Week 03-2026

# Strategisch Dreigingsadvies: Geopolitieke Cyberrisico's en de Veiligheid van de Vitale Infrastructuur (2026)

## 1. Introductie: Het Veranderende Dreigingslandschap

De operationele werkelijkheid van januari 2026 dwingt ons tot een fundamentele herwaardering van onze nationale veiligheidsstrategie. De grens tussen conventionele fysieke sabotage en digitale interventie is definitief gewist. Cyberoperaties zijn geëvolueerd van ondersteunende inlichtingenactiviteiten naar primaire aanvalsvectoren die de fysieke integriteit van de vitale sector direct ondermijnen. In dit landschap is digitale soevereiniteit geen abstract ideaal meer, maar een randvoorwaarde voor maatschappelijke stabiliteit.De Cyber Security Raad (CSR) waarschuwt indringend voor grootschalige maatschappelijke ontwrichting indien de huidige onderinvestering aanhoudt. De noodzaak voor een structurele investering van **690 miljoen euro** is onomstotelijk; dit kapitaal is vereist om onze vitale processen te harden tegen statelijke actoren die de fundamenten van onze economie en zorg trachten te destabiliseren. Zonder centrale beleidsregie en deze financiële injectie verliest Nederland de regie over zijn eigen kritieke infrastructuren. De recente gecoördineerde operaties tegen de Europese energievoorziening vormen de voorbode van een escalatie die onze volledige aandacht opeist.

## 2. Casusanalyse: De Aanval op de Poolse Energie-infrastructuur

Het gebruik van vitale voorzieningen als geopolitiek drukmiddel is een strategische realiteit geworden. De aanval op het Poolse elektriciteitsnet in december 2025, toegeschreven aan de Russische geheime diensten, dient als een dwingend casestudy voor de kwetsbaarheid van de energietransitie.De aanvallers kozen bewust voor een tactische verschuiving: niet de centrale opwekking, maar de **communicatie tussen installaties voor hernieuwbare energie en distributienetbeheerders** was het doelwit. Deze decentrale architectuur vormt een kritiek nieuw aanvalspunt. De transitie naar groene energie is, zonder stringente hardening van de onderliggende protocollen, inherent een security-regressie. De schaal van deze dreiging is ongekend:

- In Polen werden in 2025 maar liefst **170.000 cyberincidenten** geregistreerd met een directe link naar statelijke actoren.
- Tijdens de kerstperiode van 2025 werd een landelijke blackout slechts ternauwernood voorkomen door autoritair ingrijpen en isolatie van netwerksegmenten.Deze sabotage bewijst dat distributienetbeheerders niet langer kunnen vertrouwen op de isolatie van hun systemen. De focus op decentrale communicatieprotocollen toont aan dat de perimeter is verschoven naar elk individueel eindpunt in de keten.

## 3. Technologische Verschuiving: Chinese Kwantumontwikkelingen

Terwijl wij onze huidige systemen proberen te patchen, vindt er een geopolitieke wedloop plaats rondom kwantumtechnologie die de huidige encryptiestandaarden binnen afzienbare tijd onhoudbaar maakt. De technologische superioriteit van China op dit gebied vormt een directe dreiging voor de vertrouwelijkheid van onze staatsgeheimen en vitale data.Volgens rapportages in de *Science and Technology Daily* en analyses van de *National University of Defence Technology* (NUDT) test het Chinese Volksbevrijdingsleger momenteel meer dan tien experimentele kwantum-cyberwapens. De kernkenmerken zijn alarmerend:

1. **Draagbare Kwantumradio:** Reeds succesvol ingezet in de Saibei-graslanden voor noodcommunicatie in omgevingen waar conventionele systemen falen.
2. **Real-time Decodering:** Prototypes van de NUDT, met een gewicht van slechts **3 kilogram** , zijn in staat om signalen over tientallen kilometers te ontvangen en real-time te decoderen.
3. **Stealth-detectie:** Een offensieve focus op het onzichtbaar verzamelen van militaire en strategische inlichtingen uit de publieke digitale ruimte.Deze ontwikkelingen dwingen ons de beveiligingsperimeter te heroverwegen. De internationale veiligheidsgemeenschap stelt vast dat kwantumtechnologie de fundamenten van detectie en encryptie onomkeerbaar zal veranderen. Data die vandaag wordt onderschept ("harvest now"), kan morgen met deze prototypes worden ontsleuteld ("decrypt later").

## 4. De Rol van AI in Offensieve Operaties en Malware

Kunstmatige intelligentie heeft de efficiëntie van cyberaanvallen naar een punt gebracht waar reactieve verdediging per definitie tekortschiet. AI wordt ingezet om malware te genereren die zich in real-time aanpast, waardoor statische scanners en reputatie-gebaseerde detectie irrelevant worden.Cruciale voorbeelden van deze escalatie zijn:

