COCOON · WHITEPAPER · SECURITY VALIDATION

Van schijnveiligheid naar aantoonbare weerbaarheid

Hybride dreigingen in Europa en de noodzaak van security validation

Een nieuwe realiteit voor Europese organisaties

Europa bevindt zich sinds 2022 in een aanhoudende fase van hybride druk. Wat begon als incidenten aan de randen van het continent, is uitgegroeid tot een patroon dat vrijwel elk NAVO-land raakt, van de Noorse fjorden tot de Poolse grens en de Duitse luchthavens. De Noord-Atlantische Raad stelde in 2024 formeel vast dat Rusland verantwoordelijk wordt gehouden voor hybride aanvallen, waaronder sabotage, cyberoperaties en desinformatie, tegen onder meer Tsjechië, Estland, Duitsland, Letland, Litouwen, Polen en het Verenigd Koninkrijk *(NAVO-verklaringen, mei en december 2024)*. Dit is geen incident, het is strategie, en de uitvoering verloopt bewust indirect: niet via herkenbare militaire eenheden, maar via lokale criminele netwerken, geronselde burgers en scheepvaart die zich moeilijk laat herleiden tot een staat (Newsmax/The Telegraph, augustus 2026; PBS News). Precies die onduidelijkheid maakt een krachtige tegenreactie lastig, en dat is ook het doel.

Het Amerikaanse Congressional Research Service bevestigt dit beeld met concrete cases: een cyberaanval op een Noorse dam in april 2025 en aanvallen op dertig Poolse energiefaciliteiten in december 2025, naast herhaalde luchtruimschendingen en fysieke sabotage tegen kritieke installaties *(CRS, augustus 2026)*. Het Belfer Center van Harvard duidt dit als een bewuste grijze-zonestrategie tegen de NAVO-oostflank: acties die net onder de drempel van artikel 5 blijven, ontworpen om nooit een formele militaire reactie uit te lokken, maar wel voortdurend druk, kosten en onzekerheid te veroorzaken *(Belfer Center, februari 2026)*.

Figuur 1. Tijdlijn van gerapporteerde hybride incidenten in Europa, 2022-2026. Eigen visualisatie op basis van de in dit document geciteerde bronnen.

Het patroon achter de incidenten

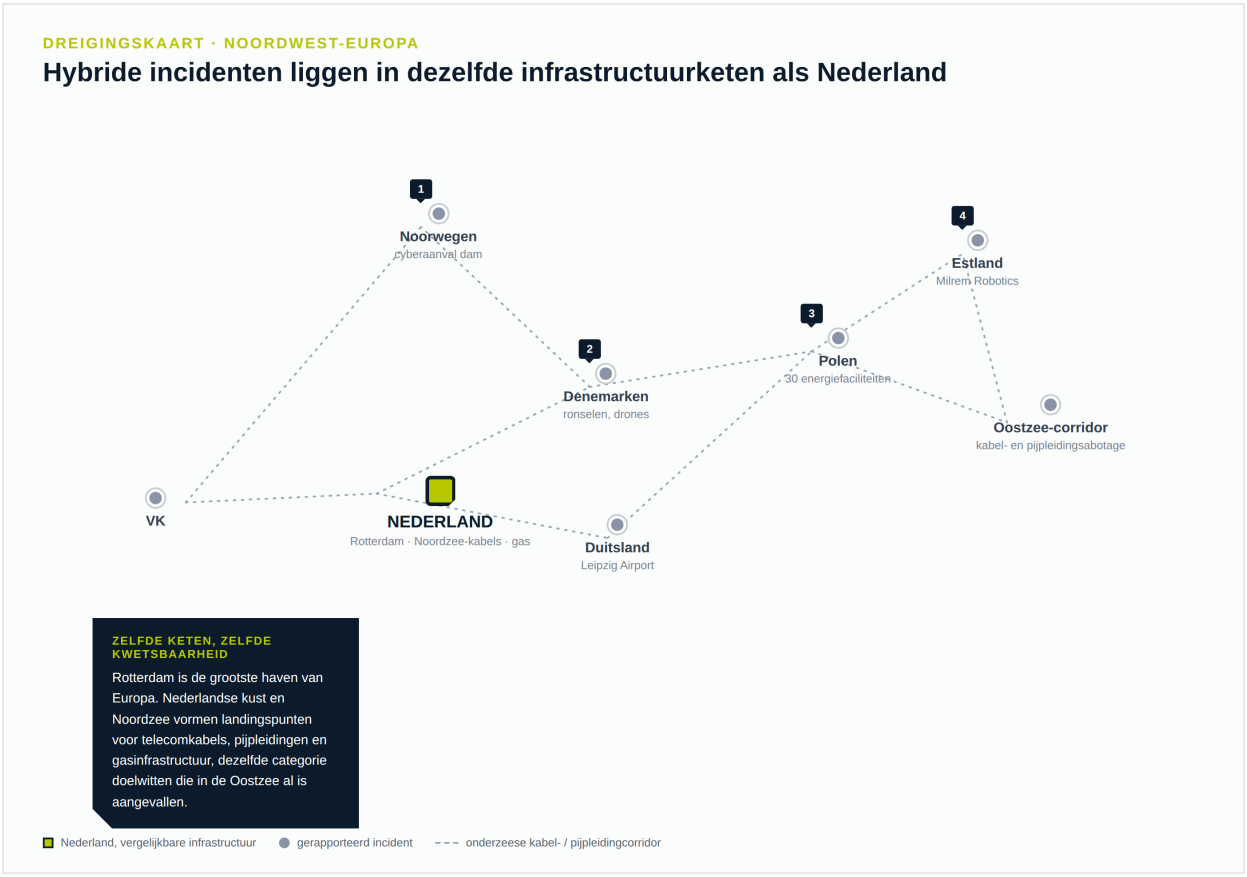
Wie de bronnen naast elkaar legt, ziet drie terugkerende lijnen, en een vierde die dichter bij huis komt dan vaak wordt aangenomen.

