drukmiddel kunnen worden ingezet. Juist die geopolitieke ontwikkelingen kunnen ervoor zorgen dat de

afhankelijkheid van digitale diensten en processen uit andere landen risicovol is of kan worden.[191]

Nederland sterk afhankelijk van de VS, veranderende politieke landschap heeft mogelijk invloed op digitale veiligheid

In de afgelopen rapportageperiode is gebleken dat onder andere Nederland sterk afhankelijk is van informatie en diensten uit de Verenigde Staten.[192] Die afhankelijkheid bestaat op verschillende manieren. Zo is de VS een belangrijke partner binnen cybersecurity en daarbij horende samenwerkingsverbanden, bijvoorbeeld vanwege het delen van inlichtingen of het gezamenlijk optreden tegen statelijke en criminele actoren. Juist in het cyberdomein is samenwerking en informatiedeling cruciaal, omdat cyberaanvallen zich niet aan landsgrenzen houden. Het delen van informatie is nodig om breder zicht te krijgen op dreigingen en waar nodig te interveniëren. Het huidige beleid van de VS kan er echter toe leiden dat de VS minder actief is of wordt in internationale samenwerkingsverbanden of dat financiële investeringen afnemen. Vanwege de belangrijke rol die de VS speelt in onder andere cybersecuritysamenwerkingsverbanden, is een actieve rol daarin belangrijk voor de digitale weerbaarheid van onder andere Nederland. De gevolgen van Amerikaanse beleidswijzigingen werden bijvoorbeeld duidelijk toen werd aangekondigd dat de subsidie voor Mitre, beheerder van de veelgebruikte Common Vulnerabilities and Exposures (CVE)-database, zou worden stopgezet.[193] Het CVE biedt een internationale standaard om digitale kwetsbaarheden te benoemen en te documenteren. Zonder deze standaard is het complexer om informatie te delen, analyseren en coördineren, wat leidt tot tragere respons op incidenten. Het wegvallen van de database zou de mondiale digitale weerbaarheid dus verlagen. Uiteindelijk maakte het Amerikaanse cybersecurityagentschap (CISA) bekend dat het de financiering in ieder geval tijdelijk over zal nemen om te voorkomen dat het CVE-programma zou wegvallen.[194]

Daarnaast is Nederland afhankelijk van vele processen en diensten van Amerikaanse technologiebedrijven. Zo is 70 tot 80 procent van de Europese markt voor clouddienstverlening in handen van Amerikaanse bedrijven.[195] De digitale afhankelijkheid van Amerikaanse techbedrijven is echter veel breder dan clouddiensten. Publieke organisaties in allerlei sectoren van de samenleving zijn in toenemende mate afhankelijk van diensten van enkele grote Amerikaanse technologiebedrijven (Big Tech) die software, AI-tools en apparatuur aanbieden.[196] Die afhankelijkheid kan risico's met zich meebrengen (zie kader hiernaast).

Grootschalige afname diensten bij Big Tech kan risico vormen

- Digitale afhankelijkheden kunnen worden vergroot, wat implicaties heeft voor de Nederlandse digitale open strategische autonomie[XII]. Zo kunnen wetten een extraterritoriale werking hebben en bestaan er beperkingen voor Nederland voor het toezicht dat kan worden uitgeoefend.
- Door grootschalige concentratie kan een *single point of failure* ontstaan. Een storing of cyberincident kan wereldwijde doorwerking krijgen. Vitale sectoren kunnen afhankelijk zijn van één aanbieder, wat betekent dat een incident bij die aanbieder grote impact kan hebben.
- De machtspositie van grote aanbieders kan worden versterkt door zowel de aanbod- als vraagzijde. Aan de aanbodzijde kunnen aanbieders een eigen ecoysteem creëren van verschillende diensten, waar organisaties lastig uit kunnen treden (*vendor lock-in*). Aan de vraagzijde kiezen organisaties veel voor de grootste aanbieders, veelal omdat (Europese) alternatieven niet voorhanden zijn of bijvoorbeeld minder functionaliteiten bieden. Ook dit vergroot de machtspositie.
- Organisaties kunnen geleidelijk aan de regie over kernprocessen verliezen, bijvoorbeeld omdat kennis weglekt, de controle over de werking van systemen afneemt of omdat de onderhandelingsruimte ten opzichte van Big Tech beperkt is.

Eén van de risico's die kan voortvloeien uit het afnemen van dergelijke diensten van Big Tech uit niet-Europese landen zoals de VS, is dat wetgeving een extraterritoriale werking kan hebben. De CLOUD-Act maakt het mogelijk dat de federale rechtshandhaving in de VS technologiebedrijven via een bevelschrift of dagvaarding kan dwingen de gevraagde gegevens van gebruikers te verstrekken, ook al zijn die gegevens opgeslagen op buitenlands grondgebied. Veel deskundigen gaan ervan uit dat dit anders is wanneer data wordt verwerkt door een Europese dienstverlener en zeker als dat gebeurt binnen Europa. Juridisch gezien ligt dat echter genuanceerder en geldt dat de Amerikaanse CLOUD-Act ook van toepassing kan zijn op gegevensverwerkingen buiten de VS, bijvoorbeeld in de EU.[197] Alhoewel Microsoft heeft gesteld dat dit nog nooit is gebeurd, erkenden medewerkers van het bedrijf dat zij vanwege deze wetgeving niet kunnen garanderen data van Europese bedrijven binnen Europa te kunnen houden.[198] Daarnaast kunnen (geo)politieke ontwikkelingen effecten hebben op de beschikbaarheid van digitale dienstverlening. Wanneer organisaties of sectoren afhankelijk zijn van dergelijke diensten uit derde landen, kan dat risico's met zich meebrengen. Het is dan ook van belang doorlopend risico's af te wegen, omdat nieuwe risico's kunnen ontstaan die eerder niet reëel waren. Hieruit vloeit voort dat dit niet enkel een vraagstuk is voor technische experts of enkel voor bepaalde (vitale) sectoren. Het kan van invloed zijn op

XII Open strategische autonomie is gedefinieerd als het vermogen van de EU om als mondiale speler, in samenwerzking met internationale partners, op basis van eigen inzichten en keuzes publieke belangen te borgen en weerbaar te zijn in een onderling verbonden wereld'.

IT-strategieën en is daarmee juist ook een vraagstuk voor governance en/of risicomanagement voor bestuurders van organisaties en bedrijven.

Achterblijvende weerbaarheid Caribisch deel Koninkrijk, mede door impact digitale afhankelijkheden

Vanwege de geografische ligging en de kleinschaligheid kunnen we de hierboven genoemde mogelijke risico's niet direct vertalen naar het Caribisch deel van het Koninkrijk.[XIII] Zo wijkt de digitale infrastructuur af van Europees Nederland, mede omdat deze deels is verouderd. Ook wordt vanwege de geografische ligging wellicht logischerwijs eerst naar de VS gekeken voor producten en diensten. Net als in Europees Nederland wordt in grote mate gebruik gemaakt van diensten van Amerikaanse Big Tech door overheden en andere organisaties, zoals van e-maildiensten. Een belangrijk verschil met Europees Nederland is dat de (internet)connectiviteit voor het overgrote deel verloopt via zeekabels via Puerto Rico naar een internetknooppunt in de VS. Ook is er met betrekking tot connectiviteit sterke onderlinge afhankelijkheid tussen de zes Caribische eilanden van het Koninkrijk. Zo is Bonaire voor internet afhankelijk van twee verbindingen die lopen via Curaçao en zijn Sint Eustatius en Saba voor hun verbindingen grotendeels afhankelijk van Sint Maarten.[199] De combinatie van deze factoren maakt dat het Caribisch deel van het Koninkrijk in hoge mate afhankelijk is voor haar digitale infrastructuur van niet-Europese Big Tech en van enkele verbindingen die bovendien naar niet-Europese landen lopen.

Daarnaast is er op de eilanden sprake van toenemende digitalisering, maar deze is nog niet op het niveau van Europees Nederland. Ook is de samenleving minder digitaal vaardig en bestaat er minder bewustzijn van digitale risico's.[200] Zo vindt interactie met de overheid en bedrijven veelal nog plaats via papier en loket. Hierop zijn diverse initiatieven gestart, zoals in de zorg.[201] Een nieuwe wet moet er voor zorgen dat burgers en bedrijven in Caribisch Nederland veilig en betrouwbaar gebruik kunnen maken van de digitale diensten van de overheid.[202] De wet beoogt de digitale dienstverlening van de (semi)overheid in Caribisch Nederland zoveel mogelijk op een gelijkwaardig niveau als in Europees Nederland te brengen. Deze koppeling met Europees Nederland introduceert nieuwe digitale risico's voor zowel het Caribisch deel van het Koninkrijk als voor Europees Nederland. Het Caribische deel van het Koninkrijk kan voor aanvallers namelijk interessant zijn als opstap om toegang te krijgen tot systemen van de Rijksoverheid. Daarmee kan toegang worden gerealiseerd tot gegevens van burgers en bedrijven en dit kan als opstap worden gebruikt voor andere systemen in Europees Nederland. De verdere koppeling met overheidssystemen maakt dat de gekoppelde systemen aan minimumeisen[XIV] moeten voldoen. Anders dan regelgeving die volgt uit deze concrete digitaliseringsslag loopt de wetgeving om veiligheid en betrouwbaarheid van digitale diensten en vitale infrastructuur te verhogen achter. EU-richtlijnen zoals de NIS2 die in Europees Nederland van kracht zijn of worden gelden niet[XV], waaronder de eis dat bedrijven maatregelen nemen om de toeleveringsketen te beveiligen en maatregelen treffen voor bedrijfscontinuïteit. De Wet bevordering digitale weerbaarheid is daarentegen wel van toepassing verklaard voor Caribisch Nederland, waardoor algemene en specifieke (dreigings)informatie kan worden gedeeld.

Er wordt in vergelijking met Europees Nederland weinig onderzoek gedaan naar digitale dreigingen richting het Caribisch deel van het Koninkrijk. Er is geen specifieke dreiging bekend, maar de dreigingen zoals beschreven in dit CSBN zijn ook hier van toepassing. Net als in de rest van de wereld vormen kwetsbare systemen een aantrekkelijk doelwit voor kwaadwillenden, wat betekent dat het tijdig en adequaat patchen van kwetsbare systemen van groot belang is. Statistieken geven weer dat de Caribische landen een hoger aantal mogelijk gecompromitteerde systemen per aantal inwoners hebben dan Europees Nederland, op sommige momenten wel meer dan drie keer zoveel. Het aantal kwetsbare systemen in Europees Nederland is groter maar de omvang van de digitale infrastructuur is ook vele malen groter[XVI]. Diverse incidenten laten ook zien dat aanvallen die we in de rest van de wereld zien ook op de eilanden plaatsvinden. Zo was de Belastingdienst op Curaçao slachtoffer van een ransomware-aanval, had het Gemeenschappelijk Hof van Justitie uitval door malware op de systemen en is er ingebroken op de e-mailaccounts van Arubaanse parlementsleden. [203],[204]

Op dit moment is de digitalisering in opmars, wat maakt dat ook in het Caribisch deel van het Koninkrijk meer digitale diensten worden ontwikkeld en afgenomen. Echter blijven wetgeving en bewustzijn over de risico's achter. Nog meer dan in Europees Nederland kunnen door de kleinschaligheid en onderlinge afhankelijkheden in het Caribisch gebied strategische afhankelijkheden worden geïntroduceerd die risico's met zich meebrengen. Gezien de geografische ligging en de beperktere mogelijkheden voor terugvalopties kan uitval van gedigitaliseerde, vitale processen meer lokale impact hebben dan in Europees Nederland en is het belang van ontwikkelen van terugvalopties groter.

