Week 48-2025

Strategische Analyse: De Convergentie van Geopolitiek en Cyberdreigingen in 2025

1.0 Inleiding: Het Digitale Domein als Geopolitiek Conflictgebied

Dit document presenteert een strategische analyse van de belangrijkste cyberdreigingen en geopolitieke ontwikkelingen die in november 2025 zijn geobserveerd. Het cyberdomein is geëvolueerd van een technisch speelveld naar een primair strijdtoneel voor geopolitieke conflicten en geavanceerde criminaliteit. De analyse van de recente gebeurtenissen toont onmiskenbaar aan hoe statelijke acties, technologische kwetsbaarheden en maatschappelijke ontwrichting onlosmakelijk met elkaar verbonden zijn. Deze convergentie vereist een adaptieve en proactieve veiligheidsstrategie van beleidsmakers, die verder moet gaan dan een reactieve, technische benadering.

Het rapport is gestructureerd rondom de centrale thema's die het huidige dreigingslandschap definiëren. We analyseren de dominante rol van statelijke actoren en hun geopolitieke motivaties. Vervolgens wordt de structurele kwetsbaarheid van onze digitale ruggengraat onderzocht, met een focus op risico's in de toeleveringsketen en kerninfrastructuren. Daarna belichten we de dubbele rol van kunstmatige intelligentie, die zowel als krachtig wapen wordt ingezet door criminelen als nieuwe kwetsbaarheden creëert in onze systemen. We staan stil bij de steeds vaker voorkomende fysieke manifestaties van cybercriminaliteit, die de grens tussen de digitale en fysieke wereld doen vervagen. Tot slot destilleren we uit deze analyse een reeks strategische imperatieven voor beleidsmakers.

Deze analyse onderstreept de urgentie van een geïntegreerd beleid dat de complexiteit van het moderne dreigingslandschap erkent, te beginnen bij de meest invloedrijke actoren: de natiestaten.

2.0 Het Geopolitieke Slagveld: Staten als Dominante Cyberactoren

De strategische dominantie van statelijke actoren in het huidige dreigingslandschap is onmiskenbaar. Nationale belangen en geopolitieke conflicten zijn de drijvende kracht achter de meest geavanceerde, persistente en ontwrichtende cyberoperaties. Deze operaties zijn niet langer uitsluitend gericht op traditionele spionage, maar worden steeds vaker ingezet voor economische sabotage, het genereren van illegale

inkomsten en het actief ondermijnen van democratische processen in andere landen. De gebeurtenissen van november 2025 illustreren een wereldwijd speelveld waarin staten hun digitale capaciteiten inzetten als een primair instrument van machtspolitiek.

2.1 De As van Destabilisatie: Rusland, Noord-Korea en Iran

Een alliantie van landen met een revisionistische agenda zet cyberoperaties in om westerse invloed te ondermijnen en eigen strategische doelen te realiseren. De synergie tussen deze actoren en hun specifieke tactieken vormen een aanzienlijke bedreiging voor de internationale stabiliteit.

- **Russische Hybride Oorlogsvoering:** Rusland blijft hybride tactieken inzetten om politieke instabiliteit te creëren. Een sprekend voorbeeld is de investering van circa **€400 miljoen** in een campagne om de parlementsverkiezingen in Moldavië te beïnvloeden door middel van cyberaanvallen en desinformatie. Tegelijkertijd voeren aan de staat gelieerde groepen als RomCom en de militaire eenheid 29155 gerichte aanvallen uit op organisaties met zelfs indirecte banden met Oekraïne, wat de brede reikwijdte van de Russische cyberagressie aantoont.
- **Noord-Koreaanse Economische Oorlogsvoering:** Noord-Korea zet zijn cybercapaciteiten primair in om internationale sancties te omzeilen en het eigen wapenprogramma te financieren. Rapporten tonen aan dat het regime circa **$2,8 miljard** aan cryptovaluta heeft gestolen. De recente hack op de Zuid-Koreaanse cryptobeurs Upbit, toegeschreven aan de Lazarus-groep, is hiervan een illustratie. Daarnaast richt het land zich met geraffineerde social engineering-campagnes specifiek op AI-ontwikkelaars om technologische kennis en toegang tot systemen te verkrijgen.
- **Iraanse Regionale Spionage:** Gelekte documenten van de Iraanse groep APT35 (ook bekend als Charming Kitten), onderdeel van de Revolutionaire Garde, onthullen een militaire en sterk gestructureerde aanpak. De operaties zijn gericht op het infiltreren van de telecom- en energiesector in het Midden-Oosten, waarbij systematisch misbruik wordt gemaakt van kwetsbaarheden in Microsoft Exchange-servers om strategische inlichtingen te verzamelen.
- **Operationele Samenwerking:** Een zorgwekkende ontwikkeling is de strategische operationele samenwerking tussen de Russische Gamaredon-

