
Het Vervaagde Slagveld
Een Analyse van Convergerende Cyberdreigingen
Intelligence Briefing: 9 december 2025
Cybercrimeinfo

De Grenzen Vervagen: Een Nieuw Dreigingsparadigma

De gebeurtenissen van de afgelopen dag tonen een dreigingslandschap waarin **traditionele scheidslijnen verdwijnen**. De **grens tussen fysieke sabotage en digitale oorlogsvoering**, **staat en crimineel**, en **aanval en verdediging** is diffuser dan ooit. Deze briefing analyseert deze convergentie aan de hand van vier kernthema's.

1. De Geopolitieke Arena

Hoe statelijke actoren digitale middelen inzetten voor fysieke en geopolitieke impact.

2. De Fundamenten onder Druk

De systematische kwetsbaarheden in de kern van onze digitale infrastructuur.

3. De Economie van Cybercrime

De industriële schaal van financiële afpersing en ontwrichting.

4. De Georganiseerde Reactie

De tegenbeweging van justitie, regelgevers en veiligheidsdiensten.

Van Digitale Inbraak naar Fysieke Sabotage: Kritieke Infrastructuur in het Vizier

Case 1 - Spoorwegsabotage in Polen

Kernpunt:
Polen vraagt Interpol om een Red Notice voor twee Oekraïners die in opdracht van de Russische militaire inlichtingendienst het Poolse spoorwegnet saboteerden (november 2025).

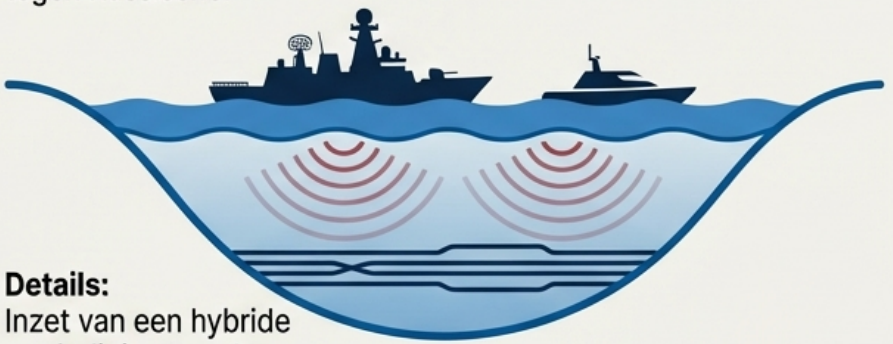
Details:
Doelwit: strategische spoorlijn naar Wit-Rusland, essentieel voor o.a. humanitaire hulp.

Quote:
Beschreven door Polen als 'staatsterrorisme'.

Case 2 - Verdediging van Onderzeese Kabels

Kernpunt:
Het VK lanceert 'Atlantic Bastion'-programma om onderzeese kabels en pijpleidingen te beschermen tegen Russische.

Impamnst:
AI -gesturan eert 'hybride 'verdedigingsmacht' via om beschermen lamels tegen Russische spionageschepen.

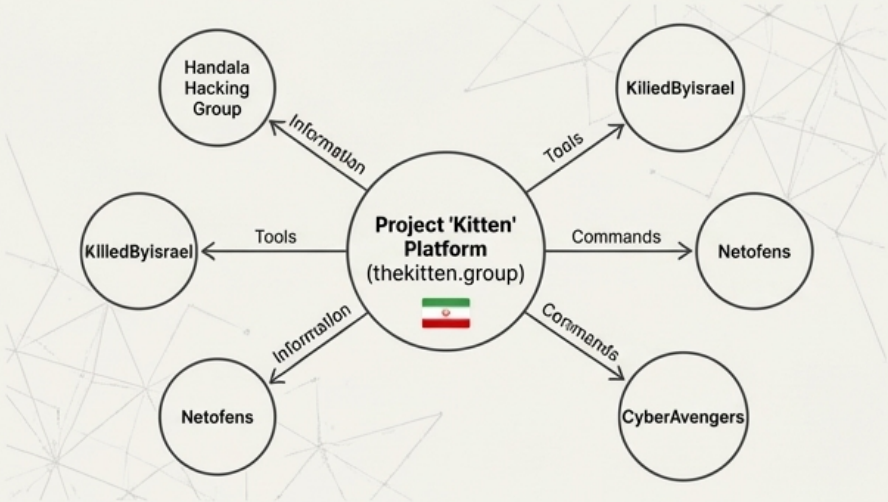


Details:
Inzet van een hybride verdedigingsmacht: oorlogsschepen, autonome vaartuigen en AI-gestuurde akoestische detectie.

