Week 52-2025

Strategisch Dreigingsrapport: Analyse van het Cyberdreigingslandschap voor Vitale Sectoren

1.0 Inleiding en Dreigingsbeeld Eind 2025

Dit strategisch dreigingsrapport biedt een essentiële analyse van het cyberdreigingslandschap zoals dat zich eind 2025 manifesteert. Deze periode wordt gekenmerkt door een zorgwekkende convergentie van escalerende geopolitieke spanningen, geavanceerde samenwerkingsverbanden tussen cybercriminelen en de snelle opkomst van disruptieve technologieën zoals kunstmatige intelligentie. Dit rapport analyseert de meest significante trends en incidenten die een direct risico vormen voor de nationale veiligheid en de continuïteit van vitale diensten in de Benelux en daarbuiten, met als doel besluitvormers te voorzien van het noodzakelijke inzicht voor een effectieve verdedigingsstrategie.

Het algehele dreigingsbeeld laat zien dat de traditionele grens tussen statelijke actoren en financieel gemotiveerde cybercriminelen steeds verder vervaagt. Staatsgelieerde groeperingen adopteren criminele tactieken voor spionage en disruptie, terwijl criminele syndicaten allianties vormen om de toenemende druk van wetshandhaving te weerstaan. De aanvalsvectoren breiden zich uit van puur digitale aanvallen naar hybride operaties die een gecoördineerde inzet omvatten tegen zowel digitale systemen als fysieke infrastructuur en cognitieve processen. Deze verschuiving vraagt om een geïntegreerde en multidimensionale benadering van nationale cybersecurity.

De volgende hoofdstukken bieden een gedetailleerde analyse van concrete, hoog-impact incidenten die dit veranderende dreigingslandschap illustreren.

2.0 Analyse van Recente Hoog-Impact Cyberaanvallen

Directe aanvallen op vitale infrastructuur en openbare diensten vormen de meest zichtbare en ontwrichtende manifestatie van de cyberdreiging. De maatschappelijke impact van dergelijke incidenten is onmiddellijk en voelbaar: ze verstoren de dagelijkse levens van miljoenen burgers, ondermijnen het vertrouwen in publieke instituties en kunnen aanzienlijke economische schade veroorzaken. Het analyseren van deze aanvallen is dan ook cruciaal om de tactieken van tegenstanders te begrijpen en de kwetsbaarheden in onze nationale weerbaarheid te identificeren.

2.1 Disruptie van Vitale Diensten door Ransomware en DDoS-aanvallen

In de laatste maanden van 2025 is een duidelijke escalatie zichtbaar in aanvallen die gericht zijn op het verstoren van essentiële diensten. Rond de kerstdagen werden de Franse post- en bankensector getroffen door een grootschalige Distributed Denial-of-Service (DDoS) aanval, die de diensten van La Poste, La Banque Postale, Caisse d'Epargne en Banque Populaire platlegde. De timing, tijdens de piekperiode van kerstpost en online aankopen, maximaliseerde de maatschappelijke hinder. Een vergelijkbaar patroon was zichtbaar in België, waar in de aanloop naar de EU-top in december een significante stijging van het aantal cyberaanvallen werd geconstateerd. Tussen 2 en 18 december werden **1.249 DDoS-aanvallen** geregistreerd, een **toename van ruim 190 procent** ten opzichte van de maand ervoor. Deze aanvallen, toegeschreven aan de pro-Russische hackersgroep **DDoSia**, escaleerden van overheidsinstellingen naar de vitale energie- en nucleaire sector, met doelwitten als het Brusselse energiebedrijf **Sibelga** en de nucleaire toeleverancier **ASCO Industries**. De timing van deze escalatie valt samen met de **Europese beraadslagingen over het gebruik van geblokkeerde Russische tegoeden**, wat een duidelijke geopolitieke motivatie suggereert.

