
bfbs Forces News
2024-04-10 T11:43:51Z
AXON FLEX 2 X83100370
Als die gehackt worden,
heeft dat directe invloed op onze omgeving.
METROPOLITAN
POLICE

Birdwatcher Group

We zitten al in een oorlog.

Maar u ziet het niet.
En u maakt er deel van uit.

Birdwatcher Group

**Tim Bosch**
CEO van Birdwatcher Group

Voormalig AIVD (Algemene Inlichtingen- en Veiligheidsdienst


# Hoe bedrijven zich aan de frontlinie van hybride oorlogsvoering bevinden

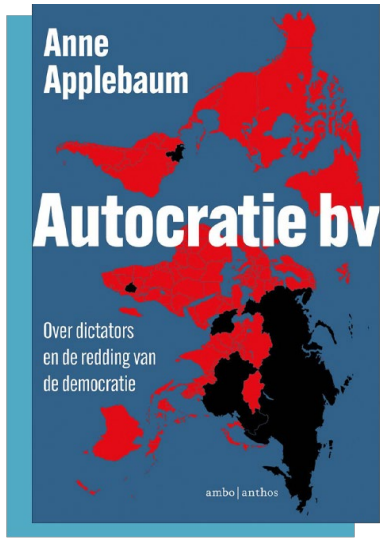
Betaalvereniging Nederland
21 mei 2026

# Modern autocratie

We bewegen van samenwerking → competitie

- Klassieke autocratie
  - Blik naar binnen gericht

- Modern autocratie:
  - Organisatie
  - Samenwerking, handel
  - Propaganda
  - **Hybride oorlogsvoerig**




Rusland maakt kapot.
China bouwt.

Birdwatcher Group

**Russia: verstoring & chaos**

sabotage

cyber operaties

desinformation

korte termijn, hoog risico, destabilis

Birdwatcher Group

**China: controle & dominantie**

technologie

supply chains

data

lange termijn, systematisch, strategi

Birdwatcher Group

**Iran: asymmetrie & beinvloeding**

proxies & plausibele ontkenning

cyber espionage

ransomware / sabotage

informatie operaties

Birdwatcher Group

**Noord Korea: inkomsten & overlevi**

cybercriminaliteit

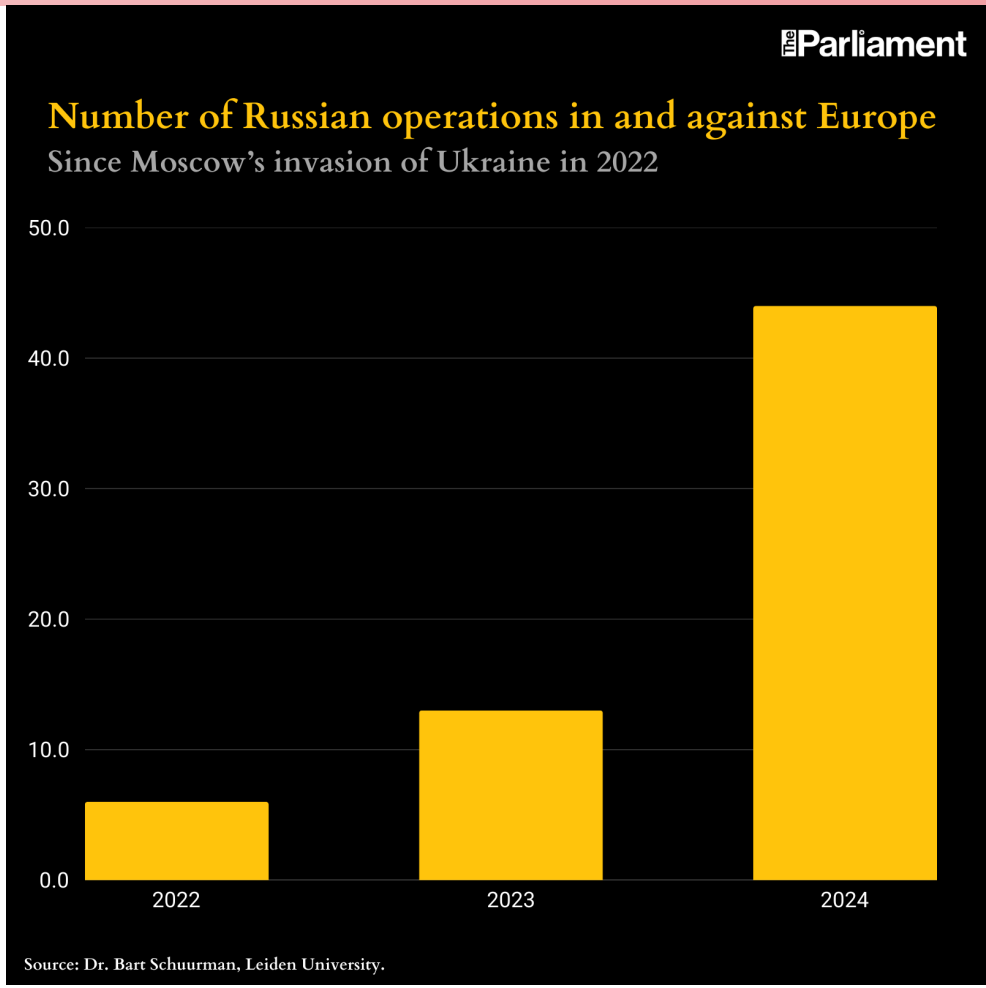
bank- en cryptodiefstal

SWIFT-aanvalllen

infiltratie via IT-werkers (Lazarus Gro

# Waarom dit nu relevant is

Hybride dreigingen zijn niet langer abstract.
Ze vormen operationele bedrijfsrisico’s.

