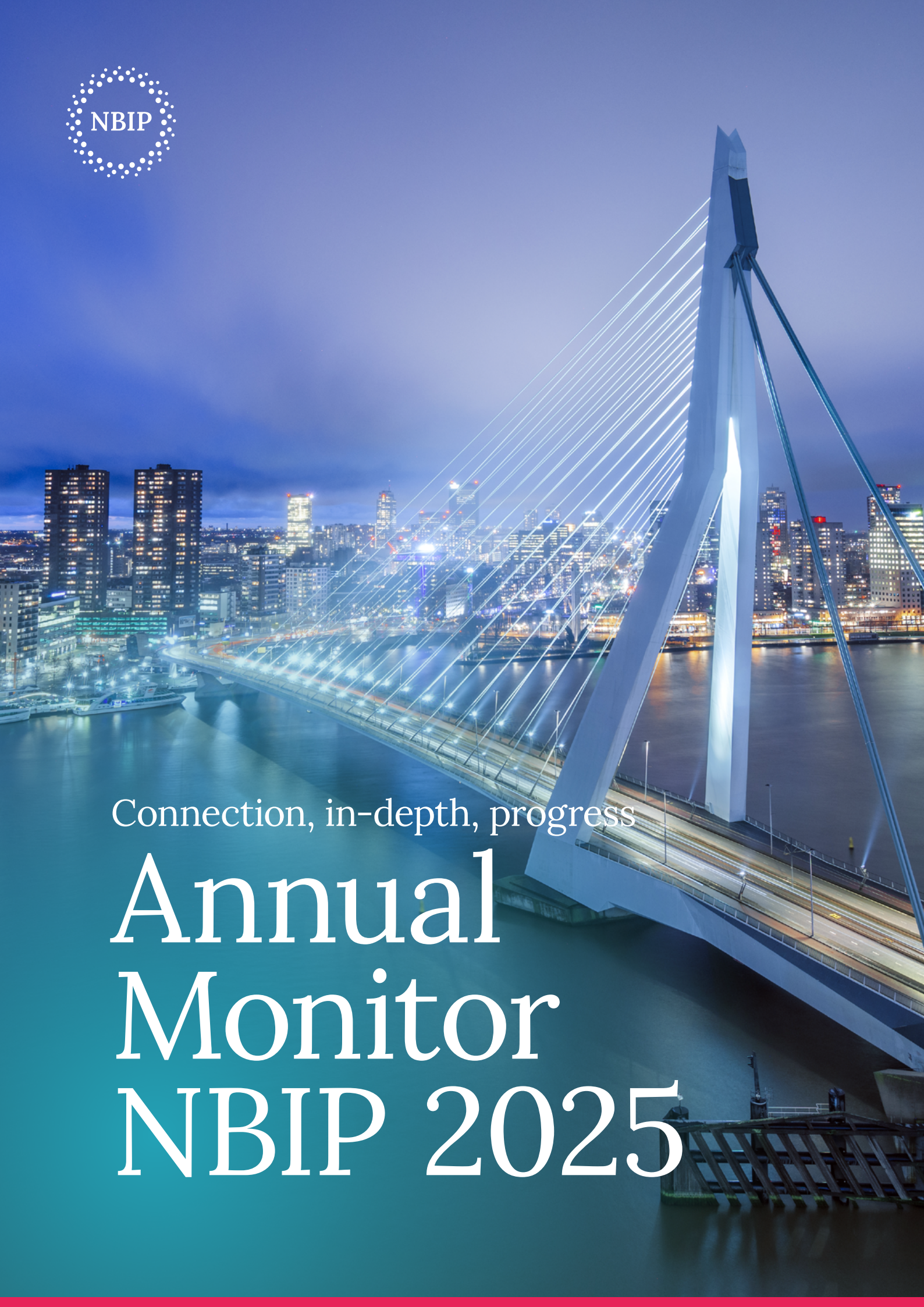


Connection, in-depth, progress

Annual Monitor NBIP 2025

Colophon

Authors

Octavia de Weerdt
General director, NBIP

Wouter Pegtel
Communications & Public Affairs Manager, NBIP

Pim Kokke
Communications Specialist, NBIP

Design

Bijdevleet, Rotterdam

For further information, see **www.nbip.nl/en**

Contents

Preface

Octavia de Weerdt
General Director NBIP

Connection, in the broadest sense of the word, is important for society. Whether it concerns connectivity or human contact, strong connections ensure that together you stand stronger. That has of course been the guiding principle of NBIP and its operational services for many years. Particularly in times of geopolitical change and tension, it is crucial to preserve unity as a sector and as a society, and to demonstrate resilience.