Naast deze verstoringsaanvallen blijft ransomware een directe bedreiging voor de bedrijfscontinuïteit. De aanval van de **Qilin**-groep op **Victoria Benelux** op 20 december illustreert de methodische aanpak van criminelen. Technische analyse toont aan dat de uiteindelijke ransomware-aanval werd voorafgegaan door voorbereidende 'infostealer'-activiteiten, waarbij gegevens van **tweeëntwintig gebruikersaccounts** werden gecompromitteerd. Deze accounts, in combinatie met externe kwetsbaarheden in het netwerk, dienden als toegangspoort voor de uiteindelijke gijzeling van systemen. Deze incidenten onderstrepen hoe zowel statelijk geïnspireerde disruptie als financieel gemotiveerde afpersing het publieke leven en de economie direct kunnen raken.

2.2 De Groeiende Hybride Dreiging voor Fysieke en Digitale Infrastructuur

De dreiging beperkt zich niet langer tot de puur digitale wereld. NAVO-commandeur Arjen Warnaar waarschuwde recentelijk voor de groeiende hybride dreiging in het 'grijze gebied' tussen oorlog en vrede, met name gericht op onderwaterinfrastructuur zoals datakabels en energieverbindingen. De combinatie van fysieke sabotage aan kabels, de inzet van een zogenaamde 'schaduwvloot' voor spionage en de toenemende aanwezigheid van drones creëert een complex en moeilijk te attribueren

dreigingsbeeld. Cyberincidenten vormen een integraal onderdeel van deze strategie om onrust te stoken zonder een openlijk militair conflict te riskeren.

De kwetsbaarheid van de Europese energiesector wordt verder geïllustreerd door de melding dat ongeautoriseerde toegang tot de systemen van een groot West-Europees energiebedrijf met een marktwaarde van **ongeveer tweehonderd miljard dollar** te koop werd aangeboden op het dark web. De handel in dergelijke *initial access* door gespecialiseerde brokers vormt een kritiek risico. Het stelt andere groeperingen, zoals ransomware-bendes of statelijke actoren, in staat om direct diep in de netwerken van vitale organisaties door te dringen, wat de weg vrijmaakt voor spionage, sabotage of grootschalige ontwrichting.

De analyse van deze incidenten toont een divers landschap van dreigingen, die worden uitgevoerd door een even divers scala aan actoren.

3.0 Profiel van Relevante Dreigingsactoren

Voor een effectieve strategische verdediging is het essentieel om niet alleen de aanvallen zelf te analyseren, maar ook de actoren die erachter schuilgaan. Het identificeren en profileren van deze groepen – of het nu staten, criminele syndicaten of insiders zijn – stelt besluitvormers in staat om hun motivaties, capaciteiten en werkwijzen te begrijpen. Dit inzicht is cruciaal om risico's beter in te schatten, middelen effectiever toe te wijzen en voorspellende analyses te maken over toekomstige dreigingen.

3.1 Staatsgelieerde Actoren en Geopolitieke Operaties

Aanvallen die worden uitgevoerd of ondersteund door staten zijn vaak het meest geavanceerd en gericht op langetermijndoelen zoals spionage, intellectuele eigendomsdiefstal en geopolitieke beïnvloeding.

Rusland: Russische actoren blijven een significante dreiging vormen, met operaties die zowel technische spionage als cognitieve oorlogsvoering omvatten. De groep **BlueDelta (APT28)**, gelieerd aan de militaire inlichtingendienst, voerde een geavanceerde en grootschalige phishingcampagne uit tegen de Oekraïense webmaildienst UKR.NET om inloggegevens te stelen. Tegelijkertijd voerde de pro-Russische groep **DDoSia** disruptieve aanvallen uit op Belgische vitale sectoren. Deze acties worden ondersteund door een bredere strategie van '**reflexieve controle**', een techniek uit de cognitieve oorlogsvoering waarbij informatie subtiel

wordt gedoseerd om tegenstanders te verleiden tot het nemen van beslissingen die de Russische agenda dienen. Het doel is het zaaien van wantrouwen en het ondermijnen van democratische processen van binnenuit.