XIII Het Caribisch deel van het Koninkrijk omvat zowel de autonome Caribische landen Aruba, Curaçao en Sint Maarten als Caribisch Nederland (Bonaire, Sint Eustatius en Saba).

XIV Onder andere de Baseline Informatiebeveiliging (BIO) en de DigiD aansluitvoorwaarden.

XV NIS2 en Cbw gelden slechts voor Rijksoverheidsorganisaties die actief zijn in Caribisch Nederland.

XVI Gegevens Shadowserver.org, er zijn geen afzonderlijke gegevens voor Caribisch Nederland.

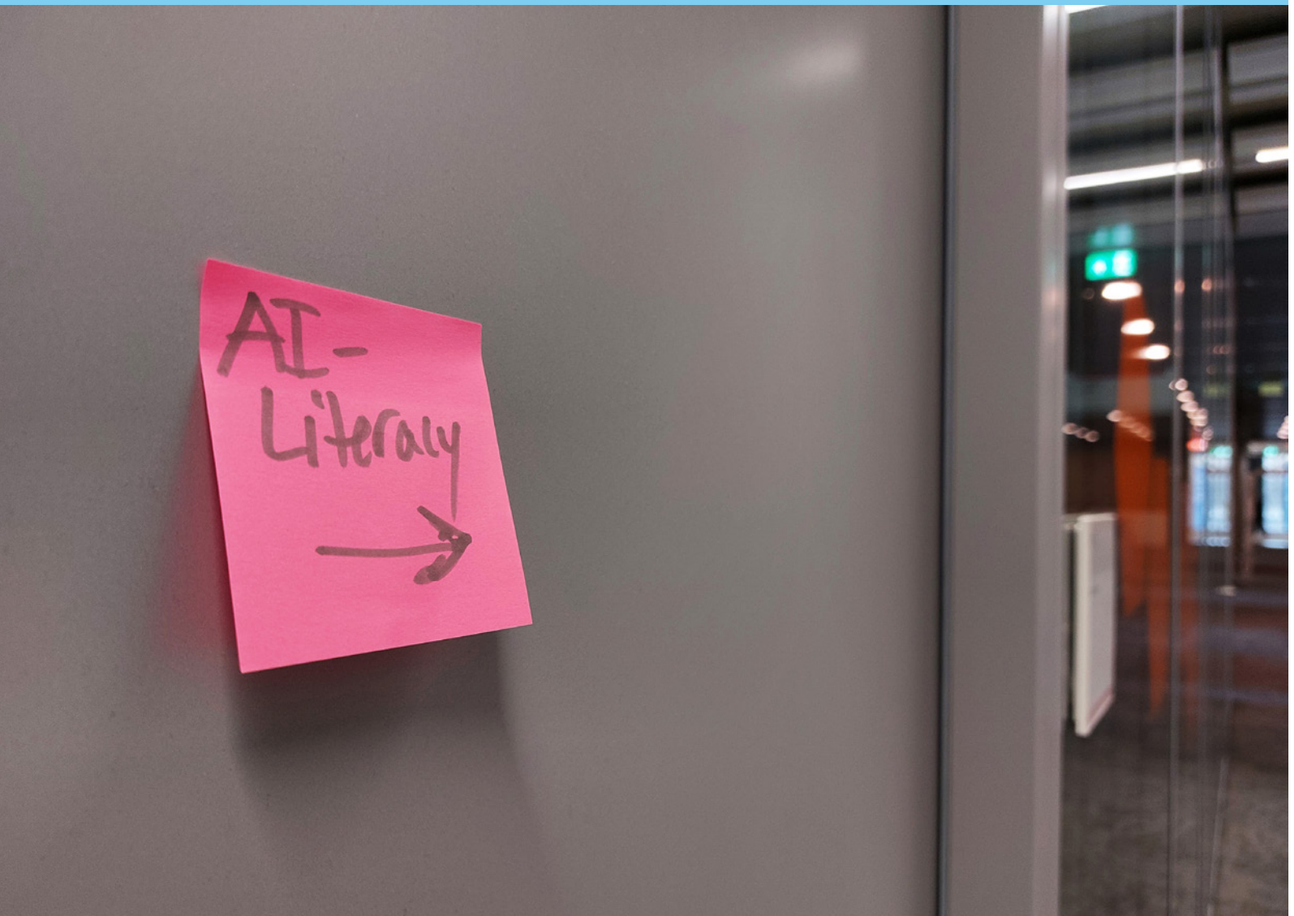
Hogere mate autonomie en inrichten terugvalopties kunnen risico's verkleinen

Zoals beschreven in dit hoofdstuk, zijn geopolitieke verhoudingen een factor die van invloed kan zijn op de mate van risico van digitale afhankelijkheden. Hoe groot die risico's zijn en in welke mate het reëel is dat die tot uiting komen, verschilt per casus. Wat echter wel een gegeven is, is dat geopolitiek in beweging is en invloed heeft op verhoudingen tussen landen. Juist in de snel veranderende geopolitieke realiteit van vandaag, is het van belang inzichtelijk te maken welke afhankelijkheden risico's met zich mee kunnen brengen en wat hiervan de gevolgen zijn. Het proberen te beperken van die risico's kan bijvoorbeeld leiden tot het streven naar een hogere mate van digitale open strategische autonomie. Bovendien is een belangrijk onderdeel van digitale weerbaarheid het hebben van terugvalopties voor digitale diensten en processen. Het hebben van terugvalopties verkleint niet alleen de potentiële impact van cyberincidenten, maar verkleint ook de risico's van afhankelijkheden.

Uit onderzoek blijkt dat organisaties binnen de Rijksoverheid veel digitale processen afnemen van een klein aantal leveranciers, waarbij weinig tot geen rekening wordt gehouden met het voorkomen van concentratierisico's. Mogelijke consequenties van concentratierisico's worden bovendien onvoldoende afgewogen op bestuurlijk niveau.[205] Dit kan leiden tot digitale monoculturen, waarin vele organisaties afhankelijk zijn van een klein aantal aanbieders.

De vergaande en onvoorziene effecten van een incident binnen een monocultuur werden duidelijk uit de storing bij het Amerikaanse cybersecuritybedrijf CrowdStrike in juli 2024.[206] Verder wegen en beschouwen overheidsorganisaties onvoldoende de (strategische) risico's van hun leveranciers en dienstverleners en blijkt dat meerdere overheidsorganisaties geen succesvolle terugvalopties hebben.[207] Uit het voorgaande blijkt dat de Rijksoverheid op verschillende punten onvoldoende aandacht besteedt aan weerbaarheid en stappen heeft te maken. Daar valt onder andere winst te behalen door afhankelijkheden doorlopend onderwerp te maken op bestuurstafels en daar gedegen risicoanalyses op uit te voeren.

Toepassingen van generatieve AI zijn voor een groot publiek toegankelijk, ook voor kwaadwillenden. AI biedt kansen maar versterkt ook bestaande digitale dreigingen.



5 Generatieve AI versterkt bestaande dreigingen voor digitale veiligheid

In de afgelopen jaren is de ontwikkeling van generatieve AI in een versnelling gekomen. De technologie achter generatieve AI vormt geen dreiging op zichzelf. Maar door specifieke toepassingen van de techniek en intenties van de actor die het inzet, kunnen hier wel dreigingen uit voortvloeien. Generatieve AI kan op verschillende manieren worden ingezet: zowel ter ondersteuning voor kwaadaardige activiteiten als ter verdediging tegen dreigingen. Op dit moment versterkt generatieve AI bestaande digitale dreigingen.

Generatieve AI versterkt bestaande digitale dreigingen

Kunstmatige intelligentie (*artificial intelligence* of AI) is een veelomvattende technologie die onze samenleving fundamenteel zal veranderen.[208] Een onderliggende vorm van deze technologie is generatieve AI. Generatieve AI is een vorm van AI die op basis van door de gebruiker gegeven opdrachten of vragen nieuwe content kan creëren uit bestaande data.[209] Veel van de AI-toepassingen die van invloed zijn op de nationale veiligheid behoren tot generatieve AI. Onder generatieve AI vallen onder ander *Large Language Models* (LLM's), die worden gebruikt om teksten te genereren. De afgelopen jaren zijn verschillende LLM's en toepassingen daarvan zoals ChatGPT, Gemini en Llama voor het grote publiek beschikbaar geworden. Al snel kwamen ook berichten naar buiten over (mogelijk) misbruik van deze systemen door kwaadwillende actoren in cyberoperaties.[210]

Generatieve AI kan worden ingezet voor offensieve en defensieve operaties

Generatieve AI kan door cyberactoren op een aantal manieren worden ingezet:[211]

1. Informatie verzamelen en detecteren van doelwitten
Cyberactoren kunnen LLM's gebruiken om snel en automatisch interessante doelwitten te detecteren en informatie over mogelijke doelwitten te verzamelen of nieuwe kwetsbare systemen vinden. Onderzoekers toonden bijvoorbeeld aan dat ChatGPT gebruikt kan worden om snel informatie te vergaren over het IT-systeem van een bank.[212] Hoewel dit soort informatie vaak ook openbaar op het internet te vinden is, kunnen LLM's het proces om deze informatie te verzamelen en te analyseren aanzienlijk versnellen.

2. Inzetten voor social engineering
Cyberactoren kunnen LLM's gebruiken om social engineering[XVII] toe te passen. LLM's bieden de mogelijkheid om foutloze teksten in verschillende talen te genereren, ook als een cyberactor die taal zelf niet machtig is.[213] Op die manier kunnen geautomatiseerd en

XVII Social engineering omvat de technieken die cybercriminelen inzetten om door middel van psychologische manipulatie slachtoffers te verleiden gevoelige gegevens prijs te geven. De aanvaller beïnvloedt de ander om vervolgens het gewenste resultaat of voordeel te halen.

zeer snel overtuigende spam- en phishingteksten worden geschreven. LLM's zijn inmiddels dermate ver ontwikkeld dat deze ook kunnen worden gebruikt om audio- en videogesprekken te interpreteren, een antwoord te formuleren en deze weer 'uit te spreken' naar het slachtoffer. Door AI te gebruiken voor dergelijke social engineering, bestaat er een grotere kans dat de ontvanger de aanvaller als betrouwbaar beoordeelt. [214] Cyberactoren kunnen met LLM's snel reageren vanuit een bepaalde context, specifieke schrijf- of spreekstijlen aannemen en daarmee overtuigend een specifiek persoon na doen.

