Verbinding, verdieping, vooruitgang

Jaarmonitor NBIP 2025

Colofon

Aan deze uitgave hebben meegewerkt

Octavia de Weerdt
algemeen directeur, Stichting NBIP

Wouter Pegtel
communicatie & public affairs manager, Stichting NBIP

Pim Kokke
communicatiespecialist, Stichting NBIP

Opmaak

Bijdevleet, Rotterdam

Voor meer informatie, zie **www.nbip.nl**

Inhoud

Voorwoord

Octavia de Weerdt
Algemeen Directeur NBIP

Verbinding is in de breedste zin van het woord belangrijk voor de samenleving. Of het nu gaat om connectiviteit of menselijk contact, sterke verbindingen zorgen ervoor dat je samen sterker staat. Dat is uiteraard al jaren het uitgangspunt van NBIP met haar operationele diensten. Met name in tijden van geopolitieke veranderingen en spanningen is het cruciaal om eenheid als sector en de samenleving te bewaren en weerbaarheid te tonen.

In het afgelopen kalenderjaar is digitale autonomie het middelpunt geworden van het nationale en Europese debat waarin concreet de vraag is gesteld hoe Europa haar eigen positie moet versterken. Tijdens ons jaarlijkse event NBIP NEXT in november 2025 organiseerde we daarom voor het eerst een tweede dag die was toegewijd aan dit onderwerp. Een van de sprekers was Cristina Caffarra van EuroStack. In nog geen twee jaar tijd is Caffarra uitgegroeid tot een van de meest prominente voorvechter voor een soevereine Europese IT-infrastructuur. In niet mis te verstane woorden gaf ze aan dat Europa zich moet focussen op haar economische toekomst en simpelweg concrete oplossingen moet bouwen.

De boodschap van Caffarra leeft onbewust en bewust al jaren binnen NBIP. Zo nemen we al een aantal jaar deel aan Europese initiatieven en ontwikkelingsprojecten, zoals IPCEI-CIS, die bouwen aan de digitale toekomst van Europa. Het doel is om de komende jaren als NBIP deze positie te verstevigen door samen met de industrie te werken aan Made in Europe diensten op basis van open source. Het elke dag bouwen aan een betrouwbaar internet wordt bij NBIP inmiddels gedaan door 20 medewerkers, elk vanuit zijn of haar specialisme. Daarmee bouwen we verder aan onze missie: het bieden van gezamenlijke faciliteiten voor digitale infrastructuuraanbieders, zodat zij hun digitale weerbaarheid en naleving van wet- en regelgeving op orde hebben. Dat is iets waar ik als directie elke dag trots op ben.

Daarnaast zorgen de nieuwe wet- en regelgeving voor digitale dienstaanbieders voor vragen binnen de sector. Een voorbeeld hiervan is de verordening en richtlijn van eEvidence die naar verwachting een grote impact gaat hebben op de internetsector. Als NBIP willen we daarom op dit wet- en regelgevingsgebied een positie innemen door onze deelnemers nadrukkelijker wegwijs te maken op dit gebied. In het afgelopen jaar zijn de eerste plannen voor de invulling hiervan gemaakt en deze worden in 2026 werkelijkheid.

In deze vernieuwde Jaarmonitor lees je meer over alle activiteiten van NBIP in het afgelopen kalenderjaar.

Veel leesplezier.

Samenvatting

Jaarmonitor 2025

De missie ‘Samen sterker voor een betrouwbaar internet’ stond in 2025 centraal bij alle activiteiten van NBIP. Er is stevig ingezet op het intensiveren van de betrokkenheid van en met deelnemers, partners en stakeholders.

Verbinding

Het aantal deelnemers van NBIP is in 2025 gegroeid. Eind 2025 had NBIP 194 deelnemers, waarvan 107 organisaties deelnemen aan de Tapdienst en 131 organisaties deelnemen aan de NaWas. Er zijn 44 organisaties die deelnemen aan beide diensten. Organisaties die zowel van de Tapdienst als de NaWas gebruikmaken, worden in het totaal aantal deelnemers van NBIP als één enkele deelnemer geteld. Hierdoor zorgen we voor een veiliger en betrouwbaarder internet.

In 2024 werden voor het eerst Lunch & Learn sessies voor deelnemers georganiseerd om een laagdrempelige manier te creëren voor deelnemers om met NBIP in contact te treden, bijgepraat te worden over recente ontwikkelingen en vragen te stellen. Deze sessies zijn in 2025 doorgezet en mogen op steeds meer belangstelling rekenen, met als hoogtepunt in oktober 2025 ruim 25 aanwezige deelnemers.

NBIP is snel gegroeid als organisatie en eindigde 2025 met zo’n 20 medewerkers met het vooruitzicht van verdere groei in 2026. Die groei zit hem onder meer in de deelname in Europese ontwikkelingsprojecten zoals IPCEI-CIS en LLMs for Europe. Het bestuur van NBIP heeft voorgesorteerd op deze groei door in 2025 een vacature voor een secretaris en een vacature voor een algemeen bestuurslid uit te zetten.

Voor beide vacatures zijn geschikte kandidaten gevonden, te weten Jeroen Stevens (Interconnect) als secretaris en Ruben van der Zwan (Worldstream & Greenhouse Datacenters) als algemeen bestuurslid. Zij zijn tijdens de deelnemersvergadering van 26 november 2025 officieel voorgedragen aan het bestuur ter benoeming. Op 23 januari 2026 werden zij formeel benoemd als bestuursleden door het bestuur van NBIP.

NBIP NEXT, het jaarlijkse kennisevent van NBIP waar sector, stakeholders en geïnteresseerden bij elkaar komen om gemeenschappelijke thema’s te bespreken, was in 2025 voor het eerst een tweedaags event. Waar op de eerste dag de gebruikelijke thema’s ‘Wet & weerbaarheid’ en ‘DDoS mitigatie’ (in samenwerking met de Anti-DDoS Coalitie) centraal stonden, werd op de tweede dag uitgebreid stilgestaan bij hét thema van 2025: digitale autonomie. Het event werd zeer goed gewaardeerd met gemiddeld een 8,8 voor beide dagen.

Verdieping

2025 stond ook in het teken van de verdieping en verbreding van de activiteiten van NBIP. In 2025 heeft NBIP haar public affairs-activiteiten verder geprofessionaliseerd. Voornaamste reden hiervoor is een tijdige aansluiting op relevante ontwikkelingen in het publieke domein die NBIP deelnemers

NBIP verbindt kennis, beleid en samenwerking om de digitale weerbaarheid van Nederland te versterken.

kunnen raken, bijvoorbeeld op het gebied van wet- en regelgeving en de operationele consequenties daarvan. Binnen het team van NBIP is iemand belast om relevante ontwikkelingen tijdig te signaleren en daarop te acteren in samenwerking met de directeur. In veel gevallen betekent dit het brengen van kennis en samenwerking met stakeholders op de volgende dossiers: 'Digitale weerbaarheid in digitale infrastructuur (inclusief digitale autonomie), Operationele compliance aan wet- en regelgeving voor aanbieders van digitale diensten, DDoS-weerbaarheid en Abuse bestrijding.' NBIP is daarnaast een van de vier leden van de coalitie Digitale Infrastructuur Nederland (DINL).

Een belangrijk moment in 2025 was op dit gebied was de bijdrage aan de position paper 'Strategische digitale autonomie en het Rijksbreed cloudbeleid' aan Tweede Kamerleden Barbara Kathmann en Jesse Six Dijkstra. De position paper is tot stand gekomen door een samenwerking tussen diverse bedrijven en organisaties. Met de bijdrage van NBIP aan de position paper is beoogd om de digitale weerbaarheid in Nederland te vergroten door een suggestie te doen voor een rijkscloudbeleid dat de risicovolle afhankelijkheden snel minimaliseert.

Tijdens de V-100 (Verantwoordingsdag) van de Tweede Kamer kreeg Octavia de Weerdt, algemeen directeur van NBIP, samen met enkele andere genodigden uit de sector, de gelegenheid om in gesprek te gaan met Kamerleden en bewindspersonen over cyberweerbaarheid. Het getal 100 staat voor de honderd burgers die worden uitgenodigd door de Kamer om de jaarverslagen van de ministers kritisch te bekijken en hierover vragen te stellen. Het doel van de V-100 is om de burger rechtstreeks te betrekken bij de controlerende taak van de Kamer. De Kamer nodigde in 2025 burgers en ondernemers uit die direct contact hebben met een of meerdere publieke dienstverleners, waaronder het Nationaal Cyber Security Centrum (NCSC).

Ontwikkeling diensten

Binnen de NaWas werd een nieuwe versie van sFlow (bij NaWas bekend als Splitflow) geïntroduceerd en biedt de dienst GRE als add-on aan voor deelnemers die niet zijn aangesloten bij een internet exchange. Ook de Tapdienst ontwikkelt zich verder, waarbij met name nadruk is gelegd op de inrichting voor eEvidence-bevelen die naar verwachting in 2026/2027 rechtstreeks door bevoegde autoriteiten van Europese lidstaten worden verstuurd.

