BOOG-IT

ONDERZOEK / 2014-2026

Nederland onder druk

Een onderzoek naar hybride dreigingen – gemaakt door mens en AI.



BASISPERIODE

1 januari 2014 t/m 31 oktober 2026

AANVULLENDE CONTROLE EN REDACTIE / 1 NOVEMBER 2026

PILOT / MENS EN AI

Publicatie-editie van 1 november 2026.
Een onafhankelijke menselijke inhoudelijke review is niet uitgevoerd.

CYBEREXPERTISE / OSINT / AI

Leeswijzer

LEESROUTE / HOOFDSTUKKEN EN BRONNEN

Lees eerst de samenvatting en onderzoeksvraag. De volgende hoofdstukken leggen de bronnen en bevindingen uit. Daarna volgen de conclusies en de verantwoording van de samenwerking tussen mens en AI. De bronverwijzingen staan achteraan. Klik op een hoofdstuk of gebruik de PDF-bladwijzers om verder te lezen.

01 Samenvatting 3

02 Onderzoeksvraag en vaste afbakening 3

03 Methode en betekenis van de gegevens 4

04 Toepassing van de RIS Propeller Intelligence Cycle 5

05 Historische samenhang 6

06 Drones, Noordzee en elektronische verstoring 7

07 Personen, instituties en afhankelijkheden 8

08 Wat de drie externe kaders toevoegen 8

09 Tegenindicaties en grenzen van de conclusies 9

10 Wat de afsluitronde over 27-31 oktober toevoegt 10

11 Hypothesen, alternatieven en zekerheid 11

12 Conclusies en gebruik voor vervolgmonitoring 12

13 Samen onderzoeken: mens en AI 12

14 Bronnen en leesverantwoording 15

Basisperiode: 1 januari 2014 t/m 31 oktober 2026. Aanvullende controle en redactie: 1 november 2026. Dit is een publicatie-editie. Een onafhankelijke menselijke inhoudelijke review is niet uitgevoerd.

Over deze editie

Zelfstandig retrospectief onderzoek op basis van openbare bronnen. Piloteditie 2026-11-01-pilot-mens-ai-r3, gebaseerd op de afgesloten kwalitatieve basiseditie van 1 november. Onderzoeksperiode en opgenomen publicaties t/m 31 oktober 2026; aanvullende controle uitgevoerd op 1 november 2026. Boog-IT. Opdracht en inhoudelijke sturing: Maurice. AI ondersteunde het onderzoek, de analyse, de tekst en controles. Boog-IT draagt de redactionele verantwoordelijkheid. Deze editie is vrijgegeven voor publicatie. Dit is een publicatie-editie. Een onafhankelijke menselijke inhoudelijke review is niet uitgevoerd. De methodologische review en gerichte inhoudelijke nacontrole staan in het reviewdossier.

01 Samenvatting

Nederland wordt in de onderzochte openbare bronnen beschreven als doelwit van spionage, beïnvloeding, repressie en verstoring, als vestigingsplaats van internationale instellingen en als schakel in digitale en economische ketens. Deze activiteiten hebben een voorgeschiedenis die vóór de grootschalige Russische invasie van Oekraïne in 2022 ligt. Het startjaar 2014 markeert de onderzoeksgrens, niet het ontstaan van hybride dreigingen. De jaarverslagen en casussen ondersteunen deze historische continuïteit; zij leveren geen volledige landelijke telling. Zie AR2014, AR2016, RF001 en K001.

De belangrijkste uitkomst is een onderscheid tussen wat aantoonbaar is gebeurd, wat een bron aan een actor toeschrijft, welke gevolgen bekend zijn en wat slechts mogelijk of vermoed wordt. De openbare bewijsbasis verschilt sterk. Een officieel toegeschreven cyberinbraak is een ander soort gegeven dan een dronemelding, een escorte van een Russisch schip, een journalistieke beschuldiging of een fictief risicoscenario. Het onderzoek brengt deze soorten informatie samen zonder ze tot één aanvalsteller of dreigingsscore op te tellen.

De verbreding naar drones, de Noordzee, economische afhankelijkheden, diaspora en internationale instellingen verandert de vraagstelling. Dit rapport is daarom een kwalitatief retrospectief onderzoek met een referentiebasis voor latere monitoring. Alleen enkele afzonderlijke bronreeksen bevatten metingen. De beschikbare gegevens onderbouwen geen representatieve stijging of daling van de totale hybride dreiging in Nederland tussen 2014 en 2026. Officiële uitspraken over toenemende dreiging blijven herkenbaar als beoordelingen van de betrokken diensten, binnen hun eigen periode en geografische bereik.

Drie recente kaders verbeteren de interpretatie. Het Dreigingsbeeld Statelijke Actoren 2025 biedt officiële duiding. De Rijksbrede Risicoanalyse 2026 helpt mogelijke gevolgen en afhankelijkheden te onderscheiden. HCSS CLARIS levert categorieën en onderzoekssporen over Chinese activiteiten. Geen van deze kaders vult ontbrekende historische incidenten automatisch aan. Het onderzoek claimt evenmin een volledige audit van die publicaties. Zie N62, PO-S002, PO-S003 en KI-S009.

02 Onderzoeksvraag en vaste afbakening

De centrale vraag luidt: welke publiek gedocumenteerde activiteiten, meldingen en officiële beoordelingen wijzen sinds 2014 op hybride dreigingen die Nederland raken, wat is bekend over actoren, middelen, doelwitten, fase en gevolgen, en welke veranderingen kunnen verantwoord worden beschreven?

Voor deze editie staat de gebeurtenisperiode vast op 1 januari 2014 tot en met 31 oktober 2026. Het jaar 2026 is onvolledig. De afsluitende bronnenronde over 27-31 oktober is op 1 november uitgevoerd; de oorspronkelijke rapportlaag 1.4 houdt haar eigen peildatum van 24 oktober. Bronnen met een andere verslagperiode behouden die periode. Een publicatie in 2026 maakt een oudere gebeurtenis niet tot een gebeurtenis uit 2026. Een onbekende gebeurtenisdatum wordt niet vervangen door een publicatiedatum.

Het geografische zwaartepunt is Europees Nederland. Daarnaast kunnen Nederlandse organisaties, personen, militaire eenheden, internationale instellingen in Nederland en concreet beschreven Nederlandse belangen in het buitenland worden geraakt. Die relaties worden afzonderlijk benoemd. Caribisch Nederland en de overige landen van het Koninkrijk zijn relevante gebieden, maar in dit corpus niet systematisch historisch onderzocht. Een vergelijking met het Koninkrijksbrede bereik van de RRA maakt die lacune zichtbaar; zij sluit haar niet.

De verbrede actorafbakening omvat Rusland, China, Iran, Turkije en andere actoren waar de geselecteerde bronnen een concrete Nederlandse relatie behandelen. Amerikaanse sancties en beschuldigingen rond Israël worden op hun eigen aard en bewijsstatus beoordeeld. De oorspronkelijke nadruk op Rusland/Oekraïne en conflicten rond het Midden-Oosten is dus verbreed. Actorselectie is geen ranglijst; nationaliteit, een buitenlandse leverancier of een zakelijk contact bewijst geen statelijke opdracht.

Inhoudelijk omvat het onderzoek cyberactiviteiten, informatiebeïnvloeding, politieke en bestuurlijke inmenging, repressie en fysiek geweld, maritieme en luchtactiviteiten, elektronische en satellietverstoring, economische en kennisafhankelijkheden en druk op internationale instellingen. Vitale infrastructuur en sectoren zoals zorg, water of financiën zijn doelwit- en gevolgomgevingen. Ze worden niet opgeteld alsof het afzonderlijke aanvalsmethoden zijn.

Een gebeurtenis komt als onderbouwde activiteit in de synthese wanneer een herleidbare bron de handeling en Nederlandse relatie ondersteunt. Het oordeel over statelijke aansturing en hybride karakter blijft daarvan gescheiden. Een melding, verdenking, aggregaat, beoordeling, scenario of open spoor behoudt zijn eigen status. Buitenlandse voorbeelden zonder aangetoonde Nederlandse relatie zijn uitsluitend context. Stuxnet valt als gebeurtenis vóór 2014 buiten de periode, ook wanneer een publicatie erover uit 2024 dateert. Het buitenlandse Zimbra-dossier X002 heeft geen vastgestelde Nederlandse slachtoffers en wordt hier uitsluitend als buitenlandse context behandeld. Zie RF010, X002 en de correctiebesluiten.

De volledige regels, inclusies, uitsluitingen en afsluitcriteria staan in Afbakening. Nieuwe bronvondsten na deze editie krijgen een afzonderlijke versie. De historische lagen blijven intact.