Iran: Na een periode van relatieve stilte is de Iraanse spionagegroep **Infy (Prince of Persia)** weer volledig operationeel. Deze groep kenmerkt zich door een focus op *stealth* en langetermijnspionage, in tegenstelling tot luidruchtigere Iraanse actoren. De technische evolutie van hun malware, met geavanceerde varianten als **Foudre** (downloader) en **Tonnerre** (spionagesoftware), toont een aanzienlijke doorontwikkeling van hun capaciteiten. De operaties van Infy, die gericht zijn op doelen in onder meer Europa, passen in een breder beeld van Iraanse cyberoperaties die steeds professioneler en bureaucratischer worden georganiseerd, vaak functionerend als overheidsafdelingen met een strikte taakverdeling.

Noord-Korea: Noord-Koreaanse agenten hanteren een unieke infiltratiestrategie die primair financieel gedreven is: het genereren van valuta voor het nationale wapenprogramma. Techgigant **Amazon** onderschepte meer dan 1.800 sollicitaties van Noord-Koreaanse agenten die via gestolen identiteiten en het gebruik van 'laptop farms' in de VS probeerden om op afstand IT-functies te bemachtigen. Door inactieve LinkedIn-profielen over te nemen, creëren ze een geloofwaardige dekmantel om westerse bedrijven te infiltreren en salarissen direct door te sluizen naar Pyongyang.

3.2 De Evolutie van het Cybercriminele Ecosysteem

Het cybercriminele landschap is zeer dynamisch en past zich continu aan. Als reactie op de toegenomen druk van wetshandhaving en de dalende bereidheid van slachtoffers om losgeld te betalen – de mediane losgeldbetaling daalde in Q3 2025 met 65% **naar ongeveer 140.000 dollar** – zoeken ransomware-groepen hun toevlucht in strategische allianties. De samenwerking die in september 2025 werd aangekondigd tussen **Qilin**, **DragonForce** en het verzwakte **LockBit** is hier een duidelijk voorbeeld van. Dergelijke coalities zijn bedoeld om middelen te bundelen en een sterker front te vormen in een steeds vijandiger klimaat.

Tegelijkertijd floreert de digitale zwarte markt, waar een breed scala aan illegale goederen en diensten wordt verhandeld die aanvallen faciliteren:

- **Geavanceerde malware:** De broncode voor een macOS Remote Access Trojan (RAT) met root-toegang wordt aangeboden voor 1 miljoen dollar. Daarnaast worden gespecialiseerde tools zoals 'fileless droppers' die

antivirussoftware omzeilen en de **NtKiller**-malware, die specifiek is ontworpen om EDR-systemen uit te schakelen, te koop aangeboden.

- **Zero-day kwetsbaarheden:** Een vermeende zero-day exploit voor de Chromium-browserengine, die de basis vormt voor Chrome en Edge, werd aangeboden voor 250.000 dollar.
- **Ongeautoriseerde netwerktoegang:** Zogenaamde *Initial Access Brokers* blijven een cruciale rol spelen. Toegang tot de systemen van een groot West-Europees energiebedrijf en tot 1.500 andere gecompromitteerde systemen werd recentelijk te koop aangeboden.
- **Gelekte databases:** Gestolen datasets, zoals die van de **European Vegetarian Union** en een **Web3-beloningsplatform** met 467.000 gebruikers, worden verhandeld voor verder misbruik.