99% van de Britse data loopt via deze kabels.

De Instrumenten van Hybride Oorlogsvoering: Gecoördineerde Hacktivisten en Autonome Systemen

Case 1 - Project 'Kitten'



Kernpunt: Een gecoördineerd platform, met vermoedelijke Iraanse banden, faciliteert hacktivistische groepen bij aanvallen op Israëlische doelen en kritieke infrastructuur.

Technische Details: Gecentraliseerde infrastructuur gehost op Iraanse servers (Pars Parva Systems) voor het delen van tools, doelen en communicatie.

Case 2 - Drones als "Vliegende Computers"

Kernpunt: BAE Systems waarschuwt: drones zijn vliegende computers zonder firewalls, eenvoudig te hacken voor spionage of aanval.

Tier 1 (Low Threat)
Commerciële drones (80% van het totaal).

Tier 2 (Medium Threat)
Aangepaste, vaste-vleugel drones.

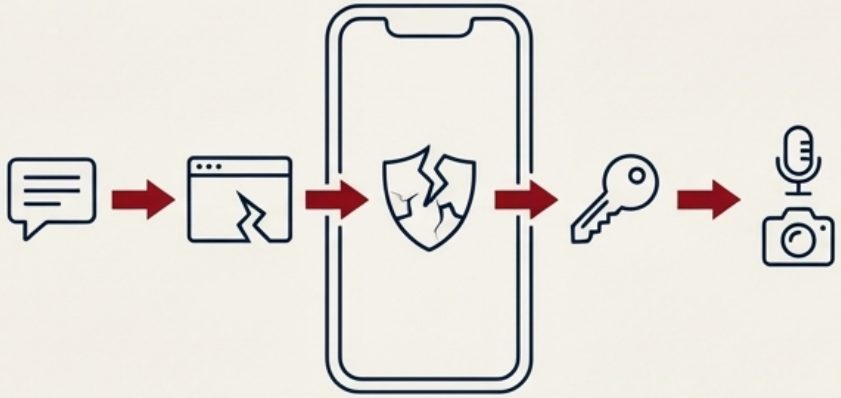
Tier 3 (High Threat)
Geavanceerde militaire systemen (Orlan-10, Shahed-136).

Dreiging varieert van commerciële drones (80% van het totaal) tot geavanceerde militaire systemen.

Toekomstige dreiging van dronezwermen: 'botnets in de lucht'.

De Fundamenten Ondermijnd: Van Mobiele Apparaten tot de Cloud Hypervisor

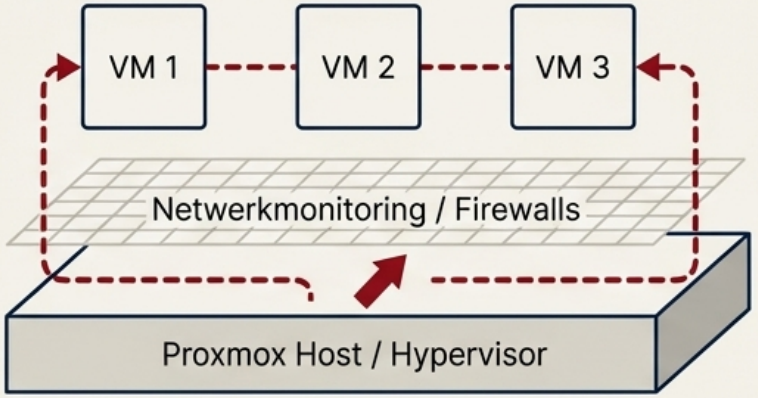
Case 1 - Predator Spyware



Kernpunt: Commercieel spywarebedrijf Intellexa misbruikte sinds 2021 maar liefst **15 zero-day kwetsbaarheden** om via versleutelde berichtenapps iOS- en Android-apparaten aan te vallen.

Mechanisme: Complexe exploit-ketens voor Remote Code Execution, Sandbox Escape en Privilege Escalation om volledige controle over microfoon en camera te krijgen.