03 Methode en betekenis van de gegevens

Het corpus is doelgericht opgebouwd uit openbare jaarverslagen, dreigingsbeelden, Kamerstukken, rechterlijke en opsporingspublicaties, berichtgeving en thematische zoekrondes. De jaarbasis behandelt 2014 tot en met 2026. Latere rondes verdiepen geselecteerde onderwerpen en voegen bronnen en tegenindicaties toe. De bewaarde zoeklogs maken de zoekvragen en feitelijk geraadpleegde passages navolgbaar. Dit is geen uitputtende systematische literatuurreview en geen steekproef met bekende selectiekansen.

Het analysemodel onderscheidt vier lagen: uitgevoerde activiteiten; voorbereiding, pogingen en interventies; officiële dreigingsbeoordelingen; en zichtbaarheid door bronnen, registratie en openbaarmaking. In de verbreding zijn meldingen, brongebonden meetreeksen, kwetsbaarheden, scenario's en nog niet geverifieerde sporen daarnaast herkenbaar gehouden. Registratieaantallen beschrijven de samenstelling van het dossier. Ze zijn geen aantallen unieke aanvallen.

Een bronbericht, een campagne, een slachtoffer, een locatie, een gebeurtenis en een interventie zijn verschillende eenheden. Hetzelfde feit kan terugkomen in een jaarverslag, een Kamerbrief en meerdere nieuwsartikelen. Ook een gezamenlijk DBSA en een daarop gebaseerd RRA-hoofdstuk zijn voor dat feit geen onafhankelijke bevestigingen. Het bronregister bewaart bewijsfamilies en overlap; waar de precieze relatie onbekend is, wordt geen ontdubbelde telling geconstrueerd.

Voor iedere inhoudelijke uitspraak moeten vier vragen te onderscheiden blijven: welke handeling is beschreven; wie doet de toeschrijving; welke uitkomst is vastgesteld; en welke alternatieve verklaring of beperking blijft bestaan? Officiële attributie kan zwaarwegend zijn, maar de onderliggende inlichtingen zijn doorgaans niet volledig openbaar. Dit onderzoek voert geen eigen forensische attributie uit. Een strafrechtelijke verdenking wordt niet als veroordeling weergegeven; een uitspraak in eerste aanleg wordt niet zonder controle onherroepelijk genoemd.

Meer zichtbare meldingen kunnen passen bij meer activiteit, maar ook bij verbeterde detectie, gewijzigde meldbereidheid, een uitgebreidere toezichtstaak of latere openbaarmaking. Het aandeel van deze oorzaken is onbekend. Geheimhouding kan de zichtbaarheid beperken; zij rechtvaardigt geen schatting van verborgen incidenten. De afwezigheid van een registratie is daarom geen bewijs van afwezigheid van dreiging.

De bronkopieën in het bijbehorende pakket dienen controle en herleidbaarheid. Een geslaagde download, een overeenkomende hash of een tekstextractie bewijst niet dat de inhoud juist of volledig gelezen is. Historische leesstatussen blijven behouden. Bij ontoegankelijke bronnen wordt onderscheid gemaakt tussen een oudere kopie, een gedeeltelijke webweergave, een zoekindexspoor en een daadwerkelijk ontbrekend origineel. Zie Bronarchief en Dataverantwoording.

04 Toepassing van de RIS Propeller Intelligence Cycle

Deze editie past het centrale Boog-IT-framework 1.1 toe, gebaseerd op Reuser(2017). De methode is tijdens deze review op 1 november expliciet gemaakt; eerdere rondes worden niet achteraf als volledig RIS-gecertificeerd gepresenteerd. De opdrachtgever vraagt een controleerbare basis voor publieksuitleg en latere updates. Het rapport moet ondersteunen welke uitspraken verantwoord op de website kunnen verschijnen en welke onderzoeksvragen prioriteit hebben.

Preparation legt vraag, bronnenkeuze, datumgrens en stopcriteria vast. Report bewaart geordende bronfeiten en onzekerheden in OSINF. Synthesis maakt de betekenis en alternatieve verklaringen zichtbaar. De samenvatting en website-uitvoer bedienen het brede publiek; bronarchief, leesnotities en besluiten blijven controleerbaar in het dossier. Reusers onderscheid tussen broninformatie en analytisch oordeel betekent dat een officieel oordeel niet door alleen een verwijzing tot eigen bewezen attributie wordt verheven. Zie methodebron AC-SO01.

De terugkoppeling met de opdrachtgever is expliciet: de opdracht voor review en afsluiting tot 31 okt autoriseert deze ronde en synthese. Tussentijdse bronbevindingen zijn in de chat teruggekoppeld. De opdrachtgever heeft de publicatie-editie vrijgegeven. Dit vervangt geen onafhankelijke menselijke inhoudelijke review. Het centrale framework voegt labels FACT, CLAIM, ASSESSMENT en HYPOTHESIS en gemotiveerde confidence toe als Boog-IT-uitwerking. Het zijn geen letterlijke eisen uit het artikel van 2017.

Bronbetrouwbaarheid, inhoudelijke bewijssterkte en analytische zekerheid worden afzonderlijk beschreven. Een FACT kan hier zijn dat het OM een bepaalde verdenking publiceert; de verdenking zelf blijft CLAIM. De zekerheid bij een conclusie zegt hoe sterk de onderbouwing is, niet hoe groot de kans op een toekomstige aanval is. Het bronregister benoemt bronfamilie, gelezen passages, belangen en beperkingen; officiële bronnen wegen zwaar voor wat de instantie zelf bekendmaakt, maar zijn geen onafhankelijke openbare toets van haar niet-openbare inlichtingen.

05 Historische samenhang

Een voorgeschiedenis vóór 2022

De bronnen vanaf 2014 beschrijven onder meer digitale spionage, inmenging en economische blootstelling. De Russische goederenboycot illustreert Nederlandse exportafhankelijkheid, maar blootstelling aan een handelsmaatregel is geen gemeten uiteindelijke schade en niet automatisch een hybride aanval. De cyberpogingen tegen de Onderzoeksraad voor Veiligheid rond het MH17-onderzoek in 2015 hebben een beperktere bewijsbasis dan de verstoorde GRU-operatie tegen de OPCW in 2018. Bij de eerste casus ontbreken onderdelen van het oorspronkelijke technische dossier; bij de tweede bevestigt Defensie de verstoring. Zie H001, RF002 en K001.

De moorden in Almere en Den Haag, en de officiële beoordeling van vermoedelijke Iraanse betrokkenheid, maken duidelijk waarom het onderzoek ook personen en repressie omvat. Het vaststaan van een moord en de inlichtingenmatige toeschrijving aan een staat zijn verschillende bewijsposities. De strafrechtelijke stand verschilt per zaak en wordt niet vanuit de ene zaak naar de andere overgenomen. De diplomatieke terugtrekking van de Turkse religieuze attaché in 2016 betreft weer een andere handeling: informatievergaring die het kabinet als ongewenste inmenging kwalificeerde. Dit rechtvaardigt geen verdenking van een hele gemeenschap. Zie K002, K003, N02 en PR-E001.

NotPetya raakte in 2017 de Rotterdamse logistieke keten. Het laat zien dat Nederlandse schade kan ontstaan als doorwerking van een internationale cyberoperatie. De GRU-routerregistratie over 2021 beschrijft misbruik van Nederlandse infrastructuur als campagneaggregaat. Het aantal Nederlandse routers en de precieze vervolgschade zijn onbekend; een herhaling in een volgend jaarverslag levert geen tweede operatie op. Zie K011 en RF001.

Van 2022 tot en met 2024

De geweigerde toegang van een Russische inlichtingenofficier tot het Internationaal Strafhof in 2022, de cyberincidenten bij het Hof en de Chinese spionagemalware op een onderzoeksnetwerk van Defensie tonen verschillende belangen en werkwijzen. Voor COATHANGER is 2023 de Nederlandse gebeurtenisperiode; de eerste openbaarmaking dateert van 6 februari 2024. De gevolgen waren volgens de aangehaalde advisory beperkt door segmentering. Een mondiale campagneperiode of wereldwijd slachtofferaantal wordt niet naar Nederland vertaald. Zie K009, K010, KI-E001 en RS-CS2024.

De beëindiging van Gazprom-leveringen aan GasTerra in 2022 is een concrete economische verstoring. GasTerra beschrijft ook vervangende inkoop en het nakomen van eigen leveringsverplichtingen. Die uitkomst begrenst de claim over maatschappelijke schade. De Chinese servicestations vormen een dossier over stations waarvan het kabinet de vestiging onacceptabel vond en onmiddellijke sluiting verlangde; het kabinet stelde de vermeende intimidatie in de geraadpleegde beantwoording uit 2023 niet vast. Zie PR-E003 en PR-E002.

