Week 43-2025

Strategisch Dreigingsrapport Cyberveiligheid Nederland 2025

1.0 Inleiding: Het Convergerende Dreigingslandschap

De Nederlandse nationale veiligheid wordt geconfronteerd met een complex en escalerend dreigingsbeeld, gekenmerkt door een strategische convergentie van geopolitieke spanningen, geavanceerde cybercriminaliteit en een toenemende afhankelijkheid van kwetsbare digitale infrastructuren. De traditionele scheidslijnen tussen statelijke spionage, sabotage en financieel gemotiveerde misdaad eroderen, waardoor een omgeving ontstaat waarin risico's zich voortdurend ontwikkelen en vermenigvuldigen. Dit rapport is opgesteld om beleidsmakers, veiligheidsprofessionals en bestuurders een geanalyseerd overzicht te bieden van de voornaamste dreigingen die de Nederlandse belangen raken, en onderbouwt de noodzaak voor een coherente en proactieve nationale cyberdefensiestrategie.

De centrale argumentatie van dit rapport is dat de huidige cyberdreigingen niet langer louter technisch van aard zijn, maar een wezenlijk en direct risico vormen voor de economische stabiliteit, de democratische processen en de maatschappelijke continuïteit van Nederland. De incidenten die in dit document worden geanalyseerd, van aanvallen op vitale sectoren tot de grootschalige diefstal van persoonsgegevens, illustreren een realiteit waarin digitale veiligheid een onmisbare pijler is geworden van onze nationale veiligheid.

Deze analyse begint met een onderzoek naar de meest prominente staat-gesponsorde actoren die hun geopolitieke ambities via digitale middelen nastreven.

2.0 Analyse van Geopolitieke Dreigingsactoren

Internationale conflicten en geopolitieke rivaliteit manifesteren zich steeds vaker in de digitale wereld. Statelijke actoren zetten geavanceerde cyberoperaties in voor spionage, sabotage en financieel gewin, wat een directe bedreiging vormt voor de Nederlandse en Europese belangen. Deze operaties zijn niet langer incidenteel, maar vormen een structureel onderdeel van het buitenlandbeleid van diverse landen, waarbij de Nederlandse vitale infrastructuur, overheid en hightechsector prominente doelwitten zijn.

2.1 Rusland: Geavanceerde Spionage en Destabilisatie

Russische statelijke hackergroepen blijven een van de meest persistente en geavanceerde dreigingen vormen. Groepen zoals **COLDRIVER** en **Star Blizzard** hebben hun aanvalscampagnes geïntensiveerd met nieuwe, moeilijk detecteerbare malwarefamilies, waaronder **NOROBOT**, **YESROBOT**, **MAYBEROBOT** en **Snappybee**. Hun operaties richten zich op strategisch belangrijke doelwitten, zoals Europese telecombedrijven en overheidsinstanties, met als doel het verzamelen van inlichtingen en het voorbereiden van destabiliserende acties. De diefstal van gevoelige data van het Britse ministerie van Defensie, waarbij persoonlijke gegevens van ongeveer 272.000 personeelsleden werden buitgemaakt, is een zorgwekkend voorbeeld. Dit incident demonstreert een strategische intentie die verder gaat dan enkel het vergaren van inlichtingen; het is gericht op het verkrijgen van pressiemiddelen en het zaaien van onrust door de persoonlijke data van defensiepersoneel van bondgenoten te compromitteren, een tactiek die institutioneel vertrouwen ondermijnt.

2.2 Noord-Korea: Financiering van Kernwapenprogramma's via Cybercrime

Noord-Korea heeft zich ontwikkeld van een regionale speler tot een serieuze mondiale cyberdreiging. De afhankelijkheid van het regime van cybercriminaliteit voor de financiering van zijn gesanctioneerde massavernietigingswapenprogramma's dicteert de keuze van doelwitten en methoden. De strategie is tweeledig: enerzijds worden spionagecampagnes uitgevoerd gericht op strategische sectoren zoals defensie en lucht- en ruimtevaart om technologische kennis te vergaren. Anderzijds is de focus op grootschalige diefstal van cryptovaluta een direct gevolg van de internationale financiële isolatie, waardoor het digitale financiële ecosysteem een primair strijdtoneel is geworden voor het regime. Hierbij worden geraffineerde methoden ingezet, zoals het plaatsen van valse IT-werknemers binnen buitenlandse bedrijven om van binnenuit toegang te krijgen tot vitale systemen.