Ten eerste de fysieke laag. In Denemarken meldden inlichtingendiensten het ronselen van burgers voor sabotage tegen defensiebedrijven, en werden drones met explosieven waargenomen bij Leipzig Airport (PBS News). Bij de Estse defensiecontractor Milrem Robotics wordt vermoedelijke brandstichting via lokale criminele netwerken onderzocht *(Newsmax/The Telegraph, augustus 2026)*. Dit zijn geen technische aanvallen op afstand, maar operaties die fysieke toegang tot terreinen, gebouwen en installaties vereisen, uitgevoerd door mensen die zich voordoen als koerier, onderaannemer of bezoeker, precies de rol die reguliere toegangscontrole en sluitrondes hoort te onderscheppen.

Ten tweede de maritieme en infrastructurele laag. Sinds 2022 zijn er herhaalde sabotage-incidenten bij telecomkabels en gaspijpleidingen op de Baltische zeebodem, uitgevoerd door schepen die als spionageschip worden geduid *(Deccan Herald, december 2024)*. De NAVO heeft inmiddels een AI-tool ontwikkeld om verdachte vaartuigen te detecteren, wat aangeeft hoe structureel dit risico inmiddels wordt ingeschat (Euronews-dossier). Deze categorie infrastructuur, onderzeese kabels en pijpleidingen, houdt niet op bij de Oostzee: hetzelfde type verbinding loopt door heel Noordwest-Europa, met Nederland als een van de dichtste landingsstroken.

Ten derde de economische impact. S&P Global Market Intelligence becijfert de schade van vermeende Russisch aangestuurde sabotage tussen 2022 en 2025 op honderden miljoenen euro's, met een verwachte verdere toename in 2026 *(S&P Global, november 2025)*. Sabotage is dus geen theoretisch risico meer, het is een kostenpost, en die kostenpost groeit.

En dat brengt de vierde lijn dichterbij dan veel organisaties beseffen. Nederland is geen toeschouwer aan de rand van dit speelveld, maar zit middenin dezelfde infrastructuurketen die hierboven wordt aangevallen. Rotterdam is de grootste haven van Europa en een knooppunt voor energie- en goederenstromen naar het hele continent. De Nederlandse Noordzeekust vormt een van de dichtste landingsstroken van Europa voor onderzeese telecomkabels en pijpleidingen, en het land herbergt met Joint Force Command Brunssum een van de belangrijkste NAVO-hoofdkwartieren op het continent. Geen van de bronnen in dit document meldt een geverifieerd incident op Nederlandse bodem, en dat is precies het punt: de afwezigheid van een incident tot nu toe is geen bewijs van weerbaarheid, het kan net zo goed betekenen dat de volgende schakel in de keten nog moet volgen. Wie het patroon van Oslo tot Tallinn ziet en de eigen infrastructuur ernaast legt, ziet geen ver-van-mijn-bedshow, maar een kwestie van wanneer, niet of.



Figuur 2. Schematische weergave van de infrastructuurketen die al is aangevallen (Noorwegen, Denemarken, Polen, Estland, Oostzee) en de vergelijkbare Nederlandse infrastructuur. Eigen visualisatie, niet cartografisch nauwkeurig.

Belangrijk om te vermelden: het gaat hier om journalistieke en beleidsanalytische bronnen, gebaseerd op westerse inlichtingendiensten. Rusland ontkent de beschuldigingen. Dat neemt niet weg dat de dreigingsperceptie bij overheden, NAVO en het bedrijfsleven inmiddels breed gedeeld wordt, en dat organisaties, ook in Nederland, er verstandig aan doen hun weerbaarheid daarop te richten, nu, niet nadat het eerste incident zich hier heeft voorgedaan.