De periode bevat daarnaast satellietverstoring met Nederlandse ontvangstgevolgen, meldingen van Noordzeeverkenningen en militaire signalering buiten Nederland. De benadering van Zr.Ms. Tromp en de NH90 op 7 juni 2024 vond plaats in de Oost-Chinese Zee. Defensie en China geven een verschillende duiding; het dossier beslist niet zelfstandig over die betwisting en bewijst geen hybride intentie. Zie RF012, G001 en KI-E002.

2025 en het onvolledige jaar 2026

Recente officiële beoordelingen beschrijven ernstige statelijke dreigingen en ontwikkelingen in sabotage, spionage en beïnvloeding. Hun geografische bereik verschilt: een Europese beoordeling is geen gemeten Nederlandse tijdreeks. Het DBSA van juli 2025 meldde toen geen bekende uitgevoerde fysieke statelijke sabotage in Nederland, maar wel voorbereidingen. Die kennisgrens kan niet zonder nieuwe beoordeling worden doorgetrokken naar heel 2026. Zie KI-A001 en N62.

De recentere registraties omvatten dronemeldingen, verdachte voorbereidingen en geweldsincidenten waarvan toedracht of opdrachtgeverschap niet steeds vaststaat. Ze vragen beoordeling per dossier. Een opgeëiste aanslag, een opsporingsverdenking en een bewezen statelijke opdracht zijn geen verwisselbare kwalificaties. De gedeeltelijke periode 2026 en selectieve openbaarmaking verhinderen een zuivere vergelijking met volledige eerdere jaren.

Deze periodisering ordent de geschiedenis. Zij vormt geen bewijs dat het aantal of de ernst van alle activiteiten per periode is toegenomen. Ook oudere gebeurtenissen kunnen pas in een latere onderzoeksronde zichtbaar worden.

06 Drones, Noordzee en elektronische verstoring

De verbreding brengt drie onderwerpen in beeld die in de oorspronkelijke monitor vooral als aggregaat voorkwamen. De winst zit in het onderscheiden van waarneming, meldsysteem, toezichtreactie, technische bevestiging en toeschrijving. Deze onderscheidingen zijn nodig voordat een uitspraak over toename betekenis krijgt.

Bij drones bestaan ten minste drie verschillende informatietypen: luchtvaartvoorvalmeldingen, veiligheidsmeldingen aan diensten en concrete waarnemingen op een locatie en datum. De ILT-jaarpublicatie 2023 en de factsheet van november 2023 geven voor dezelfde historische jaren verschillende waarden. Voor 2022 komt de som van drie kolommen in de jaarpublicatie op 174 en die in de factsheet op 218. De verklaring is niet vastgesteld. De reeksen blijven daarom afzonderlijk; ontbrekende categorieën zijn geen nul en het eerste halfjaar 2023 is geen volledig jaar. Zie SP-T001, SP-T002, SP-S005 en SP-S006.

De AIVD beschrijft meer dronemeldingen in 2025 en vermeldt dat Russische betrokkenheid veelal niet kon worden bevestigd. De waarnemingen bij Volkel en Eindhoven in hetzelfde novemberweekend zijn afzonderlijke registraties van plaats en dag; zij bewijzen geen drie onafhankelijke operaties en geven geen exact aantal unieke toestellen. Het historische getal over 2014 is een secundair brongetal en wordt niet aan de latere ILT-tabellen vastgeknoopt tot één reeks. Zie SP-A001, SP-E001, SP-E002, SP-E003 en SP-T003.

Op de Noordzee maken officiële publicaties en berichtgeving onderscheid tussen Russische scheepsbewegingen, begeleiding en vermoedelijke verkenning. De geregistreerde begeleidingen nemen in de betrokken bronreeks toe van 20 in 2024 tot 61 in 2025. Dat is een verandering in geregistreerde begeleidingen. Hoeveel daarvan samenhangt met activiteit, toezichtbeleid, capaciteit of detectie is onbekend. De uitbreiding van de permanente taak vanaf juli 2023 maakt de vergelijking met eerdere jaren extra lastig. De twaalf begeleidingen in januari en februari 2026 worden niet naar een jaarcijfer geëxtrapoleerd. Zie SP-T004, SP-T005 en SP-T006.

Een ontbrekende AIS-positie in een publieke waarneming bewijst niet zonder meer een bewust uitgeschakelde transponder. Dekking, ontvangst, objectidentiteit, periode en bronkwaliteit moeten worden gecontroleerd. Verdacht vaarpatroon, verkenning van infrastructuur, kabelschade, opzet en daderschap

zijn afzonderlijke claims. In dit dossier is geen eigen historische AIS-dataset of onafhankelijke technische verificatie beschikbaar. De Nederlandse EEZ, territoriale zee, bredere Noordzee en Oostzee mogen evenmin als één locatie worden behandeld. Zie SP-E008, SP-E009, N14 en de open onderzoeksvragen.

Bij elektronische verstoring vermelden ILT-bronnen sterke veranderingen in gemelde gps-problemen en meldteksten met het woord spoofing. De reeks met circa 153 meldingen in 2023 en 1.318 in 2024 betreft gebeurtenissen buiten het Nederlandse luchtruim bij vluchten met een Nederlandse relatie. Zij is geen telling van aanvallen binnen Nederland en geen zelfstandig technisch bewijs van een actor. De bredere gps-reeks kan met deze deelcategorie overlappen. De storing bij Vlissingen laat bovendien zien waarom een onbedoelde oorzaak apart moet blijven. Zie SP-T007, SP-T008 en SP-E010.

07 Personen, instituties en afhankelijkheden

Een analyse van hybride dreiging die alleen technische infrastructuur onderzoekt, mist repressie tegen personen, politieke beïnvloeding en druk op instellingen. De prioriteitenronde voegt deze dimensies toe. De registraties over diaspora en intimidatie hebben niet overal een exact aantal slachtoffers of een afgebakende gebeurtenisdatum. Een algemene beoordeling blijft een beoordeling; zij wordt niet omgezet in een reeks fictieve incidenten. Zie PR-A001, PR-E004 en PR-A002.

Voor politieke invloed moet onderscheid worden gemaakt tussen belangstelling, contact, verspreiding, betaling en aantoonbaar effect. De Nederlandse voorgeschiedenis van Voice of Europe bewijst geen Russische aansturing vanaf de oprichting en geen betaling aan Nederlandse politici. Europese voorbeelden van benadering leveren die ontbrekende Nederlandse deelclaim evenmin. Het DBSA kwalificeert de gekende heimelijke beïnvloedingspogingen en hun effecten in Nederland als relatief klein; dat oordeel wordt hier niet uitgebreid tot alle vormen van repressie. Zie RF008, PR-A003 en KI-A002.

Internationale instellingen kunnen tegelijk worden geraakt door infiltratie, cyberactiviteiten, intimidatie en openlijke politieke of juridische druk. Sancties tegen het Internationaal Strafhof worden daarom als beleids- en belangencontext beschreven, met hun eigen besluitbasis. Ze worden niet gelijkgesteld aan clandestiene operaties. De nog onvoldoende gecontroleerde claim over een latere sanctie-uitbreiding blijft een open spoor. Zie C001, G003 en RF013.

Economische afhankelijkheid wordt pas een concreet drukmiddel als de inzet daarvan is onderbouwd. Een mogelijke ketenuitval is vervolgens nog geen waargenomen gevolg. Dit onderscheid geldt voor energie, cloud, telecom, kennis, logistiek en financiën. De sectorcodering in het dossier is een analytische ordening en geen wettelijke aanwijzing van vitale aanbieders. Voor drinkwater, waterbeheer, zorg, betalingen en chemische of nucleaire processen ontbreekt een systematische historische incidentenreeks. Zie PR-A004, KI-A004 en Open punten.

08 Wat de drie externe kaders toevoegen

Het DBSA 2025 biedt een samenhangende officiële beoordeling van statelijke actoren. Het ondersteunt de brede indeling naar middelen en doelwitten en begrenst enkele interpretaties: betere zichtbaarheid kan tot meer waarnemingen leiden; economische of diplomatieke handelingen zijn niet vanzelf onrechtmatig; fysieke sabotage, voorbereiding en digitale verstoring moeten worden onderscheiden. De informatiepositie van de diensten verschilt van die van een openbaar dossier. Het onderzoek neemt hun oordelen met bron en datum over, zonder te doen alsof de onderliggende geheime gegevens zelfstandig zijn gecontroleerd. Zie N62 en KI-A001 tot en met KI-A003.

De RRA 2026 behandelt een breder scala aan moedwillige en niet-moedwillige gevaren. Zij gebruikt fictieve, plausibele scenario's om risico's en mogelijke gevolgen te beoordelen. De zes nationale veiligheidsbelangen helpen vragen te stellen over doorwerking naar fysieke, economische en ecologische veiligheid, territoriale veiligheid, sociale en politieke stabiliteit en de internationale rechtsorde. Deze scenario's worden niet als werkelijk gebeurde sabotage of als historische slachtoffers ingevoerd. Ook een voorbeeld over Caribische kabels blijft fictief. Zie PO-S002, KI-A004 en KI-A005.