Het Clean Networks initatief, wat officieel nog in de projectfase zit, heeft grote stappen gezet in het gezamenlijk bestrijden van abuse. In 2025 is het projectmanagement verder geprofessionaliseerd om Clean Networks effectief te sturen binnen een complexer wordend landschap van wet- en regelgeving. Ook zijn de technische fundamenten voor data-analyse verder uitgebouwd, met een focus op het ondersteunen van abusemeldingen en de methodologische ontwikkeling van de sector-benchmark. In het afgelopen jaar is ook blijvend geïnvesteerd in de positionering van Clean Networks binnen de Nederlandse en Europese markt. Daarnaast is de projectduur van Clean Networks verlengd tot en met 31 december 2027. Dit was noodzakelijk vanwege de vertraagde initiële subsidieverlening en de tijd die benodigd was voor het werven van gespecialiseerd personeel.

Vooruitgang

De komende jaren is de inzet om de operationele compliance en cyberweerbaarheid van de digitale infrastructuur in Nederland en Europa verder te verstevigen. De basis hiervoor blijven de gemeenschappelijke faciliteiten zoals de NaWas, Tapdienst en Clean Networks. Daarbij wordt steeds ingezet op digitaal autonome, open source (door)ontwikkeling.

Met deze ontwikkelingen volgt NBIP de visie die mede is ingezet en uitgewerkt in de Europese projecten waaraan NBIP deelneemt. Door de komende jaren deel te blijven nemen aan nieuwe EU-projecten kan de dienstverlening voor deelnemers niet alleen doorlopend gemoderniseerd en verbeterd worden, maar kunnen ook nieuwe diensten worden ontwikkeld. Deze diensten passen in de nieuwe raamwerken rondom digitale autonomie, zodat de betrouwbaarheid en interoperabiliteit geborgd worden.

Met de implementatie van het eEvidence-wetgevingspakket start tot slot een nieuwe fase voor de Tapdienst. De verwachting is dat het aantal te verwerken bevragingen flink gaat toenemen, wat ook effect gaat hebben op de Tapdienst. NBIP is op Europees niveau betrokken in de expertgroep van de Europese Commissie voor de technische implementatie van eEvidence. Daarnaast is de stichting ook nationaal betrokken bij de implementatie, onder meer bij technische sessies van het ministerie van Justitie & Veiligheid.

Over NBIP

Stichting Nationale Beheersorganisatie Internet Providers (NBIP) zet zich in voor een betrouwbaar en veilig internet door aanbieders van digitale infrastructuur te voorzien van gemeenschappelijke diensten. Op deze manier voldoen zij aan de (wettelijke) vereisten en versterken zij hun digitale weerbaarheid.

Alles wat NBIP doet, is vanuit de overtuiging dat de internetsector samen sterker staat voor een schoner, veiliger en betrouwbaar internet en dat iedereen daar baat bij heeft.

In 2001 is NBIP opgericht door zes internetproviders (ISP's). De stichting werd in het leven geroepen om uitvoering te geven aan de wettelijke aftapverplichtingen die deze ISP's hadden onder de Telecommunicatiewet. 25 jaar later bestaat de Tapdienst nog steeds. Deze dienst voorziet in de behoefte van aanbieders om de naleving van de aftapverplichting uit te besteden aan een professionele organisatie waarbij onafhankelijkheid geborgd is. De stichting bouwt, onderhoudt en beheert de infrastructuur en kennis die nodig is om namens deelnemers uitvoering te geven aan tapvorderingen.

Het coöperatieve model van de Tapdienst heeft in 2014 navolging gekregen met de Nationale Wasstraat (NaWas). Deze collectieve oplossing voor de mitigatie van DDoS-aanvallen is naar hetzelfde model als de Tapdienst opgezet. Het collectieve probleem van DDoS wordt door deelnemers aan de NaWas gezamenlijk aangepakt, waarbij deelnemers naar rato bijdragen aan de instandhouding, onderhoud, vernieuwing en uitbreiding van de dienst. De dagelijkse operatie is in handen van in networking en DDoS gespecialiseerde engineers in dienst van de stichting.

In 2022 is een volgende dienst gelanceerd: Clean Networks. Dit platform informeert deelnemers over beveiligingskwetsbaarheden en abuse zoals botnets of spamservers in hun netwerk. Deelnemers ondertekenen de sectorale gedragscode internet abuse, sectorbrede afspraken waarmee providers zich committeren aan het voorkomen, opsporen, mitigeren en verwijderen van abuse en kwetsbaarheden in hun netwerk. Clean Networks fungeert tevens als sectoraal Cyber Security Incident Response Team (CSIRT).

In het verlengde van deze activiteiten heeft NBIP zich ontwikkeld tot expertisecentrum voor lawful interception en lawful disclosure, DDoS en mitigatie daarvan en internet abuse en detectie en mitigatie van beveiligingskwetsbaarheden in de dagelijkse operatie van providers. Er wordt nauw samengewerkt met verschillende partners, waaronder brancheorganisaties, de overheid, coalities en publiek-private samenwerkingen op zowel nationaal als Europees niveau.

Een voorbeeld hiervan is het Connect2Data project in samenwerking met Connect2Trust. Dit project, gerealiseerd met steun van het SIDN Fonds, is bedoeld voor organisaties die van het Nationaal Cyber Security Centrum (NCSC) of via schakelorganisaties als Connect2Trust en NBIP dreigingsinformatie over hun netwerken willen ontvangen. Door de verzameling van de benodigde technische gegevens te automatiseren, worden registraties actueler en eenvoudiger waardoor veel relevantere dreigingsinformatie kan worden aangeleverd.

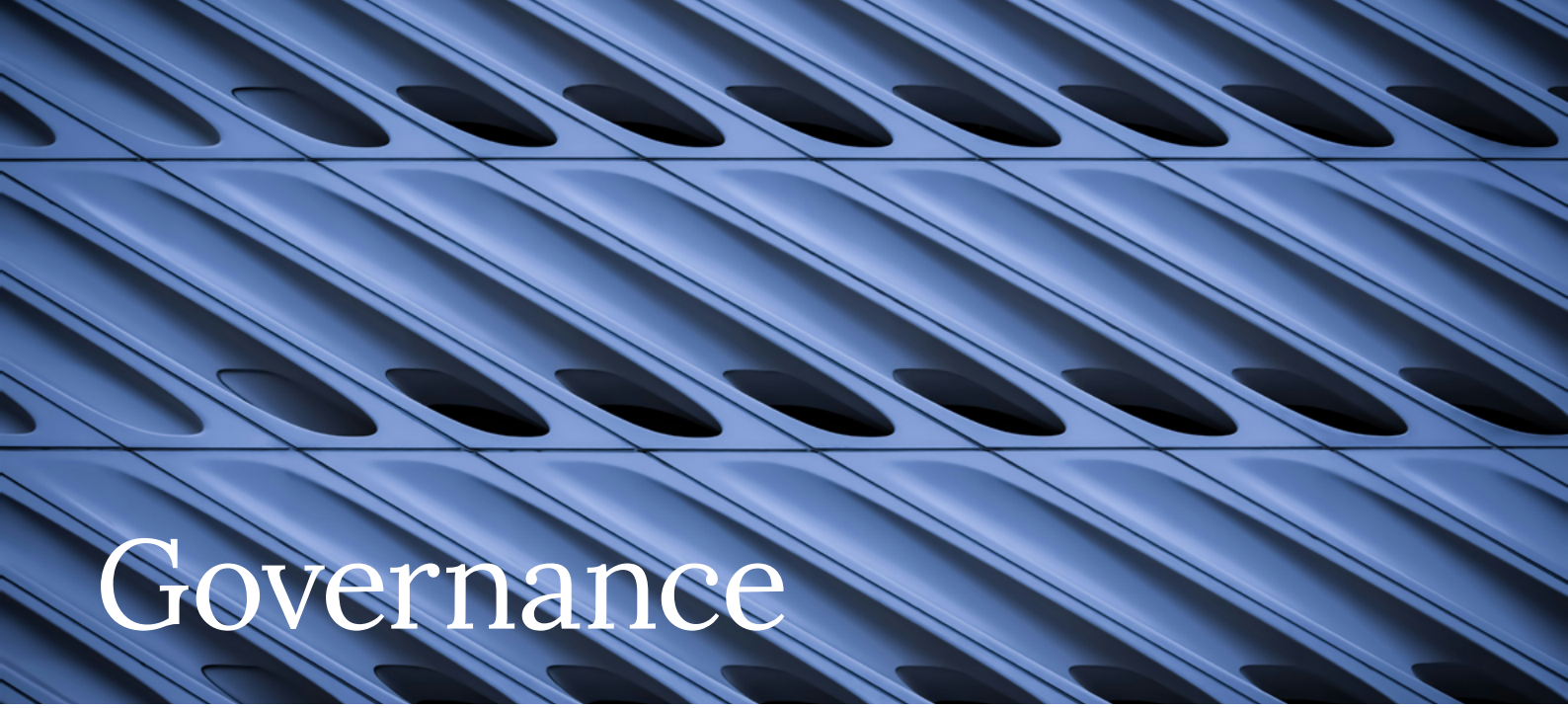
NBIP werkt in Europees verband aan de ontwikkeling van nieuwe tooling en diensten om de cyberweerbaarheid van de digitale infrastructuur verder te versterken. Door deel te nemen aan Europese projecten onder bij voorbeeld de Horizon Europe en Digital Europe programma's, of bij te dragen vanuit een consortium onder het IPCEI instrumentarium van de Europese Commissie, zorgt NBIP ook in de toekomst voor een betrouwbaar internet.

