Week 47-2025

Analyse van het Geopolitieke Cyberdreigingslandschap: Tactieken, Actoren en Strategische Implicaties

1.0 Inleiding: De Convergentie van Digitale en Fysieke Conflictzones

Het hedendaagse cyberdreigingslandschap wordt gekenmerkt door een versnelde convergentie van de digitale en fysieke wereld, waarbij de grenzen tussen beide domeinen vervagen. Incidenten zijn niet langer beperkt tot datadiefstal of de verstoring van onlinediensten; ze manifesteren zich steeds vaker als doelgerichte acties met tastbare, kinetische gevolgen. De recente sabotage van een cruciale Poolse spoorlijn, uitgevoerd door Oekraïense staatsburgers in opdracht van Russische inlichtingendiensten, illustreert hoe digitale planning en fysieke aanvallen samensmelten tot een geïntegreerde strategie. Deze hybride benadering, waarbij cyberoperaties dienen ter voorbereiding, ondersteuning of zelfs als alternatief voor militaire acties, vormt een fundamentele uitdaging voor de (inter)nationale veiligheid.

Dit document biedt een strategische analyse van de meest recente tactieken en de modus operandi van de belangrijkste statelijke actoren die in dit domein opereren. Door hun methoden te ontleden en hun strategische doelen te duiden, wordt een helder beeld geschetst van de implicaties voor de veiligheid van vitale sectoren en de stabiliteit van de internationale orde. De volgende analyse richt zich op de specifieke technieken die door deze actoren worden ingezet om hun invloed te maximaliseren en detectie te omzeilen.

2.0 Het Evoluerende Tactische Arsenaal van Statelijke Actoren

De strategische wedloop in cyberspace wordt gedreven door technologische innovatie. Deze sectie analyseert de tactische verschuiving van statelijke actoren naar methoden die inherent vertrouwen in systemen misbruiken om defensieve maatregelen te omzeilen en hun impact te maximaliseren. Dit resulteert in een operationele voorkeur voor geavanceerde technieken die zowel complexe softwarekwetsbaarheden als het menselijk vertrouwen in digitale processen exploiteren. De meest effectieve campagnes combineren vaak meerdere van deze technieken om een gelaagde aanval op te bouwen die moeilijk te detecteren en te mitigeren is.

2.1 DLL-Sideloading: Misbruik van Vertrouwen in Legitieme Software

De persistente utiliteit van DLL-sideloading onder elite statelijke actoren onderstreept een strategische voorkeur voor technieken die inherent vertrouwen binnen besturingssystemen exploiteren, een kwetsbaarheid die puur signature-based verdedigingsmechanismen moeilijk kunnen adresseren. **DLL-sideloading** is een techniek waarbij aanvallers een kwaadaardig DLL-bestand (Dynamic Link Library), vaak met dezelfde naam als een legitieme maar afwezige DLL, in de map van een vertrouwde applicatie plaatsen. Wanneer de applicatie start, laadt deze onbedoeld de kwaadaardige DLL in plaats van de legitieme versie, waardoor de aanvaller code kan uitvoeren binnen de context van een vertrouwd en vaak digitaal ondertekend proces.

Deze methode is bijzonder effectief omdat de kwaadaardige activiteit wordt gemaskeerd door een legitiem programma, wat detectie door traditionele beveiligingsmaatregelen zoals antivirussoftware en applicatie-whitelisting bemoeilijkt. Recente incidenten tonen de brede inzet door diverse statelijke actoren aan:

- De aan Rusland gelinkte groep **APT28 (Fancy Bear)** integreert DLL-sideloading via OneDrive.exe als integraal onderdeel van de *NotDoor* malware-operatie.
- Een **China-Nexus APT-groep** zette de techniek in bij aanvallen op overheden in Zuidoost-Azië, waarbij legitieme software van Adobe en OBS werd misbruikt.
- Noord-Koreaanse actoren pasten de methode toe in **Operation DreamJob** door een kwaadaardige DLL te verpakken met een legitieme versie van SumatraPDF.exe.
- Chinese hackers misbruikten DLL-sideloading via ETDCtrlHelper.exe om de **ShadowPad** malware te verspreiden na het exploiteren van een kwetsbaarheid in Microsoft WSUS.

2.2 Exploitatie van Zero-Day Kwetsbaarheden: De Race Tegen de Klok

Zero-day kwetsbaarheden – beveiligingslekken die nog onbekend zijn bij de softwareontwikkelaar en waarvoor dus nog geen patch bestaat – vertegenwoordigen een van de meest waardevolle middelen voor een aanvaller. Het bezit van een zero-day biedt een tijdelijk, maar krachtig, venster van opportuniteit om systemen te compromitteren voordat verdedigers kunnen reageren. Zowel statelijke actoren als

geavanceerde cybercriminele groepen investeren aanzienlijk in het ontdekken en verwerven van deze kwetsbaarheden.