Acht themarapporten zijn in de eerdere integratieronde gericht gelezen; vier andere thema's zijn inhoudelijk alleen via het hoofdrapport gescreend. Het downloaden van de overige volledige documenten voor dit archief verandert die leesgrens niet. De niet-openbare verhaallijnen van de combinatiescenario's over sanctiepolitiek en Big Tech zijn niet verkregen. De verwijzing vanuit het hoofdrapport naar het DBSA toont bovendien dat conclusies tussen deze publicaties kunnen worden doorgegeven. Zie KI-A006 en Dataverantwoording.

CLARIS is verwant door de ordening van activiteiten naar tactiek, doelwit en sector, maar heeft een andere actor- en geografische afbakening. Vijftien zichtbare Nederlandlabels zijn als onderzoeksspoor geregistreerd: twee zijn uitgewerkt, één verwijst naar een bestaand dossier en twaalf blijven ongeverifieerd. In de methodenota en dashboardweergave zijn verschillende periodeaanduidingen aangetroffen. Een tijdas die doorloopt tot 2026 is geen bewijs van complete dekking tot die datum. De databron wordt daarom niet automatisch geïmporteerd als Nederlandse jaarreeks. Het colofon noemt financiering door de Taipei Representative Office; de auteurs verklaren onafhankelijkheid. Beschikbare berichtgeving, attributie en selectie blijven methodische beperkingen. Zie KI-S009, KI-A007 en het register.

Naast deze drie kaders is de methodologie van Dreigingsmonitor geraadpleegd. Termfrequentie in een vaste verzameling jaarverslagen onderzoekt een ander verschijnsel dan een casusdossier: institutionele aandacht in tekst is niet hetzelfde als incidentfrequentie. Die vergelijking is een vergelijking van onderzoeksontwerp, geen kwaliteitsrangschikking. Er is geen systematische inventarisatie van alle Nederlandse onderzoeken verricht; dit rapport claimt daarom niet het grootste, eerste of meest volledige onderzoek van zijn soort te zijn. Zie PO-S001.

09 Tegenindicaties en grenzen van de conclusies

Tegenindicaties maken deel uit van het resultaat. Bij K005 is verhindering van netwerktoegang beschreven; verijdeling van bewezen sabotage blijft onbekend. Bij de chipinformatiezaak gelden de bewezen feiten in eerste aanleg naast gedeeltelijke vrijspraken, met onbekende rechtsmiddelstatus. De testpakketten uit Amsterdam bewijzen geen voorkomen vliegtuigaanslag en de beschuldiging tegen de verzenders is ingetrokken. Geconfisqueerde zonnepanelen werden later teruggegeven. Deze verschillen verhinderen dat iedere poging, verstoring of beschuldiging als gerealiseerde schade wordt gepresenteerd. Zie K005, RF005, RF011, RF007 en Verwerking.

De politiehackclaim uit 2017, de TU/e-zaak, de latere ICC-sanctieclaim en de specifieke claim over Oekraïense MH17-spionage hebben nog ontbrekende primaire onderbouwing of beperkte bronlezing. Het dossier houdt deze sporen zichtbaar, met ontkenningen waar vastgelegd. Ze dragen geen bevestigde conclusie over statelijke aansturing. Open sporen zijn onderzoekstaken, geen vermoedelijke incidenten die alvast in een totaal mogen worden opgenomen. Zie RF003, RF004, RF013 en RF014.

De bronnenverzameling bevat ongelijkmatige jaar- en sectordekking, veranderende definities en gedeeltelijk ontoegankelijke originelen. De selectie van berichtgeving is niet representatief voor alle media. Er kan daarom geen uitspraak worden gedaan over een landelijk verijdelingspercentage, alle unieke drones,

alle verdachte scheepsreizen, alle slachtoffers, totale maatschappelijke schade of procentuele groei van de werkelijke dreiging. Een samengestelde score zou verschillende en deels overlappende eenheden een schijnbaar gemeenschappelijke maat geven.

10 Wat de afsluitronde over 27–31 oktober toevoegt

Dreiging via mensen met toegang

De AIVD publiceerde op 28 oktober een waarschuwing en brochure over dreiging van binnenuit. Personen met huidige of vroegere toegang kunnen informatie weggeven of activiteiten mogelijk maken. De dienst onderscheidt bewuste medewerking en onbewuste schade. De brochure bevat illustratieve voorbeelden; die zijn geen nieuw geregistreerde Nederlandse spionagegevallen. De URL noemt27 oktober, maar de zichtbare publicatie- en metadatadatum zijn28 oktober. AIVD-bericht, AC-A001; AC-S002/011.

Spoor: concretere gevolgen van een oudere gebeurtenis

G005 blijft het bestaande aggregaat over 15 september 2026. De oorspronkelijke Kamerantwoorden van 28 oktober noemen40 verstoringen en een NS-schatting van ruim 44.000 niet-gemaakte reizen. Dit zijn geen40 unieke aanvallen en geen44.000 unieke slachtoffers. De eerdere35 meldingen uit N19 worden niet stilzwijgend vervangen: de eenheden en afbakening zijn niet als identiek vastgesteld. Volgens de antwoorden voorkwam de beveiliging op veel locaties ernstigere ongelukken; de exacte financiële impact is onbekend. De bron stelt geen buitenlandse opdrachtgever vast. Het bedrag van 197 miljoen euro betreft beschikbare investeringsmiddelen voor spoor/TEN-T, geen gemeten schade en geen bewijs van effect. Kamerantwoord2026D53822, AC-S003/008.

Eemshaven: een aanhouding, onduidelijkheid over de overige meldingen

Op 28 oktober werd via burgemeester en politie bekend dat op 20 oktober een dronebestuurder was aangehouden. Volgens ANP en Eemskrant is hij vrijgelaten en blijft hij verdachte. De man woont in België; zijn nationaliteit is niet bekendgemaakt. De beschreven overname van de dronebesturing is via berichtgeving onderbouwd, zonder eigen technisch dossier. Een verband met andere Groningse waarnemingen is vooralsnog niet vastgesteld. Motief, opdrachtgever en unieke aantallen blijven onbekend. Geen bewezen Russische operatie uit deze aanhouding afleiden. ANP, Eemskrant; AC-E001, AC-S006/007.

Nieuw opsporingsbericht over mogelijke diensten voor een buitenlandse mogendheid

OM en politie meldden op 28 oktober dat op 27 oktober een al gedetineerde man opnieuw was aangehouden. De nieuwe verdenking betreft handelingen voor een buitenlandse mogendheid, waaronder intimidatie en bedreiging bij bijeenkomsten in 2025–2026. De aanhouding is een opsporingshandeling; de onderliggende intimidatie en statelijke aansturing blijven verdenkingen. De bron benoemt geen specifieke opdrachtgever. De aangekondigde voorgeleiding op 30 oktober is geen gelezen rechterlijk besluit; de uitkomst daarvan is niet vastgesteld. OM en politie vormen hier dezelfde bewijsfamilie. OM; AC-E002, AC-S021/023.

Bescherming op zee en Koninkrijkscontext

Op 29 oktober kondigde Defensie aan dat EU/NAVO-samenwerking hubs in Riga en Scheveningen versterkt; in Scheveningen gaat het om SeaSEC en veiligheid op en onder water, waaronder kabels en leidingen. Op 30 oktober kreeg Defensie volgens het ministerie een permanente monitoringtaak rond het Caribisch deel van het Koninkrijk. Beide zijn maatregelen/mandaten. Ze bewijzen geen extra aanvallen of al behaald veiligheidseffect en sluiten de historische Caribische dekkingslacune niet. Hubs, Caribisch mandaat; AC-R001/002, AC-S004/005.

Aanvullende cyberduiding en een journalistiek spoor

Het NCSC-bericht van 7 oktober over verwachte Chinese cyberaanvallen via routers, VPN-servers en firewalls is als oudere bronaanvulling opgenomen. De diensten verwachten groei en verwijzen naar eerder getroffen Nederlandse organisaties; dit is geen gemeten groeipercentage of nieuw oktoberincident. Het onderliggende cyberadvies is deze ronde niet integraal beoordeeld. NCSC; AC-A002, AC-S009.

FTM publiceerde op 31 oktober onderzoek naar advertentiedata en Gazprom. De gelezen beschikbare hoofdtekst beschrijft een Spaanse test en een eerdere Nederlandse relatie. FTM meldt tegelijk dat het tijdens het eigen onderzoek geen verkeer tussen Between Digital en Mediahuis/De Telegraaf vond. De ruwe onderzoeksdata zijn niet verkregen of gereproduceerd; wat met verzamelde gegevens gebeurt blijft onduidelijk. Dit is een journalistieke claim en onderzoeksspoor, geen bewezen Nederlandse rekruterings- of sabotageoperatie. FTM; AC-C001, AC-S013.