Missie en Visie

NBIP biedt aanbieders van digitale infrastructuur collectieve compliance- en cybersecuritydiensten die onmisbaar zijn vanwege beschikbaarheid of wettelijke vereisten. Door krachten, kennis en middelen te bundelen, organiseren deelnemers gemeenschappelijk hun digitale weerbaarheid en operationele naleving van wet- en regelgeving.

> *"Samen sterker voor een betrouwbaar internet."*

De diensten die NBIP biedt, zijn voor deelnemers dan ook efficiënter collectief te exploiteren dan individueel. Dankzij deze gezamenlijke aanpak hebben zowel grote als kleine aanbieders op een laagdrempelige en kostenefficiënte manier hun zaken op orde.
Aan de basis van de non-profit opzet van NBIP staat het beginsel dat samenwerking de belangrijkste manier is sterker te staan voor een betrouwbaar internet. NBIP levert haar collectieve diensten vanuit de gedachte dat een veilig internet een gezamenlijke verantwoordelijkheid is, en werkt daarom zonder winstoogmerk om dit doel te bereiken.



Governance

Het bestuur van NBIP is samengesteld uit bestuursleden die tenminste voor de helft voortkomen uit het midden van de deelnemers van NBIP. Het bestuur is verantwoordelijk voor de vorming van beleid, financiële controle en verantwoording en een behoedzame omgang met de stichting en de belangen van deelnemers die erin verenigd zijn.

Het bestuur bestond in 2025 uit vier leden: een voorzitter, een penningmeester en twee algemene bestuursleden waarvan één het vicevoorzitterschap vervult. In 2025 zijn twee vacatures ontstaan die door het bestuur zijn uitgezet binnen de Raad van Deelnemers. Hierbij ging het om de posities van secretaris en algemeen bestuurslid. Na de procedures zijn Jeroen Stevens (secretaris) en Ruben van der Zwan (algemeen bestuurslid) toegetreden tot het bestuur van NBIP.

Bestuursleden worden voorgedragen door de Raad van Deelnemers, waarin alle deelnemers van NBIP zijn vertegenwoordigd. Zij kunnen onder meer bij monde van de voorzitter van de Raad van Deelnemers het bestuur bevragen en van gevraagd en ongevraagd van advies voorzien. De voorzitter van de Raad van Deelnemers mag bestuursvergaderingen bijwonen, heeft inzage in notulen van die vergaderingen en heeft als een van de belangrijkste taken om namens deelnemers onderwerpen te agenderen bij het bestuur. Het bestuur is eindverantwoordelijk voor alle besluitvorming in de stichting.

De directie van NBIP is verantwoordelijk voor de uitvoering van het beleid zoals vastgesteld door het bestuur en legt verantwoording af over behaalde resultaten. De algemeen directeur is autonoom binnen de uitgezette kaders om haar opdracht uit te voeren. De algemeen directeur geeft leiding aan organisatie, daarbij sinds 2025 ondersteund door een vierkoppig managementteam.

Bestuur

Ludo Baauw
Voorzitter

Ludo Baauw is voorzitter van NBIP. Als voorzitter leidt hij het bestuur en ziet samen met de bestuursleden toe op de koers van de stichting. Hij staat in nauw contact met onder meer de Raad van Deelnemers, andere stakeholders en partners in de sector. In het dagelijks leven is hij CEO van IMG (Intermax Group).

Rick Sulman
Vice-voorzitter & bestuurslid

Rick Sulman is bestuurslid en vice-voorzitter van NBIP. Als bestuurslid speelt hij een rol in de governance van de organisatie en houdt hij zich bezig met toezicht op ethisch, transparant en effectief bestuur. Daarnaast ziet Rick toe op de belangen van VoIP providers binnen de stichting. In zijn dagelijkse werk is hij CEO van telecom operator Speakup B.V.

Jeroen Stevens
Secretaris

Jeroen Stevens is secretaris bij NBIP. Hij zet zich in voor thema's die raken aan digitale weerbaarheid, continuïteit en innovatie binnen de sector. Vanuit zijn rol als secretaris volgt hij de actualiteit in de branche op de voet en denkt hij mee over hoe NBIP hier proactief op kan inspelen.

Tjebbe de Winter
Penningmeester

Tjebbe de Winter is penningmeester van NBIP. Hij ziet als penningmeester toe op de financiële gezondheid en stabiliteit van de stichting. Met meer dan 25 jaar ervaring in ISP-technologie en netwerken kan hij goed de technische afwegingen en consequenties van de financiële plaat doorzien. Daarnaast is Tjebbe is een van de oprichters en directeuren van Cyso Group.

Bestuur

Mike Janssen
Algemeen bestuurslid

Mike Janssen is bestuurslid bij NBIP. Hij zet zich in voor een veilige digitale infrastructuur. Mike richt zich op strategische besluitvorming en versterkt samenwerkingen om cybersecurity-uitdagingen, zoals DDoS-aanvallen, gezamenlijk aan te pakken. Daarnaast is Mike actief als CIO bij ITQ en houdt zich daar bezig met de algemene en digitale strategie.

Ruben van der Zwan
Algemeen bestuurslid

Ruben van der Zwan is algemeen bestuurslid bij NBIP. Hij heeft meer dan twintig jaar ervaring binnen de sector. Ruben zet zich in voor een veiliger en beter functionerend internet. Daarnaast is hij actief als CEO van Worldstream en Greenhouse Datacenters.

Raad van Deelnemers

Frans ter Borg
Voorzitter

De deelnemers van NBIP worden vertegenwoordigd in de Raad van Deelnemers. Zij komen minimaal één keer per jaar bijeen voor de algemene deelnemersvergadering. De Raad van Deelnemers geeft gevraagd en ongevraagd advies aan het bestuur van NBIP. Voorzitter van de Raad van Deelnemers is Frans ter Borg. Frans is oprichter en CTO van Quanza.

Ontwikkeling Diensten

Tapdienst

NBIP fungeert als een centraal loket voor lastgevers van vorderingen. In de praktijk betekent dit dat bevoegde lastgevers contact zoeken met NBIP als zij een vordering hebben voor een deelnemer aan de Tapdienst. NBIP draagt vervolgens zorg voor de technische, juridische en administratieve aspecten van deze verzoeken.

Aanbieders van openbare elektronische communicatie-diensten of -netwerken moeten gegevens over klanten kunnen verstrekken of een tap kunnen plaatsen als dat wordt gevorderd door instanties die daartoe wettelijk bevoegd zijn. In Nederland is de wettelijke grondslag hiervoor vastgelegd in hoofdstuk 13 van de Telecommunicatiewet en de Wet op de inlichtingen- en veiligheidsdiensten (Wiv).

De bevoegdheden van de opsporingsdiensten zijn beschreven in het Wetboek voor Strafvordering, Boek I, artikelen 126m tot en met 126nb.

In artikel 126m SV is de telefoon- en internettap vastgelegd als een bijzondere opsporingsbevoegdheid. Deze bijzondere opsporingsbevoegdheid kan volgens de Wet Bijzondere Opsporingsbevoegdheden (Wet BOB) alleen worden ingezet op basis van deze drie titels:

1 Er moet een verdenking zijn dat een misdrijf is begaan (titel VI a);
2 Er moet een redelijk vermoeden dat misdrijven, zoals omschreven in artikel 67 lid 1 Sv,
   - In georganiseerd verband worden beraamd
   - of gepleegd die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd
   - of gepleegd een ernstige inbreuk op de rechtsorde opleveren (titel V)
3 Er moeten aanwijzingen zijn dat er een terroristisch misdrijf wordt gepleegd (titel V b)

NBIP ontvangt namens de aangesloten deelnemer de vorderingen en controleert ook of de inhoud van de vordering volgens de wettelijke eisen is opgesteld. Wanneer dit zo is, zorgt NBIP namens de desbetreffende deelnemers ervoor dat tijdig aan de vordering wordt voldaan. Mocht een vordering toch niet voldoen aan de gestelde eisen, dan wijst NBIP de verzoeken af en stelt de aanvrager hiervan op de hoogte.