In the past calendar year, digital autonomy has become the focal point of the national and European debate, in which a concrete question has been raised of how Europe should strengthen its own position. At our annual NBIP NEXT annual event in November 2025, we therefore organised a second day for the first time, dedicated to this topic. One of the speakers was Cristina Caffarra of EuroStack. In less than two years, Caffarra has grown into one of the most prominent champions of a sovereign European IT infrastructure. In no uncertain terms, she indicated that Europe must focus on its economic future and simply build concrete solutions.

This message has lived within NBIP — consciously and unconsciously — for many years. For instance, we have been participating for several years in European initiatives and development projects, such as IPCEI-CIS, that are building the digital future of Europe. The goal is for NBIP to strengthen this position in the coming years by working together with the industry on Made in Europe services based on open source.

Building a reliable internet every day is now carried out at NBIP by 20 employees, each contributing from their own area of expertise. In doing so, we continue to build on our mission: providing shared facilities for digital infrastructure providers, so that they have their digital resilience and regulatory compliance in order. That is something I, as director, am proud of every day.

In addition, the new legislation and regulations are giving rise to questions within the sector. One example of this is the eEvidence regulation and directive, which is expected to have a significant impact on the internet sector. As NBIP, we therefore wish to take a position in this area of legislation and regulation by guiding our members more explicitly in this domain. In the past year, the first plans for how to do this were made, and these will become a reality in 2026.

In this renewed Annual Monitor, you can read more about all of NBIP's activities over the past calendar year.

Enjoy reading.

Summary

Annual Monitor 2025

The mission 'Stronger together for a resilient internet' was key to all of NBIP's activities in 2025. Significant efforts were made to strengthen engagement with participants, partners and stakeholders.

Connection

The number of NBIP participants has grown in 2025. By the end of 2025, NBIP had 194 participants, of which 107 organisations participate in the Lawful Interception and Disclosure Service and 131 organisations participate in the NaWas. There are 44 organisations participating in both services. Organisations that use both the Lawful Interception and Disclosure Service and NaWas are counted as a single participant in the total number of NBIP participants. In this way, NBIP contributes to a stronger and more resilient internet.

In 2024, Lunch & Learn sessions were organised for participants for the first time, providing an accessible way to engage with NBIP, catch up on recent developments, and ask questions. These sessions continued in 2025 and have attracted growing interest, culminating in October 2025 with over 25 participants in attendance.

Following the transition year of 2024, NBIP grew rapidly as an organisation and ended 2025 with around 20 staff members, with the prospect of further growth in 2026. This growth is driven, among other things, by participation in European development projects such as IPCEI-CIS and LLMs for Europe. The NBIP board has prepared for this growth by advertising a vacancy for a secretary and a vacancy for a general board member in 2025. Suitable candidates have been found for both vacancies, namely Jeroen Stevens (Interconnect) as secretary and Ruben van der Zwan (Worldstream & Greenhouse Datacenters) as a general board member. They were officially nominated to the board for appointment during the members' meeting on 26 November 2025. On 23 January 2026, they were formally appointed as board members by the NBIP board.

NBIP NEXT, our annual knowledge event where the sector, stakeholders and interested parties come together, was held as a two-day event for the first time in 2025. Whilst the first day focused on the usual themes of 'Law & Resilience' and 'DDoS Mitigation' (in collaboration with the Anti-DDoS Coalition), the second day was devoted to the key theme of 2025: digital autonomy. The event was very well received, with an average rating of 8.8 for both days.

In-depth

2025 was also marked by the deepening and diversification of NBIP's activities. In 2025, NBIP further professionalised its public affairs activities. The main reason for this is to ensure timely alignment with relevant developments in the public domain that may affect NBIP participants, for example in the field of legislation and regulations and their operational consequences. Within the NBIP team, one

NBIP connects knowledge, policy, and collaboration to strengthen the digital resilience of the Netherlands.

person is tasked with identifying relevant developments on time and acting upon them in collaboration with the general director. In many cases, this involves sharing knowledge and collaborating with stakeholders on the following issues: 'Digital resilience in digital infrastructure (including digital autonomy), operational compliance with legislation and regulations for digital service providers, DDoS resilience and combating abuse.' NBIP is also one of the four members of the Digital Infrastructure Netherlands (DINL) coalition.