Case 2 - Proxmox Hypervisor Kwetsbaarheid

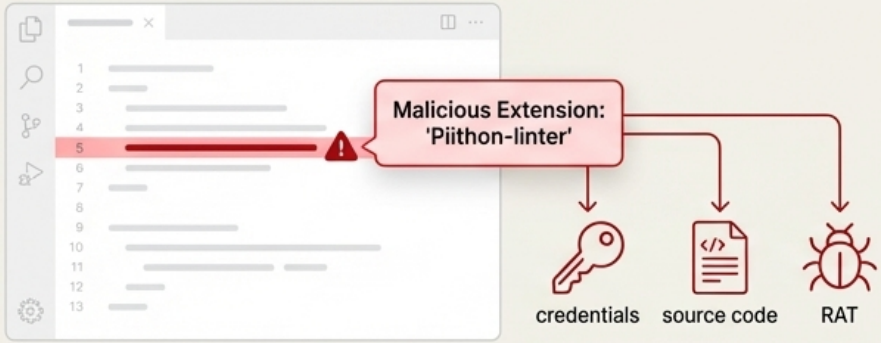


Kernpunt: Aanvallers kunnen via **'living off the hypervisor'**-technieken en de QEMU-gastagent onopgemerkt lateraal bewegen tussen virtuele machines.

Impact: Toegang tot alle VM's op een host zonder detecteerbare netwerkverbindingen of firewall-logs, wat traditionele detectie omzeilt.

De Software Supply Chain als Doelwit: Compromittering bij de Bron

Case 1 - Kwaadaardige Ontwikkeltools

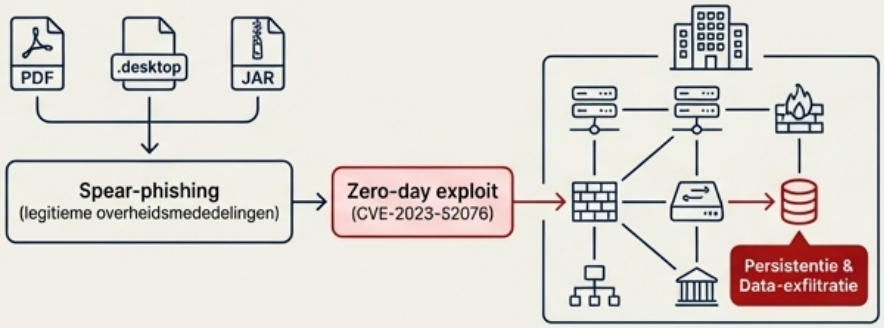


Kernpunt: Hackers publiceren schadelijke extensies op de marktplaatsen van populaire editors zoals Visual Studio Code en Cursor AI.

Voorbeeld: Een verkeerd gespelde ‘Pithon-linter’ extensie werd goedgekeurd en kon broncode en credentials stelen, en een RAT installeren.

Mechanisme: De extensie wordt automatisch uitgevoerd bij het opstarten van de editor en kan detecteren of beveiligingssoftware draait.

Case 2 - APT32/OceanLotus

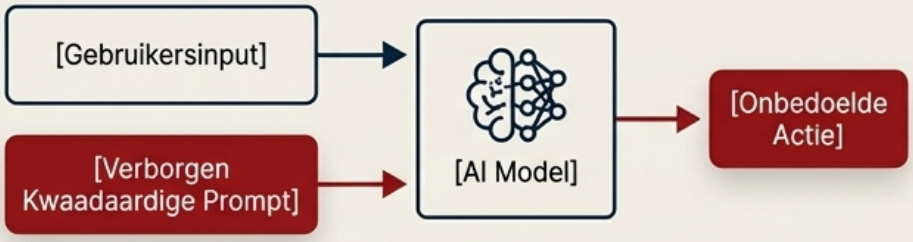


Kernpunt: De geavanceerde groep APT32/OceanLotus voert supply chain-aanvallen uit op IT-ecosystemen van kritieke infrastructuren.

Technieken: Gebruik van kwaadaardige .desktop-bestanden, PDF's en JAR-archieven, vermomd als legitieme overheidsmededelingen.