Alle werkzaamheden die NBIP uitvoert bij het aannemen, verwerken en uitvoeren van vorderingen, gebeurt met strikte naleving van de wetgeving en onder strenge veiligheidsmaatregelen om de vertrouwelijkheid en integriteit van de gegevens te waarborgen.

Dossier: eEvidence

De aankomende wetgeving rondom eEvidence zorgt ervoor dat bevoegde justitiële autoriteiten uit lidstaten van de EU in principe per 18 augustus 2026 rechtstreeks toegang tot elektronisch bewijs-materiaal (e-evidence) kunnen opvragen bij aanbieders van digitale diensten in andere Europese lidstaten. De aanbieders moeten dan binnen 10 dagen (nu: 120 dagen) de verzochte informatie en/of gegevens verstrekken en in sommige gevallen binnen 8 uur. De verwachting is dat het aantal verzoeken voor aanbieders gaat toenemen.

De achtergrond van eEvidence
Volgens de Europese Commissie wordt inmiddels bij meer dan de helft van alle strafrechtelijke onderzoeken het verzoek ingediend door instanties om elektronisch bewijs ('e-evidence') te verkrijgen. Denk hierbij aan e-mails, chatberichten en accountinformatie. Dit wordt ook wel historische gegevens genoemd. Het verkrijgen van deze gegevens is echter een langdurig juridisch proces als deze gegevens staan opgeslagen op servers die zich in andere Europese landen bevinden. Daarom heeft de Europese Commissie een verordening en een richtlijn voorgesteld onder de noemer van eEvidence. Beiden zijn aangenomen door het Europees Parlement. De richtlijn moet in 2026 zijn omgezet door lidstaten en de verordening wordt op 18 augustus 2026 van kracht in de gehele EU.

Waar bestaat eEvidence uit?
De verordening werkt rechtstreeks, wat wil zeggen dat deze niet wordt omgezet in nationale wetgeving maar rechtstreeks in de lidstaten van kracht wordt. Dit gebeurt op 18 augustus 2026.

Binnen de verordening is de juridische basis vastgelegd voor het feit dat bevoegde instanties toegang krijgen tot de opgeslagen gegevens binnen een lidstaat. Dit valt onder het verstrekkingsbevel. Hierin staat ook dat aanbieders binnen 10 dagen, of in dringende gevallen binnen 8 uur, antwoorden moeten verstrekken. Op dit moment geldt hier nog een tijdsduur voor van 120 dagen bij een verstrekkingsbevel en bij de procedure voor wederzijdse rechtshulp geldt een periode van tien maanden.

Met het bewaringsbevel wordt voorkomen dat een aanbieder elektronisch bewijs-materiaal wist terwijl het verstrekkings¬bevel nog in behandeling is.

Voor wie geldt eEvidence straks?
Het eEvidence-wetgevingspakket geldt straks voor aanbieders die de volgende diensten aanbieden:

- elektronische communicatiediensten
- internetdomeinnamen en IP-nummering
- communicatie-, opslag- en verwerkingsdiensten, waaronder social mediaplatforms, hosting platforms en gaming diensten.

eEvidence in de praktijk
In Europa wordt een eEvidence-platform ontwikkeld, waarbij in iedere Europese lidstaat een aansluitpunt is voor de toegang, het verzenden en ontvangen van verzoeken. Dit platform zal door zowel de aanvrager als de verstrekker worden gebruikt.

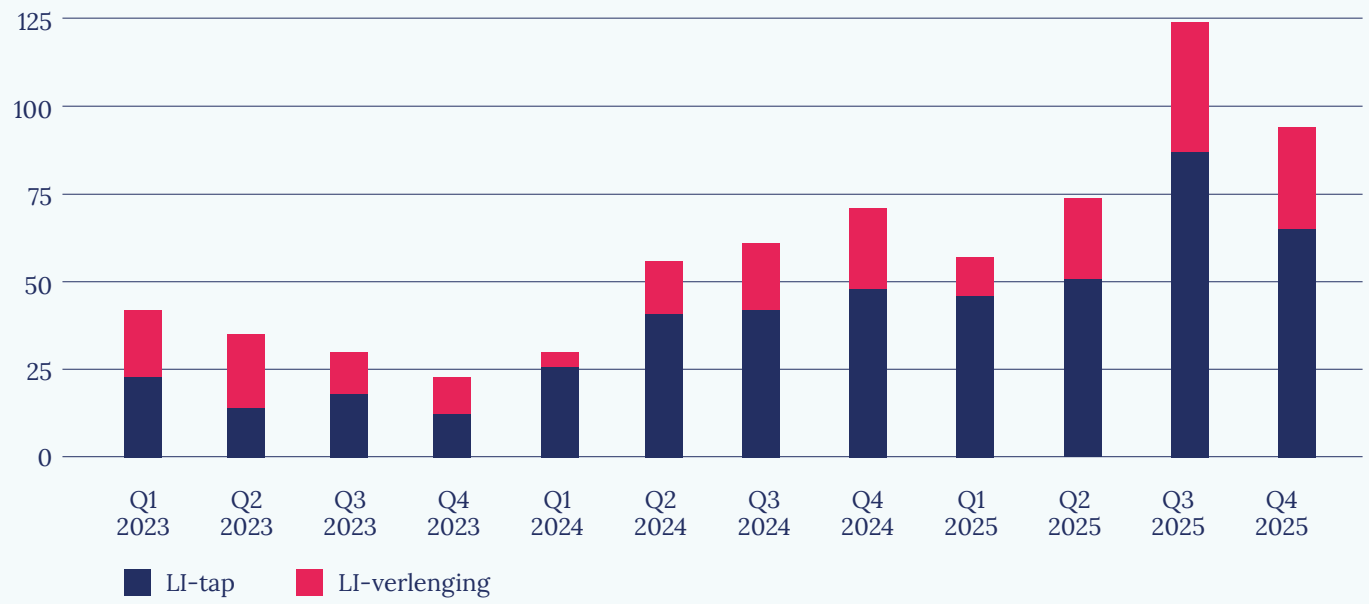
eEvidence & NBIP Tapdienst
NBIP verwacht dat door eEvidence het aantal lawful disclosure bevelen toeneemt. Aanbieders die in andere lidstaten diensten leveren, moeten voorbereid zijn op eEvidence en bevelen kunnen verwerken. Zij moeten zich daartoe onder meer registreren en vrij specifiek aangeven welke diensten zij leveren. De verwachting is dat meer partijen zich bij NBIP gaan melden om aan eEvidence te kunnen voldoen. Daarom wordt de Tapdienst zo ingericht dat straks ook eEvidence-bevelen voor deelnemers van NBIP worden verwerkt. Daarbij is de insteek om enerzijds de bestaande operationele en juridische expertise op het gebied van lawful disclosure binnen NBIP in te zetten om deelnemers snel en effectief compliant te maken.

Tegelijkertijd zullen nieuw opgedane ervaringen en juridische kennis gedeeld worden met deelnemers in een nog op te zetten werkgroep specifiek voor dit thema. Vanzelfsprekend blijft de gemeenschappelijke, non-profit benadering met oog voor zowel de belangen van deelnemers als stakeholders hierbij het primaire uitgangspunt.