Incident/Bevinding	Context en Impact
Clop-extortiegroep misbruikt Oracle zero-day	De groep gebruikte een zero-day kwetsbaarheid in Oracle E-Business Suite om een datalek bij technologiebedrijf Logitech te veroorzaken.
Verkoop van Windows/Office zero-day	Op een darkweb-marktplaats werd een zero-day exploit te koop aangeboden voor $300.000, die code-uitvoering op afstand mogelijk maakt zonder interactie van de gebruiker.
Zero-day in Microsoft-ondertekende driver	Een kwetsbaarheid in een door Microsoft ondertekende driver werd op het darkweb aangeboden als middel om EDR/XDR-beveiligingssystemen te omzeilen.
Samenwerking Kimsuky en Lazarus	Noord-Koreaanse groepen bundelden hun krachten om gezamenlijk zero-day kwetsbaarheden te misbruiken voor spionage en de diefstal van cryptocurrency.

2.3 De Rol van Kunstmatige Intelligentie (AI) in Cybercriminaliteit

De opkomst van toegankelijke en krachtige AI-modellen heeft een nieuw tijdperk ingeluid voor cybercriminaliteit. Waar geavanceerde aanvallen voorheen specialistische kennis vereisten, verlaagt AI de drempel aanzienlijk en vergroot het de schaal en effectiviteit van kwaadaardige operaties.

1. **Automatisering van Social Engineering:** AI wordt ingezet om 'pig-butchering' fraude op te schalen. AI-assistenten creëren zeer geloofwaardige valse identiteiten met door AI gegenereerde foto's en onderhouden geautomatiseerde, overtuigende gesprekken met slachtoffers, waardoor de operaties efficiënter en moeilijker te herkennen zijn.
2. **Verlaging van de Technische Drempel:** Tools die op het darkweb worden aangeboden, zoals de AI-tool *Xanthorox*, stellen criminelen met beperkte technische vaardigheden in staat om op aanvraag kwaadaardige code te genereren. Met eenvoudige tekstinstructies kan de tool functionele malware, inclusief ransomware, produceren.

3. **Genereren van Geloofwaardige Desinformatie:** AI-technologie kan stemmen en muziek genereren die nauwelijks van echt te onderscheiden zijn. Dit opent nieuwe mogelijkheden voor digitale misleiding en identiteitsfraude, zoals deepfake-audio voor social engineering of het creëren van grootschalige desinformatiecampagnes.
4. **Geautomatiseerde Spionage-operaties:** Hoewel er scepsis heerst binnen de cybersecuritygemeenschap, claimde AI-bedrijf Anthropic dat de door China gesponsorde groep GTG-1002 hun Claude Code AI-model misbruikte om een grotendeels geautomatiseerde spionageoperatie uit te voeren. Dit illustreert de potentie, maar ook de onzekerheid, rond de inzet van AI voor autonome cyberaanvallen.

De inzet van dit geavanceerde tactische arsenaal is niet willekeurig, maar wordt gedreven door de specifieke strategische doelstellingen van de geopolitieke actoren die erachter schuilgaan.

3.0 Profielanalyse van Geopolitieke Dreigingsactoren

Hoewel de gebruikte tactieken vaak overlappen, verschillen de strategische doelstellingen en de modus operandi van statelijke actoren significant. Deze verschillen worden gevormd door de geopolitieke ambities, economische behoeften en militaire doctrines van de respectievelijke landen. De volgende sectie analyseert de specifieke activiteiten van Noord-Korea, China, Rusland en Iran op basis van recente incidenten om een duidelijker profiel van deze dreigingsactoren te schetsen.

3.1 Noord-Korea: Financiële Gewin en Gerichte Spionage

Noord-Koreaanse hackergroepen opereren met een duidelijke dubbele focus: het genereren van illegale inkomsten om het regime te financieren en het stelen van strategisch waardevolle informatie, met name op militair en technologisch gebied.

- **Infiltratie en Inkomstengeneratie:** Een geraffineerde methode omvat het plaatsen van Noord-Koreaanse spionnen bij Amerikaanse techbedrijven. Onder valse identiteiten bemachtigen zij ICT-posities en gebruiken 'laptop-farms' – ruimtes waar laptops op afstand vanuit Noord-Korea worden bestuurd – om inkomsten te genereren en bedrijfsnetwerken te infiltreren. De APT38-groep is gelinkt aan grootschalige diefstal van cryptocurrency die op deze manier wordt gefaciliteerd.