3.3 De Insider Threat: Risico's van Binnenuit en via Externe Partners

De dreiging komt niet altijd van buitenaf. Het risico van insiders, zowel kwaadwillend als nalatig, blijft een significante kwetsbaarheid. Het recente datalek bij **Proximus** illustreert dit perfect. Een medewerker van een externe partner verkreeg op ongeautoriseerde wijze toegang tot de centrale klantendatabase, waardoor namen, adressen, e-mailadressen en telefoonnummers van een groot aantal klanten werden blootgesteld. Proximus waarschuwde direct voor het verhoogde risico op vervolgfraude, zoals gerichte phishing-aanvallen. Dit incident staat voor een *onopzettelijk* insider-risico dat voortkomt uit een complex partner-ecosysteem. De pogingen van **Noord-Koreaanse agenten** om te solliciteren bij techbedrijven illustreren daarentegen een *opzettelijke, staatsgesponsorde* infiltratie, wat de volledige breedte van de insider-dreiging aantoont.

Deze analyse van de actoren laat zien *wie* de dreiging vormt. Het volgende hoofdstuk richt zich op *hoe* deze actoren te werk gaan.

4.0 Analyse van Tactieken, Technieken en Procedures (TTP's)

Inzicht in de aanvalsmethoden – de Tactieken, Technieken en Procedures (TTP's) – die dreigingsactoren hanteren, is van fundamenteel belang voor een proactieve verdediging. Door te begrijpen hoe aanvallers opereren, van de initiële infiltratie tot de uiteindelijke impact, kunnen organisaties hun verdedigingsmaatregelen beter

afstemmen, detectiemechanismen verfijnen en de weerbaarheid van hun personeel vergroten.

4.1 Geavanceerde Phishing en Social Engineering

Phishing en social engineering blijven de meest voorkomende methoden om een eerste voet aan de grond te krijgen. Aanvallers innoveren continu om traditionele verdedigingslinies en het bewustzijn van gebruikers te omzeilen.

Techniek	Analyse en Impact
Device Code Phishing	Aanvallers misbruiken op grote schaal de legitieme OAuth 2.0-apparaatautorisatieflow om Microsoft 365-accounts over te nemen. Door slachtoffers te verleiden een apparaatcode in te voeren op de officiële Microsoft-verificatiepagina, verkrijgen aanvallers een autorisatietoken. Omdat dit proces gebruikmaakt van legitieme Microsoft-domeinen, worden traditionele e-mailfilters en het wantrouwen van gebruikers effectief omzeild.
AI-Gedreven Misleiding	De explosieve groei van de Nomani-beleggingsfraude toont de kracht van AI in social engineering. Criminelen zetten hoogwaardige deepfake-video's van bekende personen in om frauduleuze investeringen aan te prijzen. Daarnaast wordt AI gebruikt voor het opstellen van foutloze en overtuigende phishing-teksten, waardoor traditionele indicatoren zoals spelfouten verdwijnen.
Misbruik van Open-Source Ecosystemen	Legitieme platforms worden steeds vaker misbruikt als infrastructuur voor aanvallen. Een recente campagne gebruikte het **npm-register** om phishing-pagina's te hosten die gericht waren op vitale sectoren. Tegelijkertijd werd de **Webrat**-malware op **GitHub** vermomd als Proof-of-Concept exploits voor recente kwetsbaarheden om security-onderzoekers in de val te lokken.
Complexe Infectieketens	Om detectie te ontwijken, bouwen aanvallers steeds complexere infectieketens. Een campagne gericht op productiebedrijven en overheden combineerde **SVG-bestanden**, kwetsbare **Office-documenten**, **steganografie** (het verbergen van code in

	afbeeldingen) en 'fileless' technieken. De uiteindelijke malware, zoals **Remcos RAT**, werd direct in het werkgeheugen geladen om geen sporen op de harde schijf achter te laten.