De AI-Paradox: Een Fundamenteel Nieuwe Kwetsbaarheid Zonder Definitieve Oplossing

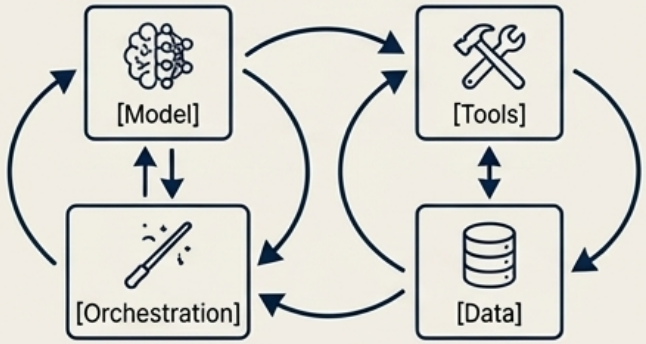
Het Probleem - Prompt Injection



Kernpunt: Het Britse NCSC waarschuwt dat er mogelijk geen **definitieve oplossing** bestaat voor **prompt injection-aanvallen**.

Uitleg: AI-modellen maken geen onderscheid tussen data en instructies, waardoor aanvallers via specifieke opdrachten het systeem kunnen manipuleren om onbedoelde acties uit te voeren of data te lekken.

De Reactie - Een Nieuw Veiligheidskader



Kernpunt: NVIDIA en Lakera AI stellen een **nieuw kader** voor om de veiligheid van **autonome, 'agentische' AI-systemen** te waarborgen.

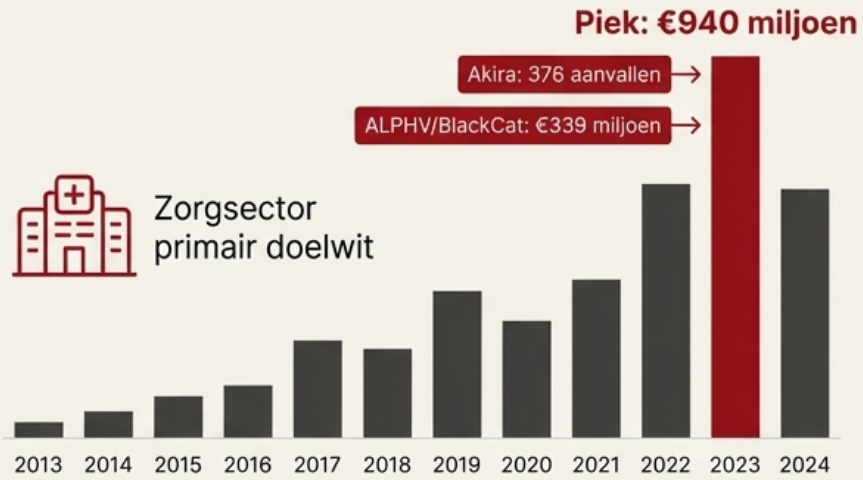
Aanpak: Behandelt veiligheid niet als een statische eigenschap, maar als een dynamisch resultaat van interacties. De **Nemotron-AIQ dataset** met 10.000 simulatiesporen is vrijgegeven om robuustere verdedigingen te ontwikkelen.

Ransomware als Industrie: Een Economie van €3,9 Miljard en de Tools die het Mogelijk Maken

De Cijfers (Data van FinCEN, VS)

€3,9 miljard

aan losgeld betaald (2013-2024)