groep en de Noord-Koreaanse Lazarus-groep. Het delen van tactieken en middelen tussen deze notoire actoren vergroot de effectiviteit en reikwijdte van hun operaties aanzienlijk, wat een verhoogde dreiging vormt voor Europese doelwitten.

2.2 China's Dubbele Strategie: Economische Spionage en Infiltratie

China hanteert een tweeledige strategie die digitale spionage combineert met langetermijninfiltratie via menselijke bronnen om zijn technologische en economische machtspositie te versterken.

- **Digitale Spionage:** Operaties van de aan China gelieerde groep APT31 illustreren de complexiteit van geopolitieke allianties in cyberspace. Deze groep voerde spionagecampagnes uit tegen de Russische IT-sector, ironisch genoeg door gebruik te maken van Russische clouddiensten zoals Yandex om detectie te omzeilen. Dit toont aan dat zelfs politieke bondgenoten niet immuun zijn voor elkaars digitale spionage.
- **Menselijke Infiltratie:** China verlegt zijn strategische focus in Europa steeds meer naar het cultiveren van menselijke bronnen. Door middel van langdurige infiltratie in academische en zakelijke netwerken worden subtiele relaties opgebouwd om toegang te krijgen tot strategische kennis en technologie, een methode die minder zichtbaar is dan directe cyberaanvallen maar minstens zo effectief.

2.3 Cybercapaciteiten als Asymmetrisch Wapen: Het Voorbeeld van Oekraïne

Oekraïne demonstreert hoe een land met beperktere conventionele middelen zijn cybercapaciteiten effectief kan inzetten als een asymmetrisch en strategisch instrument. Door operaties uit te voeren in de 'grijze zone' slaagt het land erin om Chinese proxynetwerken en logistieke ketens wereldwijd te verstoren die de Russische oorlogsinspanningen ondersteunen. Deze acties, die directe militaire escalatie vermijden, bieden waardevolle inzichten voor westerse landen over de inzet van cyberoperaties in hybride conflicten en de mogelijkheid om invloedssferen van grootmachten te ondermijnen.

De geavanceerde methoden van deze statelijke actoren zijn direct afhankelijk van de kwetsbaarheden in de digitale infrastructuren die zij aanvallen, wat ons leidt naar de fragiliteit van onze eigen digitale ruggengraat.

3.0 De Kwetsbaarheid van de Digitale Ruggengraat: Keten- en Infrastructuurrisico's

De strategische kwetsbaarheid van onze moderne, onderling verbonden digitale ecosystemen kan niet worden onderschat. De diepe afhankelijkheid van externe leveranciers, gedeelde dienstverleners en open-source softwarecomponenten creëert een complex web van risico's. De zwakste schakel in deze digitale toeleveringsketen vormt een toegangspoort die door zowel statelijke actoren als cybercriminelen wordt geëxploiteerd om op grote schaal toegang te verkrijgen tot vitale systemen en gevoelige data.

3.1 Supply Chain-aanvallen: Het Domino-effect van Gecompromitteerde Leveranciers

Aanvallen via de toeleveringsketen bewijzen keer op keer dat de beveiliging van een organisatie slechts zo sterk is als die van haar minst beveiligde partner. Recente incidenten illustreren dit domino-effect.