4.2 Exploitatie van Software- en Supply Chain-Kwetsbaarheden

Data van honeypot-sensoren in de Benelux toont een gerichte aanpak van aanvallers. Terwijl de wereldwijde trend zich focust op kwetsbaarheden in IoT-apparatuur, ligt de focus in **Nederland** significant hoger op enterprise-oplossingen, met name de data-analysetool **Metabase**. In **België** is de aanvalsintensiteit lager, met een focus op kwetsbaarheden in netwerkapparatuur van **Zyxel/Billion**. Dit duidt op een gedifferentieerde strategie, afgestemd op de technologische infrastructuur per regio.

Recentelijk zijn diverse zeer kritieke softwarekwetsbaarheden gerapporteerd die onmiddellijke aandacht vereisen:

1. **HPE OneView (CVSS 10.0):** Een authenticatie-bypass in de REST API stelt ongeautoriseerde aanvallers in staat om op afstand willekeurige code uit te voeren.
2. **n8n (CVSS 9.9):** Een kwetsbaarheid in het workflow-automatiseringsplatform maakt het voor geauthenticeerde gebruikers mogelijk om willekeurige code op de server uit te voeren.
3. **WatchGuard (zero-day):** Een zero-day kwetsbaarheid in Firebox-appliances stelt ongeauthenticeerde aanvallers in staat om op afstand de controle over te nemen via IKEv2 VPN-onderhandelingen.
4. **M-Files Server:** Een kritiek lek stelt aanvallers in staat de identiteit van andere gebruikers aan te nemen en namens hen ongeautoriseerde acties uit te voeren.

Het risico is niet beperkt tot de eigen software. Het datalek bij **Nissan**, waarbij gegevens van meer dan 21.000 klanten werden blootgesteld, was het directe gevolg van een inbraak bij softwareleverancier **Red Hat**. Dit supply chain-incident trof ook andere grote organisaties, waaronder de luchtvaartmaatschappij **Delta Airlines** en **ING**, en illustreert hoe een kwetsbaarheid bij één leverancier een cascade-effect kan hebben op talloze afhankelijke partijen.

4.3 Fysieke en Gebruikersgerelateerde Kwetsbaarheden

Naast softwarematige kwetsbaarheden blijven fysieke en door gebruikers veroorzaakte lekken een risico. Onderzoek in België toonde aan dat tientallen onbeveiligde IP-camera's in woningen en bedrijven live via het internet te volgen zijn. De oorzaken zijn vaak eenvoudig: het niet wijzigen van standaardwachtwoorden en het onnodig openzetten van internetpoorten. De gevolgen kunnen ernstig zijn, zoals blijkt uit een vergelijkbaar incident in Zuid-Korea, waar beelden van 120.000 gehackte camera's werden buitgemaakt en deels doorverkocht aan pornosites. Dit benadrukt de gedeelde verantwoordelijkheid van zowel gebruikers, die hun apparaten correct moeten configureren, als fabrikanten, die veilige standaardinstellingen moeten afdwingen.

De analyse van deze tactieken toont aan dat de dreiging op alle lagen van de digitale en fysieke infrastructuur aanwezig is, wat leidt tot een bredere strategische discussie over toekomstige risico's en de noodzaak van digitale autonomie.

5.0 Toekomstige Dreigingen en Strategische Overwegingen

Een effectieve nationale veiligheidsstrategie vereist niet alleen een reactie op de dreigingen van vandaag, maar ook een proactieve visie op de risico's van morgen. Dit hoofdstuk verlegt het perspectief naar opkomende technologische en geopolitieke ontwikkelingen die het dreigingslandschap fundamenteel zullen veranderen. Anticiperen op deze verschuivingen is essentieel om tijdig beleid te ontwikkelen dat de nationale soevereiniteit en veiligheid waarborgt.

5.1 Technologische Convergentie: De Impact van AI, Robotica en BCI's

De convergentie van verschillende technologische domeinen creëert nieuwe en complexe dreigingsscenario's. Europol waarschuwt dat tegen 2035 de criminele inzet van **robotica en AI-gestuurde drones** zal leiden tot nieuwe vormen van spionage, smokkel en intimidatie. De grens tussen de fysieke en digitale wereld vervaagt verder, wat nieuwe uitdagingen voor de rechtshandhaving met zich meebrengt.