11 Hypothesen, alternatieven en zekerheid

H1: meer zichtbare registraties weerspiegelen mede betere detectie, registratie of openbaarmaking. H2: er vinden daadwerkelijk meer of ernstiger activiteiten plaats. H3: specifieke gebeurtenissen hebben een onbedoelde, binnenlandse of andere niet-statelijke oorzaak. Dit zijn toetsbare verklaringen; H1 en H2 kunnen tegelijk gelden. Het verschijnen van de Eemshaven-aanhouding in de media acht dagen na de gebeurtenis ondersteunt het belang van openbaarmakingsvertraging, zonder een algemene verklaring voor alle meldingen te leveren. Officiële dreigingsoordelen ondersteunen H2 op onderdelen; zonder vergelijkbare nationale gegevens is hun aandeel niet te berekenen. De niet-vastgestelde opdrachtgever bij G005 en AC-E001 houdt H3 open, zonder die verklaring als bewezen te kiezen. Deze kwalitatieve vergelijking is geen kwantitatieve ACH-score.

AC-K001 - ASSESSMENT, MODERATE CONFIDENCE: officiële beoordelingen ondersteunen toegenomen dreiging op belangrijke onderdelen, vooral vanuit Rusland. Hun informatiepositie is relevant, maar onderliggende gegevens zijn niet volledig openbaar en publicaties kunnen dezelfde familie delen. Hoge zekerheid dat de beoordeling bestaat is geen hoge zekerheid in ieder onderliggend geval.

AC-K002 - ASSESSMENT, HIGH CONFIDENCE: een eigen landelijk groeipercentage, aanvalstotaal of totale schade is met dit selectieve corpus niet verantwoord te berekenen. De gedocumenteerde selectie, ontbrekende jaren en verschillende meeteenheden dragen deze conclusie.

AC-K003 - ASSESSMENT, MODERATE CONFIDENCE: menselijke toegang en druk op personen verdienen expliciete aandacht. AIVD, eerdere persoonsdossiers en de nieuwe opsporingsverdenking onderbouwen die onderzoeksprioriteit. Schuld, omvang en opdrachtgever blijven per geval te beoordelen. AC-K004 - ASSESSMENT, MODERATE CONFIDENCE: concrete gevolgen zijn voor sommige dossiers beter te beschrijven dan een nationale totaalimpact; de reizigersschatting bij G005 ondersteunt dit, met onbekende ruwe data en euro-schade.

12 Conclusies en gebruik voor vervolgmonitoring

Het onderzoek onderbouwt een brede, reeds vóór 2022 aanwezige geschiedenis van activiteiten en dreigingsbeoordelingen met een Nederlandse relatie. Het laat zien hoe dezelfde samenleving rechtstreeks doelwit kan zijn, gastland van internationale instellingen kan vormen en via internationale ketens kan worden geraakt. De bewijssterkte en maatschappelijke gevolgen moeten per dossier worden beoordeeld.

De verbreding maakt duidelijk dat drones, Noordzeeactiviteiten en elektronische verstoring niet mogen ontbreken, maar ook niet zonder technische bevestiging en een duidelijke teleenheid tot bewezen vijandige operaties mogen worden verklaard. Economische, politieke en persoonlijke kwetsbaarheden horen bij dezelfde onderzoeksopgave, met afzonderlijke criteria voor concrete handelingen en gevolgen.

De beschikbare bronreeksen maken beperkte uitspraken over geregistreerde meldingen of begeleidingen mogelijk. De totale ontwikkeling van Nederlandse hybride activiteit, ernst of impact tussen 2014 en 2026 blijft met dit corpus niet kwantificeerbaar. Dat is een inhoudelijke uitkomst, geen reden om onbekende waarden in te vullen.

De praktische opbrengst is een versiegebonden, controleerbare referentiebasis voor vervolgmonitoring. Nieuwe gebeurtenissen, latere openbaarmakingen van oude gebeurtenissen, gewijzigde attributies en gewijzigde officiële beoordelingen moeten als verschillende soorten wijzigingen worden opgeslagen. Vervolgonderzoek heeft vooral waarde als het ontbrekende primaire stukken, onduidelijke definities en historische sectorlacunes gericht oplost. De volledige lijst met heropeningsvoorwaarden staat in Open punten.

De synthese is vrijgegeven voor publicatie binnen de vastgezette kwalitatieve scope. Een onafhankelijke menselijke inhoudelijke review is niet uitgevoerd. Publicatie loopt uitsluitend via het afzonderlijke Boog-IT-websiteproject. Het interne pakket met bronkopieën, zoeklogs en controlegegevens is geen publieke website-export.

De basisperiode t/m 31 oktober is hiermee binnen de kwalitatieve scope afgesloten. De aanvullende broncontrole en redactie zijn uitgevoerd op 1 november. Afsluiting sluit bestaande bron-, sector- en verificatielacunes niet. Nieuwe informatie vanaf 1 november wordt in de vervolglaag opgenomen, met gebeurtenisdatum en bekendmakingsdatum afzonderlijk. Een onafhankelijke menselijke inhoudelijke review is niet uitgevoerd.

13 Samen onderzoeken: mens en AI

Dit onderzoek is de eerste casus van een Boog-IT-pilot: hoe kunnen een mens en kunstmatige intelligentie (AI) samen een begrijpelijk en controleerbaar onderzoek maken? Het onderwerp is hybride dreiging. De pilot gaat over de manier waarop we dat onderzoek uitvoeren. De twee vragen houden we uit elkaar: een bruikbaar onderzoeksrapport bewijst nog niet dat deze werkwijze beter is dan andere werkwijzen.

De visie van Boog-IT

Voor Boog-IT staat OSINT aan het begin van een nieuwe fase. OSINT is onderzoek waarbij we informatie uit openbare bronnen verzamelen, beoordelen en omzetten in bruikbare inzichten. Met hulp van AI willen we dat onderzoek sneller uitvoeren, meer relevante bronnen betrekken en onderwerpen beter in samenhang begrijpen. Denk aan de verbinding tussen digitale aanvallen, druk op mensen, economische afhankelijkheden en de bescherming van infrastructuur.

Boog-IT wil hierin pionieren door expertise in het cyberdomein te verbinden met OSINT en AI. Cyberexpertise helpt technische gebeurtenissen en kwetsbaarheden te begrijpen. OSINT geeft richting aan het zoeken en beoordelen van openbare informatie. AI ondersteunt het verwerken van informatie, het leggen van mogelijke verbanden en het helder opschrijven van bevindingen. Menselijke expertise en beoordeling blijven nodig om richting te geven, aannames te toetsen en conclusies te verantwoorden.

Openbaar is meer dan online

Niet alle informatie is openbaar. Ook is niet alle openbare informatie online te vinden: denk aan boeken, fysieke archieven en stukken die alleen ter inzage beschikbaar zijn. Een onderzoek dat uitsluitend zoekmachines gebruikt, kan daardoor relevante bronnen missen.

Andersom is online vindbaarheid niet hetzelfde als beschikbaarheid als openbare bron. Een zoekresultaat of een werkende link zegt op zichzelf niet voor wie informatie toegankelijk of bestemd is. Bij afgeschermde, gelekte of onbedoeld blootgestelde gegevens moeten herkomst, toegangsvoorwaarden en geschiktheid voor dit onderzoek afzonderlijk worden beoordeeld.

Een openbare bron hoeft bovendien niet gratis te zijn. Een boek, krantenabonnement of commerciële databank kan voor het publiek beschikbaar zijn. Openbare beschikbaarheid betekent ook niet dat materiaal vrij mag worden hergebruikt. Vindbaarheid, toegang en hergebruik zijn verschillende vragen. Met open source bedoelen we hier openbare informatiebronnen; dat zegt niets over een vrije software- of hergebruiklicentie.

Onderzoek met zichtbare grenzen

AI maakt ontbrekende informatie niet vanzelf beschikbaar en een voorgesteld verband is nog geen vastgestelde samenhang. We houden daarom bij welke bronnen werkelijk zijn geraadpleegd, welke passages de conclusies dragen en wat onbekend blijft. Voor dit onderzoek is de dekking van niet-digitale bronnen niet systematisch vastgesteld; hun mogelijke belang is geen claim dat ze al volledig zijn onderzocht.