3. Malware genereren en cyberaanvallen uitvoeren
LLM's stellen cyberactoren in staat om cyberaanvallen uit te voeren die ze technisch gezien niet zouden kunnen doen zonder de hulp van AI. Cyberactoren die deze technische kennis wel hebben, kunnen dat met AI sneller en eenvoudiger doen.[215] Verschillende LLM's zijn (ook) getraind op verschillende programmeertalen, waardoor cyberactoren ze kunnen gebruiken of behulpzaam zijn bij het schrijven van malware.[216] Zo kunnen cyberactoren als het ware sparren met het model om effectieve code te schrijven en/of voor het vinden van kwetsbaarheden in code. Hierbij is op dit moment nog steeds enige kennis van programmeren of kwetsbaarheden noodzakelijk.[217] Malware zelf kan door AI ook intelligenter worden doordat het zelflerende eigenschappen krijgt, waarmee het zelfstandig nieuwe kwetsbaarheden kan vinden en hier vervolgens misbruik van maken. Doordat aanvallen steeds beter vermomd worden, kan malware lange tijd onopgemerkt geïnstalleerd zijn op een apparaat en zich verspreiden naar andere apparaten en netwerken.[218] Daarbij kan AI malware ook helpen door snel grote hoeveelheden data te analyseren om te identificeren wat waardevol is en wat niet.

4. Inzetten ter verdediging
Het vermogen van AI-algoritmes om grote hoeveelheden gegevens snel te analyseren en afwijkende patronen te herkennen kan ook worden gebruikt bij de verdediging tegen cyberaanvallen.[219] Zo kan AI netwerkverkeer analyseren om ongebruikelijk verkeer te detecteren dat wijst op potentiële cyberdreigingen. AI kan ook worden gebruikt voor het verwerven en verwerken van bedreigingsinformatie en het analyseren van malware.[220]

Naast het inzetten van generatieve AI voor offensieve en defensieve operaties, vormt generatieve AI op zichzelf een mogelijk doelwit. Hierbij gaat het om aanvallen die gericht zijn op het verstoren of misleiden van AI-systemen, inclusief pogingen de trainingsdata te beïnvloeden of de AI op ongepaste wijze te manipuleren.[221] Zo kunnen AI-systemen worden aangevallen met zogeheten 'adversarial attacks', welke zeer complex zijn om te detecteren. Met zulke aanvallen kunnen aanvallers bijvoorbeeld trainingsdata van een model proberen te achterhalen.

Generatieve AI versterkt bestaande dreigingen, inzet door kwaadwillenden aannemelijk

Voor generatieve AI geldt dat de technologie zelf geen dreiging vormt voor de nationale veiligheid. De dreiging schuilt in de specifieke toepassing van de techniek en de intenties van de actor die hier gebruik van maakt.[222] Wel blijkt uit de invalshoeken zoals hierboven beschreven, dat cyberaanvallen met behulp van generatieve AI minder technische kennis en capaciteit vereisen. Dit maakt het voor een bredere groep actoren mogelijk om aanvallen uit te voeren. Bovendien kunnen (voorbereidingen voor) aanvallen met behulp van generatieve AI op veel grotere schaal en sneller plaatsvinden.

Cybersecuritybedrijf Symantec rapporteerde een stijging te zien in het aantal cyberaanvallen door cybercriminelen waarbij LLM's werden gebruikt om code te genereren voor malware.[223] Volgens cybersecuritybedrijf Talos maken cybercriminelen in toenemende mate gebruik van 'ongecensureerde LLM's', oftewel LLM's die zonder beperkingen of waarborgen werken. Voor sommige van deze ongecensureerde LLM's wordt actief gepromoot dat er bijvoorbeeld malware en phishing pagina's mee kunnen worden gecreëerd.[224] Gezien de brede beschikbaarheid en snelle doorontwikkeling van generatieve AI, is het aannemelijk dat criminele actoren hier gebruik van zullen blijven maken of het gebruik hiervan zullen intensiveren.

Voor statelijke actoren geldt dat de MIVD en AIVD op basis van eigenstandige inlichtingen het gebruik van generatieve AI hebben onderkend bij meerdere statelijke actoren. Ook Google rapporteert dat verschillende APT's, waaronder afkomstig uit Iran en Rusland, gebruik maken van LLM's voor verschillende (vroege) fases van cyberaanvallen.[225] Het laat zich moeilijk voorspellen op welke manier AI de werkwijze van statelijke actoren wereldwijd zal veranderen. De diensten beschikken over inlichtingen dat statelijke cyberactoren interesse hebben in het gebruik van AI, onder andere voor het uitvoeren van digitale beïnvloedingsoperaties. Met de operationele inzet van AI zullen de capaciteiten van deze cyberactoren om digitale beïnvloedingsoperaties uit te voeren zeer waarschijnlijk aanzienlijk toenemen. Dit zal het complexer maken om beïnvloedingsoperaties te onderkennen en ontkrachten. De diensten achten dit een zorgwekkende ontwikkeling.

Bijlagen

De afgelopen periode zorgden meerdere DDoS-aanvallen voor (tijdelijke) verstoringen van diensten. Zo vonden van januari tot en met maart 2025 vier aanvallen plaats waardoor DigiD een uur of langer niet beschikbaar was. Daardoor waren ook aanverwante diensten beperkt beschikbaar en konden gebruikers tijdelijk niet inloggen.

1 Verantwoording

Doel en afbakening

Het Cybersecuritybeeld Nederland 2025 (CSBN 2025) biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de digitale weerbaarheid en tot slot digitale risico's. Daarnaast heeft het tot doel om inzicht te geven in mogelijke veranderingen in de strategische thema's die in het CSBN 2022 zijn uitgewerkt. Deze thema's vormden een inhoudelijke basis voor de Nederlandse Cybersecurity Strategie 2022-2028. Het CSBN 2025 vormt een inhoudelijke basis voor de evaluatie van het daarvan afgeleide actieplan.

Het accent ligt op de nationale veiligheid. Digitalisering biedt vele kansen, maar leent zich ook voor allerlei vormen van misbruik en er kan sprake zijn van uitval. Het CSBN richt zich niet op de kansen van digitalisering. Het CSBN richt zich wél op verstoringen van (kritische) processen met een digitaal component.

Het CSBN is primair bedoeld voor strategie- en beleidsvorming op nationaal niveau. Het beoogt het kabinet, de leden van de Eerste en Tweede Kamer, ambtenaren, beleidsmakers, overige bestuurders, directies en andere geïnteresseerden inzicht te geven in de digitale risico's voor Nederland. Cybersecuritybedrijven en –professionals gebruiken het CSBN als referentiekader richting de eigen bestuurders of klanten. Het CSBN is ook bedoeld als hulpmiddel voor risicomanagement, waarbij het zich specifiek richt op de identificatie en analyse van risico's, een van de stappen in een risicomanagementproces. Tot slot is het CSBN beschikbaar voor het brede publiek.

Leeswijzer

Dit CSBN bestaat uit een zelfstandig leesbaar Kernhoofdstuk (Hoofdstuk 1) waarin de hoofdboodschappen zijn verwoord. Het Kernhoofdstuk is gebaseerd op de verdiepende hoofdstukken met verschillende thema's, daarom bevat het Kernhoofdstuk geen bronvermelding. Deze indeling beoogt dat lezers uit verschillende doelgroepen door het CSBN kunnen navigeren en zich kunnen richten op de onderwerpen die aansluiten bij hun professionele rol of interesse. De verdiepende hoofdstukken hebben de volgende thema's:

- Hoofdstuk 1, het Jaarbeeld, geeft een overzicht van relevante incidenten in de periode juli 2024 t/m augustus 2025. Het hoofdstuk omvat ook duiding van de incidenten, gevat in rode draden.
- Hoofdstuk 2 beschrijft een toename in statelijke cybercapaciteiten en hoe staten vermengen met niet-statelijke actoren en/of private organisaties.
- Hoofdstuk 3 beschrijft de interesse van kwaadwillende actoren in de telecomsector als zijnde een vitale sector naar aanleiding van een cybercampagne elders in de wereld.
- Hoofdstuk 4 beschrijft de risico's die kunnen voortvloeien uit digitale afhankelijkheden en hoe veranderende geopolitieke omstandigheden van invloed kunnen zijn voor de risicobeoordeling van afhankelijkheden.
- Hoofdstuk 5 beschrijft dat generatieve AI bestaande dreigingen voor digitale veiligheid versterkt en hoe LLM's kunnen worden ingezet voor zowel offensieve als defensieve operaties.

Verantwoording wijze van totstandkoming

Het Cybersecuritybeeld Nederland wordt jaarlijks vastgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Daarbij wordt dankbaar gebruik gemaakt van de informatie, de inzichten en de expertise van overheidsdiensten, organisaties in vitale processen, de wetenschap en andere partijen.

De totstandkoming van het CSBN kent drie fasen:

1. Analyseren.
De NCTV verzamelt en analyseert relevante informatie over incidenten, trends en verschuivingen op het gebied van de driehoek belang, dreiging en weerbaarheid. De volgende vragen liggen ten grondslag aan het CSBN:

- Welke relevante incidenten hebben in de periode van juli 2024 tot en met augustus 2025 in Nederland of in vergelijkbare landen plaatsgevonden en tot welke nieuwe inzichten leiden die?
- Welke bredere politieke, economische, sociale en technologische ontwikkelingen en factoren hebben naar verwachting de komende jaren invloed op digitale veiligheid? Welke ontwikkelingen kunnen gamechangers zijn?
- Welke veranderingen zijn te identificeren in digitale dreigingen die de nationale veiligheid aantasten? Denk hierbij aan de aard en omvang van de dreiging, doelwitten, actoren, kwetsbaarheden, vormen van uitval en werkwijzen actoren.
- Welke veranderingen zijn te identificeren, die van invloed zijn op belangen die kunnen worden aangetast wanneer cyberincidenten zich voordoen? En wat kan de impact daarvan zijn?
- Welke veranderingen zijn te identificeren in de mate waarin Nederland weerbaar is tegen die digitale dreigingen?
- In hoeverre treden veranderingen op in de grootste risico's voor de nationale veiligheid van Nederland?

Analisten van de NCTV hebben aan de hand van deze vragen een eerste inventarisatie van 'ingrediënten' voor het CSBN gemaakt. Deze zijn in een drietal sessies besproken met experts van publieke organisaties en aangevuld met inzichten. Daarnaast zijn experts bevraagd op specifieke onderdelen in dit CSBN, zoals de dreiging richting de telecomsector en de staat van digitale veiligheid in Caribisch Nederland.

2. Schrijven en collegiaal toetsen.
Na afronding van de analysefase zijn concepthoofdstukken geschreven door afzonderlijke auteurs. Het Jaarbeeld is tussentijds getoetst bij collega's van de NCTV, het NCSC en bij de AIVD en de MIVD. Op verschillende onderdelen is actief meegeschreven door onder andere het OM, THTC, het ministerie van Buitenlandse Zaken en de AIVD en MIVD.

3. Valideren.
Het CSBN kent een uitgebreid validatietraject, waarbij de concepttekst ter commentaar wordt voorgelegd aan interne en externe partners. Na het verwerken van het verzamelde commentaar wordt de definitieve tekst opgemaakt en door de NCTV vastgesteld. Na de publicatie van het CSBN vindt een primair interne evaluatie plaats. De verzamelde feedback wordt vervolgens verwerkt in het CSBN-traject van het volgende jaar.