2.3 Iran: Systematische Aanvallen op Overheidsinstellingen

De Iraanse hackergroep **MuddyWater** (ook bekend als Static Kitten) heeft zijn capaciteiten gedemonstreerd met systematische aanvallen op overheidsinstellingen wereldwijd. De groep is verantwoordelijk voor een grootschalige phishingcampagne die gericht was op meer dan 100 overheidsinstanties. Via besmette Word-documenten werd de 'Phoenix'-backdoor geïnstalleerd, een geavanceerd stuk malware dat in staat is systeeminformatie te verzamelen, verbinding te maken met een command-and-control-server en data te exfiltreren. Deze operaties tonen de

intentie en het vermogen van Iran om op grote schaal digitale spionage uit te voeren tegen overheidsdoelwitten.

2.4 Cyberspanningen tussen de Verenigde Staten en China

De oplopende spanningen tussen de Verenigde Staten en China uiten zich ook in wederzijdse beschuldigingen van cyberaanvallen op kritieke infrastructuur. Recentelijk beschuldigde China de Amerikaanse National Security Agency (NSA) van het uitvoeren van aanvallen op zijn nationale tijdcentrum. Een aanval op een dergelijke faciliteit vormt een strategische dreiging voor het vermogen van een land om kritieke operaties te synchroniseren. Dit kan potentieel uiteenlopende sectoren ontwrichten, van financiële markttransacties en het beheer van het energienet tot militaire command-and-control-systemen, wat het een hoogwaardig strategisch doelwit maakt in hybride oorlogsvoering. Deze ontwikkelingen illustreren de complexiteit en de risico's van de toenemende digitale confrontatie tussen wereldmachten.

De dreiging is echter niet beperkt tot staten; een professioneel en zeer georganiseerd ecosysteem van cybercriminelen vormt een even grote uitdaging.

3.0 De Evolutie van Cybercriminaliteit en Agressieve Aanvalsmethoden

Het cybercriminele ecosysteem heeft zich de afgelopen jaren sterk geprofessionaliseerd. Aanvallers hanteren geavanceerde businessmodellen en ontwikkelen technieken die traditionele beveiligingsmaatregelen steeds vaker omzeilen. Deze professionaliseringsslag heeft geleid tot een aanhoudende en dynamische dreiging voor Nederlandse organisaties, variërend van MKB-bedrijven tot kritieke dienstverleners.

3.1 De Impact van Ransomware-as-a-Service (RaaS)

Het Ransomware-as-a-Service (RaaS) model heeft de drempel voor het uitvoeren van gijzelsoftware-aanvallen aanzienlijk verlaagd en de impact ervan vergroot. Recente incidenten in Nederland illustreren de ernstige gevolgen. De aanval op afvalverwerker **Omrin** leidde tot aanzienlijke operationele verstoringen. Bij Albert Heijn-franchisenemer **Bun** werden door de **ThreeAM**-groep duizenden persoonsgegevens van medewerkers gestolen, waaronder kopieën van paspoorten, salarisinformatie en medische gegevens, met de dreiging deze publiek te maken. De

sectorbrede en internationale schaal van deze dreiging wordt onderstreept door de aanval op een Frans ziekenhuis, dat gedwongen werd terug te vallen op pen en papier, en de wereldwijde campagne van de **Qilin**-groep die al 700 organisaties heeft getroffen.

3.2 De Professionalisering van de Infostealer-Malware-Industrie

Er is een geavanceerd crimineel netwerk ontstaan rondom 'infostealer'-malware, die is ontworpen om op grote schaal inloggegevens en andere gevoelige data te stelen. De omvang van dit probleem is immens: recentelijk werden **183 miljoen gecompromitteerde e-mailadressen**, afkomstig uit stealer logs, toegevoegd aan de database van Have I Been Pwned. Onderzoek toont aan dat één enkel Telegram-account dagelijks tot 50 miljoen gestolen inloggegevens kan verwerken. Malwarefamilies als **SnakeStealer**, **Lumma Stealer** en **SharkStealer** worden steeds geavanceerder. SharkStealer maakt bijvoorbeeld gebruik van de blockchain voor command-and-control (C2) communicatie, een techniek die traditionele detectiemethoden effectief omzeilt. De verwachting is dat deze 'as-a-service' modellen voor datadiefstal verder zullen commercialiseren, wat zal leiden tot een toename van laagdrempelige, maar zeer impactvolle, aanvallen op Nederlandse organisaties.