Met deze pilot wil Boog-IT een werkwijze ontwikkelen waarin cyberexpertise, brononderzoek en AI elkaar versterken. Sneller, breder en integraler onderzoek is onze ambitie. In vervolgupdates willen we beoordelen wat deze samenwerking daadwerkelijk oplevert. Deze pilot bevat nog geen gemeten tijdwinst, kostenbesparing of bewezen kwaliteitsvoorsprong. Pionieren beschrijft onze inzet om de aanpak te ontwikkelen en ervan te leren; het is geen claim dat Boog-IT de eerste of enige partij is die zo werkt.

Wat Maurice heeft bijgedragen

Maurice bepaalde het doel en stuurde de inhoudelijke verbreding. Hij vroeg onder meer om drones, activiteiten op de Noordzee en druk op mensen mee te nemen. Ook vroeg hij om begrijpelijke taal, vergelijking met bestaande onderzoeken, bewaring van bronnen en een afzonderlijke AI-review. Hij zette de basisperiode vast tot en met 31 oktober 2026 en koos voor deze pilot met mens en AI.

Maurice is opdrachtgever en beoogd eindredacteur. Boog-IT draagt de redactionele verantwoordelijkheid. Deze editie is door de opdrachtgever vrijgegeven voor publicatie. Dat is geen onafhankelijke inhoudelijke review. Uit zijn sturing volgt niet dat hij iedere bron persoonlijk heeft gecontroleerd of alle conclusies al heeft goedgekeurd.

Wat AI heeft bijgedragen

De AI-assistent hielp bronnen vinden, passages lezen, documenten opslaan en informatie ordenen. AI maakte voorstellen voor de analyse, schreef en herschreef teksten en voerde controles op bestanden, verwijzingen en PDF's uit. Er zijn ook afzonderlijke AI-reviews uitgevoerd. De bronregisters en onderzoekslogs leggen vast welke stukken zijn gelezen en waar beperkingen zitten; een opgeslagen document is niet automatisch volledig gelezen of inhoudelijk bevestigd.

Een AI-review kan fouten aanwijzen, maar ook dezelfde blinde vlekken hebben als de AI die de tekst schreef. Zij vervangt geen onafhankelijke menselijke inhoudelijke review. Die beoordeling en een test met lezers zonder voorkennis staan nog open.

Hoe we controle mogelijk maken

We onderscheiden wat een bron meldt, wat daarvan is onderbouwd en welke conclusie we zelf trekken. Een melding is geen bewezen aanval. Een bronbestand en een controle op ongewijzigde opslag bewijzen niet dat de inhoud klopt. Bij belangrijke conclusies leggen we uit hoe zeker we zijn en waarom.

De afsluitende methodereview gebruikt de RIS Propeller Intelligence Cycle van Arno Reuser (2017). Daarbij staan de informatiebehoefte en terugkoppeling met de opdrachtgever centraal. De concrete toepassing en grenzen zijn beschreven in de onderzoeksverantwoording. De aanvullende bewijslabels en zekerheidsniveaus zijn een Boog-IT-uitwerking. Dit is geen RIS-certificering en geen claim dat alle historische onderzoeksrondes deze methode al volledig volgden.

De afzonderlijke AI-review van de afsluitende basiseditie leidde tot drie vastgelegde verbeteringen: de verwijzingen naar de geldende afbakening en open vragen zijn verduidelijkt; de samenvatting vermeldt nu dat de vrijgelaten dronebestuurder verdachte blijft; en de samenvatting maakte de toenmalige onderzoeksstatus expliciet. Dit laat zien wat die controle opleverde. Het bewijst niet dat alle fouten zijn gevonden of dat AI nauwkeuriger werkt dan een mens.

Wat we met de pilot willen leren

De hoofdvraag voor de pilot is: hoe helpt deze samenwerking om openbare bronnen te vertalen naar een begrijpelijk verhaal waarvan lezers de onderbouwing en grenzen kunnen nagaan? Bij volgende updates willen we vastleggen of uitspraken naar de juiste bronpassage leiden, welke inhoudelijke correcties nodig zijn, wat lezers begrijpen en welke keuzes de eindredacteur maakt.

Het evaluatieplan is op 1 november 2026 toegevoegd, nadat het onderzoek al was begonnen. Er is geen vooraf opgezet vergelijkend experiment uitgevoerd. Tijdwinst, kostenbesparing en een nauwkeurigheidspercentage zijn niet gemeten. De eerste lessen en uitgevoerde controles zijn vastgelegd; een volledige evaluatie moet nog volgen.

Wat de lezer nu krijgt

Een uitgebreid onderzoek op basis van geselecteerde openbare bronnen over 1 januari 2014 tot en met 31 oktober 2026, met een samenvatting, bronverwijzingen en expliciete onzekerheden. De aanvullende broncontrole en deze redactie zijn uitgevoerd op 1 november. Deze piloteditie verandert de inhoudelijke onderzoeksgrens en dreigingsconclusies niet.

Vanaf november volgen maandrondes op initiatief van Maurice. Per kwartaal is een publicatie-update voorzien via het afzonderlijke websiteproject; de eerste vervolgperiode is november-december 2026. Nieuwe gegevens en correcties krijgen een eigen datum en versie, zodat zichtbaar blijft wat wanneer bekend was.

14 Bronnen en leesverantwoording

Oudere bronkaarten en passages blijven bewaard in het onderzoeksdossier van 26 oktober. De nieuwe bronnenronde heeft eigen bronkopieën, leesnotities en open vragen. Hieronder staan de gebruikte openbare verwijzingen. Het vermelden van een bron betekent geen integrale verificatie of onafhankelijk bewijs.

N20 Foreign Office Minister condemns Russia for NotPetya attacks

https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks

N21 Lessen uit crises en mini-crises 2017 - Cyberaanval op Maersk

https://nipv.nl/documenten/lessen-uit-crises-en-mini-crises-2017/

N22 Ook bij tegenslag en rampspoed: de haven moet door

https://publications.portofrotterdam.com/havenkrant-68/ook-bij-tegenslag-en-rampspoed-de-haven-moet-door

N01 Russian cyber operation disrupted

https://www.ministryofdefence.nl/topics/c/cyber-security/russian-cyber-operation

PR-S006 Over de grens - statelijke inmenging in diasporagemeenschappen

https://www.aivd.nl/site/binaries/site-content/collections/documents/2024/10/17/over-de-grens-statelijke-inmenging-in-diasporagemeenschappen-in-nederland/Over%2Bde%2Bgrens.%2BStatelijke%2Binmenging%2Bin%2Bdiasporagemeenschappen%2Bin%2BNederland.pdf

RS-MV2021 MIVD openbaar jaarverslag 2021

https://zoek.officielebekendmakingen.nl/blg-1028578.pdf

RS-MV2022 MIVD openbaar jaarverslag 2022

https://open.overheid.nl/documenten/ronl-fe92eb9796cac86ecf33c8fdd97167cd1543df8a/pdf

https://www.rijksoverheid.nl/documenten/2023/04/19/openbaar-jaarverslag-2022-mivd

RS-MV2023 MIVD openbaar jaarverslag 2023

https://berthub.eu/tkconv/getraw/2024D15864

https://www.defensie.nl/binaries/defensie/documenten/jaarverslagen/2024/04/18/jaarverslag-mivd-2023/MIVD_Openbaar%2Bjaarverslag%2B2023%2B_18april.pdf

RS-P003 Verstoring van het Cyclops Blink-botnet

https://www.justice.gov/archives/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation

N05 Russische brutaliteit om samenleving te ontwrichten neemt toe

https://www.defensie.nl/nieuws/20250422-russische-brutaliteit-om-samenleving-te-ontwrichten-neemt-toe

N28 AIVD jaarverslag 2025 - Rusland

https://www.aivd.nl/actueel/magazines/jaarverslag/jaarverslag/2025/rusland

AS001 Boycot raakt exporteurs nauwelijks

https://www.cbs.nl/nl-nl/achtergrond/2014/33/boycot-raakt-exporteurs-nauwelijks

RM001 Russische internetspionnen wilden MH17-rapport hacken

https://nos.nl/artikel/2064585-russische-internetspionnen-wilden-mh17-rapport-hacken

RS-P004 Hazards Ahead - TrendLabs 3Q 2015 Security Roundup

https://documents.trendmicro.com/assets/wp/rpt-hazards-ahead.pdf

N02 Iran likely involved in assassinations in the Netherlands

https://english.aivd.nl/latest/news/2019/01/08/iran-likely-involved-in-assassinations-in-the-netherlands

N03 23 jaar en 6 maanden celstraf voor moord op een Iraanse man in Almere in 2015

https://www.rechtspraak.nl/organisatie-en-contact/organisatie/gerechtshoven/gerechtshof-arnhem-leeuwarden/nieuws/2022/11/23-jaar-en-6-maanden-celstraf-voor-moord-op-een-iraanse-man-in-almere-in-2015