2 Methodologische toelichting cijfers ransomware-aanvallen

Toelichting cijfers Jaarbeeld samenwerkingsproject Melissa

Het Jaarbeeld Melissa compileert informatie over ransomware-incidenten bij grotere organisaties (vanaf ca. 100 fte). Het is gebaseerd op incidentinformatie van het OM, de politie, het NCSC, Cyberveilig Nederland en diverse private partijen. Wat betreft de bedrijven gaat het om bedrijven die aan incidentresponse doen bij ransomware-aanvallen. Incidenten zijn beoordeeld door security-experts die een specifieke afbakening van de definitie ransomware hanteren. Melissa hanteert als definitie voor ransomware: *"... aanvallers gijzelen data van het slachtoffer en gebruiken drukmiddelen om het slachtoffer over te halen"*.[226] Hierdoor kan dit jaarbeeld afwijken van andere jaarbeelden waarbij uitvraag is gedaan bij burgers en/of kleinere organisaties. Vanwege het anonimiseren van de data is perfect ontdubbelen niet mogelijk. Daarom wordt er gesproken over een schatting van unieke incidenten.[227] Opgemerkt moet worden dat uitgegaan wordt van de initiële ransomware-aanval. Zo telt een aanval op een serviceprovider met tientallen klanten die ook slachtoffer worden van dezelfde aanval, als één aanval.[228]

Het Jaarbeeld Ransomware 2024 beschrijft dat van de 121 ransomware-aanvallen er 76 bekend waren via aangiften bij de politie en 20 via incident response bedrijven. Daarbovenop waren 25 aanvallen bekend bij zowel incident response bedrijven als bij de politie.

Toelichting cijfers Autoriteit Persoonsgegevens (AP)

De cijfers zijn gebaseerd op een analyse van gemelde datalekken bij de AP in 2024.[229] De AP hanteert als definitie voor ransomware: *"... een vorm van malware (kwaadaardige software) die een computer of bestanden gijzelt. Meestal wordt daarna betaling geëist."*

Uitsluitend exfiltratie, zonder versleuteling of zonder eis tot betaling van losgeld, valt onder (andere vormen van) malware. Vergelijkbaar met de systematiek van het project Melissa zijn de cijfers van de AP enkel gebaseerd op de eerste aanval, dus als één ransomware-aanval leidt tot tien meldingen bij de AP, wordt dit als één gerekend in de cijfers. De meldingen zelf zijn afkomstig van de verwerkingsverantwoordelijken. Dit kan het bedrijf zijn waar de aanval heeft plaatsgevonden en/of een ander bedrijf als hun verwerker (denk aan een ICT-leverancier) door ransomware is geraakt waarbij data van het bedrijf ook is getroffen. Een ransomware-aanval waarbij persoonsgegevens zijn getroffen, moet worden gemeld tenzij er geen risico is voor personen. Dat kan betekenen dat ook als geen data is ge-exfiltreerd er nog steeds een meldplicht is. Voor versleuteling hebben de hackers immers toegang gehad tot persoonsgegevens. De AP vond 112 ransomware-aanvallen in 2024.

Het werkelijke aantal kan hoger zijn dan 112 doordat:

- Er ondanks de wettelijke verplichting geen melding is gedaan;
- Er geen toegang is verkregen tot persoonsgegevens: dat lijkt niet heel waarschijnlijk doordat vrijwel altijd wel sprake is van opslag van persoonsgegevens;
- De ransomware aanval vroegtijdig is voorkomen;

Het gaat om een buitenlandse vestiging van een organisatie met een hoofdvestiging in een ander land. De datalekmelding wordt dan bij een buitenlandse toezichthouder gedaan.

Verschil cijfers project Melissa en die van de AP

Feit is dat het aantal gemelde ransomware-aanvallen bij Melissa groter is dan wat er door de AP is gerapporteerd. Een verklaring daarvoor kan zijn dat er geen persoonsgegevens geraakt werden bij de door de AP gemelde incidenten. Daarnaast zou het verschil in cijfers voort kunnen komen uit hantering van net andere definities van ransomware.

In beginsel mag worden aangenomen dat vrijwel voor alle ransomware-aanvallen een wettelijke verplichting bestaat om deze te melden bij de AP. Het is immers zeer aannemelijk dat de aanvallers inzage hebben gehad in persoonsgevoelige data. In welke mate ransomware-aanvallen waarover Melissa rapporteert zijn gemeld aan de AP, is niet bekend.

3 Bronnen en referenties

1 ‘Logius wil nieuwe aanpak voor “slimmere en minder voorspelbare” ddos-aanvallen’ , Tweakers, 28-03-2025, https://tweakers.net/nieuws/233350/logius-wil-nieuwe-aanpak-voor-slimmere-en-minder-voorspelbare-ddos-aanvallen.html.

2 Jaarbeeld Ransomware 2024, NCSC, 17-02-2025, https://www.ncsc.nl/documenten/publicaties/2025/02/17/jaarbeeld-ransomeware-2024.

3 ‘Rapportage datalekken 2024’, Autoriteit Persoonsgegevens, 03-07-2025, https://www.autoriteitpersoonsgegevens.nl/documenten/rapportage-datalekken-2024.

4 ‘Veranderende wereldorde bevestigt belang van een weerbaar Nederland’, NCTV, 17-07-2025, https://www.nctv.nl/actueel/nieuws/2025/07/17/veranderende-wereldorde-bevestigen-belang-van-een-weerbaar-nederland.

5 Cybersecuritybeeld Nederland 2024, NCTV, 28-10-2024, https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/nieuws/2024/10/28/cybersecuritybeeld-2024-turbulente-tijden-onvoorziene-effecten.

6 Openbaar jaarverslag 2024, Militaire Inlichtingen- en Veiligheidsdienst, MIVD, 22-04-2025, https://www.defensie.nl/downloads/jaarverslagen/2025/04/22/openbaar-jaarverslag-2024-militaire-inlichtingen--en-veiligheidsdienst.

7 ‘Internationale politiediensten pakken met Operation Endgame door in bestrijding ransomware’, Politie.nl, 23-05-2025, https://www.politie.nl/nieuws/2025/mei/22/11-internationale-politiediensten-pakken-met-operation-endgame-door-in-bestrijding-ransomware.html.

8 ‘Internationale opsporingsdiensten ontmantelen infostealers’, politie.nl, 29-10-2024, https://www.politie.nl/nieuws/2024/oktober/29/internationale-opsporingsdiensten-ontmantelen-infostealers.html.

9 https://www.politie.nl/nieuws/2025/mei/7/11-opnieuw-wereldwijde-politieacties-tegen-ddos.html, politie.nl, 07-05-2025, https://www.politie.nl/nieuws/2025/mei/7/11-opnieuw-wereldwijde-politieacties-tegen-ddos.html.

10 ‘Internationale cybercrime aangepakt: Politie Amsterdam en FBI ontmantelen proxydienst Anyproxy’, politie.nl, 12-05-2025 , https://www.politie.nl/nieuws/2025/mei/9/internationale-cybercrime-aangepakt-politie-amsterdam-en-fbi-ontmantelen-proxydienst-anyproxy.html

11 ‘Sleuteldienst voor ontwikkelaars van malware onderuitgehaald’, politie.nl, 30-05-2025, https://www.politie.nl/nieuws/2025/mei/30/11-sleuteldienst-voor-ontwikkelaars-van-malware-onderuitgehaald.html.

12 ‘BKA and FIOD shut down cryptocurrency swap service eXch. € 34 million in cryptocurrency has been seized during the operation’, FIOD, 09-05-2025, https://www.fiod.nl/bka-and-fiod-shut-down-cryptocurrency-swap-service-exch-e-34-million-in-cryptocurrency-has-been-seized-during-the-operation/.

13 ‘Nederland lanceert internationaal netwerk voor daderpreventie cybercrime: InterCOP’, politie.nl, 15-06-2023, https://www.politie.nl/nieuws/2023/juni/15/11-nederland-lanceert-internation-aal-netwerk-voor-daderpreventie-cybercrime-intercop.html.

14 ‘Internationale politiediensten pakken met Operation Endgame door in bestrijding ransomware’, politie.nl, 23-05-2025, https://www.politie.nl/nieuws/2025/mei/22/11-internationale-politiediensten-pakken-met-operation-endgame-door-in-bestrijding-ransomware.html.

15 ‘Internationale opsporingsdiensten ontmantelen infostealers’, politie.nl, 29-10-2024, https://www.politie.nl/nieuws/2024/oktober/29/internationale-opsporingsdiensten-ontmantelen-infostealers.html.

16 ‘Internationale operatie tegen hackgroep NoName057(16)’, Politie, 16-07-2025, https://www.politie.nl/nieuws/2025/juli/16/06-internationale-operatie-tegen-hackgroep-noname057l6.html.

17 ‘”Onze aanvallen gaan door!”: Pro-Russische hackers willen wraak na internationale politieactie’, Pointer, 08-08-2025, https://pointer.kro-ncrv.nl/aanvallen-gaan-door-pro-russische-hackers-wraak-internationale-politieactie.

18 ‘ECLI:NL:RBROT:2025:2492’, uitspraken.rechtspraak.nl, 21-02-2025, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBROT:2025:2492&showbutton=true&idx=3.

19 ‘ECLI:NL:RBROT:2025:2515’, uitspraken.rechtspraak.nl, 21-02-2025, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBROT:2025:2515&showbutton=true&idx=2.

20 ‘Cyber-attacks: Council extends sanctions and legal framework’, European Council, 12-05-2025, https://www.consilium.europa.eu/en/press/press-releases/2025/05/12/cyber-attacks-council-extends-sanctions-and-legal-framework/.

21 ‘MIVD waarschuwt: Russen hebben het gemunt op westerse hulp aan Oekraïne’, MIVD, 05-09-2024, https://www.defensie.nl/actueel/nieuws/2024/09/05/mivd-waarschuwt-russen-hebben-het-gemunt-op-westerse-hulp-aan-oekraine.

22 ‘Cyber-attacks: three individuals added to EU sanctions list for malicious cyber activities against Estonia’, European Council, 27-01-2025, https://www.consilium.europa.eu/en/press/press-releases/2025/01/27/cyber-attacks-three-individuals-added-to-eu-sanctions-list-for-malicious-cyber-activities-against-estonia/.

23 ‘Onbekende Russische groep achter hacks Nederlandse doelen’, AIVD, 27-05-2025, https://www.aivd.nl/actueel/nieuws/2025/05/27/onbekende-russische-groep-achter-hacks-nederlandse-doelen.

24 ‘Russian hybrid threats: EU lists further 21 individuals and 6 entities and introduces sectoral measures in response to destabilising activities against the EU, its member states and international partners’, European Council, 20-05-2025, https://www.consilium.europa.eu/en/press/press-releases/2025/05/20/russian-hybrid-threats-eu-lists-further-21-individuals-and-6-entities-and-introduces-sectoral-measures-in-response-to-destabilising-activities-against-the-eu-its-member-states-and-international-partners/.

25 ‘Helping our customers through the CrowdStrike outage’, Microsoft, 20-07-2024, https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/.

26 ‘CrowdStrike: logicafout zorgde voor blue screen of death bij computers’, Security.nl, 20-07-2024, https://www.security.nl/posting/850698/CrowdStrike%3A+logicafout+zorgde+voor+blue+screen+of+death+bij+computers.

27 Cybersecuritybeeld Nederland 2024, NCTV, 28-10-2024, https://www.nctv.nl/documenten/publicaties/2024/10/28/cybersecuritybeeld-nederland-2024.

28 ‘Ook ministerie van Buitenlandse Zaken getroffen door storing’, NRC, 19-06-2024, https://www.nrc.nl/nieuws/2024/07/19/ook-ministerie-van-buitenlandse-zaken-getroffen-door-storing-a4860171.

29 ‘Systemen bij overheidsdiensten plat door storing bij ministerie van Defensie’,NOS,28-08-2024,https://nos.nl/artikel/2534851-systemen-bij-overheidsdiensten-plat-door-storing-bij-ministerie-van-defensie.