Een actuele en fundamentele kwetsbaarheid bevindt zich in de kern van de huidige AI-revolutie. Zowel **OpenAI** als het Britse **NCSC** waarschuwen dat **'prompt injection'** in AI-browsers een structureel risico vormt dat mogelijk nooit volledig technisch kan worden opgelost. Omdat AI-modellen geen strikt onderscheid maken tussen instructies en data, kunnen kwaadwillenden via verborgen opdrachten op

websites de controle over een AI-browser overnemen, met verstrekkende gevolgen voor de privacy en veiligheid van gebruikers.

Tegelijkertijd vinden er doorbraken plaats op het gebied van **Brain-Computer Interfaces (BCI)**. Een recente klinische proef in China toonde aan dat een patiënt via een draadloos implantaat direct kan communiceren met externe netwerken en het Internet of Things. Hoewel de medische toepassingen veelbelovend zijn, creëert de directe koppeling van neurale interfaces aan het internet ongekende beveiligingsrisico's, variërend van datadiefstal tot de manipulatie van fysieke systemen.

5.2 De Strijd om Digitale Soevereiniteit in Europa

De diepe afhankelijkheid van niet-Europese, met name Amerikaanse, technologie vormt een groeiend strategisch risico. De recente overname van de Nederlandse cloudprovider **Solvinity** door het Amerikaanse **Kyndryl** legt deze kwetsbaarheid bloot. Vitale Nederlandse overheidssystemen, waaronder DigiD, vallen hierdoor onder een Amerikaans moederbedrijf. Dit brengt het risico met zich mee dat de Amerikaanse overheid via wetgeving zoals de **Cloud Act** toegang kan eisen tot gevoelige data, ongeacht waar de servers fysiek staan.

Als reactie op deze afhankelijkheid nemen diverse Europese landen concrete stappen om hun digitale autonomie te vergroten:

- De Duitse deelstaat **Sleeswijk-Holstein** is bezig 30.000 ambtenaren over te zetten op open-source alternatieven zoals LibreOffice en Mozilla Thunderbird.
- **Oostenrijk** heeft zijn ministerie van Economische Zaken volledig overgezet op de Europese clouddienst Nextcloud.
- **Frankrijk** hanteert voor gevoelige dossiers binnen zijn ministeries een volledig eigen, soevereine cloudomgeving.

Deze initiatieven tonen een groeiend besef dat digitale soevereiniteit geen abstract concept is, maar een concrete voorwaarde voor het waarborgen van de nationale veiligheid en de continuïteit van de overheid.

5.3 Regulering, Respons en Maatschappelijk Debat

Overheden en regelgevers worstelen met de vraag hoe zij moeten reageren op de snel evoluerende digitale dreigingen en maatschappelijke dilemma's. De respons

varieert van lokale initiatieven tot internationale handhaving en principiële debatten over privacy en controle.