N48 Arrest ECLI:NL:GHARL:2022:10113

https://data.rechtspraak.nl/uitspraken/content?id=ECLI:NL:GHARL:2022:10113

N04 Verdachten aangehouden onderzoek dood Iraanse man

https://www.politie.nl/nieuws/2025/mei/16/06-verdachten-aangehouden-onderzoek-dood-iraanse-man.html

N42 Verdachten niet vervolgd voor dood Iraanse man, onderzoek schutter loopt nog

https://www.om.nl/actueel/nieuws/2026/04/03/verdachten-niet-vervolgd-voor-dood-iraanse-man-onderzoek-schutter-loopt-nog

PR-S004 Kamerbrief over Diyanet-vertegenwoordiger

https://zoek.officielebekendmakingen.nl/kst-32824-177.html

PR-S005 Kamerbrief onderzoek Turkse religieuze organisaties

https://zoek.officielebekendmakingen.nl/kst-32824-198.html

N12 AIVD verstoort activiteiten Russische inlichtingenofficier richting Internationaal Strafhof

https://www.aivd.nl/actueel/nieuws/2022/06/16/aivd-verstoort-activiteiten-russische-inlichtingenofficier-richting-internationaal-strafhof

N13 War crimes tribunal says September cyberattack was spying attempt

https://www.reuters.com/world/war-crimes-tribunal-says-september-cyberattack-was-spying-attempt-2023-10-20/

RS-CS2024 Cybersecuritybeeld Nederland 2024

https://www.nctv.nl/site/binaries/site-content/collections/documents/2024/10/28/cybersecuritybeeld-nederland-2024/CSBN%2B2024%2BA4%2B-%2BWebversie%2BDEF%2B-%2Bkopie.pdf

KI-S012 Kamerbrief - informatiedeling COATHANGER

https://zoek.officielebekendmakingen.nl/kst-30821-239.html

KI-S013 NCSC - bredere COATHANGER-campagne

https://www.ncsc.nl/nieuws/aanhoudende-statelijke-cyberspionagecampagne-kwetsbare-edge-devices

KI-S014 MIVD/AIVD - COATHANGER advisory

https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-coathanger-tlp-clear/TLP-CLEAR%2BMIVD%2BAIVD%2BAdvisory%2BCOATHANGER.pdf

PR-S001 GasTerra jaarverslag 2022 - materiële onderwerpen

https://jaarverslagen.gasterra.nl/jaarverslag-2022/materiele-onderwerpen

PR-S002 GasTerra: besluit over betalingseisen Gazprom

https://www.gasterra.nl/en/news/gasterra-will-not-go-along-with-gazproms-payment-demands

PR-S003 Kamerantwoorden Chinese politiebureaus - vervolgonderzoek

https://www.tweedekamer.nl/downloads/document?id=2023D30544

RM013 Verantwoording van onderzoek naar verstoring van BabyTV

https://nos.nl/nieuwsuur/artikel/2544558-verantwoording-en-bronnen-bij-de-ophef-aflevering-over-de-verstoringen-van-babytv

KI-S010 Defensie - benadering Zr.Ms. Tromp

https://www.defensie.nl/actueel/nieuws/2024/06/07/marineschip-benaderd-door-chinese-helikopter-en-gevechtsvliegtuigen

KI-S011 Chinese defensiewoordvoerder - reactie op Tromp

https://eng.mod.gov.cn/xb/News_213114/TopStories/16315244.html

N62 Dreigingsbeeld Statelijke Actoren 2025

https://www.nctv.nl/site/binaries/site-content/collections/documents/2025/07/17/dreigingsbeeld-statelijke-actoren-2025/Dreigingsbeeld%2BStatelijke%2BActoren%2B(DBSA)%2B2025.pdf

SP-S005 ILT Jaarpublicatie ABL 2023

https://www.ilent.nl/documenten/luchtvaart/voorvallen-luchtvaart/publicaties/jaarpublicatie-analysebureau-luchtvaartvoorvallen-2023

SP-S006 ILT Factsheet Gemelde dronevoorvallen

https://www.ilent.nl/documenten/luchtvaart/drones-rpas/factsheets/factsheet-drones-2023

SP-S003 Ongewenste drone-activiteiten boven Defensieterreinen

https://zoek.officielebekendmakingen.nl/kst-30806-59.html

SP-S020 Verslag overleg bestrijding drones, 36858-6

https://zoek.officielebekendmakingen.nl/kst-36858-6.html

SP-S013 NOS: Meer ongelukken met drones

https://nos.nl/artikel/2042966-meer-ongelukken-met-drones

N14 Antwoorden Noordzee-spionage, nr. 360

https://zoek.officielebekendmakingen.nl/ah-tk-20242025-360.html

SP-S010 Algemene Rekenkamer: Verantwoordingsonderzoek IenW, MF en DF 2025

https://www.tweedekamer.nl/downloads/document?id=2026D23148

SP-S001 Marine begeleidde bijna dubbel zoveel Russische schepen op de Noordzee

https://nos.nl/artikel/2550962-marine-begeleidde-bijna-dubbel-zoveel-russische-schepen-op-de-noordzee

SP-S015 Defensie Jaarverslag 2016: vragen en antwoorden, 34725-X-9

https://zoek.officielebekendmakingen.nl/kst-34725-X-9.html

SP-S021 Pointer: Russische schepen bespioneren ongemoeid onze wateren

https://pointer.kro-ncrv.nl/russische-schepen-bespioneren-ongemoeid-onze-wateren

SP-S009 Pointer: Rusland bespioneert systematisch onze wateren

https://pointer.kro-ncrv.nl/rusland-bespioneert-systematisch-onze-wateren

SP-S008 ILT Jaarpublicatie ABL 2024

https://www.ilent.nl/documenten/luchtvaart/voorvallen-luchtvaart/publicaties/jaarpublicatie-analysebureau-luchtvaartvoorvallen-2024

SP-S011 Agentschap Telecom Jaarbericht 2021

https://www.rdi.nl/site/binaries/site-content/collections/documenten/2022/04/21/jaarbericht-2021/Jaarbericht%2BAgentschap%2BTelecom%2B2021.pdf

RS-P008 EU-sancties tegen Voice of Europe en twee betrokkenen

https://www.consilium.europa.eu/en/press/press-releases/2024/05/27/information-manipulation-in-russia-s-war-of-aggression-against-ukraine-eu-lists-two-individuals-and-one-entity/

RM009 Zo werd een Nederlandse nieuwssite een Russisch propagandakanaal

https://nos.nl/nieuwsuur/artikel/2514611-zo-werd-radicaal-rechtse-nederlandse-nieuwssite-een-russisch-propagandakanaal

N16 Imposing Sanctions on the International Criminal Court

https://www.whitehouse.gov/presidential-actions/2025/02/imposing-sanctions-on-the-international-criminal-court/

N15 Surveillance and interference: Israel's covert war on the ICC exposed

https://www.972mag.com/icc-israel-surveillance-investigation/

N47 Antwoorden over Israëlische inlichtingendiensten en het Internationaal Strafhof

https://open.overheid.nl/documenten/1859d7c5-5e54-42d8-b060-4c4b7aa59420/file

RS-P010 ICC-bericht over sancties tegen de instelling · controle nog beperkt

https://www.icc-cpi.int/news/icc-strongly-rejects-us-sanctions-against-institution

RM014 Nederland bereidt zich voor op verdere VS-sancties tegen Strafhof

https://nos.nl/artikel/2632708-nederland-wapent-zich-met-europese-bondgenoten-tegen-vs-aanval-op-strafhof

N29 Dreigingslandschap Vitale Infrastructuur 2025

https://www.nctv.nl/site/binaries/site-content/collections/documents/2025/07/23/dreigingslandschap-vitale-infrastructuur/Dreigingslandschap%2BVitale%2BInfrastructuur%2B(2025).pdf

KI-S001 RRA2026 - Cyberdreigingen

https://www.nctv.nl/site/binaries/site-content/collections/documents/2026/10/16/themarapport-cyberdreigingen-2026/themarapport-cyberdreigingen-2026-beveiligd2.pdf

KI-S005 RRA2026 - Combinatiescenario Big Tech

https://www.nctv.nl/site/binaries/site-content/collections/documents/2026/10/16/themarapport-combinatiescenario-de-duistere-kanten-van-big-tech-2026/themarapport-combinatiescenario-de-duistere-kanten-van-big-tech-2026-beveiligd2.pdf

KI-S007 RRA2026 - Combinatiescenario Water

https://www.nctv.nl/site/binaries/site-content/collections/documents/2026/10/16/themarapport-combinatiescenario-water-een-zegen-of-een-vloek-2026/themarapport-combinatiescenario-water-een-zegen-of-een-vloek-2026-beveiligd.pdf