30 ‘Kamerbrief over IT storing bij Defensie en andere overheidsdiensten’, Rijksoverheid, 28-08-2024, https://www.rijksoverheid.nl/documenten/kamerstukken/2024/08/29/kamerbrief-it-storing-bij-defensie-en-andere-overheidsdiensten-tk.

31 ‘Evaluatie NAFIN storing’, Tweede Kamer, 20-03-2025, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2025Z06099&did=2025D14107.

32 ‘Kamerbrief update hack bij politie’, rijksoverheid.nl, 09-10-2024, https://www.rijksoverheid.nl/documenten/kamerstukken/2024/10/09/tk-update-over-hack-bij-de-politie.

33 ‘Onbekende Russische groep achter hacks Nederlandse doelen’, Ministerie van Defensie, 27-05-2025, https://www.defensie.nl/actueel/nieuws/2025/05/27/onbekende-russische-groep-achter-hacks-nederlandse-doelen.

34 ‘Fortinet bevestigt cyberaanval, mogelijk 440GB aan bedrijfsgegevens gestolen’, Tweakers, 13-09-2024, https://tweakers.net/nieuws/226550/fortinet-bevestigt-cyberaanval-mogelijk-440gb-aan-bedrijfsgegevens-gestolen.html.

35 Op basis van interne informatie afkomstig van het NCSC.

36 Op basis van interne informatie afkomstig van het NCSC.

37 ‘Storing bij gemeenten, afspraken vallen uit’, De Gelderlander, 10-10-204

38 ‘Investigating FortiManager Zero-Day Exploitation (CVE-2024-47575)’, Google Mandiant, 24-10-2024, https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575.

39 ‘Datalek bij gemeente Velsen’, Noordhollands Dagblad, 23-10-2024.

40 ‘E-mailadressen honderden gezinnen op straat door hack bij jeugdzorg-medewerker’, RTL, 09-10-2024, https://www.rtl.nl/nieuws/binnenland/artikel/5474670/e-mailadressen-gezinnen-jeugdzorg-eindhoven-brabant-hack.

41 ‘Clop ransomware is now extorting 66 Cleo data-theft victims’, Bleepingcomputer, 24-12-2024, https://www.bleepingcomputer.com/news/security/clop-ransomware-is-now-extorting-66-cleo-data-theft-victims/.

42 ‘Russische cybercriminelen konden data Centric stelen door soft-warelek’, FD, 24-01-2025, https://fd.nl/bedrijfsleven/1543474/russische-cybercriminelen-konden-data-centric-stelen-door-soft-warelek.

43 Amersfoort slachtoffer van aanval op testomgeving Centric, iBestuur, 27-01-2025, https://ibestuur.nl/artikel/amersfoort-slachtoffer-van-aanval-op-testomgeving-centric/.

44 ‘Ahold Delhaize getroffen door grote ransomware-aanval, claimt aan Rusland gelieerde hackersgroep’, BNR, 17-04-2025, https://www.bnr.nl/nieuws/tech-innovatie/10571730/ahold-delhaize-getroffen-door-grote-ransomware-aanval-claimt-hackersgroep.

45 ‘Ahold waarschuwt duizenden medewerkers na datadiefstal’, Tweakers, 23-04-2025, https://tweakers.net/nieuws/234224/ahold-waarschuwt-duizenden-medewerkers-na-datadiefstal.html.

46 ‘Cyberaanval Amerikaanse tak Ahold trof 2,2 miljoen mensen’, Tweakers, 28-06-2025, https://tweakers.net/nieuws/236716/cyberaanval-amerikaanse-tak-ahold-trof-2-komma-2-miljoen-mensen.html.

47 ‘Gegevens 100.000 inwoners Amersfoort gelekt na hack bij softwarele-verancier’, Tweakers 03-12-2024, https://tweakers.net/nieuws/229362/gegevens-100000-inwoners-amersfoort-gelekt-na-hack-bij-soft-wareleverancier.html.

48 ‘Gemeente Arnhem lekt gevoelige persoonsgegevens tientallen inwoners’, security.nl, 28-02-2025, https://www.security.nl/posting/878120/Gemeente+Arnhem+lekt+gevoelige+persoonsgegevens+tientallen+inwoners.

49 ‘Gemeenten Tubbergen en Dinkelland lekken gegevens inwoners’, security.nl, 02-12-2024, https://www.security.nl/posting/867600/Gemeenten+Tubbergen+en+Dinkelland+lekken+gegevens+inwoners.

50 ‘Rumoerige jaarwisseling met heftige incidenten’, politie.nl, 03-01-205, https://www.politie.nl/nieuws/2025/januari/1/00-jaarwisseling.html.

51 ‘Noodknop politie haperde tijdens Nieuwjaarsnacht: “Door oog van naald gekropen”’, nu.nl, 02-01-2025, https://www.nu.nl/tech/6340992/noodknop-politie-haperde-tijdens-nieuwjaarsnacht-door-oog-van-naald-gekropen.html.

52 ‘Update cyberaanval: dinsdag nog geen onderwijs’, tue.nl, 13-01-2025, https://www.tue.nl/nieuws-en-evenementen/nieuwsoverzicht/13-01-2025-update-cyberaanval-dinsdag-nog-geen-onderwijs.

53 ‘TU/e handelde goed bij cyberaanval, maar er zijn ook leerpunten’, TU/e, 19-05-2025, https://www.tue.nl/nieuws-en-evenementen/nieuwsoverzicht/19-05-2025-tue-handelde-goed-bij-cyberaanval-maar-er-zijn-ook-leerpunten.

54 ‘Storing DigiD werd veroorzaakt door grote ddos-aanval’, NOS.nl, 15-01-2025,https://nos.nl/artikel/2551874-storing-digid-werd-veroorzaakt-door-grote-ddos-aanval.

55 ‘SURF en onderwijsinstellingen opnieuw getroffen door ddos-aanval’, Tweakers, 16-01-2025, https://tweakers.net/nieuws/230886/surf-en-onderwijsinstellingen-opnieuw-getroffen-door-ddos-aanval.html.

56 ‘Opnieuw computerprobleem in ziekenhuis Rijnstate: ‘Maar zorg kan nu gewoon doorgaan’’, AD/Algemeen Dagblad, 16-01-2025, https://www.gelderlander.nl/arnhem/opnieuw-softwareprobleem-in-ziekenhuis-rijnstate-maar-zorg-kan-nu-gewoon-doorgaan~a32a715c/.

57 ‘Computerstoring bij ziekenhuis Arnhem verholpen’, nos.nl,14-01-2025, https://nos.nl/artikel/2551724-computerstoring-bij-ziekenhuis-arnhem-verholpen.

58 ‘Gegevens van 2.200 gebruikers buitgemaakt bij hack website raad Almere, dader onbekend’, Omroep Flevoland, 23-01-2025, https://www.omroepflevoland.nl/nieuws/412942/gegevens-van-2-200-gebruikers-buitgemaakt-bij-hack-website-raad-almere-dader-onbekend.

59 ‘UAC-0063: Cyber Espionage Operation Expanding from Central Asia’, Bitdefender, 12-02-2025, https://www.bitdefender.com/en-us/blog/businessinsights/uac-0063-cyber-espionage-operation-expanding-from-central-asia.

60 ‘Italië: WhatsApp-gebruikers met Nederlands nummer doelwit spyware-aanval’, security.nl, 06-02-2025, https://www.security.nl/posting/875185/Itali%C3%AB%3A+WhatsApp-gebruikers+met+Nederlands+nummer+doelwit+spyware-aanval.

61 ‘WhatsApp says it disrupted a hacking campaign targeting journalists with Paragon spyware, techcrunch.com, 31-01-2025, https://techcrunch.com/2025/01/31/whatsapp-says-it-disrupted-a-hacking-campaign-targeting-journalists-with-spyware/.

62 ‘Politienummer 0900-8844 tijdelijk niet bereikbaar door een storing’, nu.nl, 25-02-2025, https://www.nu.nl/tech/6347195/politienummer-0900-8844-tijdelijk-niet-bereikbaar-door-een-storing.html.

63 ‘DigiD heeft last van storing door “terugkerende ddos-aanvallen”’, Tweakers, 03-03-2025, https://tweakers.net/nieuws/232452/digid-heeft-last-van-storing-door-terugkerende-ddos-aanvallen.html.

64 ‘DigiD was door ddos-aanval korte tijd ‘beperkt beschikbaar’’, security.nl, 13-03-2025, https://www.security.nl/posting/879866/DigiD+was+door+ddos-aanval+korte+tijd+%27beperkt+beschikbaar%27.

65 ‘DigiD kampt met slimmere ddos-aanvallen: ‘Vaak werk van verveelde tieners’’, nu.nl, 27-03-2025, https://www.nu.nl/tech/6350621/digid-kampt-met-slimmere-ddos-aanvallen-vaak-werk-van-verveelde-tieners.html.

66 ‘ICT-storing OM verholpen’, om.nl, 02-04-2025, https://www.om.nl/actueel/nieuws/2025/04/02/ict-storing-om-verholpen.

67 ‘Crowdstrike Global Threat Report 2025’, crowdstrike.com, 27-02-2025, https://www.securityweek.com/wp-content/uploads/2025/02/CrowdStrikeGlobalThreatReport2025.pdf.

68 ‘DigiD is opnieuw “beperkt beschikbaar” door ddos-aanvallen’, Tweakers, 09-04-2025, https://tweakers.net/nieuws/233740/digid-is-opnieuw-beperkt-beschikbaar-door-ddos-aanvallen.html.

69 ‘Kamerbrief over datalek in gepubliceerde documenten Rijksoverheid’, rijksoverheid.nl, 18-04-2025, https://www.rijksoverheid.nl/documenten/kamerstukken/2025/04/18/kamerbrief-over-datalek-in-gepubliceerde-documenten-van-de-rijksoverheid.

70 ‘Betalingsbedrijf Adyen meerdere keren getroffen door cyberaanval’, RTL, 22-04-2025, https://www.rtl.nl/nieuws/artikel/5505378/betalingsbedrijf-adyen-meerdere-keren-getroffen-door-cyberaanval.

71 ‘Ruim vijftig websites Nederland deze week doelwit pro-Russische hackersgroep’, NOS, 03-05-2025, https://nos.nl/artikel/2565889-ruim-vijftig-websites-nederland-deze-week-doelwit-pro-russische-hackersgroep.

72 ‘MIVD: Nederland ook doelwit spionagecampagne Russische hackers’, Ministerie van Defensie, 21-05-2025, https://www.defensie.nl/actueel/nieuws/2025/05/21/mivd-nederland-ook-doelwit-spionagecampagne-russische-hackers.

73 ‘Tiental organisaties in Nederland op de korrel van Russische hackers-groep, meldt NCSC’, AG Connect, 23-06-2025, https://www.agconnect.nl/maatschappij/security/nederlandse-organisaties-aangevallen-door-russische-hackers.

74 ‘Websites van gemeenten en provincies slechter bereikbaar door mogelijke aanval’, Nu.nl, 23-06-2025, https://www.nu.nl/tech/6360048/websites-van-gemeenten-en-provincies-slechter-bereikbaar-door-mogelijke-aanval.html.

75 ‘International Criminal Court targeted by new “sophisticated” attack’, The Record, 01-07-2025, https://therecord.media/international-criminal-court-cyberattack-2025.