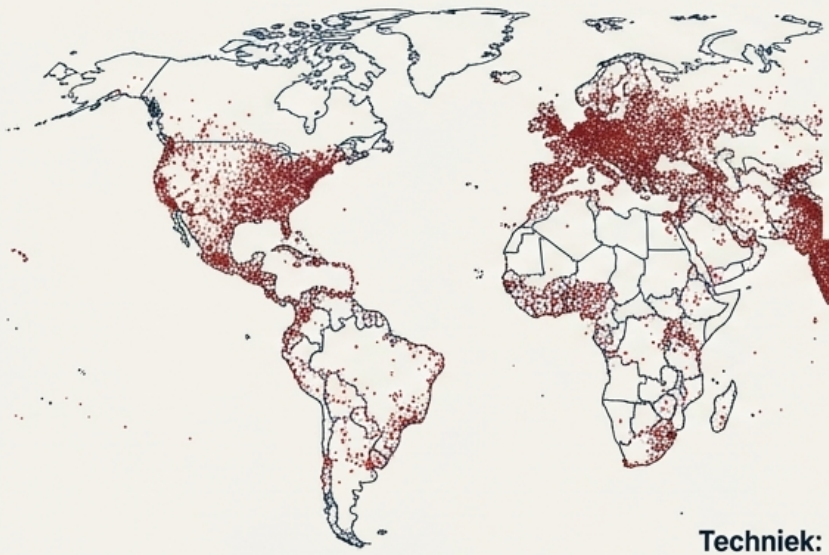


De 'Enabler' - Shanya EDR Killer

Functie: Een 'packer-as-a-service' tool ontworpen om beveiligingssoftware (EDR) uit te schakelen ter voorbereiding op een ransomware-infectie.

Ontwrichting op Grote Schaal: Van Staat-achtige Criminele Netwerken tot Sabotage van Publieke Diensten

Case 1 - Indonesisch Goknetwerk

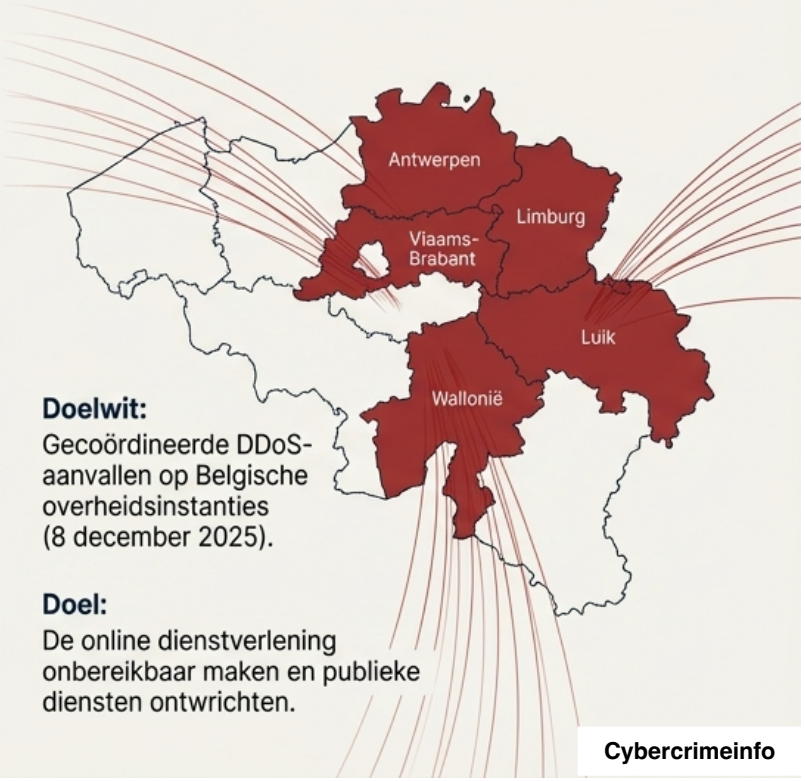


Schaal:
Een enorm netwerk, 14+ jaar actief, met kenmerken van staatssponsoring.

Infrastructuur:
~328.000 domeinen wereldwijd, duizenden kwaadaardige Android-apps verspreid via publieke AWS S3-buckets.

Techniek:
Gebruikt Google's Firebase Cloud Messaging voor C2-communicatie om traditionele detectie te omzeilen.

Case 2 - NoName DDoS-aanvallen

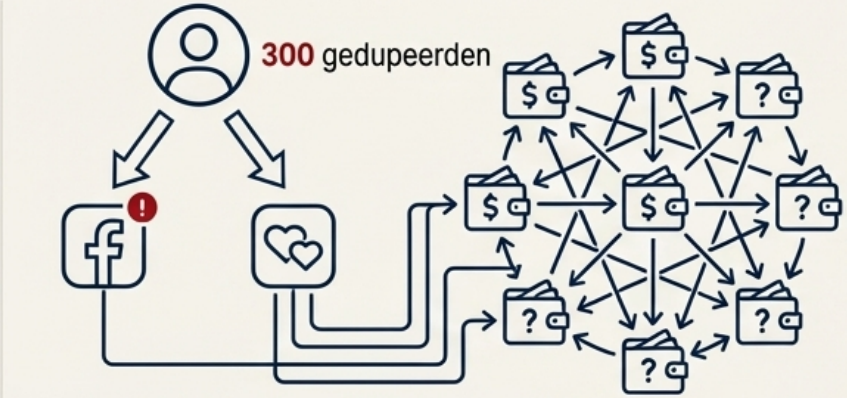


Doelwit:
Gecoördineerde DDoS-aanvallen op Belgische overheidsinstanties (8 december 2025).