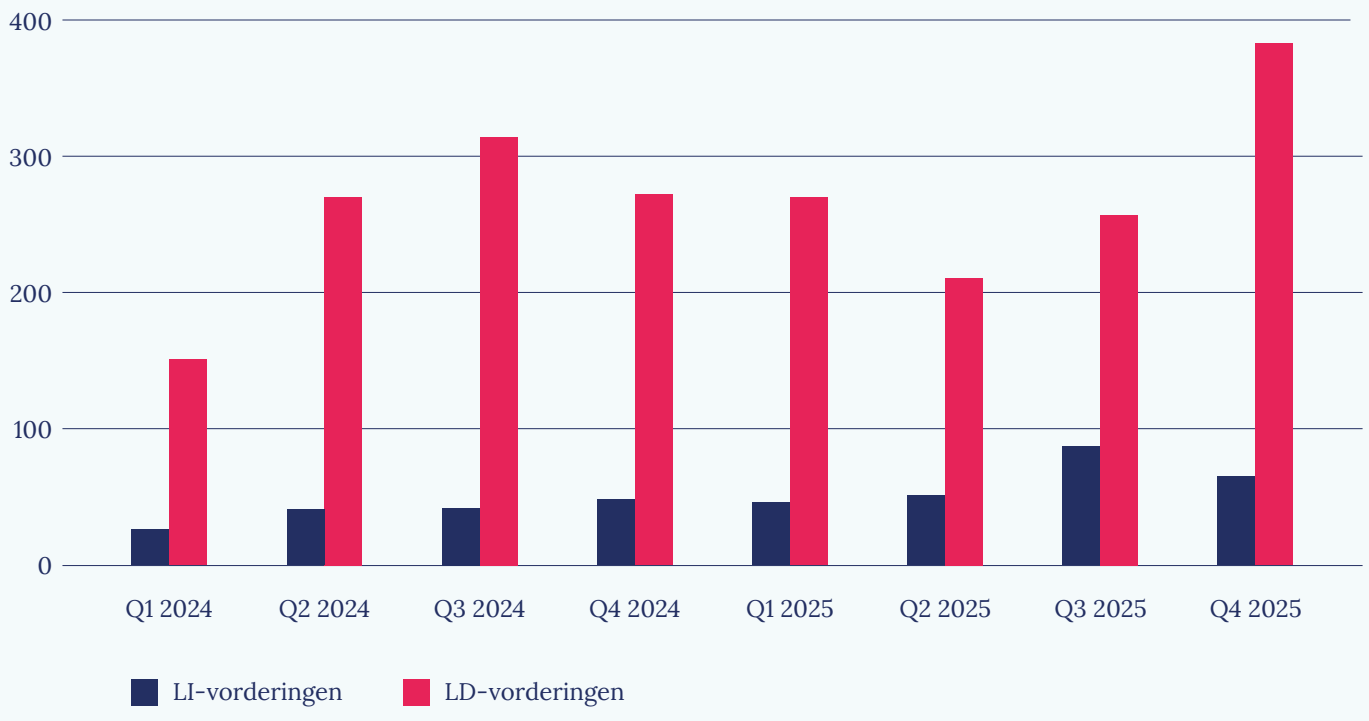
Cijfers

Tapdienst 2025

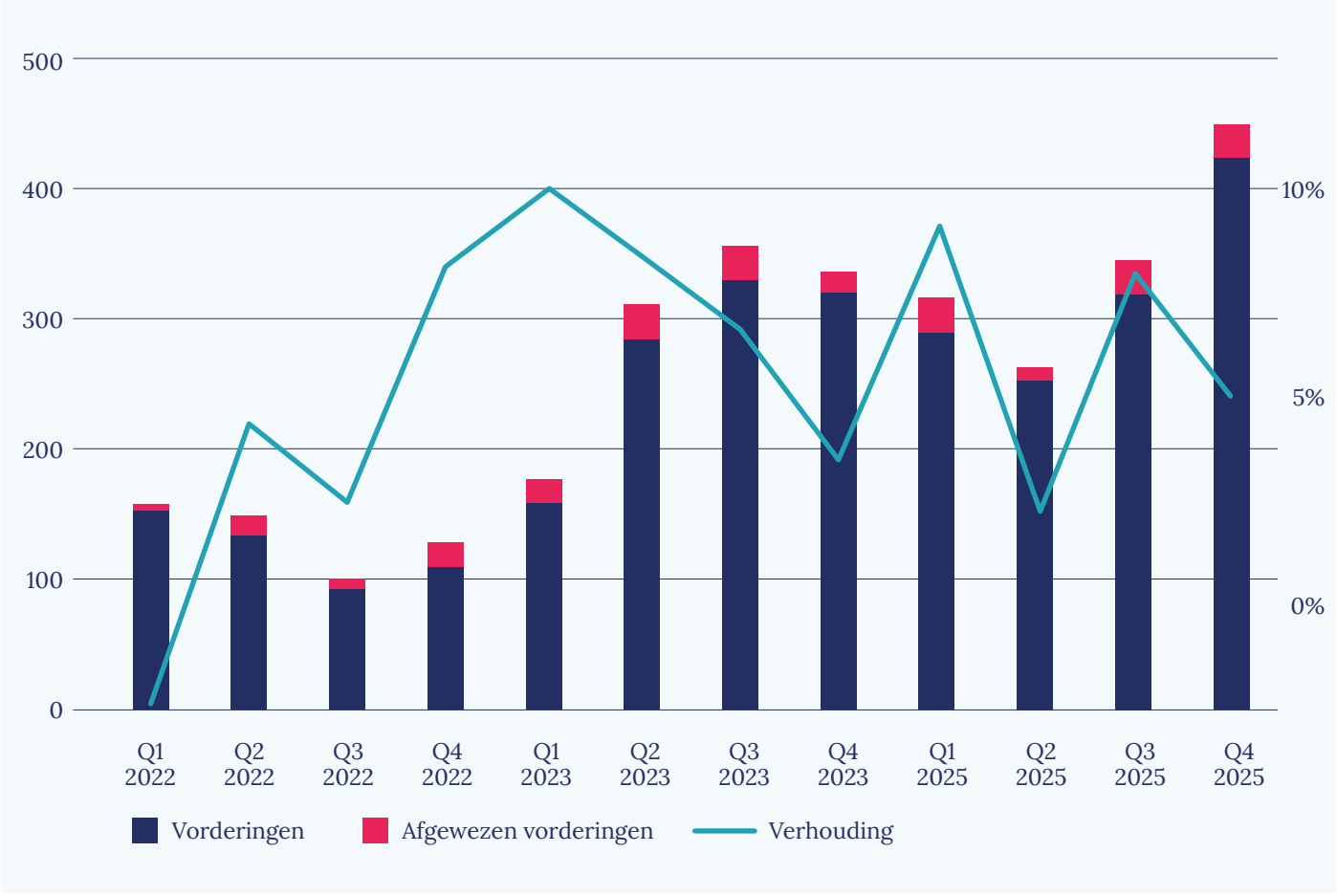
Totaal aantal LI-taps en LI-verlengingen per kwartaal



Aantal LI-vorderingen versus LD-vorderingen per kwartaal



Totaal aantal vorderingen versus afgewezen per kwartaal



Ontwikkeling Diensten

NaWas

NaWas is een collectieve 24/7 DDoS-mitigatiedienst voor aanbieders van digitale infrastructuur en diensten. De non-profit opzet van de dienst geeft aanbieders van iedere omvang de mogelijkheid om zich tegen relatief lage kosten te beschermen tegen DDoS-aanvallen.

In 2025 hebben heeft de ambitie nog breder in Europa deze gemeenschappelijke dienst aan te bieden, verder vorm gekregen. Zo hebben is een samenwerking aangegaan met ERA-IX waardoor de NaWas per direct beschikbaar op het ERA-IX platform in meerdere landen in Europa.

Verder is de infrastructuur van de NaWas verder geoptimaliseerd en de capaciteit verder uitgebreid. Na een succesvolle bèta-fase is Spliflow 2.0 (sFlow) eind 2025 volledig uitgerold als add-on voor deelnemers. Met Splitflow 2.0 kunnen deelnemers het verloop van de aanval volgen, weten wanneer de aanval ten einde is en verbeterde inzichten krijgen. Ook is een GRE-tunnel als add-on toegevoegd aan de NaWas. Dit is met name relevant voor aanbieders zoals VoIP-providers die niet zijn aangesloten bij een internet-exchange. Zij beschikken nu over een alternatief om schoon verkeer terug te ontvangen van de NaWas tijdens een DDoS-aanval.

Cijfers

NaWas 2025

NaWas statistieken 2025

5865
gemitigeerde aanvallen

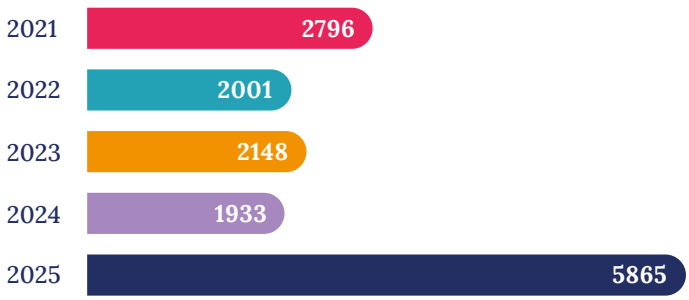
16.07
gemiddeld aantal gemitigeerde aanvallen per dag

305 Gbps
maximale omvang

Top 5 aanvallen in 2025

1. **HTTP Flooding**
2. **DNS Amplification**
3. **DNS Request Flood**
4. **TCP SYN Flooding**
5. **Malform TCP with port 0**

Aantal aanvallen per jaar



Cijfers

NaWas 2025

Trends 2025

1

Toename van langdurige aanvallen, verdeeld over meerdere dagen

Een belangrijke trend in 2025 was dat steeds meer aanvallen van langere duur zijn. In sommige gevallen waren deze aanvallen verdeeld over meerdere dagen én meerdere hosts in hetzelfde netwerk. Hierbij is er sprake geweest van het type aanval genaamd ‘carpet bomb’. Bij ‘carpet bombing’ worden aanvallen op meerdere IP-adressen uitgevoerd in plaats van op één IP-adres. Vaak is bij deze aanvallen sprake van een ‘low-and-wide’ effect. Hierbij lijkt het in eerste instantie erop dat een single IP-adres het dataverkeer aankan, omdat de limiet (bijv. 20 Mbps) op individueel niveau niet wordt overschreden. Maar wanneer het volledige netwerk wordt meegewogen in de optelsom, dan kan deze toch hard worden geraakt. Bewustzijn over dit type aanval is met name belangrijk voor organisaties met een publieke infrastructuur moet een grote voetafdruk. Dit soort aanvallen kan namelijk voor een langere operationele druk zorgen.