Incident	Strategische Implicatie
Datalek bij **Iberia** via een externe leverancier.	Toont aan dat zelfs zonder compromittering van financiële data, het lekken van persoons- en loyaliteitsgegevens de reputatie en het klantvertrouwen ernstig kan schaden.
Verstoringen bij **Londense gemeenten** door aanval op gedeelde dienstverlener.	Illustreert hoe een aanval op één leverancier de publieke dienstverlening van meerdere overheidsinstanties tegelijk kan platleggen, wat de maatschappelijke impact verveelvoudigt.
Datalek bij telecomgigant **Comcast** via een voormalige partner.	Benadrukt het "long tail" risico: zelfs nadat een partnerschap is beëindigd, kunnen achtergebleven data of verbindingen nog steeds een ingang voor aanvallers vormen.
Qilin-ransomwareaanval op de Zuid-Koreaanse financiële sector via MSP.	Laat zien hoe een gecompromitteerde Managed Service Provider (MSP) als springplank kan dienen

	voor een gecoördineerde, sectorbrede aanval met verwoestende gevolgen.
Datalekken bij **Trezor** en **SitusAMC** via derde partijen.	Onderstreept dat de hele keten, van e-mailmarketingproviders (Mailchimp) tot cruciale partners van grootbanken, een potentieel doelwit is dat de data van eindklanten in gevaar brengt.

3.2 Corruptie in de Code: De Softwaretoeleveringsketen als Aanvalsvector

Aanvallers richten zich steeds vaker op de bouwstenen van software zelf, waardoor kwaadaardige code diep in systemen kan worden verankerd nog voordat deze in gebruik worden genomen.

1. **Manipulatie van Open-Source Repositories:** De infectie van honderden pakketten in de npm-registry, zoals bij de **TruffleHog** en **Shai Hulud** campagnes, demonstreert de schaalbaarheid van deze aanvallen. Noord-Koreaanse actoren verspreidden de **OtterCookie-malware** via npm en GitHub, waarmee ze specifiek ontwikkelaars in de crypto-industrie aanvielen.
2. **Misbruik van Ontwikkelplatformen:** De aanval via een valse **'prettier-vscode-plus'** extensie op de populaire Visual Studio Code Marketplace toont hoe aanvallers het vertrouwen in legitieme ontwikkelaarstools misbruiken om malware zoals de **Anivia Stealer** te verspreiden onder een technisch vaardige doelgroep.
3. **Risico's van Verouderde Code:** Het structurele risico van verwaarloosde softwarecomponenten wordt geïllustreerd door legacy Python-pakketten die verwijzen naar het verlopen en te koop staande domein python-distribute[.]org. Dit opent een directe route voor systeeminfiltratie zodra een kwaadwillende dit domein registreert.

3.3 Fundamentele Systeembreuken: Kwetsbaarheden in Kerninfrastructuur

Naast de toeleveringsketen blijven ook fundamentele kwetsbaarheden in hardware, software en protocollen een significant risico vormen voor de stabiliteit van onze digitale infrastructuur.

- **Edge Devices als Toegangspoort:** Het Cybersecuritybeeld Nederland 2025 bevestigt dat *edge devices* zoals firewalls en VPN-servers populaire

doelwitten zijn. Met name Chinese statelijke actoren exploiteren deze toegangspunten om diep in bedrijfs- en overheidsnetwerken door te dringen.

- **Protocollen en Hardware:** Het aanhoudende misbruik van het verouderde en onveilige NTLM-authenticatieprotocol in bedrijfsnetwerken blijft een ernstig risico. Dit wordt verergerd door kritieke kwetsbaarheden in wijdverbreide consumentenhardware, zoals de recente lekken in Asus-routers.
- **Opkomende Risicodomeinen:** De snelle opkomst van nieuwe technologische domeinen, zoals de ontwikkeling van datacenters in de ruimte, introduceert volledig nieuwe en vooralsnog onderbelichte veiligheidsvraagstukken met betrekking tot databeveiliging en de fysieke integriteit van infrastructuren buiten de aardse jurisdictie.

Deze veelzijdige en diepgewortelde kwetsbaarheden worden verder versneld en geëxploiteerd door de opkomst van kunstmatige intelligentie, een technologie die zowel nieuwe aanvalsmethoden creëert als zelf een doelwit wordt.