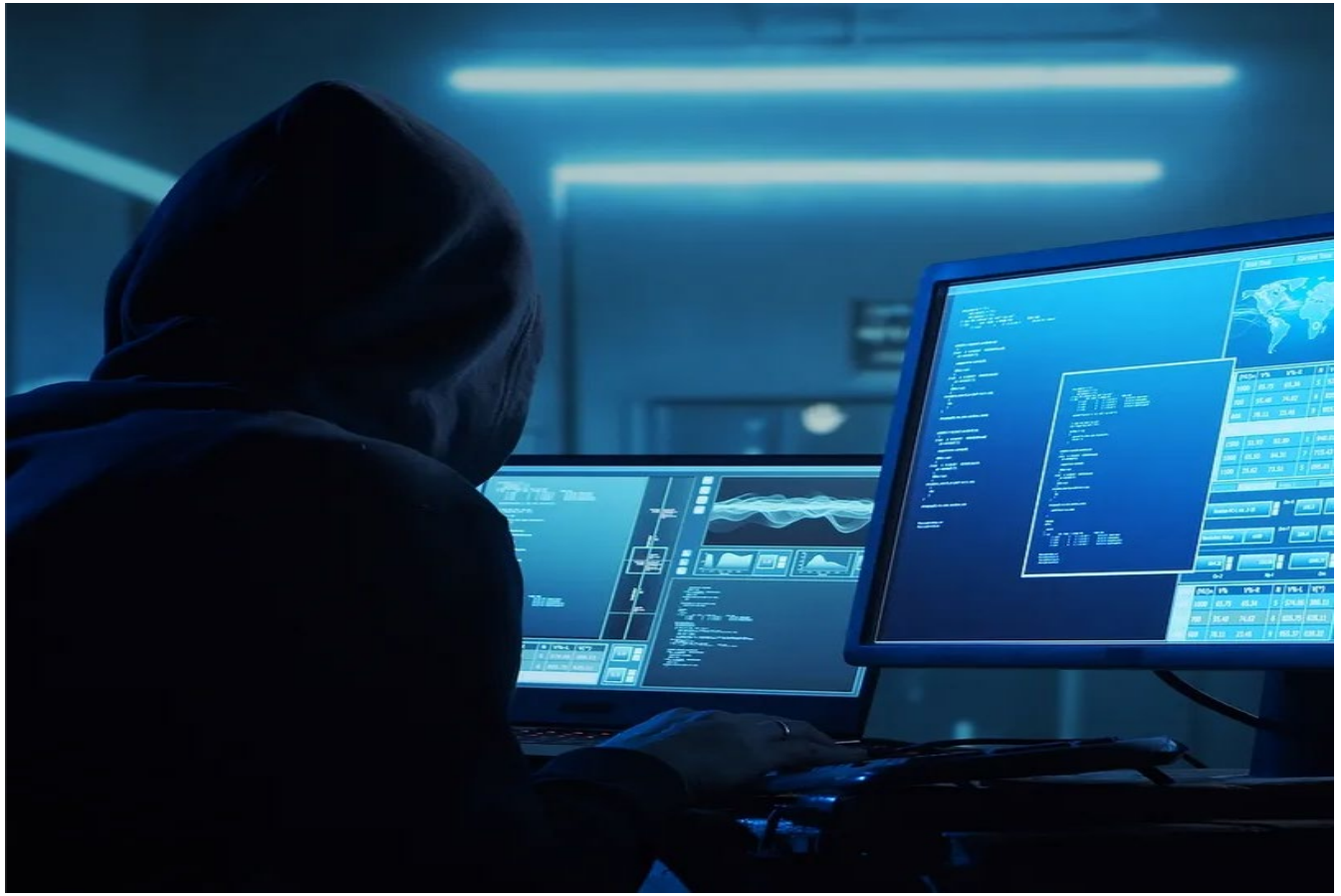


# Hybride oorlogsvoering

Het gecoordineerde gebruik van:

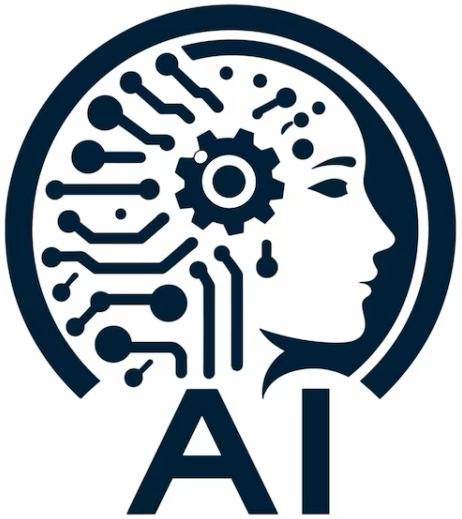
- cyber
- economische druk
- (des)informatie
- spionage
- sabotage