2

Meer aanvallen die lijken op normaal verkeer

NaWas heeft in 2025 vaker aanvallen gemitigeerd die leken op het normale verkeer van de dienst waarop de aanvallen waren gericht. Een voorbeeld hiervan was bijvoorbeeld UDP-verkeer wat verliep door SIP-gateways en sterk leek op verwachte telefoonsignaleringen. DDoS-aanvallers passen hun aanvalsmethoden hierop aan door op te gaan in de verwachte telefoniesignalering. Hierdoor wordt detectie en filtering moeilijker voor providers die realtime communicatiediensten of andere gespecialiseerde, op het internet gerichte diensten aanbieden.

3

Webapplicaties meest aangevallen doelwit, toename aanvallen HTTP/3 QUIC

Een belangrijke trend in 2025 was dat steeds meer aanvallen van langere duur zijn. In sommige gevallen waren deze aanvallen verdeeld over meerdere dagen én meerdere hosts in hetzelfde netwerk. Hierbij is er sprake geweest van het type aanval genaamd ‘carpet bomb’. Bij ‘carpet bombing’ worden aanvallen op meerdere IP-adressen uitgevoerd in plaats van op één IP-adres. Vaak is bij deze aanvallen sprake van een ‘low-and-wide’ effect. Hierbij lijkt het in eerste instantie erop dat een single IP-adres het dataverkeer aankan, omdat de limiet (bijv. 20 Mbps) op individueel niveau niet wordt overschreden. Maar wanneer het volledige netwerk wordt meegewogen in de optelsom, dan kan deze toch hard worden geraakt. Bewustzijn over dit type aanval is met name belangrijk voor organisaties met een publieke infrastructuur moet een grote voetafdruk. Dit soort aanvallen kan namelijk voor een langere operationele druk zorgen.

Ontwikkeling Diensten

Clean Networks

Clean Networks bestaat uit twee pijlers: een threat intelligence platform voor aanbieders van digitale infrastructuur en een gedragscode waarmee die aanbieders zich toeleggen op het voorkomen en actief opsporen & verwijderen van abuse in hun netwerken.

In 2025 is het projectmanagement verder geprofessionaliseerd om het Clean Networks-initiatief effectief te sturen binnen een complexer wordend landschap van wet- en regelgeving. De focus lag op de structurele inrichting van werkpakketten, de intensieve afstemming met stakeholders en een fundamentele inhoudelijke herijking naar aanleiding van de aankomende Cyberbeveiligingswet (Cbw) en de digitale-dienstenverordening (DSA). Tevens is actief bijgedragen aan landelijke beleidsvorming, zoals de verkenning naar de aanpak van 'bad hosting' in samenwerking met het Ministerie van Justitie en Veiligheid.

Technische implementaties

De technische fundamenten voor data-analyse zijn verder uitgebouwd, met een focus op het ondersteunen van abusemeldingen en de methodologische ontwikkeling van de sector-benchmark. Deze activiteit heeft een sterk operationeel karakter, vergelijkbaar met de abuse follow-up processen, waarbij sprake is van continue verbetering van bestaande analysemethodieken. De nadruk lag op het verbeteren van de interne datastructuur, het valideren van legitieme informatiebronnen en het inrichten van een schaalbare meldarchitectuur. Er is gewerkt aan een Proof of Concept (PoC) voor de combinatie van MISP en AbuseIO. Daarnaast zijn verkennende stappen gezet richting automatische compliancevalidatie, zoals controle op verwijzingen naar Acceptable Use Policies (AUP's) en notice-and-takedown-procedures in het kader van de komende Cbw.

Clean Networks is verder gegroeid als operationeel platform voor abuse follow-up, waarbij invulling is gegeven aan de rol van strategisch informatieknooppunt. Binnen de CSIRT-werkwijze van NBIP zijn meldingen over kwetsbaarheden, abuse en overtredingen van gedrags- en notice-and-take-down-verplichtingen ontvangen, beoordeeld en waar nodig doorgezet naar deelnemers. Parallel daaraan is gewerkt aan het verbeteren van meldstructuur, validatielogica en rapportageformats. Ook zijn informele checks uitgevoerd op verwijzingen naar abuse policies, AUP's en NTD-procedures.

Daarnaast is de abuse follow-up gekoppeld aan het werk aan de nieuwe gedragscodes, en voorbereidende acties richting geautomatiseerde compliancevalidatie. De meldstructuur werd versterkt als integraal onderdeel van Clean Networks als coördinerend platform voor abuse response binnen Nederland.

> “Aanbieders die de Gedragscode Abusebestrijding ondertekenen, hebben een streepje voor in de markt”

Marktpositionering

In het afgelopen jaar is er ook blijvend geïnvesteerd in de positionering van Clean Networks binnen de Nederlandse en Europese markt. Er is actief deelgenomen aan sectorbijeenkomsten, waaronder CloudFest, het Anti-Abuse Netwerk, overleggen vanuit de Dutch Cloud Community (DCC), ATKM-afstemming, en de werkgroepen rondom bad hosting en trusted notifiers. Er zijn samenwerkingen opgezet met onder andere Connect2Trust, SIDN, VvR, DCC en TU Delft. Clean Networks heeft daarnaast bijgedragen aan het opstellen van het bouwplan voor het Cyberweerbaarheidsnetwerk, specifiek binnen de functie “Informatiedeling”.

Daarnaast is ook de projectduur van Clean Networks verlengd tot en met 31 december 2027. Dit was noodzakelijk vanwege de vertraagde initiële subsidieverlening en de tijd die benodigd was voor het werven van gespecialiseerd personeel. Ook zijn de voorbereidingen gestart voor de publicatie van gedragscode 3.0, het benchmarktraject met TU Delft en het technisch fundament van het Clean Networks-platform. Deze stappen markeren de overgang naar een uitvoerende fase in 2026 en 2027.

Cijfers

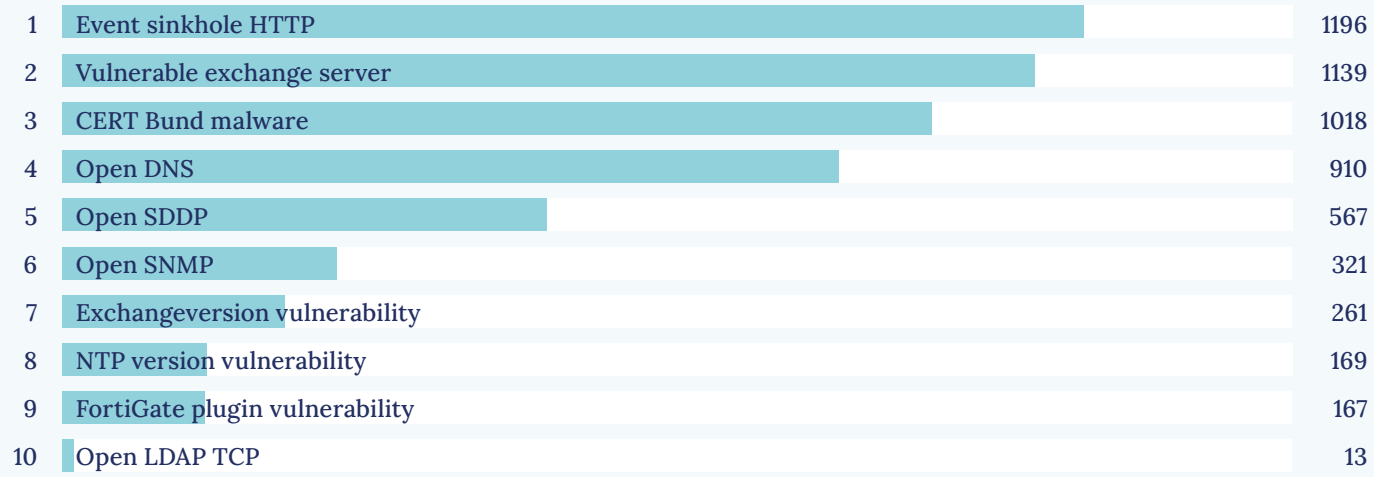
Clean Networks 2025

Toelichting

Clean Networks verspreidt informatie over beveiligingskwetsbaarheden en abuse aan aanbieders van digitale infrastructuur. Deze meldingen zijn toegesneden op individuele deelnemers die zich hebben aangemeld voor de threat intelligence feed van Clean Networks, zodat zij gericht kunnen handelen.