4.0 Kunstmatige Intelligentie: De Dubbelrol als Wapen en Kwetsbaarheid

De transformerende impact van kunstmatige intelligentie (AI) op het cyberdreigingslandschap is tweeledig en complex. Enerzijds vergroot AI de efficiëntie, schaal en toegankelijkheid van geavanceerde cyberaanvallen, waardoor de drempel voor cybercriminaliteit drastisch wordt verlaagd. Anderzijds introduceert de implementatie van AI in onze systemen nieuwe, complexe kwetsbaarheden die nog niet volledig worden begrepen. Deze dubbele rol stelt beleidsmakers voor een unieke uitdaging: het mitigeren van AI-gedreven dreigingen en tegelijkertijd het beveiligen van de AI-systemen waar we steeds afhankelijker van worden.

4.1 AI als Aanvalsinstrument: De Democratisering van Geavanceerde Cybercrime

AI-technologie functioneert als een *force multiplier* voor kwaadwillenden, waardoor geavanceerde aanvalstechnieken beschikbaar komen voor een veel breder publiek.

- **Generatieve AI voor Social Engineering:** Rondom Black Friday werd generatieve AI op grote schaal ingezet om uiterst overtuigende nepwebsites en phishingadvertenties te creëren. Deze AI-gegenereerde content is vaak nauwelijks van echt te onderscheiden, waardoor consumenten effectiever worden misleid.

- **Kwaadaardige Taalmodellen (LLMs):** De opkomst van gespecialiseerde, vrij verkrijgbare tools zoals **WormGPT 4** en **KawaiiGPT** is bijzonder zorgwekkend. Deze modellen zijn specifiek ontworpen om onervaren hackers te assisteren bij het genereren van functionerende ransomware, geavanceerde phishingmails en scripts voor laterale bewegingen binnen een netwerk.
- **Potentieel voor Autonome Malware:** Criminelen experimenteren actief met legitieme modellen zoals GPT-4 om malware te schrijven die zichzelf dynamisch kan aanpassen. Het doel is om malware te creëren die zijn eigen code herschrijft om detectie door antivirusscanners te omzeilen, wat een nieuwe generatie van ongrijpbare dreigingen inluidt.
- **Desinformatie op Schaal:** De ontwikkeling van volledig AI-gegenereerde films, zoals gedemonstreerd door Luma AI, is een voorbode van de volgende stap in desinformatie. Het potentieel om op grote schaal hyperrealistische deepfakes te produceren, vormt een ernstige bedreiging voor de publieke opinie en democratische processen.

4.2 AI als Kwetsbaarheid: Nieuwe Risico's in Algoritmische Systemen

De integratie van AI in software en diensten creëert tegelijkertijd nieuwe en unieke aanvalsvectoren die specifiek gericht zijn op de logica en data-afhankelijkheid van deze systemen.

- **Gemanipuleerde Code-generatie:** Onderzoek naar het Chinese AI-model **DeepSeek-R1** toonde aan dat de kwaliteit en veiligheid van de gegenereerde code significant afneemt wanneer het model wordt gevoed met politiek gevoelige termen. Het model produceerde bewust onveilige code, wat wijst op ingebouwde censuurmechanismen die onbedoelde, maar ernstige veiligheidsrisico's kunnen introduceren.
- **Injectie-aanvallen op AI-agenten:** Microsofts nieuwe *agentic AI-functie* illustreert een fundamenteel nieuw risico: **'cross-prompt injectie'**. Hierbij kunnen aanvallers via gemanipuleerde documenten of data-invoer de AI-agenten onbedoeld schadelijke opdrachten laten uitvoeren, zoals het stelen van data of het installeren van malware, volledig buiten het zicht van de gebruiker.

De toenemende verwevenheid van AI met onze digitale levens overstijgt de technologische abstractie en leidt tot steeds meer concrete, fysieke gevolgen voor de veiligheid van burgers en de samenleving.

5.0 De Vervaging van Grenzen: De Fysieke Impact van Cybercriminaliteit

De strategische betekenis van de convergentie tussen de digitale en fysieke wereld kan niet langer worden genegeerd. Cyberdreigingen zijn niet meer beperkt tot datadiefstal of financiële fraude op afstand; ze manifesteren zich steeds vaker in direct fysiek geweld, maatschappelijke ontwrichting en de facilitering van traditionele zware criminaliteit. Deze vervaging van grenzen vereist een geïntegreerde aanpak van veiligheidsdiensten, waarbij digitale en fysieke opsporing hand in hand gaan en de veiligheid van burgers centraal staat.