3.3 Verfijning van Social Engineering en Phishingtechnieken

Analyse van recente campagnes onthult een duidelijke trend richting het uitbuiten van de raakvlakken tussen technologie en menselijk vertrouwen. Aanvallers focussen op het omzeilen van moderne beveiligingscontroles zoals MFA en misbruiken de geloofwaardigheid van legitieme platforms zoals TikTok om malware te verspreiden. De meest effectieve recente methoden zijn:

- **MFA-omzeiling:** De inzet van geavanceerde phishing-sites die specifiek zijn ontworpen om niet alleen wachtwoorden, maar ook de eenmalige codes (OTP's) van multi-factor authenticatie (MFA) te stelen.
- **Misbruik van legitieme platformen:** Kwaadaardige PowerShell-scripts worden verspreid via populaire platforms zoals **TikTok**, vermomd als activatiegidsen voor software, om zo infostealer-malware te installeren.
- **Aanvallen op mobiel bankieren:** Zoals de aanval op klanten van de Belgische bank **KBC**, waarbij oplichters zich voordeden als

telecommedewerkers en slachtoffers overhaalden een malafide app via WhatsApp te installeren om zo controle over hun bankrekening te krijgen.

- **Spearphishing op hoog niveau:** De **PhantomCaptcha**-aanval, gericht op humanitaire organisaties zoals het Rode Kruis en UNICEF in de context van de oorlog in Oekraïne, gebruikte valse CAPTCHA-verificaties om een Remote Access Trojan (RAT) te installeren.

De professionalisering van de cybercrime-economie is een overkoepelende trend. Er is een duidelijke arbeidsverdeling zichtbaar, met gespecialiseerde actoren zoals malware-ontwikkelaars, 'initial access brokers' en ransomware-filialen, die samen een ecosysteem vormen dat legitieme bedrijfsmodellen spiegelt. Dit maakt de dreiging niet alleen geavanceerder, maar ook schaalbaarder en veerkrachtiger.

De effectiviteit van deze criminele methoden is direct afhankelijk van de technologische kwetsbaarheden die zij misbruiken, welke in het volgende hoofdstuk worden onderzocht.

4.0 Technologische Kwetsbaarheden als Primaire Aanvalsvectoren

Ongeacht de actor of de aanvalsmethode maken cyberaanvallen vrijwel altijd misbruik van specifieke technologische zwakheden in software, hardware of netwerkconfiguraties. De snelle digitalisering en de toenemende complexiteit van moderne IT-omgevingen creëren een constant groeiend aanvalsoppervlak, waarbij kwetsbaarheden de primaire toegangspoorten voor aanvallers vormen.

4.1 Kritieke Kwetsbaarheden in Bedrijfssoftware en Webapplicaties

Een aanzienlijk deel van de succesvolle aanvallen is terug te voeren op het niet tijdig patchen van bekende, kritieke kwetsbaarheden in wijdverbreide bedrijfssoftware. De onderstaande tabel geeft een overzicht van recente, ernstige dreigingen.

Software/Platform	Geïdentificeerde Dreiging
Adobe Commerce / Magento	Kritieke kwetsbaarheid die volledige overname van webshops mogelijk maakt (Remote Code Execution, RCE).

Microsoft (ASP.NET, WSUS, M365)	Diverse ernstige lekken, waaronder HTTP-request smuggling in Kestrel, een RCE-kwetsbaarheid in WSUS (CVSS 9.8) en misbruik van de 'Direct Send'-functie in Exchange Online voor phishing.
Ivanti Connect Secure	Een RCE-kwetsbaarheid waarvoor een publiek beschikbare Python-exploit is ontdekt, wat de kans op misbruik aanzienlijk vergroot.
WordPress Plugins (GutenKit, Hunk Companion)	Actief misbruikte kwetsbaarheden die de installatie van willekeurige plugins en RCE mogelijk maken op tienduizenden websites, ondanks dat patches al lang beschikbaar zijn.
Diverse Enterprise Tools	Actief misbruikte kwetsbaarheden in veelgebruikte tools zoals **JetBrains TeamCity**, **Atlassian Confluence**, **Metabase** en **Redis**.

4.2 Risico's in Netwerkinfrastructuur en IoT-Apparatuur

Netwerkapparatuur zoals firewalls en routers, evenals Internet-of-Things (IoT)-apparaten, vormen vaak de frontlinie van de digitale verdediging van een organisatie. Kwetsbaarheden in deze apparaten bieden aanvallers een directe ingang tot interne netwerken. Recente voorbeelden zijn een RCE-kwetsbaarheid in **WatchGuard Firebox-firewalls**, ernstige lekken in **Zyxel firewalls** en **TP-Link Omada Gateways**, en kwetsbaarheden in de **Philips Hue Bridge** die tijdens Pwn2Own werden onthuld. De wijdverspreide aanwezigheid van 2.573 kwetsbare WatchGuard-firewalls in Nederland en België vormt een significant risico voor de digitale soevereiniteit, omdat deze apparaten als springplank kunnen dienen voor grootschalige aanvallen op onze vitale infrastructuur.