In 2025 hebben we **18.553** notificaties gedeeld over een totaal aantal van **287.007** IP-adressen. In 2024 waren dat **8.367** notificaties over een totaal aantal van **254.132** IP- adressen.

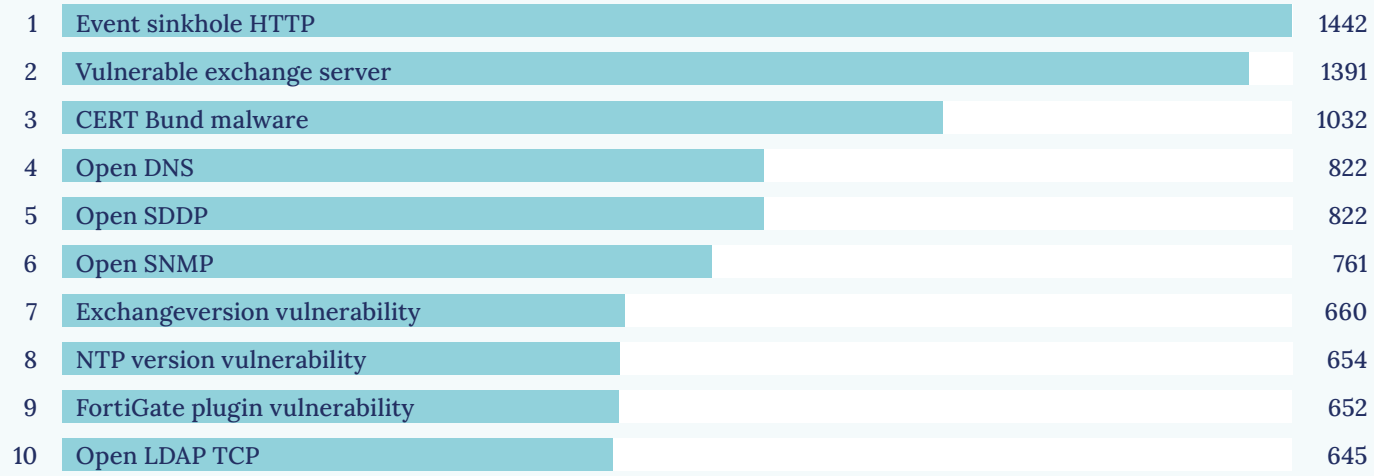
Top 10 Threat Types (gemeten in aantal verstuurde notificaties) 2024



Totaal aantal verstuurde notificaties (2024) — **8.367**

Totaal aantal IP-adressen (2024) — **254.132**

Top 10 Threat Types (gemeten in aantal verstuurde notificaties) 2025



Totaal aantal verstuurde notificaties (2025) — **18.553**

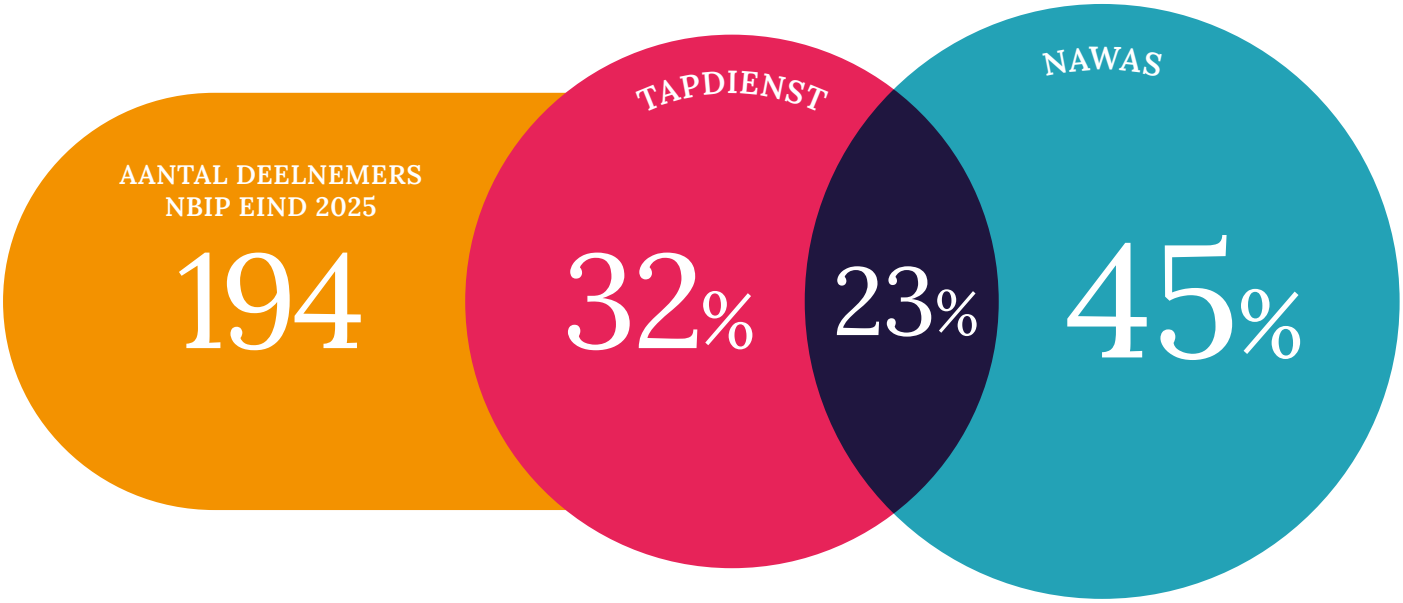
Totaal aantal IP-adressen (2025) — **287.007**

Ontwikkeling deelnemers

In 2025 was er sprake van een lichte consolidatie van het aantal nieuwe deelnemers. Tegelijkertijd zien we ook dat deelnemers die gebruik maken van de Tapdienst of NaWas ervoor kiest om beide diensten af te nemen. Zo besloot één Tapdienst deelnemer om in 2025 ook NaWas te gebruiken en waren er 5 NaWas deelnemers die nu ook gebruikmaken van de Tapdienst.

Voor de Tapdienst zien we een groeiende interesse voor de dienst vanuit MVNO' en MVNE's. Daarnaast neemt ook de interesse in NaWas toe. Dit komt voornamelijk omdat er steeds meer nadruk wordt gelegd op DDoS-oplossingen van Europese bodem, waarbij de NaWas al jaren haar sporen heeft verdiend in de sector.

NBIP had eind 2025 ruim 194 deelnemers, waarvan 107 organisaties deelnemen aan de Tapdienst en 131 organisaties deelnemen aan de NaWas. Er zijn 44 organisaties die deelnemen aan beide diensten. Organisaties die zowel van de Tapdienst als de NaWas gebruikmaken, worden in het totaal aantal deelnemers van NBIP als één enkele deelnemer geteld.



Public affairs

NBIP levert waar nodig en relevant graag haar bijdrage aan dossiers die van belang zijn voor haar deelnemers en een veilig en betrouwbaar internet. Dat doet NBIP onder meer door gevraagd en ongevraagd haar zienswijze te leveren op wetsvoorstellen, regelgeving en beleid en deel te nemen in verschillende publiek-private samenwerkingen. NBIP is samen met AMS-IX, SIDN en SURF deelnemer van de koepel Digitale Infrastructuur Nederland (DINL). NBIP neemt daarnaast deel aan uiteenlopende publiek-private samenwerkingen, waaronder de anti-DDoS-coalitie.

De insteek bij de public affairs activiteiten van NBIP is steeds om praktische uitdagingen bij het voldoen aan wet- en regelgeving die spelen bij deelnemers over te brengen aan de juiste overlegtafels. Doordat NBIP ook operationeel actief is met haar diensten, kan het hierdoor een helder beeld schetsen hoe wetgeving en beleid uiteindelijk in de dagelijkse praktijk hun uitwerking hebben. Dat doen we structureel op vier dossiers.

- Digitale weerbaarheid en digitale autonomie in digitale infrastructuur
- Operationele compliance aan wet- en regelgeving
- DDoS-bescherming
- Abuse preventie

NBIP is van origine geen brancheorganisatie, maar levert operationele diensten ten gunste van deelnemers. Door de combinatie van de public affairs activiteiten én de dienstverlening kunnen de belangen van deelnemers van NBIP nadrukkelijker worden benadrukt bij politieke stakeholders.

Ontwikkelingen 2025

In 2025 zijn grote stappen gezet rondom de public affairs activiteiten van NBIP. Binnen het team is iemand nu dedicated actief op public affairs vlak. Samen met de directeur wordt er gewerkt aan de uitgezette koers op basis van de eerdergenoemde dossiers waar NBIP actief op is.

Daarnaast zijn concrete acties ondernomen op de vier dossiers. Zo is de samenwerking met het Nationaal Cyber Security Centrum (NCSC) geïntensiveerd. Een ander hoogtepunt binnen onze public affairs activiteiten was de uitnodiging voor de V-100 (Verantwoordingsdag) in de Tweede Kamer. Tijdens deze dag worden jaarlijks 100 burgers uitgenodigd die direct contact hebben met een of meerdere publieke instanties. Het getal 100 staat voor de honderd burgers die worden uitgenodigd door de Kamer om de jaarverslagen van de ministers kritisch te bekijken en hierover de ministers te bevragen.