5.1 Van Digitale Diefstal naar Fysiek Gevaar

De overgang van de digitale naar de fysieke wereld is voor criminelen een logische stap om de opbrengst van hun activiteiten te maximaliseren, met directe en gewelddadige gevolgen voor slachtoffers.

- **Geweld tegen Cryptobezitters:** In Nederland gebruiken criminelen digitale middelen, zoals valse belastingformulieren, om de fysieke adressen en vermogensgegevens van cryptobezitters te achterhalen. Deze informatie wordt vervolgens gebruikt om gerichte en gewelddadige overvallen en zelfs ontvoeringen uit te voeren.
- **Helpdeskfraude met Fysieke Component:** De modus operandi van bankhelpdeskfraude is geëvolueerd. Na een manipulatief telefoongesprek komt een nepagent of -bankmedewerker fysiek aan de deur om bankpassen, sieraden en andere waardevolle spullen op te halen. Casussen in Hilversum, Etten-Leur en Rotterdam tonen aan dat dit een landelijk en succesvol fenomeen is, vaak gericht op ouderen.
- **Digitale Stalking en Intimidatie:** De zaak van 'proxystalking' in Stabroek illustreert hoe digitale middelen worden ingezet voor ernstige psychologische en fysieke intimidatie. Door anoniem diensten zoals begrafenisondernemers naar het huis van een slachtoffer te sturen, creëren daders een sfeer van terreur zonder fysiek aanwezig te zijn.

5.2 De Facilitering van Georganiseerde Misdaad

Cybercriminaliteit is een onmisbaar en integraal onderdeel geworden van de operaties van traditionele criminele netwerken, die digitale middelen gebruiken om hun illegale activiteiten efficiënter en heimelijker uit te voeren.

- **Drugshandel:** In de haven van Antwerpen werd een medewerker van een expeditiebedrijf gerekruteerd door een drugsbende met de opdracht om de computersystemen van zijn werkgever te hacken. Het doel was om de logistieke planning te manipuleren en zo de smokkel van honderden kilo's cocaïne te faciliteren.
- **Mensenhandel en Gedwongen Fraude:** INTERPOL waarschuwt voor de wereldwijde opkomst van transnationale oplichtingscentra. In deze centra worden slachtoffers van mensenhandel gedwongen om op grote schaal online fraude te plegen, zoals beleggingsfraude en *romance scams*.
- **Industriële Oplichting:** De schaal van deze operaties is industrieel. Vanuit professionele callcenters in Belgrado worden via gerichte Facebook-advertenties op grote schaal slachtoffers in heel Europa gemaakt van beleggingsfraude, gedreven door een harde bonuscultuur.

Deze toenemende en veelzijdige dreigingen, die zowel de digitale als fysieke veiligheid van burgers en de samenleving raken, vereisen een robuust en coherent beleidsantwoord.

6.0 Strategische Imperatieven: Naar een Adaptieve en Soevereine Veiligheidsstrategie

De geanalyseerde trends tonen een dreigingslandschap in snelle transformatie. De geopolitisering van het cyberdomein, de systemische fragiliteit van digitale toeleveringsketens en de versmelting van digitale en fysieke dreigingen maken duidelijk dat een reactieve houding niet langer volstaat. Nederland heeft een herziene nationale veiligheidsstrategie nodig die proactief, adaptief en geïntegreerd is. Deze strategie moet gericht zijn op het versterken van onze digitale soevereiniteit, het verhogen van de weerbaarheid van de gehele samenleving en het intensiveren van internationale samenwerking om grensoverschrijdende dreigingen het hoofd te bieden.

6.1 De Balans tussen Soevereiniteit en Internationale Afhankelijkheid

Het streven naar nationale controle over vitale digitale infrastructuren staat op gespannen voet met de realiteit van een geglobaliseerde digitale economie die gedomineerd wordt door een klein aantal buitenlandse techgiganten. Recente casussen illustreren dit dilemma.