76 ‘OM van internet af vanwege ‘kwetsbaarheid’, misbruik niet uitgesloten’, NOS, 18-07-2025, https://nos.nl/artikel/2575495.

77 ‘Advocaten hebben last van hack OM en zijn kritisch: “Post is geen oplossing”’, NOS, 26-7-2025, https://nos.nl/artikel/2576449.

78 ‘Openbaar Ministerie gaat geleidelijk weer online’, NOS, 04-08-2025, https://nos.nl/artikel/2577569.

79 ‘Casus: Citrix kwetsbaarheid’, NCSC, 22-07-2025, https://www.ncsc.nl/actueel/nieuws/2025/07/22/casus-citrix-kwetsbaarheid.

80 ‘Onderzoek informatiebeveiliging’, DJI, 29-07-2025, https://www.dji.nl/actueel/nieuws/2025/07/29/onderzoek-informatiebeveiliging.

81 ‘Disrupting active exploitation of on-premises SharePoint vulnerabilities’, Microsoft, 22-07-2025, https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/#storm-2603.

82 ‘Casus: Microsoft SharePoint Server kwetsbaarheden’, NCSC, 23-07-2025, https://www.ncsc.nl/actueel/nieuws/2025/07/23/casus-microsoft-sharepoint.

83 ‘SharePoint-servers 145 organisaties wereldwijd getroffen bij aanvallen’, security.nl, 29-07-2025, https://www.security.nl/posting/898699/SharePoint-servers+145+organisaties+wereldwijd+getroffen+bij+aanvallen.

84 ‘Z-CERT over de ransomware-aanval bij Clinical Diagnostics NMDL (Eurofins)’, Z-CERT, 11-08-2025, https://z-cert.nl/actueel/nieuws/ransomware-aanval.

85 ‘Minister en Kamerlid in datalek laboratorium: adres, bsn en medisch onderzoek op straat’, RTL, 12-08-2025, https://www.rtl.nl/nieuws/binnenland/artikel/5522904/ministers-kamerleden-datalek-laboratorium-hack-woonadres-bsn.

86 ‘Hackersgroep Nova wil geen losgeld meer van gehackte Clinical Diagnostics’, BNR, 21-08-2025, https://www.bnr.nl/podcast/tech-update/10581247/hackersgroep-nova-wil-geen-losgeld-meer-van-gehackte-clinical-diagnostics.

87 ‘Gehackt laboratorium heeft losgeld betaald: ‘Miljoenen euro’s geëist’’, RTL, 13-08-2025, https://www.rtl.nl/nieuws/binnenland/artikel/5523036/hack-laboratorium-cybercriminelen-ransomware-losgeld-betaald-data.

88 ‘Werkzaamheden instanties Caribische eilanden verstoord door hacks’, NOS, 02-08-2025, https://nos.nl/artikel/2577274-werkzaamheden-instanties-caribische-eilanden-verstoord-door-hacks.

89 ‘Hack bij KLM; gegevens van klanten gestolen, AD, 06-08-2025, https://www.ad.nl/amsterdam/hack-bij-klm-gegevens-van-klanten-gestolen~aca46219/.

90 ‘Nederlandse providers doelwit van Salt Typhoon’, Defensie, 28-08-2025, https://www.defensie.nl/actueel/nieuws/2025/08/28/nederlandse-providers-doelwit-van-salt-typhoon.

91 ‘Frankrijk beschuldigt Rusland van cyberaanvallen bij verkiezingen en Spelen’, Nu.nl, 29-4-2025, https://www.nu.nl/buitenland/6354185/frankrijk-beschuldigt-rusland-van-cyberaanvallen-bij-verkiezingen-en-spelen.html.

92 ‘Cyprus’ critical infrastructure targeted by coordinated cyberattacks linked to pro-Palestine groups’, The Record, 21-10-2024, https://therecord.media/cyprus-critical-infrastructure-cyberattack-israel-palestine.

93 ‘Meet NailaoLocker: a ransomware distributed in Europe by ShadowPad and PlugX backdoors’, orangecyberdefense.com, 18-02-2025, https://www.orangecyberdefense.com/global/blog/cert-news/meet-nailaolocker-a-ransomware-distributed-in-europe-by-shadow-pad-and-plugx-backdoors

94 ‘Windows Remote Desktop Protocol: Remote to Rogue’, Google, 07-04-2025, https://cloud.google.com/blog/topics/threat-intelligence/windows-rogue-remote-desktop-protocol

95 ‘Ransomware attack hits German pharmaceutical wholesaler, disrupts medicine supplies’, The Record, 01-11-2024, https://therecord.media/ransomware-attack-hits-german-pharmaceutical-wholesaler-disruptions.

96 ‘Blue Yonder SaaS giant breached by Termite ransomware gang’, bleepingcomputer.com, 06-12-2024, https://www.bleepingcomputer.com/news/security/blue-yonder-saas-giant-breached-by-termite-ransomware-gang/.

97 ‘Softwareleverancier van Jumbo en HEMA is gehackt, “geen hinder voor klanten”’, Tweakers, 27-11-2024, https://tweakers.net/nieuws/229168/softwareleverancier-van-jumbo-en-hema-is-gehackt-geen-hinder-voor-klanten.html.

98 ‘U.S. Wiretap Systems Targeted in China-Linked Hack; AT&T and Verizon are among the broadband providers that were breached’, The Wall Street Journal, 05-10-2024, https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b.

99 ‘White House Says at Least 8 US Telecom Firms, Dozens of Nations Impacted by China Hacking Campaign’, securityweek.com, 05-12-2024, https://www.securityweek.com/white-house-says-at-least-8-us-telecom-firms-dozens-of-nations-impacted-by-china-hacking-campaign/.

100 ‘US agencies confirm Beijing-linked telecom breach involving call records of politicians, wiretaps’, The Record, 14-11-2024, https://therecord.media/us-agencies-confirm-china-telecom-hack-wiretaps.

101 ‘U.S. Wiretap Systems Targeted in China-Linked Hack’, The Wall Street Journal,05-10-2024, https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b?-mod=hp_lead_pos1.

102 ‘The cyber threat against the Danish water sector’, cfcs.dk, 04-02-2024, https://www.cfcs.dk/globalassets/cfcs/dokumenter/trussels-vurderinger/en/-the-cyber-threat-against-the-danish-water-sector-february-2025-.pdf.

103 ‘Datahandelaar lekt locatiegegevens van mogelijk miljoenen mensen’, security.nl, 13-01-2025, https://www.security.nl/posting/872156/Datahandelaar+lekt+locatiegegevens+van+mogelijk+miljoenen+mensen.

104 ‘Italiaans ziekenhuis via lek in firewall getroffen door ransomware-aanval’, security.nl, 24-01-2025, https://www.security.nl/posting/873753/Italiaans+ziekenhuis+via+lek+in+firewall+getroffen+door+ransomware-aanval.

105 ‘Cyber threat bulletin: People’s Republic of China cyber threat activity: PRC cyber actors target telecommunications companies as part of a global cyberespionage campaign’, Canadian Centre for Cyber Security, 19-06-2025, https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-prc-cyber-actors-target-telecommunications-companies-global-cyberespionage-campaign.

106 ‘FBI: Noord-Korea is verantwoordelijk voor hack cryptobeurs Bybit’, Tweakers, 27-02-2025, https://tweakers.net/nieuws/232310/fbi-noord-korea-is-verantwoordelijk-voor-hack-cryptobeurs-bybit.html.

107 ‘North Koreans finish initial laundering stage after more than $1 billion stolen from Bybit’, The Record, 04-03-2025, https://therecord.media/north-koreans-initial-laundering-bybit-hack

108 https://www.standaard.be/politiek/wallonie-getroffen-door-grootschalige-cyberinbraak/58953114.html.

109 https://research.checkpoint.com/2025/apt29-phishing-campaign/.

110 ‘Norway spy chief blames Russian hackers for dam sabotage in April’, Reuters, 13-08-2025, https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/.

111 ‘Britse supermarktketen Co-op meldt lege schappen door cyberaanval’, 12-05-2025, Security.nl, https://www.security.nl/posting/887521/Britse+supermarktketen+Co-op+meldt+lege+schappen+door+cyberaanval.

112 ‘Co-op boss confirms all 6.5m members had data stolen’, BBC, 16-07-2025, https://www.bbc.com/news/articles/cqlopleo66po.

113 ‘Scattered Spider Behind Cyberattacks on M&S and Co-op, Causing Up to $592M in Damages’, 21-06-2025, The Hacker News, https://thehackernews.com/2025/06/scattered-spider-behind-cyberattacks-on.html.

114 ‘CrowdStrike Services Observes SCATTERED SPIDER Escalate Attacks Across Industries’, CrowdStrike, 02-06-2025, https://www.crowdstrike.com/en-us/blog/crowdstrike-services-observes-scattered-spider-escalate-attacks/.

115 ‘Orange, France’s largest telecoms company, hit by cyberattack’, The Record, 29-07-2025,https://therecord.media/orange-telecom-france-cyberattack.

116 ‘Orange Telecom bevestigt publicatie van gestolen data op internet’, security.nl, 23-08-2025, https://www.security.nl/posting/901877/Orange+Telecom+bevestigt+publicatie+van+gestolen+data+op+internet.

117 ‘Luxembourg probes reported attack on Huawei tech that caused nationwide telecoms outage’, The Record, 01-08-2025, https://therecord.media/luxembourg-telecom-outage-reported-cyberattack-huawei-tech.

118 ‘Orange België meldt hack waarbij gegevens van 850.000 klanten zijn gestolen’, Tweakers, 20-08-2025, https://tweakers.net/nieuws/238256/orange-belgie-meldt-hack-waarbij-gegevens-van-850000-klanten-zijn-gestolen.html.

119 ‘Gegevens van 6,4 miljoen klanten van Bouygues Telecom gestolen bij datalek’, Tweakers, 07-08-2025, https://tweakers.net/nieuws/237874/gegevens-van-6-komma-4-miljoen-klanten-van-bouygues-telecom-gestolen-bij-datalek.html.

120 ‘Google: data potentiële Ads-klanten gestolen bij inbraak Salesforce-omgeving’, Security.nl, 11-08-2025, https://www.security.nl/posting/900106/Google%3A+data+potenti%C3%ABle+Ads-klanten+gestolen+bij+inbraak+Salesforce-omgeving.

121 ‘Cisco lekt persoonlijke gegevens van gebruikers op Cisco.com’, Security.nl, 05-08-2025, https://www.security.nl/posting/899574/Cisco+lekt+persoonlijke+gegevens+van+gebruikers+op+Cisco_com.

122 ‘Verzekeraar Allianz slachtoffer in golf Salesforce-hacks’, Techzine, 13-08-2025, https://www.techzine.nl/nieuws/security/568452/verzekeraar-allianz-slachtoffer-in-golf-salesforce-hacks/.

123 ‘Colt Telecom attack claimed by WarLock ransomware, data up for sale’, Bleepingcomputer, 15-08-2025, https://www.bleepingcomputer.com/news/security/colt-telecom-attack-claimed-by-warlock-ransomware-data-up-for-sale/.

124 ‘Widespread Data Theft Targets Salesforce Instances via Salesloft Drift’, Google, 26-08-2025, https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift.