4.3 Cloud Security: Afhankelijkheid en Geconfigureerde Risico's

De toenemende afhankelijkheid van een beperkt aantal grote, Amerikaanse cloud-leveranciers brengt significante risico's met zich mee. De **Autoriteit Financiële Markten (AFM) en De Nederlandsche Bank (DNB)** hebben gewaarschuwd voor de concentratierisico’s, waarbij een storing bij één leverancier de gehele financiële sector kan ontwrichten. Naast deze strategische afhankelijkheid vormen verkeerde configuraties een direct risico. Een recente rechtszaak tegen een Friese IT-

leverancier onderstreept dit. De leverancier werd aansprakelijk gesteld voor de schade na een hack op een Azure-omgeving, omdat **multi-factor authenticatie (MFA)** niet verplicht was ingeschakeld, waardoor een aanvaller de servers kon misbruiken voor cryptomining.

Deze analyse van diepgewortelde technologische kwetsbaarheden toont aan dat een puur defensieve houding ontoereikend is; het vereist een proactieve, nationale strategie die zowel de technische weerbaarheid verhoogt als de politieke en maatschappelijke context adresseert.

5.0 De Noodzaak voor een Robuuste Nationale Cyberdefensiestrategie

De bevindingen in dit rapport schetsen een dreigingslandschap dat zowel veelzijdig als hardnekkig is. De professionele ransomware-campagnes uit hoofdstuk 3, direct mogelijk gemaakt door de wijdverspreide technologische kwetsbaarheden geanalyseerd in hoofdstuk 4, van ongepatchte bedrijfssoftware tot verkeerd geconfigureerde cloudomgevingen, vereisen een gecoördineerde, proactieve en weerbare nationale cyberdefensiestrategie. Het beschermen van de Nederlandse economische, maatschappelijke en democratische belangen in het digitale tijdperk is een strategisch imperatief dat een brede, nationale respons vereist.

5.1 Politieke Consensus en Beleidsrichtingen

Uit de verkiezingsprogramma's voor 2025 blijkt een brede politieke consensus over de *noodzaak* om te investeren in digitale veiligheid. Hoewel de accenten verschillen, erkennen vrijwel alle partijen de urgentie van het thema. De voorgestelde beleidsrichtingen kunnen worden gegroepeerd rond de volgende kernpunten:

1. **Versterking van Europese Samenwerking:** Partijen als de VVD en Volt pleiten expliciet voor een gezamenlijke digitale verdediging en de oprichting van een Europese digitale veiligheidsunie. Deze visie sluit aan bij de operationele realiteit waarin de AIVD en MIVD hun focus al meer op samenwerking met Europese partners leggen, mede ingegeven door de toegenomen Russische dreiging.
2. **Digitale Autonomie en Soevereiniteit:** In lijn met de waarschuwingen van de AFM en DNB leggen partijen als het CDA en GroenLinks/PVDA de nadruk op het verminderen van de strategische afhankelijkheid van buitenlandse, met

name Amerikaanse, techbedrijven. Het doel is de digitale soevereiniteit van Nederland en Europa te vergroten.

3. **Versterking van Wetgeving en Toezicht:** Voorstellen van de ChristenUnie en JA21 richten zich op het aanscherpen van regelgeving en het vergroten van de verantwoordelijkheid van zowel de overheid als het bedrijfsleven voor het beveiligen van digitale systemen en data.
4. **Investeren in Kennis en Ethiek:** Partijen als D66 en GroenLinks/PVDA benadrukken het belang van een ethisch kader voor de ontwikkeling en inzet van nieuwe technologieën zoals AI. Dit wordt ondersteund door de oproep van de Autoriteit Persoonsgegevens om AI-geletterdheid verplicht te stellen voor personeel binnen organisaties om een verantwoord gebruik te waarborgen.

5.2 Strategische Aanbevelingen en Conclusie

De cyberdreigingen waarmee Nederland wordt geconfronteerd zijn reëel, veelzijdig en constant in ontwikkeling. Een effectieve nationale strategie kan zich niet beperken tot louter technologische oplossingen. Het vereist een integrale aanpak die rust op meerdere pijlers: intensieve internationale samenwerking binnen de EU en met gelijkgestemde partners, robuuste publiek-private partnerschappen om informatie te delen en gezamenlijk op te treden, en heldere wetgevende kaders die verantwoordelijkheden vastleggen en toezicht mogelijk maken.

Uiteindelijk is de kern van een succesvolle strategie het verhogen van de digitale weerbaarheid van de gehele samenleving, van individuele burgers en het MKB tot de vitale infrastructuur en de overheid zelf. Het implementeren van een dergelijke alomvattende en toekomstbestendige strategie is geen keuze, maar een urgente prioriteit voor het waarborgen van de veiligheid, stabiliteit en welvaart van Nederland in het digitale tijdperk.