Ook heeft NBIP haar visie gedeeld op het toezicht rondom de aankomende eEvidence-verordening en bijbehorende richtlijn.

Position paper 'Strategische digitale autonomie en het Rijksbreed cloudbeleid'

De afgelopen tijd is op een snel tempo duidelijk geworden dat flinke risico's zijn op het gebied van onze digitale afhankelijkheid. Het feit dat de toegang tot veelgebruikte clouddiensten kan worden ingezet als geopolitiek pressiemiddel is slechts één voorbeeld van. Deze afhankelijkheid zorgt daarom voor onnodige en bovenal risicovolle afhankelijkheid. Er moet daarom per direct concrete stappen worden omgezet om de genoemde afhankelijkheid af te bouwen.

Daarom is afgelopen jaar de position paper 'Strategische digitale autonomie en het Rijksbreed cloudbeleid gepresenteerd aan Tweede Kamerleden Barbara Kathmann en Jesse Six Dijkstra. De position paper is tot stand gekomen door een samenwerking tussen diverse bedrijven en organisaties.

Het doel van de position paper is om een visie te presenteren over de invulling van het cloudbeleid binnen het Rijk. Op basis van deze visie zijn de volgende drie concrete acties uit voortgevloeid:

1. Creëer een nieuwe categorie van clouddiensten voor gevoelige overheidsdata, essentiële overheidsdiensten en kritieke fysieke infrastructuur waaraan extra aanbestedingseisen worden gesteld op het gebied van digitale strategische autonomie.
2. Stimuleer keuzevrijheid en eerlijke concurrentie in de cloudmarkt door voor niet-kritieke clouddiensten dataportabiliteit en interoperabiliteit verplicht te stellen en door gedegen exit-strategieën te implementeren. Dit voorkomt bovendien het risico van vendor lock-in, waarbij migratie naar een andere leverancier nagenoeg onmogelijk is door complexiteit en/of hoge kosten.
3. Blijf de regierol binnen de overheid met betrekking tot het inkoopbeleid van clouddiensten benadrukken. Deze rol is cruciaal om op de lange termijn een succesvol cloudbeleid te voeren.

NBIP in Europa

NBIP speelt een belangrijke rol in als ontwikkelaar en verbinder om de strategische digitale autonomie van Europa te versterken. Concreet betekent dit dat NBIP oplossingen ontwikkelt om de digitale weerbaarheid van de digitale infrastructuursector te vergroten. Daarnaast participeert NBIP in verschillende Europese projecten en samenwerkingsverbanden en levert actief kennis en expertise.

Een van de belangrijkste redenen voor deze positionering is het groeiende besef van de ongewenste afhankelijkheid van niet-Europese cloudaanbieders en haar diensten in Europa. Het gebrek aan Made in Europe-oplossingen is daarom een grote uitdaging. Tegelijkertijd bestaan ook op andere vlakken afhankelijkheden die ongewenst zijn en ingezet kunnen worden als geopolitiek drukmiddel, bijvoorbeeld op het gebied van security-oplossingen, dreigingsinformatie en informatie over kwetsbaarheden en abuse. Binnen dat laatste heeft NBIP met Clean Networks al stappen gezet om deelnemers te ondersteunen bij de bestrijding van abuse.

IPCEI-CIS: MISD

NBIP onderschrijft de urgente noodzaak van een eigen cloudinfrastructuur voor Europa en neemt daarom ook deel aan IPCEI-CIS via het Modular Integrated Sustainable Datacenter (MISD) project. Binnen dit project nemen zeven organisaties deel in een consortium, ieder met een eigen specialisatie. NBIP neemt hierbij het cybersecurity deel voor haar rekening.

Het doel van het Modular Integrated Sustainable Datacenter (MISD) project is om een nieuw modulair, duurzaam en secure by design ontwerp te ontwikkelen dat ingezet wordt op plekken dichtbij eindgebruikers (edge computing). De innovaties en ontwikkelingen die worden gerealiseerd binnen het project, komen samen in een gevalideerde, gedistribueerde opstelling in een field lab. De looptijd van het project is 5 jaar (2024 tot 2029).

In het afgelopen jaar is het testbed als gecontroleerde omgeving om nieuwe cyberbeveilingstoepassingen te testen, verder ontwikkeld. Daarnaast is de aanzet die in 2024 is gemaakt voor de gedecentraliseerde mitigatietechnieken verder ontwikkeld. Hierbij zijn ook de eerste succesvolle testen uitgevoerd.

Lidmaatschap European Cyber Security Organisation (ECSO)

In het afgelopen jaar is NBIP lid geworden van de European Cyber Security Organisation (ECSO). De ECSO is een pan-Europese, privaat-publieke federatie zonder winstoogmerk. Deze federatie zet zich sinds 2016 in voor de versterking

van Europa's weerbaarheid op het gebied van cybersecurity en strategische autonomie. Inmiddels zijn meer dan 300 organisaties, verdeeld over 30 landen, lid van de federatie. De beslissing om lid te worden van de ECSO past naadloos in de missie van NBIP om nog nadrukkelijker in Europa onze expertise van lawful interception/disclosure, DDoS-mitigatie en threat intelligence te delen. Daarnaast kan de kennis wordt opgedaan binnen ECSO gebruikt worden ten behoeve van NBIP-deelnemers.

Expertgroep eEvidence binnen Europese Commissie
Voor de praktische uitvoering van eEvidence wordt gebruik gemaakt van een Europees platform voor de toegang, het verzenden en ontvangen van bewarings- en verstrekkingsbevelen. Zoals eerder beschreven in deze Jaarmonitor in de sectie Dossier eEvidence wordt dit platform door zowel de aanvrager als de verstrekker gebruikt.

De Europese Commissie heeft bij de ontwikkeling van dit platform een technische commissie in het leven geroepen. Hierin nemen vanuit heel Europa overheidsinstanties, die verantwoordelijk zijn voor de implementatie van eEvidence, en experts uit de sector deel om zo een betrouwbaar en gebruiksvriendelijk portaal te bouwen. NBIP is vanuit haar lawful disclosure expertise sinds het begin betrokken en meegedacht over de technische invulling van het platform.

Op de zeepkist

In 2025 heeft NBIP op verschillende manieren haar kennis gedeeld binnen en buiten de sector. Zo gaven we diverse presentaties in binnen- en buitenland over onze diensten en projecten. Daarnaast hebben we bij verschillende media de missie van NBIP over het voetlicht kunnen brengen.

Presentaties

ONE Conference 2025
InCyber Forum – *deelname round table DDoS mitigation*
IPCEI-CIS General Assembly
European Peering Forum
MORE-IP 2025
LINX 124
Lekker weer NLNOG
RONOG10
DKNOG15
NBIP NEXT 2025

Artikelen, interviews, podcasts

8ra Cloud Edge Continuum — *NBIP General Director Octavia de Weerdt on how cybersecurity could become Europe's strategic edge* ↗

SovereignEdge.EU — *For a critical digital infrastructure in our own hands* ↗

NRC — *Cyberveiligheid is een collectieve zaak (ingezonden brief)* ↗

Over NBIP

De stichting Nationale Beheersorganisatie Internet Providers (NBIP) is in 2001 opgericht als uitvoeringsinstituut voor tapbevelen die voortvloeien uit de Telecommunicatiewet. Tegenwoordig is de NBIP uitgegroeid tot het expertisecentrum voor DDoS-mitigatie, Lawful Interception en Threat Intelligence-analyse voor internet-, hosting- en cloudproviders in Nederland en Europa.

NBIP heeft de missie om aanbieders van digitale infrastructuur te helpen aan hun operationele compliance te voldoen met diensten die efficiënt te exploiteren zijn. Deelnemers kunnen dure of complexe faciliteiten die ze niet de hele tijd nodig hebben gezamenlijk via NBIP gebruiken. Het bekendste voorbeeld hiervan is de Nationale Wasstraat (NaWas), het grootste non-profit DDoS scrubbing center ter wereld waarvan meer dan 130 organisaties in 9 Europese landen gebruikmaken. NBIP is door de jaren heen uitgegroeid tot een vaste waarde in het Nederlandse internetlandschap.

Met zo'n 200 deelnemers, een internationale aanwezigheid en betrokkenheid bij strategische Europese ontwikkelingstrajecten, is bewezen dat de filosofie van NBIP ook in de praktijk werkt. Zowel aanbieders van digitale infrastructuur als publieke en private partners weten hun weg naar NBIP te vinden.

Kijk voor meer informatie en actuele ontwikkelingen op nbip.nl

NBIP nationale beheersorganisatie internet providers