Doel:
De online dienstverlening onbereikbaar maken en publieke diensten ontwrichten.

De Menselijke Maat: De Directe Impact van Fraude en Datadiefstal op Burgers

Case - Beleggings- en Vacaturefraude



Kernpunt: Politie Oost-Nederland benadert **300 gedupeerden** die cryptovaluta overmaakten naar frauduleuze wallets.

Methode: Slachtoffers verleid via sociale media of datingapps (boilerroomfraude). Schade varieert van enkele euro's tot tienduizenden euro's per persoon.

Samenwerking: Onderzoek in samenwerking met Europol en Coinbase.

Preventief Advies - Infostealers

Consequent uitloggen	Cookies verwijderen	Vermijd 'onthoud mij'

Kernpunt: Het Australische Cyber Security Centre (ACSC) waarschuwt voor een toename van infostealer-malware die onopgemerkt inloggegevens steelt.

Advies: Consequent uitloggen en cookies verwijderen beperkt de hoeveelheid data die gestolen kan worden. Wees voorzichtig met de automatische aanvulfunctie van browsers.

De Tegenbeweging: Internationale Rechtshandhaving en Interne Bedrijfsbeveiliging

Internationale Samenwerking - Europol's Taskforce GRIMM

- **Resultaat**
  In de eerste 6 maanden sinds de lancering (april 2025) zijn **193 arrestaties** verricht.
- **Focus**
  Aanpak van **'Geweld-als-Dienst'** (VaaS) netwerken die jongeren ronselen voor zware misdrijven.
- **Relevantie**
  Operaties vonden plaats in meerdere Europese landen, waaronder Nederland en België.

Juridische Precedenten - De Zaak van de Fietswinkel

- **Uitspraak**
  Rechtbank Midden-Nederland oordeelt dat een fietswinkelketen een medewerker op staande voet mocht ontslaan.
- **Feiten**
  De medewerker probeerde **malware te installeren** via een USB-stick, had **toegang tot de mailbox** van een collega en **ontvreemdde een laptop**.
- **Implicatie**
  De uitspraak onderstreept het recht van werkgevers om streng op te treden tegen **'insider threats'** die de bedrijfsveiligheid in gevaar brengen.

Regulering als Schild: Nieuwe Kaders voor Digitale Identiteit en Privacy

Proactieve Regulering (EU)

Gastmodus (Minimale Data) ⟷ Account (Gepersonaliseerde Ervaring)

- **EDPB**: De Europese privacytoezichthouders pleiten voor online aankopen zonder verplicht account. Webwinkels zouden een ‘gastmodus’ moeten aanbieden om **dataminimalisatie** te bevorderen.
- **Meta**: Onder druk van Europese regelgeving (**GDPR**) geeft Meta gebruikers op Facebook en Instagram **meer controle** over het delen van data voor gepersonaliseerde advertenties.

Innovatie in Publieke Diensten (België)

- **MyGov.be app**: Vanaf volgend jaar wordt een **volwaardige digitale identiteitskaart** ondersteund met dezelfde juridische waarde als de fysieke kaart.
- **Privacyvoordeel**: Gebruikers kunnen **selectief gegevens delen** (bv. enkel bewijs van meerderjarigheid tonen zonder geboortedatum of adres te onthullen).