RS-MV2024 MIVD openbaar jaarverslag 2024

https://open.overheid.nl/documenten/204ba7fc-ee17-4209-b5c7-fdeaa21180ca/file

https://www.rijksoverheid.nl/documenten/2025/04/22/mivd-openbaar-jaarverslag-2024

RM008 AIVD: opgepakte werknemer ASML had contact met Russische geheime dienst

https://www.nhnieuws.nl/nieuws/n176412/aivd-opgepakte-werknemer-asml-had-contact-met-russische-geheime-dienst

RS-P001 Vonnis ECLI:NL:RBROT:2025:8322

https://uitspraken.rechtspraak.nl/details?id=ECLI%3ANL%3ARBROT%3A2025%3A8322

https://data.rechtspraak.nl/uitspraken/content?id=ECLI:NL:RBROT:2025:8322

RS-P002 Strafeis in de chipinformatiezaak

https://www.om.nl/actueel/nieuws/2025/06/26/om-eist-celstraf-tegen-rus-voor-verkoop-bedrijfsgeheime-chipinformatie-aan-rusland

RM012 Verkenning van luchtpostroute met testpakketten uit Amsterdam

https://nos.nl/nieuwsuur/collectie/13998/artikel/2571889-man-in-nederland-ingehuurd-voor-verkenning-aanslag-met-dhl-pakket

RS-P007 Antwoorden over Nederlandse ontwikkelingsprojecten op de Westelijke Jordaanoever

https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?did=2025D01845&id=2024Z18884

RM003 Russen zaten in 2017 in Nederlandse politiesystemen

https://nos.nl/artikel/2384080-russen-zaten-in-2017-in-nederlandse-politiesystemen

RS-P005 Commissiedebat MH17 van 16 juni 2021

https://www.tweedekamer.nl/kamerstukken/commissieverslagen/detail?did=2021D25273&id=2021D25273

RM002 Universiteit Eindhoven ontslaat Russische onderzoeker om spionage

https://nos.nl/artikel/2049315-universiteit-eindhoven-ontslaat-russische-onderzoeker-om-spionage

RS-P009 Gezamenlijke overheidsreactie bij berichtgeving over MH17-spionage

https://www.rtlnieuws.nl/sites/default/files/content/documents/2018/06/26/REAX-MINISTERIES.pdf

RM011 Nederlander bij Stuxnet-operatie volgens Volkskrant-onderzoek

https://www.nhnieuws.nl/nieuws/n137413/nederlander-saboteerde-atoomcomplex-in-iran-den-haag-wist-niets

N18 Russische hackersgroep Laundry Bear hackt Zimbra mailservers

https://www.aivd.nl/actueel/nieuws/2026/07/23/russische-hackersgroep-laundry-bear-hackt-zimbra-mailservers

PO-S002 Rijksbrede Risicoanalyse Nationale Veiligheid 2026 - hoofdrapport

https://www.nctv.nl/site/binaries/site-content/collections/documents/2026/10/16/rijksbrede-risicoanalyse-nationale-veiligheid-2026/rijksbrede-risicoanalyse-nationale-veiligheid-2026-beveiligd.pdf

KI-S003 RRA2026 - Ongewenste inmenging en beïnvloeding

https://www.nctv.nl/site/binaries/site-content/collections/documents/2026/10/16/themarapport-ongewenste-inmenging-en-beinvloeding-2026/themarapport-ongewenste-inmenging-en-beinvloeding-2026-beveiligd-05-08-2026.pdf

KI-S008 RRA2026 - Internationale en militaire dreigingen

https://www.nctv.nl/site/binaries/site-content/collections/documents/2026/10/16/themarapport-internationale-en-militaire-dreigingen-2026/themarapport-internationale-en-militaire-dreigingen-beveiligd-05-08-206.pdf

PO-S003 HCSS CLARIS - project en Nederlandse dashboardselectie

https://hcss.nl/chinese-latent-activity-and-related-interference-scanner-claris/

KI-S009 HCSS CLARIS - Methodological Notes

https://hcss.nl/wp-content/uploads/2026/02/CLARIS-TRON-Methodological-notes-1.pdf

PO-S001 Dreigingsmonitor - methodologie en datakwaliteit

https://dreigingsmonitor.nl/methodologie/

AC-S001 Reuser (2017) - The RIS Open Source Intelligence Cycle

https://rieas.gr/images/jmbi/ReuserArno.pdf

Geen empirische bron voor Nederlandse incidenten. Gerichte lezing, geen methodologische certificering.

AC-S002 Interne dreigingen vormen een groeiend risico voor organisaties

https://www.aivd.nl/actueel/nieuws/2026/10/27/interne-dreigingen-vormen-een-groeiend-risico-voor-organisaties

URL bevat 27 oktober, zichtbare datum en datePublished zijn 28 oktober. Onderliggende dienstgegevens niet openbaar.

AC-S003 Antwoorden weerbaarheid spoor na sabotage Prinsjesdag - 2026D53822

https://www.tweedekamer.nl/downloads/document?id=2026D53822

44.000 is een NS-schatting van niet-gemaakte reizen. 40 verstoringen niet gelijk aan unieke aanvallen; geen actor vastgesteld.

AC-S004 Innovatiehubs om Europa sneller en beter tegen drones te beschermen

https://www.defensie.nl/nieuws/20261029-innovatiehubs-om-europa-sneller-en-beter-tegen-drones-te-beschermen

Aankondiging/samenwerking, geen bewezen operationeel effect of nieuw sabotagegeval.

AC-S005 Defensie versterkt monitoren veiligheid in Caribisch gebied

https://www.defensie.nl/nieuws/20261030-defensie-versterkt-monitoren-veiligheid-in-caribisch-gebied

Geen uitbreiding tot volledige Caribische historische dekking; geen nieuwe incidententelling.

AC-S006 Man aangehouden voor vliegen met drone boven Eemshaven

https://www.rd.nl/a/man-aangehouden-voor-het-vliegen-met-drone-boven-eemshaven

In België woonachtig; nationaliteit niet bekendgemaakt. Politieverklaring via journalistiek, geen eigen technisch droneonderzoek.

AC-S007 Politie houdt man aan voor vliegen met drone boven Eemshaven

https://www.eemskrant.nl/politie-houdt-man-aan-voor-vliegen-met-drone-boven-eemshaven/

Dezelfde politie-/burgemeestersfamilie als ANP; geen onafhankelijke extra bevestiging. Grote drone met kleine drones onbevestigd.

AC-S008 Metadata Kamerantwoord 2026D53822

https://www.tweedekamer.nl/kamerstukken/detail?did=2026D53822&id=2026D53822

Geen zelfstandige tweede bron voor de schade-inschatting.

AC-S009 Veiligheidsdiensten verwachten toename Chinese cyberaanvallen

https://www.ncsc.nl/nieuws/veiligheidsdiensten-verwachten-toename-chinese-cyberaanvallen

Terugwerkende bronaanvulling van vóór 27 oktober. Verwachting is geen gemeten landelijke toename. Onderliggende cyberadvies niet integraal gelezen in deze ronde.

AC-S011 Weerbaar tegen dreigingen van binnenuit - Herkennen en voorkomen

https://www.aivd.nl/site/binaries/site-content/collections/documents/2026/10/27/weerbaar-tegen-dreigingen-van-binnenuit/weerbaar-tegen-dreigingen-van-binnenuit.pdf

Vijftien PDF-pagina's aanwezig; niet integraal inhoudelijk beoordeeld. Fictieve/illustratieve voorbeelden niet als casussen registreren. Gedrukte paginanummers staan per spread.

AC-S013 Hoe jouw privégegevens via energiegigant Gazprom in het Kremlin kunnen belanden

https://www.ftm.nl/artikelen/hoe-jouw-privegegevens-via-energiegigant-gazprom-in-het-kremlin-kunnen-belanden

Eigen ruwe onderzoeksdata en technisch bewijsmateriaal niet verkregen of gereproduceerd. Geen bewezen Nederlandse sabotage of rekrutering afleiden. Openbare respons gelezen ondanks accountverwijzingen; geen accounttoegang gebruikt.

AC-S021 Man verdacht van verlenen van diensten voor buitenlandse mogendheid

https://www.politie.nl/nieuws/2026/oktober/28/11-man-verdacht-van-verlenen-van-diensten-voor-buitenlandse-mogendheid.html

Verdenking geen bewezen onderliggende intimidatie of opdracht. Bron benoemt geen specifieke opdrachtgever; uitslag voorgeleiding niet vastgesteld.

AC-S023 Man verdacht van verlenen van diensten voor buitenlandse mogendheid

https://www.om.nl/actueel/nieuws/2026/10/28/man-verdacht-van-verlenen-van-diensten-voor-buitenlandse-mogendheid

Zelfde onderzoeksfamilie als politie. Geen onafhankelijke bevestiging van schuld of statelijke aansturing.