125 ‘BREAKING: UNC6395 – The Biggest SaaS Breach of 2025’, Obsidian, 28-08-2025, https://www.obsidiansecurity.com/blog/unc6395-salesloft.

126 ‘Zscaler, Palo Alto Networks Breached via Salesloft Drift’, DarkReading, 02-09-2025, https://www.darkreading.com/cyberattacks-data-breaches/zscaler-palo-alto-networks-breached-salesloft-drift.

127 ‘Cloudflare bevestigt impact Salesloft Drift-datalek op klanten’, Techzine, 03-09-2025, https://www.techzine.nl/nieuws/security/569168/cloudflare-bevestigt-impact-salesloft-drift-datalek-op-klanten/.

128 ‘Statement on cyber incident’, Jaguar Land Rover, 02-09-2025, https://media.jaguarlandrover.com/news/2025/09/statement-cyber-incident.

129 ‘Statement on cyber incident’, Jaguar Land Rover, 10-09-2025, https://media.jaguarlandrover.com/news/2025/09/statement-cyber-incident-1.

130 ‘M&S hackers claim to be behind Jaguar Land Rover cyber attack’, BBC, 03-09-2025, https://www.bbc.com/news/articles/c4gqepe53550.

131 Jaarverslag 2024, AIVD, 24-04-2025, https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2024

132 Idem.

133 Dreigingsbeeld Statelijke Actoren (DBSA) 2025, AIVD, MIVD, NCTV, 17-07-2025, https://www.nctv.nl/documenten/2025/07/17/dreigingsbeeld-statelijke-actoren-2025.

134 ‘Veranderende wereldorde bevestigt belang van een weerbaar Nederland’, NCTV, 17-07-2025, https://www.nctv.nl/actueel/nieuws/2025/07/17/veranderende-wereldorde-bevestigen-belang-van-een-weerbaar-nederland.

135 Openbaar jaarverslag 2024, MIVD, 22-05-2025, https://www.defensie.nl/downloads/jaarverslagen/2025/04/22/openbaar-jaarverslag-2024-militaire-inlichtingen--en-veiligheidsdienst.

136 ‘“Onze aanvallen gaan door!”: Pro-Russische hackers willen wraak na internationale politieactie’, Pointer, 08-08-2025, https://pointer.kro-ncrv.nl/aanvallen-gaan-door-pro-russische-hackers-wraak-internationale-politieactie; ‘“I’ll be back”: pro-Russische hackersgroep is ondanks grote Europol-actie actiever dan ooit, ook in België’, VRT, 08-08-2025, https://www.vrt.be/vrtnws/nl/2025/08/06/check-pro-russische-hackers-noname-actief-europol/.

137 'AIVD en MIVD onderkennen nieuwe Russische cyberactor', AIVD & MIVD, 27-05-2025, https://www.aivd.nl/documenten/publicaties/2025/05/27/aivd-en-mivd-onderkennen-nieuwe-russische-cyberactor.

138 Idem.

139 Openbaar jaarverslag 2024, MIVD, 22-05-2025, https://www.defensie.nl/downloads/jaarverslagen/2025/04/22/openbaar-jaarverslag-2024-militaire-inlichtingen--en-veiligheidsdienst.

140 Dreigingsbeeld Statelijke Actoren (DBSA) 2025, AIVD, MIVD, NCTV, 17-07-2025, https://www.nctv.nl/documenten/2025/07/17/dreigingsbeeld-statelijke-actoren-2025.

141 Jaarverslag 2024, AIVD, 24-04-2025, https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2024.

142 Openbaar jaarverslag 2024, MIVD, 22-05-2025, https://www.defensie.nl/downloads/jaarverslagen/2025/04/22/openbaar-jaarverslag-2024-militaire-inlichtingen--en-veiligheidsdienst.

143 Idem.

144 Idem.

145 Jaarverslag 2024, AIVD, 24-04-2025, https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2024.

146 Idem.

147 Idem.

148 'The most notorious instances of commercial spyware', Kaspersky, 21-03-2024, https://www.kaspersky.com/blog/commercial-spyware/50813/; 'Buying Spying: How the commercial surveillance industry works and what can be done about it', Google Threat Analysis Group, 06-02-2024, https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/.

149 'Strengthening America's Resilience Against the PRC Cyber Threats', Cybersecurity and Infrastructure Security Agency (CISA), 15-01-2025, https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats.

150 'Cisco Confirms Salt Typhoon Exploited CVE-2018-0171 to Target U.S. Telecom Networks', The Hacker News, 21-02-2025, https://thehackernews.com/2025/02/cisco-confirms-salt-typhoon-exploited.html.

151 'China used three private companies to hack global telecoms, U.S. says', NBC News, 22-09-2025, https://www.nbcnews.com/tech/security/china-used-three-private-companies-hack-global-telecoms-us-says-rcna227543.

152 'At least 8 US telcos, dozens of countries impacted by Salt Typhoon breaches, White House says', The Record, 05-12-2024, https://therecord.media/eight-telcos-breached-salt-typhoon-nsc.

153 'Chinese Hackers Are Said to Have Targeten Phones Used by Trump and Vance', The New York Times, 25-10-2024, https://www.nytimes.com/2024/10/25/us/politics/trump-vance-hack.html.

154 'How Chinese Hackers Graduated From Clumsy Corporate Thieves to Military Weapons', The Wall Street Journal, 04-01-2025, https://www.wsj.com/tech/cybersecurity/typhoon-china-hackers-military-weapons-97d4ef95?msockid=30240.

155 'Panorama de la Cybermenace 2024', ANSSI, 11-03-2025, https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-003/.

156 'Top senator calls Salt Typhoon 'worst telecom hack in our nation's history', The Washington Post, 21-11-2024, https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/.

157 'Nederlandse providers doelwit van Salt Typhoon', Defensie.nl, 28-08-2025, https://www.defensie.nl/actueel/nieuws/2025/08/28/nederlandse-providers-doelwit-van-salt-typhoon.

158 'Kleine Nederlandse providers waren volgens AIVD doelwit van Chinese hackersgroep', Tweakers.net, 28-08-2025, https://tweakers.net/nieuws/238510/kleine-nederlandse-providers-waren-volgens-aivd-doelwit-van-chinese-hackersgroep.html.

159 'China used three private companies to hack global telecoms, U.S. says', NBC News, 22-09-2025, https://www.nbcnews.com/tech/security/china-used-three-private-companies-hack-global-telecoms-us-says-rcna227543.

160 'Top senator calls Salt Typhoon 'worst telecom hack in our nation's history', The Washington Post, 21-11-2024, https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/.

161 Idem.

162 'Telecom giant Viasat breached by China's Salt Typhoon hackers', BleepingComputer, 19-06-2025, https://www.bleepingcomputer.com/news/security/telecom-giant-viasat-breached-by-chinas-salt-typhoon-hackers/.

163 'Cyber threat bulletin: People's Republic of China cyber threat activity: PRC cyber actors target telecommunications companies as part of global espionage campaign, 19-06-2025, https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-prc-cyber-actors-target-telecommunications-companies-global-cyberespionage-campaign.

164 'China's Salt Typhoon Hackers Target Canadian Telecom Firms', SecurityWeek, 23-06-2025, https://www.securityweek.com/chinas-salt-typhoon-hackers-target-canadian-telecom-firms/.

165 'Cybertruslen mod telesektoren i Danmark/De cyberdreiging voor de telecommunicatiesector', Styrelsen for Samfundssikkerhedspressekontakt/SAMSIK, 13-03-2025, https://www.cfcs.dk/da/nyheder/2025/ny-trusselsvurdering---telesektoren/.

166 'Panorama de la cybermenace 2024', ANSSI, 11-03-2025, https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-003/.

167 Idem.

168 Idem.

169 Dreigingslandschap Vitale Infrastructuur (2025), 24-07-2025, NCTV, https://www.nctv.nl/documenten/publicaties/2025/07/23/dreigingslandschap-vitale-infrastructuur.

170 'De staat van de digitale infrastructuur', EZ, 22-01-2024, https://open.overheid.nl/documenten/9c5f2d91-fafc-405e-b330-96d6211677bc/file.

171 'Vooral jongeren en ouderen pinnen vaker aan de kassa', De Nederlandsche Bank, '01-04-2025', https://www.dnb.nl/algemeen-nieuws/nieuws-2025/vooral-jongeren-en-ouderen-pinnen-vaker-aan-de-kassa/.

172 'Cybertruslen mod telesektoren i Danmark/De cyberdreiging voor de telecommunicatiesector', Styrelsen for Samfundssikkerhedspressekontakt/SAMSIK, 13-03-2025, https://www.cfcs.dk/da/nyheder/2025/ny-trusselsvurdering---telesektoren/.

173 Jaarverslag 2024, AIVD, 24-04-2025, https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2024.

174 Idem.

175 https://zoek.officielebekendmakingen.nl/kst-30821-92.html.

176 'Cybertruslen mod telesektoren i Danmark/De cyberdreiging voor de telecommunicatiesector', Styrelsen for Samfundssikkerhedspressekontakt/SAMSIK.

177 'Russian hackers infiltrated Ukrainian telecom giant months before cyberattack', The Record, 04-01-2025, https://therecord.media/russians-infiltrated-kyivstar-months-before.

178 'Cybersecuritybeeld Nederland 2024', NCTV, 28-10-2024, https://www.nctv.nl/documenten/publicaties/2024/10/28/cybersecuritybeeld-nederland-2024.

179 'Toenemende en veranderende dreigingen op infrastructuur', 24-07-2025, NCTV, https://www.nctv.nl/actueel/nieuws/2025/07/24/toenemende-en-veranderende-dreigingen-op-vitale-infrastructuur.

180 https://www.nctv.nl/onderwerpen/cyberbeveiligingswet.

181 Interview met de RDI, 2025.

182 'Aftapvoorziening Vodafone niet voldoende beveiligd: boete van €2,25 miljoen voor Vodafone, RDI, 22-10-2024, https://www.rdi.nl/actueel/nieuws/2024/10/22/aftapvoorziening-vodafone-niet-voldoende-beveiligd.

183 Idem.

184 'Tekortkomingen in beveiliging van aftapvoorziening', RDI, 30-08-2022, https://www.rdi.nl/actueel/nieuws/2022/08/30/tekortkomingen-in-beveiliging-van-aftapvoorziening-kpn.

185 https://www.defensie.nl/actueel/nieuws/2025/08/28/nederlandse-providers-doelwit-van-salt-typhoon, Ministerie van Defensie, 28-08-2025.

186 'Voortgang kabinetsaanpak risicovolle strategische afhankelijkheden', Ministerie van Economische Zaken, 21-10-2024, https://open.overheid.nl/documenten/18329adb-dac7-45ab-bba4-0c777758528f/file.

187 Aanbieden Agenda Digitale Open Strategische Autonomie, Ministerie van Economische Zaken en Klimaat, 17-10-2023, https://www.rijksoverheid.nl/documenten/kamerstukken/2023/10/17/kamerbrief-aanbieden-agenda-digitale-open-strategische-autonomie-coco-5-oktober.

188 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Long-term competitiveness of the EU: looking beyond 2030, Europese Commissie, 16-03-2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1668.

189 'Agenda digitale open strategische autonomie', Ministerie van Economische Zaken en Klimaat, 17-10-2023, https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa.

190 Idem.

191 Korte toespraak van minister-president Dick Schoof bij de opening van de One Conference, Den Haag, 30-09-2025, https://www.rijksoverheid.nl/documenten/toespraken/2025/09/30/toespraak-minister-president-schoof-bij-opening-one-conference-den-haag.