- **MonetaStealer:** Ontdekt op 6 januari 2026. Deze malware maakt gebruik van AI-gegenereerde code en is een **Mach-O binary** die zich vermomt als een Windows .exe (Portfolio_Review.exe). Bij ontdekking was de **detectieratio op VirusTotal nul** , omdat de code geen bekende signaturen bevat.
- **Reprompt-aanvallen:** Deze methodiek misbruikt de **"q" URL-parameter** binnen Microsoft Copilot om indirect prompts te injecteren. Dit bewijst dat "link trust" in 2026 dood is; zelfs een legitieme Microsoft-link kan fungeren als kanaal voor data-exfiltratie.
- **Impersonatie via RedVDS:** De onlangs ontmantelde RedVDS-infrastructuur faciliteerde op grote schaal AI-gestuurde voice cloning en face-swapping voor Business Email Compromise (BEC), waarbij 191.000 organisaties werden getroffen.| Kenmerk | Traditionele Malware | AI-Verbeterde Malware || ------ | ------ | ------ || **Detecteerbaarheid** | Gebaseerd op vaste signatures (relatief hoog). | **Zero-signature nature** ; unieke payloads per download omzeilen scanners. || **Reactiesnelheid** | Statisch; vereist handmatige updates. | Past gedrag in real-time aan de omgeving aan (context-aware). || **Aanvalsvector** | Voorspelbare templates. | Hoogwaardige deepfakes en misbruik van AI-parameters (bijv. Reprompt). |

De kwetsbaarheid is verschoven van de AI-modellen naar de workflows waarin zij opereren. Beveiliging moet zich daarom richten op de volledige keten van input en output.

## 5. Sectorale Impact: Zorg, Financiën en Logistiek

De onderlinge afhankelijkheid binnen de Benelux zorgt ervoor dat lokale incidenten direct leiden tot regionale cascade-effecten.

- **Zorg:** Op **dinsdag 13 januari 2026** trof een ransomware-aanval het ziekenhuis **AZ Monica** . Alle servers werden uitgeschakeld, waardoor de zorgcapaciteit halveerde en personeel gedwongen werd terug te vallen op papier. De onmogelijkheid om CT- of MRI-scans uit te voeren leidde tot een kritieke belasting van omliggende instellingen.
- **Financiën:** De fraude via gehackte Booking.com-accounts is geëscaleerd naar **65.000 euro schade** in 2025, vergeleken met 25.000 euro in 2024. Deze **stijging van 160%** onderstreept de effectiviteit van aanvallen op de supply chain van boekingssystemen.
- **Logistiek & Cloud:** De opkomst van **CastleLoader** , gericht op Europese kritieke infrastructuur, toont de focus op de logistieke sector. Tegelijkertijd legde de **"CodeBreach"** kwetsbaarheid in AWS CodeBuild een fundamenteel risico bloot. Door een misconfiguratie in **webhook-filters** en foutieve **reguliere expressies** (het ontbreken van begin/eind-regels) konden GitHub-repositories van projecten zoals *aws-sdk-js-v3* en *amazon-corretto-crypto-provider* worden gekaapt.

## 6. Strategische Aanbevelingen voor Toekomstbestendig Beleid

Gezien de vijandige omgeving volstaat een defensieve houding niet langer. Wij adviseren de volgende directieve maatregelen:

- **Automatisering van het SOC:** Verschuiving van handmatige validatie naar geautomatiseerde gedragsanalyse. Het SOC moet specifiek uitgerust worden met tools die **AI-driven obfuscation** , zoals interactieve CAPTCHA’s en QR-codes, autonoom kunnen analyseren en omzeilen.
- **Workflowbeveiliging voor AI:** Een onmiddellijke inventarisatie van alle AI-agenten. Beperk de rechten van AI-systemen strikt binnen de netwerkperimeter en implementeer output-filters tegen data-exfiltratie.
- **Endpoint Reduction via AppGuard-methodiek:** Minimaliseer het aanvalsoppervlak fundamenteel. In plaats van te vertrouwen op detectie van "het kwaadaardige", moet de focus liggen op het strikt inperken van wat processen *mogen* uitvoeren op endpoints.
- **Agressief Patch-management:** Onmiddellijke actie op kwetsbaarheden met een CVSS-score van 9+. Prioriteit ligt bij **FortiSIEM (CVE-2025-64155, score 9.4)** en **FortiFone (CVE-2025-47855, score 9.3)** .
- **Implementatie Cyberbeveiligingswet:** Gebruik de Cyberbeveiligingswet (NIS2-implementatie) als dwingend instrument voor compliance binnen de vitale sector, ondersteund door de geadviseerde 690 miljoen euro aan structurele financiering.

## 7. Conclusie: Urgentie en Soevereiniteit

De convergentie van Russische sabotage, Chinese kwantumsprongen en de onzichtbare dreiging van AI-malware vormt een existentieel risico voor de digitale soevereiniteit van

Nederland. We bevinden ons op een historisch kantelpunt; digitale kwetsbaarheid vertaalt zich vandaag direct in fysieke onveiligheid en maatschappelijke ontwrichting.Het is niet langer de vraag of onze systemen worden gepenetreerd, maar hoe autonoom we kunnen blijven functioneren onder voortdurende aanval. Centrale beleidsregie en de directe toewijzing van middelen voor digitale autonomie zijn geen opties, maar noodzakelijke voorwaarden om de stabiliteit van Nederland in 2026 te waarborgen. De tijd van reactief beheer is definitief voorbij; veiligheid vereist een autoritaire, offensieve verdedigingshouding.