Strategische Versterking: De AIVD Positioneert Zich voor de Toekomst

Algemene Inlichtingen- en Veiligheidsdienst (AIVD)

Positie: **Directeur Operatiën**
Naam: **Georg Driegen**
Datum: **Per 1 januari 2026**

Verantwoordelijkheden

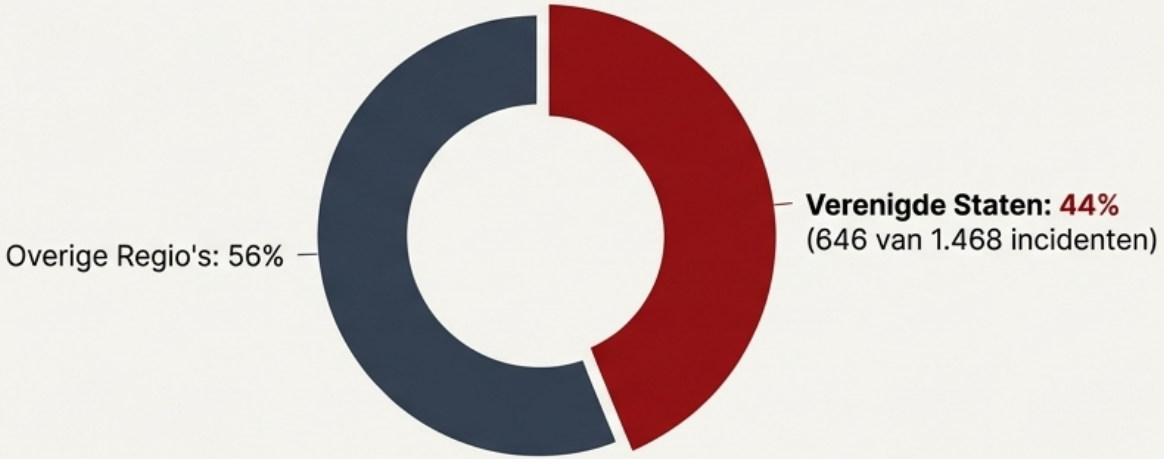
Aansturen van alle inlichtingenactiviteiten, inclusief **technische en cyberoperaties**.

Context

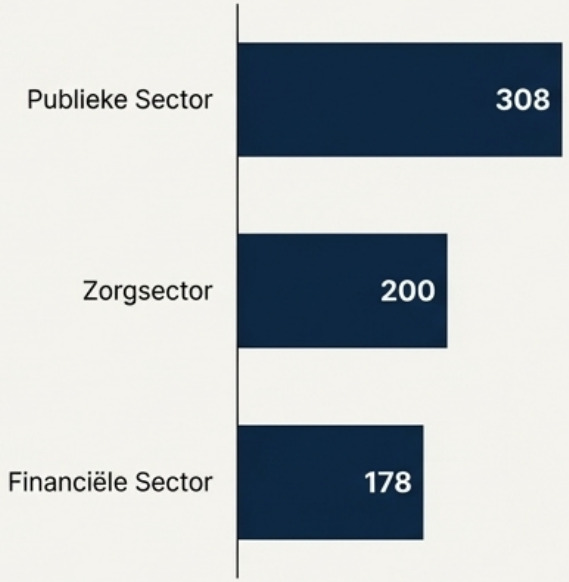
De benoeming komt op een moment van **toenemende en complexere dreigingen**. De taak is het **versterken van de inlichtingenpositie** van Nederland.

Een Wereldwijd Perspectief: Financiële Motieven Domineren het Dreigingslandschap

Bron van Wereldwijde Cyberaanvallen (2024-2025)



Meest Getroffen Sectoren



1.013 van 1.468 aanvallen hadden financieel gewin als primair doel.

Prognose: De wereldwijde kosten van cybercriminaliteit worden geschat op **$15,63 biljoen** in 2029.

Conclusie: Navigeren door het Vervaagde Slagveld Vereist een Geïntegreerde Visie

Synthese van de Analyse

- **Fysiek en Digitaal** zijn **verweven**: Sabotage van spoorwegen en onderzeese kabels bewijst dat cyber een **kinetische dimensie** heeft.
- **De hele keten** is een **doelwit**: Van de ontwikkelaarstool en de hypervisor tot de eindgebruiker; kwetsbaarheden zijn **systemisch**.
- **Cybercrime** is een **geïndustrialiseerde economie**: De schaal van ransomware en fraude, ondersteund door een professionele tool-markt, vereist een economische analyse.
- **Verdediging** is **multidimensionaal**: Een effectieve respons combineert technologie, internationale rechtshandhaving, proactieve regulering en strategische versterking.

Het beschermen van onze belangen in dit vervaagde slagveld vraagt om meer dan technische oplossingen alleen. Het vereist een geïntegreerde, intelligence-gedreven veiligheidsstrategie die geopolitieke, technische en economische realiteiten met elkaar verbindt.