- **Technologische Spionage:** De Lazarus-groep heeft de *ScoringMathTea* Remote Access Trojan (RAT) ontwikkeld, specifiek gericht op bedrijven die UAV-technologie (drones) aan Oekraïne leveren. Het doel is het stelen van productiekennis en intellectueel eigendom om de eigen militaire capaciteiten te versterken.
- **Gecoördineerde Operaties:** Een zorgwekkende samenwerking is geobserveerd tussen de Kimsuky- en Lazarus-groepen. Deze operaties volgen een gefaseerd model: Kimsuky fungeert als de initiële toegangs- en verkenningseenheid via gerichte phishingcampagnes. Zodra toegang is verkregen, neemt Lazarus de operatie over om geavanceerde zero-day kwetsbaarheden te misbruiken voor diepere infiltratie en de diefstal van cryptocurrency.

3.2 China: Economische en Strategische Inlichtingenvergaring

De cyberoperaties van China zijn overwegend gericht op het verkrijgen van een economisch en geopolitiek voordeel door middel van grootschalige spionage. De tactieken zijn vaak geavanceerd en gericht op het onopgemerkt verzamelen van data op de lange termijn.

- **Spionage via Social Engineering:** De Britse veiligheidsdienst MI5 heeft gewaarschuwd voor Chinese spionage via LinkedIn. Hierbij leggen nep-headhunters contact met doelwitten, waaronder parlementsleden en andere belangrijke functionarissen, om gevoelige informatie te ontfutselen.
- **Geraffineerde Supply Chain Aanvallen:** De groep APT24 voerde een geavanceerde supply chain-aanval uit door een Taiwanees marketingbedrijf te compromitteren dat JavaScript-bibliotheken levert. Door kwaadaardige code in deze gedeelde bibliotheken te injecteren, was de groep in staat duizenden websites van klanten te infecteren en bezoekers met malware te bestoken.
- **Exploitatie van Bedrijfsinfrastructuur:** Chinese hackers misbruikten een kritieke kwetsbaarheid in Microsoft WSUS (Windows Server Update Services). Deze kwetsbaarheid werd ingezet om de *ShadowPad* malware te verspreiden via de DLL-sideloading techniek, waarmee zij volledige controle over gecompromitteerde bedrijfsnetwerken konden verkrijgen en een complete, gelaagde aanvalsketen demonstreerden.

3.3 Rusland: Destabilisatie door Hybride Dreigingen

De Russische strategie kenmerkt zich door een naadloze integratie van digitale aanvallen, fysieke sabotage en desinformatie, met als doel Europese landen te destabiliseren en de steun voor Oekraïne te ondermijnen.

- **Fysieke Sabotage:** Een explosie op de spoorlijn tussen Warschau en Lublin in Polen wordt door de Poolse regering beschouwd als een doelbewuste sabotageactie. De actie werd in opdracht van Russische inlichtingendiensten uitgevoerd door twee Oekraïense staatsburgers, wat het gebruik van buitenlandse proxy's in hybride operaties illustreert.
- **Digitale Infiltratie:** De aan APT28 (Fancy Bear) gelinkte *NotDoor* malware wordt ingezet om systemen te infiltreren. Deze malware maakt gebruik van Outlook-macro’s en DLL-sideloading om onopgemerkt gegevens te stelen, wat wijst op een aanhoudende focus op heimelijke spionage.
- **Ondersteuning van Cybercriminaliteit:** Rusland faciliteert cybercriminaliteit door een veilige haven te bieden aan 'bulletproof' hostingproviders zoals Media Land. Deze providers ondersteunen de infrastructuur van beruchte ransomwarebendes als LockBit. Deze stilzwijgende staatssteun voor criminele infrastructuur dient een dubbel doel: het biedt plausibele ontkenning en bevordert tegelijkertijd een disruptief ecosysteem dat kan worden ingezet voor staatsdoeleinden.

3.4 Iran: Cyberoperaties als Verlengstuk van Militaire Acties

Iraanse hackergroepen zetten hun cybercapaciteiten steeds vaker in ter directe ondersteuning van fysieke, militaire operaties. De groep **Imperial Kitten**, die gelinkt wordt aan de Iraanse Revolutionaire Garde (IRGC), heeft dit op duidelijke wijze gedemonstreerd. Door het hacken van het **Automatic Identification System (AIS)** en CCTV-camera's van schepen verzamelden zij real-time informatie over maritieme doelen. Deze digitale verkenning diende niet alleen spionagedoeleinden, maar werd direct gebruikt om de coördinatie en effectiviteit van fysieke raketaanvallen te verbeteren.

Dit patroon van digitaal ondersteunde kinetische aanvallen door diverse statelijke actoren bevestigt dat cyberoperaties niet langer een afzonderlijk slagveld vormen,

maar een kritisch en geïntegreerd onderdeel zijn van de moderne hybride oorlogsvoering.