Onder de drempel van oorlog



# Technologische middelen

- Razendsnelle ontwikkeling
- Breed inzetbaar




# Hoe ziet dit er uit in de praktijk?

- spionage
- supply chain verstoring
- cyber aanvallen
- Infrastructuur sabotage
- invloed & desinformatie

# Case: DHL pakketjes - gecoordineerde sabotage

- Juli 2024: branden in DHL hubs (VK & Duitsland)

- Pakketjes met verborgen brandbommen

- Oorsprong traceerbaar naar Litouwen

- Gelinkt aan Russisch GRU netwerk

- Doel: testen postroutes naar VS/Canada

# Case: recente aanvallen op Polen’s energienetwerk

- Eerste cyberaanval ooit op gedecentraliseerde energiesystemen
- Aan Rusland gelinkte actoren verstoorden wine-, zonne- en warmtekrachtkoppeling-installaties
- Langdurige voorbereiding, potentieel voor impact in de echte wereld
- Bedrijfssystemen als strategische doelwitten

Waarom een Russische aanval op Poolse energiebronnen ook een waarschuwing is voor Nederland

- Huib Modderkolk, Volkskrant, 1 februari 2026

# Banken / betaingsverkeer specifiek

- **SWIFT Bangladesh Bank Heist (2016)**

Hackers infiltreerden de centrale bank van Bangladesh en stuurden frauduleuze SWIFT-berichten naar de Federal Reserve Bank of New York > $81 miljoen buitgemaakt

> Statelijke actor achter: Noord Korea

- **Russische invasie Oekraïne — cyberaanvallen op banken (2022)**

Voorafgaand aan de invasie:

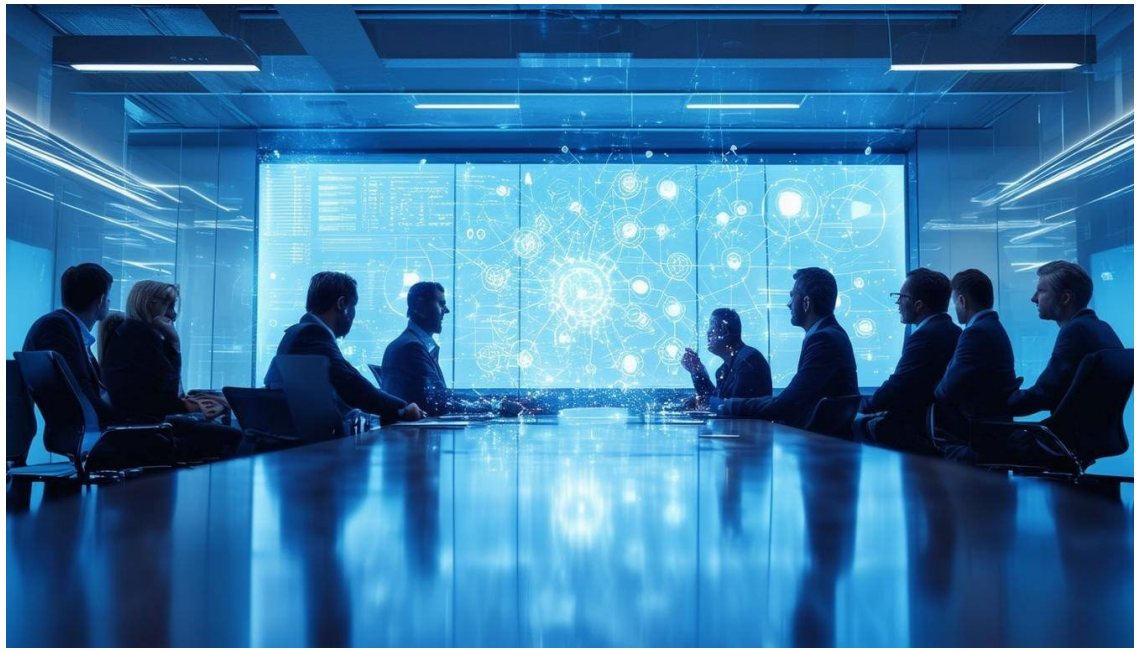
- DDoS-aanvallen op Oekraïense banken,
- verstoring mobiele banking apps,
- ATM-paniek,
- desinformatie over bankstabiliteit.

# Nederland is een strategisch doelwit

- logistieke hub
- digitale infrastructuur
- high-tech sectoren
- open economie

# Waarom is dit relevant in de boardrooms?

- geopolitiek beinvloedt besluitvorming
- Risico’s bevinden zich buiten de balance sheets
- bedrijven zijn directe targets




*“He who can handle the quickest rate of change survives.”* — **Col. John Boyd**

Birdwatcher Group

**Dank voor uw aandacht**

info@birdwatchergroup.com
tim@birdwatchergroup.com

www.birdwatchergroup.com