- **De Solvinity Casus:** De voorgenomen overname van het Nederlandse cloudbedrijf Solvinity door het Amerikaanse Kyndryl heeft geleid tot aanzienlijke politieke en veiligheidszorgen. Omdat Solvinity cruciale overheidsdiensten zoals DigiD host, roept de overname fundamentele vragen op over datasoevereiniteit en de mogelijke toegang van buitenlandse mogendheden tot gevoelige burgerdata.
- **Het 'Chatcontrole' Debat:** Het Europese voorstel voor chatcontrole plaatste Nederland voor een complexe beleidsmatige afweging tussen criminaliteitsbestrijding en digitale veiligheid. Mede op basis van een scherpe waarschuwing van de AIVD over de onacceptabele risico's die massasurveillance met zich meebrengt voor de encryptie en de algehele digitale weerbaarheid, heeft Nederland uiteindelijk 'nee' gestemd.
- **Proactieve Soevereiniteitsinitiatieven:** Als reactie op de afhankelijkheid van grote techbedrijven, nemen Nederlandse onderwijs- en onderzoeksinstellingen het heft in eigen handen. Door gezamenlijk over te stappen op open-source alternatieven zoals Nextcloud, zetten zij een concrete stap richting meer controle over hun eigen data en digitale infrastructuur.

6.2 De Staat van Nationale Weerbaarheid

Ondanks toenemende bewustwording en investeringen, tonen recente analyses aan dat de weerbaarheid van Nederland op alle niveaus – overheid, bedrijfsleven en burger – zorgwekkende tekortkomingen vertoont.

1. **Overheid:** De NCTV waarschuwt in het Cybersecuritybeeld Nederland 2025 voor een 'vals gevoel van veiligheid' binnen de Rijksoverheid. De basisbeveiliging schiet vaak tekort en het vermogen om aanvallen zelfstandig te detecteren en mitigeren is onvoldoende, wat de overheid kwetsbaar maakt voor spionage en sabotage.
2. **Bedrijfsleven:** Het Nederlandse bedrijfsleven is alarmerend kwetsbaar voor digitale ontwrichting. Onderzoek toont aan dat een uitval van ICT-diensten van

slechts een halve dag al tot ernstige operationele problemen leidt. Tegelijkertijd blijft het bewustzijn over de impact van geopolitieke risico's op de bedrijfsvoering zorgwekkend laag.

3. **Burger:** Op individueel niveau bestaat er een gevaarlijke kloof tussen perceptie en realiteit. Onderzoek wijst uit dat Nederlanders hun eigen vermogen om online oplichting en desinformatie te herkennen significant overschatten, wat hen een gemakkelijk doelwit maakt voor social engineering en fraude.

6.3 Aanbevelingen voor Beleidsmakers

Op basis van deze analyse zijn de volgende strategische aanbevelingen geformuleerd om de nationale cyberveiligheid op een toekomstbestendige manier te versterken:

1. **Versterk Internationale Samenwerking en Inlichtingenuitwisseling:** De toenemende samenwerking tussen statelijke actoren (zoals Rusland en Noord-Korea) en de transnationale aard van georganiseerde cybercrime vereisen een intensivering van de internationale respons. Investeer in een versterkt internationaal juridisch en operationeel kader, onder meer via INTERPOL, om gezamenlijk op te treden, inlichtingen effectiever te delen en cybercriminelen wereldwijd te kunnen vervolgen.
2. **Investeer in Publiek-Private Weerbaarheid:** Implementeer concrete programma's om de digitale basishygiëne op grote schaal te verhogen. Dit omvat ondersteuning voor het MKB naar Brits voorbeeld, het afdwingen van hogere veiligheidsstandaarden binnen de Rijksoverheid, en het lanceren van grootschalige, continue publiekscampagnes die de digitale geletterdheid en het risicobewustzijn van burgers structureel verbeteren.
3. **Ontwikkel Adaptief Beleid voor Opkomende Technologieën:** Ga van een reactieve naar een proactieve houding ten aanzien van technologische innovatie. Ontwikkel een nationale beleidsagenda gericht op de veiligheid en beheersing van AI, inclusief de risico's van AI als wapen en de kwetsbaarheden in AI-systemen. Versterk tevens de bescherming van vitale infrastructuren tegen nieuwe fysieke en digitale dreigingen, zoals geïllustreerd door de recente drone-incursies boven strategische locaties als vliegbasis Volkel, en geavanceerde aanvallen op de softwaretoeleveringsketen.