- **Lokale Weerbaarheid:** In Vlaanderen hebben 21 gemeenten de handen ineengeslagen om een technologisch noodplan te implementeren. Dit plan omvat geavanceerde back-upsystemen en een draaiboek voor crisiscommunicatie om de publieke dienstverlening te garanderen, zelfs tijdens een grootschalige cyberaanval.
- **Toezicht en Handhaving:** Toezichthouders treden steeds vaker handhavend op. De Italiaanse mededingingsautoriteit legde **Apple** een boete op van 98 miljoen euro wegens het App Tracking Transparency-beleid en greep in tegen **Meta's** plannen om concurrerende AI-chatbots van WhatsApp te weren. In Frankrijk kreeg softwarebedrijf **Nexpublica** een boete van 1,7 miljoen euro voor verwijtbare nalatigheid na een datalek.
- **Leeftijdsverificatie:** Het debat over online leeftijdsverificatie is complex. Terwijl **Nederland** plannen ontwikkelt voor de online verkoop van alcohol en **Zuid-Korea** gezichtsherkenning verplicht stelt voor nieuwe telefoonnummers, heeft een rechter in **Texas (VS)** vergelijkbare wetgeving geblokkeerd vanwege strijdigheid met de vrijheid van meningsuiting. Organisaties zoals **Mozilla** blijven kritisch en stellen dat dergelijke maatregelen de onderliggende problemen van online platforms niet oplossen.
- **Privacy en Gebruikerscontrole:** In Nederland is een maatschappelijk debat gaande over de wenselijkheid van een '**digitale rode knop**', een centrale voorziening waarmee burgers met één druk op de knop hun persoonsgegevens bij online platforms kunnen wissen. Het kabinet heeft hierop terughoudend gereageerd en wijst op de bestaande rechten binnen de AVG en de verantwoordelijkheid van de toezichthouders.

Deze ontwikkelingen illustreren de complexiteit van het creëren van een veilig, soeverein en vrij digitaal domein en vormen de opmaat naar de strategische conclusies van dit rapport.

6.0 Conclusies en Strategische Implicaties

De analyses in dit rapport schetsen een dreigingslandschap dat complexer, meer verweven en dynamischer is dan ooit tevoren. De dreigingen zijn multidimensionaal

en overstijgen de traditionele grenzen tussen geopolitiek en criminaliteit, en tussen de digitale en de fysieke wereld. Een effectieve nationale strategie vereist dan ook een geïntegreerde aanpak die verder gaat dan louter technische maatregelen en die rekening houdt met de strategische, economische en maatschappelijke dimensies van cybersecurity.

Op basis van de geobserveerde trends en incidenten kunnen de volgende drie strategische risico's voor besluitvormers worden gedestilleerd:

1. **Toenemende verwevenheid van geopolitiek en cyberdreigingen:** Aanvallen op vitale infrastructuur, zoals de energiesector en communicatienetwerken, hebben steeds vaker een duidelijke geopolitieke dimensie. Statelijke actoren zetten cyberoperaties in als instrument voor spionage, disruptie en cognitieve oorlogsvoering. Tactieken zoals 'reflexieve controle' en desinformatie zijn niet langer randverschijnselen, maar vormen een structurele bedreiging voor de stabiliteit van democratische instituties en het maatschappelijk vertrouwen.
2. **Ondermijning van digitale soevereiniteit:** De diepe en groeiende afhankelijkheid van niet-Europese technologische infrastructuren en software vormt een fundamenteel strategisch risico. De overname van cruciale cloudproviders door buitenlandse entiteiten en de extraterritoriale werking van wetgeving zoals de Amerikaanse Cloud Act maken de continuïteit van overheidsdiensten en de bescherming van nationale data kwetsbaar voor de politieke en juridische agenda's van andere landen. Dit maakt een versnelde transitie naar betrouwbare en autonome Europese alternatieven noodzakelijk.
3. **De industrialisatie van social engineering en de mens als zwakste schakel:** De inzet van kunstmatige intelligentie voor het creëren van deepfakes en foutloze phishing-berichten, gecombineerd met de professionalisering van aanvalstechnieken zoals *device code phishing*, maakt de menselijke factor tot de meest geëxploiteerde kwetsbaarheid. Traditionele verdedigingsmechanismen en bewustwordingstrainingen volstaan niet langer. Dit risico vereist een continue investering in zowel geavanceerde technische detectie als in de weerbaarheid van burgers en medewerkers tegen steeds verfijndere vormen van psychologische manipulatie.

Het huidige en toekomstige dreigingslandschap wacht niet op reactie, maar eist proactief en strategisch handelen om de veiligheid, welvaart en soevereiniteit van onze samenleving te waarborgen.