192 'Samenleving kwetsbaar: digitale afhankelijkheid is meer dan cloud bij de overheid', Rathenau Instituut, 09-07-2025,https://www.rathenau.nl/nl/digitalisering/naar-een-nieuwe-verhouding-tot-technologiebedrijven/samenleving-kwetsbaar-digitale-afhankelijkheid-meer-dan-cloud-bij-de-overheid?utm_source=Laposta&utm_campaign=Nieuwsbrief%20juli&utm_medium=email; 'Minister: volledige afhankelijkheid niet-Europese techbedrijven onwenselijk', Security.nl, 07-07-2025, https://www.security.nl/posting/895166/Minister%3A+volledige+afhankelijkheid+niet-Europese+techbedrijven+onwenselijk; 'Overheid leunt veel meer op Amerikaanse cloud dan bekend: "Meelezen is makkelijk"', NOS, 31-05-2025, https://nos.nl/artikel/2569392; 'Amerikaanse bedrijven domineren Europese markt voor cybersecurity', Security.nl, 30-04-2025, https://www.security.nl/posting/886170/Amerikaanse+bedrijven+domineren+Europese+markt+voor+cybersecurity; 'Bedrijven onderzoeken ontsnapping uit de Amerikaanse cloud', Financieel Dagblad, 21-04-2025, https://fd.nl/bedrijfsleven/1552548/bedrijven-onderzoeken-ontsnapping-uit-amerikaanse-cloud; 'Europese techbedrijven willen "radicale actie" tegen afhankelijkheid van Amerikaanse Big Tech', NRC, 18-03-2025, https://www.nrc.nl/nieuws/2025/03/18/europese-techbedrijven-willen-radicale-actie-tegen-afhankelijkheid-van-amerikaanse-big-tech-a4886724.

193 'Beheer van CVE-bugs komt in gevaar door verlopen contract met Mitre Corporation', Tweakers, 16-04-2025, https://tweakers.net/nieuws/233988/beheer-van-cve-bugs-komt-in-gevaar-door-verlopen-contract-met-mitre-corporation.html.

194 'Amerikaanse cybersecurityagentschap redt CVE-programma met financiering', Tweakers, 16-04-2024, https://tweakers.net/nieuws/234022/amerikaans-cybersecurityagentschap-redt-cve-programma-met-financiering.html.

195 'Nederland en de EU: Zet in op cloudsoevereiniteit', Clingendael, 16-4-2024, https://www.clingendael.org/publication/nederland-en-de-eu-zet-op-cloudsoevereiniteit#:~:text=Amerikaanse%20bedrijven%2070%2D80%20procent%20van%20de%20Europese%20markt%20voor%20clouddiensten.

196 'Samenleving kwetsbaar: digitale afhankelijkheid is meer dan cloud bij de overheid', Rathenau Instituut, 09-07-2025, https://www.rathenau.nl/nl/digitalisering/naar-een-nieuwe-verhouding-tot-technologiebedrijven/samenleving-kwetsbaar-digitale-afhankelijkheid-meer-dan-cloud-bij-de-overheid?utm_source=Laposta&utm_campaign=Nieuwsbrief%20juli&utm_medium=email.

197 'De werking van de CLOUD-Act bij dataopslag in Europa', NCSC, 16-08-2022, https://www.ncsc.nl/actueel/weblog/weblog/2022/de-werking-van-de-cloud-act-bij-dataopslag-in-europa.

198 'Microsoft admits it 'cannot guarantee' data sovereignty', the Register, 25-07-2025,https://www.theregister.com/2025/07/25/microsoft_admits_it_cannot_guarantee/.

199 https://www.submarinecablemap.com/, https://www.rijksoverheid.nl/documenten/beleidsnotas/2024/09/23/kamerbrief-voortgangsupdate-onderzeese-datakabels-kamerbrief-voortgangsupdate-onderzeese-datakabels.

200 https://www.digitaleoverheid.nl/kabinetsbeleid-digitalisering/werkagenda/versterken-digitale-samenleving-op-caribisch-deel-koninkrijk/.

201 https://www.rijksoverheid.nl/documenten/kamerstukken/2025/06/19/kamerbrief-over-voortgang-digitalisering-van-de-zorg-in-caribisch-nederland-2025.

202 https://www.eerstekamer.nl/wetsvoorstel/36639_wet_invoering_bsn_en.

203 https://belastingdienst.cw/beperkte-dienstverlening-belastingdienst-na-ransomware-aanval/.

204 https://nos.nl/artikel/2577274-werkzaamheden-instanties-caribische-eilanden-verstoord-door-hacks, https://therecord.media/aruba-curacao-governments-cyberattacks.

205 'Van kwetsbaar naar weerbaar', Algemene Bestuursdienst, 12-09-2025, https://www.rijksoverheid.nl/documenten/rapporten/2025/09/12/rapport-van-kwetsbaar-naar-weerbaar.

206 Cybersecuritybeeld Nederland 2024, NCTV, https://www.nctv.nl/documenten/2024/10/28/cybersecuritybeeld-nederland-2024.

207 'Van kwetsbaar naar weerbaar', Algemene Bestuursdienst, 12-09-2025, https://www.rijksoverheid.nl/documenten/rapporten/2025/09/12/rapport-van-kwetsbaar-naar-weerbaar.

208 'AI versterkt bestaande dreigingen voor nationale veiligheid', NCTV, 10-12-2024, https://www.nctv.nl/actueel/nieuws/2024/12/09/ai-versterkt-bestaande-dreigingen-voor-nationale-veiligheid.

209 Cybersecuritybeeld Nederland 2023, NCTV, 03-07-2023, https://www.nctv.nl/documenten/publicaties/2023/07/03/cybersecuritybeeld-nederland-2023.

210 'OPWNAI: Cybercriminals starting to use ChatGPT', Check Point Research, 06-01-2023, https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/. 'Versterkte dreigingen in een wereld vol kunstmatige intelligentie', AIVD, MIVD, NCTV, 10-12-2024, https://www.nctv.nl/documenten/publicaties/2024/12/09/versterkte-dreigingen-in-een-wereld-vol-kunstmatige-intelligentie.

211 'Versterkte dreigingen in een wereld vol kunstmatige intelligentie', AIVD, MIVD, NCTV, 10-12-2024, https://www.nctv.nl/documenten/publicaties/2024/12/09/versterkte-dreigingen-in-een-wereld-vol-kunstmatige-intelligentie.

212 'Beyond the Safeguards: Exploring the Security Risks of ChatGPT', Erik Derner & Kristina Batistic, 13-05-2023, https://arxiv.org/abs/2305.08005.

213 'Beyond the Safeguards: Exploring the Security Risks of ChatGPT', Erik Derner & Kristina Batistic, 13-05-2023, https://arxiv.org/abs/2305.08005, 'ChatGPT and large language models: what's the risk?', National Cyber Security Centre, 10-03-2023, https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk.

214 'Phishing and Social Engineering in the Age of LLMs', S. Gallagher et al., in 'Large Language Models in Cybersecurity', A. Kucharavy, O. Plancherel, V. Mulder, A. Mermoud, en V. Lenders (eds.)., Springer, 2024, https://library.oapen.org/bitstream/handle/20.500.12657/90897/978-3-031-54827-7.pdf#page=94.

215 Cybersecuritybeeld Nederland 2023, NCTV, 03-07-2025, https://www.nctv.nl/documenten/publicaties/2023/07/03/cybersecuritybeeld-nederland-2023.

216 'ChatGPT and large language models: what's the risk?', National Cyber Security Centre, 10-03-2023, https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk.

217 Idem.

218 'Versterkte dreigingen in een wereld vol kunstmatige intelligentie', AIVD, MIVD, NCTV, 10-12-2024, https://www.nctv.nl/documenten/publicaties/2024/12/09/versterkte-dreigingen-in-een-wereld-vol-kunstmatige-intelligentie.

219 'Human-competitive AI will disrupt the cyber security industry; prepare now!', Partnership for Cyber Security Innovation, 19-09-2023, https://pcsi.nl/nl/nieuws/vision-paper-human-competitive-ai-will-disrupt-the-cyber-security-industry-prepare-now/.

220 Idem.

221 'Generatieve AI: een transformatieve impact op cybersecurity', AIVD en RDI, 17-10-2024, https://www.aivd.nl/documenten/publicaties/2024/10/17/generatieve-ai.-een-transformatieve-impact-op-cybersecurity.

222 'Versterkte dreigingen in een wereld vol kunstmatige intelligentie', AIVD, MIVD, NCTV, 10-12-2024, https://www.nctv.nl/documenten/publicaties/2024/12/09/versterkte-dreigingen-in-een-wereld-vol-kunstmatige-intelligentie.

223 'Growing Number of Threats Leveraging AI', Symantec, 25-07-2024, https://www.security.com/threat-intelligence/malware-ai-llm.

224 'Cybercriminal abuse of large language models', Cisco Talos, 25-05-2025, https://blog.talosintelligence.com/cybercriminal-abuse-of-large-language-models/.

225 'Adversarial Misuse of Generative AI', Google Threat Intelligence, 29-01-2025, https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai.

226 Jaarbeeld Ransomware 2024, Project Melissa, 17-02-2025, https://www.ncsc.nl/documenten/publicaties/2025/02/17/jaarbeeld-ransomeware-2024.

227 Idem.

228 Toelichting medewerker project Melissa tijdens interview.

229 'Datalekkenrapportage 2024: datadiefstal bijna verdubbeld', Autoriteit Persoonsgegevens, 03-07-2025, https://www.autoriteitpersoonsgegevens.nl/documenten/rapportage-datalekken-2024.

Colofon

Het Cybersecuritybeeld Nederland 2025 (CSBN 2025) biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de digitale weerbaarheid en tot slot de digitale risico's. Daarnaast vormt het CSBN 2025 een inhoudelijke basis voor de evaluatie van het actieplan voor de Nederlandse Cybersecurity Strategie 2022-2028. De focus van het CSBN ligt op de nationale veiligheid.

Het CSBN is opgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De NCTV heeft dankbaar gebruikgemaakt van de informatie, de inzichten en de expertise van overheidsdiensten, aanbieders van vitale processen, wetenschappers en andere partijen. Ook de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD) dragen substantieel bij aan het CSBN. Het CSBN wordt jaarlijks door de NCTV vastgesteld.

De NCTV draagt samen met partners uit het veiligheidsdomein bij aan een veilig en stabiel Nederland door dreigingen te onderkennen en de weerbaarheid en bescherming van nationale veiligheidsbelangen te versterken. Doel is het voorkomen en beperken van maatschappelijke ontwrichting. Als coördinator zorgt de NCTV voor de strategische verbinding tussen alle betrokken partners in het veiligheidsdomein, voor het reduceren van nationale veiligheidsrisico's en - als het erop aan komt - het beheersen van nationale crises.

Het NCSC draagt bij aan het digitaal weerbaar maken van Nederland en daarmee aan het creëren van een gunstig digitaal klimaat voor organisaties en de samenleving. Dat doet het NCSC door in samenwerking met publieke en private partners in binnen- en buitenland de digitale weerbaarheid van organisaties te bevorderen. Ook helpt het NCSC cyberincidenten en -crises met een ontwrichtend karakter te voorkomen en de impact ervan te beperken.

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 2025