Het echte probleem: schijnveiligheid

De reflex van veel organisaties is het uitbreiden van maatregelen: meer camera's, meer toegangscontrole, meer procedures. Maar de kern van het probleem zit niet in de afwezigheid van maatregelen, die zijn er in de meeste organisaties wel. De kern zit in de vraag of ze daadwerkelijk werken op het moment dat iemand ze bewust probeert te omzeilen.

Dit is het verschil tussen een audit en validatie. Een audit stelt vast of een maatregel aanwezig is en of beleid gevolgd wordt, op basis van documenten en interviews. Validatie test of die maatregel in de praktijk standhoudt tegen een realistisch scenario. "Er is een camera" is geen antwoord. "De camera detecteert afwijkend gedrag en leidt aantoonbaar tot de juiste actie" wel. Zonder die toets ontstaat schijnveiligheid: het gevoel van beveiligd zijn, zonder het bewijs. De vraag is niet óf een organisatie beveiligingsmaatregelen heeft. De vraag is of ze functioneren wanneer iemand ze daadwerkelijk test.

Gezien de aard van de hierboven beschreven dreigingen, gericht op fysieke toegang, sluitrondes, menselijk handelen onder druk en de opvolging van alarmen, is precies dit het domein waar schijnveiligheid het grootste risico vormt.

De veiligheidsketen als toetsingskader

Weerbaarheid tegen hybride dreigingen valt uiteen in een keten van acht schakels, die elk afzonderlijk moeten kloppen. Faalt een schakel, dan faalt de keten.

01 **Intelligence**
Weten welke dreigingsactoren en modus operandi relevant zijn voor de eigen sector en locatie, toegespitst op reële casuïstiek zoals hierboven beschreven, niet in algemene termen.

02 **Voorbereiding**
Die kennis vertalen naar scenario's, protocollen en toegewezen verantwoordelijkheden, voordat een incident zich voordoet.

03 **Fysieke toegang**
De eerste harde test: houden hekwerk, sluizen en toegangscontrole stand tegen een vastberaden poging, ook buiten kantooruren.

04 **Detectie**
Wordt afwijkend gedrag daadwerkelijk gezien, door camera's, sensoren of surveillance, in plaats van dat beelden ongezien blijven.

05 **Beoordeling**
De menselijke schakel: wordt een signaal correct geïnterpreteerd als dreiging, of verdwijnt het in de ruis.

06 **Respons**
Komt de juiste actie op gang binnen een realistische tijd, door de juiste mensen.

07 **Escalatie**
Komt een incident tijdig bij de juiste laag in de organisatie of bij autoriteiten terecht.

08 **Continuïteit**
Herstel en lering: functioneert de organisatie door, en wordt de keten na een incident aantoonbaar sterker.

De rol van Cocoon

De dreigingen in dit document combineren cyber en fysiek, maar de toegang tot een dam, een energiecentrale of een defensiebedrijf loopt uiteindelijk via een hek, een sluis of een persoon die naar binnen wordt gelaten. Cocoon positioneert zich niet langer als aanbieder van bewustwording alleen, maar als partij voor fysieke security validation: testen, verbeteren, borgen. Dat sluit direct aan op de keten hierboven. In plaats van te veronderstellen dat intelligence, detectie of respons werken, toetst Cocoon iedere schakel onafhankelijk aan realistische scenario's, gebaseerd op de actuele dreigingsontwikkeling in Europa. Waar een audit een momentopname biedt, levert Cocoon het bewijs dat een maatregel het houdt onder druk, en waar dat niet zo is, de concrete verbetering die volgt.

Daarmee voorkomt Cocoon precies het risico dat de bronnen in dit document blootleggen: organisaties die denken weerbaar te zijn tegen sabotage, ronselpraktijken of fysieke inbraak, maar dat nooit hebben getoetst. Security validation maakt zichtbaar of beveiligingsmaatregelen in de praktijk daadwerkelijk effectief zijn tegen realistische dreigingen, en borgt vervolgens dat verbeteringen ook beklijven. Wij leveren geen rapport. Wij bouwen aan weerbaarheid.

TESTEN · VERBETEREN · BORGEN

Voor organisaties die serieus werk willen maken van weerbaarheid tegen de dreigingen die in dit document zijn beschreven, is een vrijblijvend gesprek met Cocoon de logische volgende stap. Wij brengen de acht schakels van uw eigen veiligheidsketen in kaart, toetsen ze tegen realistische scenario's, en laten zwart op wit zien waar u staat, en wat er nodig is om van schijnveiligheid naar aantoonbare weerbaarheid te komen.