4.0 De Realiteit van Hybride Oorlogsvoering

Hybride oorlogsvoering is de strategische combinatie van conventionele militaire acties, irreguliere tactieken, cyberaanvallen en desinformatie om de politieke, militaire en maatschappelijke structuren van een tegenstander te ondermijnen. Recente gebeurtenissen tonen onomstotelijk aan dat dit geen theoretisch concept meer is, maar een actieve en groeiende dreiging voor de (inter)nationale veiligheid. Staten gebruiken een gecoördineerde aanpak over meerdere domeinen heen om hun doelen te bereiken, vaak onder de drempel van een openlijk gewapend conflict.

De onderstaande tabel illustreert de multidimensionale aard van deze dreigingen aan de hand van recente incidenten.

Domein	Incident	Strategisch Doel
Fysiek & Digitaal	Sabotage van de Poolse spoorlijn door Rusland.	Verstoring van logistieke steun aan Oekraïne en destabilisatie van een NAVO-lidstaat.
Maritiem & Digitaal	Iraanse hackers die AIS-data gebruiken voor raketaanvallen.	Vergroten van de effectiviteit van kinetische aanvallen en projectie van militaire macht.
Civiel & Digitaal	Nederlandse overheidscampagne 'Denk vooruit' als reactie op mogelijke stroomuitval door cyberaanvallen.	Versterken van maatschappelijke weerbaarheid tegen aanvallen op kritieke infrastructuur.

Deze geïntegreerde dreigingen hebben diepgaande strategische implicaties voor zowel overheden als private organisaties.

5.0 Strategische Implicaties en Conclusies

De geanalyseerde dreigingen en tactieken tonen aan dat cyberaanvallen niet langer geïsoleerde technische incidenten zijn, maar structurele componenten van geopolitieke competitie en conflict. Deze verschuiving heeft diepgaande strategische implicaties voor de veiligheid van vitale sectoren, de stabiliteit van de economie en de soevereiniteit van naties. Het vermogen om digitale netwerken te beschermen is

direct verbonden met het vermogen om de fysieke en economische veiligheid te waarborgen.

De belangrijkste strategische implicaties zijn als volgt:

1. **Verhoogde Kwetsbaarheid van Vitale Sectoren:** Kritieke infrastructuur, zoals de gezondheidszorg, transport en energie, is een primair doelwit geworden. Netwerkstoringen bij ziekenhuizen, zoals bij het **Máxima Medisch Centrum**, kunnen direct leiden tot het annuleren van operaties en behandelingen. De datadiefstal bij de Italiaanse spoorwegen (**FS Italiane**) via een dienstverlener toont de kwetsbaarheid van transportnetwerken. Wereldwijde storingen bij centrale internetinfrastructuur, zoals de **Cloudflare-storing**, leggen de systeembrede risico's bloot die ontstaan door afhankelijkheid van een beperkt aantal cruciale spelers.
2. **Systemische Risico's door Supply Chain Aanvallen:** Aanvallers richten zich steeds vaker op de software supply chain. Door leveranciers van veelgebruikte software (zoals **Citrix** en **Oracle**) of externe IT-dienstverleners (zoals **Almaviva**) te compromitteren, kunnen aanvallers een kettingreactie veroorzaken die de veiligheid van honderden of zelfs duizenden organisaties tegelijkertijd ondermijnt. Dit creëert een systemisch risico dat moeilijk te beheren is voor individuele organisaties.
3. **Uitdagingen voor Digitale Soevereiniteit:** De afhankelijkheid van buitenlandse technologie en dienstverleners creëert politieke en veiligheidsdilemma's. De overname van het Nederlandse cloudbedrijf **Solvinity**, dat vitale diensten als DigiD host, door een Amerikaans bedrijf leidde tot Kamervragen over de potentiële invloed van Amerikaanse wetgeving (zoals de CLOUD Act) op de privacy van Nederlandse overheidsgegevens. Dit incident staat niet op zichzelf en voedt de bredere EU-inspanningen om de digitale soevereiniteit te versterken en de controle over kritieke digitale infrastructuur te behouden.

De convergentie van digitale en fysieke dreigingen, aangedreven door geopolitieke motieven, vereist een fundamentele herziening van de benadering van cyberveiligheid. Een reactieve en gefragmenteerde aanpak volstaat niet langer. Het is noodzakelijk om te investeren in een integrale, proactieve en internationale strategie die publiek-private samenwerking bevordert, de weerbaarheid van kritieke

infrastructuren verhoogt en de digitale soevereiniteit waarborgt. Alleen door deze gecoördineerde inspanningen kan de weerbaarheid tegen deze geavanceerde en geopolitiek gemotiveerde dreigingen effectief worden verhoogd.