A key moment in 2025 in this area was the contribution to the position paper 'Strategic Digital Autonomy and the Government-wide Cloud Policy' submitted to Members of Parliament Barbara Kathmann and Jesse Six Dijkstra. The position paper was produced through a collaboration between various companies and organisations. NBIP's contribution to the position paper aimed to enhance digital resilience in the Netherlands by proposing a government cloud policy that rapidly minimises high-risk dependencies.

During the House of Representatives' V-100 (Accountability Day), Octavia de Weerdt, general director of NBIP, along with several other guests from the sector, had the opportunity to discuss cyber resilience with MPs and government ministers. The number 100 represents the hundred citizens invited by the House to critically examine the ministers' annual reports and ask questions about them. The goal of the V-100 is to involve citizens directly in the House's oversight role. In 2025, the House invited citizens and entrepreneurs who have direct contact with one or more public service providers, including the National Cyber Security Centre (NCSC).

Development of Services

A new version of sFlow (known as Splitflow within NaWas) has been introduced, and the service offers GRE as an add-on for participants who are not connected to an internet exchange. The Lawful Interception and Disclosure Service is also continuing to develop, with particular emphasis on the infrastructure for eEvidence warrants, which are expected to be sent directly by competent authorities of European Member States in 2026/2027.

The Clean Networks initiative has made significant progress in the joint fight against abuse. In 2025, project management was further professionalised to ensure the effective steering of Clean Networks within an increasingly complex regulatory landscape. The technical foundations for data analysis were also further developed, with a focus on supporting abuse reports and the methodological development of the benchmark. Over the past year, there has also been continued investment in positioning Clean Networks within the Dutch and European markets. In addition, the duration of the Clean Networks project has been extended until 31 December 2027. This was necessary due to the delay in the initial grant allocation and the time required to recruit specialist staff.

Progress

Over the coming years, the aim is to further strengthen the operational compliance and cyber resilience of the digital infrastructure in the Netherlands and Europe. Shared services such as NaWas, Lawful Interception and Disclosure and Clean Networks will continue to form the basis for this. In doing so, the focus will remain on digitally autonomous, open-source development and refinement.

This commitment also stems from the European projects in which NBIP participates. The aim for the coming years is to continue participating in new projects. In this way, not only can the services provided to participants be continuously modernised and improved, but new services can also be developed that are embedded within new frameworks surrounding digital autonomy, thereby ensuring reliability and interoperability.

Finally, with the implementation of the eEvidence legislative package, a new phase is beginning for Lawful Interception and Disclosure. It is expected that the number of requests to be processed will increase significantly, which will also have an impact on the Interception Service. At European level, NBIP is involved in the European Commission's expert group for the technical implementation of eEvidence. In addition, the foundation is also involved in the implementation at national level, including in technical sessions organised by the Ministry of Justice and Security.

About NBIP

NBIP helps digital infrastructure providers to cover specific legal obligations and operational risks. We do this through joint services, knowledge and advice, and in intensive collaboration with public & private partners. This way, we are stronger together for a resilient internet.

NBIP was founded in 2001 by six Dutch Internet service providers (ISPs) The foundation was created to implement the legal tapping obligations these ISPs had under the Dutch Telecommunications Act More than 20 years later, the Lawful Interception & Disclosure Service still exists It meets the need of providers to outsource compliance with the lawful interception obligation they have under Dutch law to a professional organization where independence is guaranteed. The NBIP foundation builds, maintains and manages the infrastructure and knowledge needed to execute wiretapping orders on behalf of participants.

The Lawful Interception & Disclosure Service's cooperative model was replicated in 2014 with the National Scrubbing Service (NaWas). This collective solution for the mitigation of DDoS attacks is set up on the same model as the Lawful Interception & Disclosure Service. The collective problem of DDoS is addressed jointly by participants in the NaWas, with participants contributing proportionally to the maintenance, upkeep, renewal and expansion of the service. Day-to-day operations are in the hands of engineers specialized in networking and DDoS employed by the foundation.

In 2022, the next project was launched: Clean Networks Platform. This platform informs participants about security vulnerabilities and abuse, such as botnets or spam servers in their network. Participants sign the industry code of conduct with industry-wide agreements that commit providers to prevent, detect, mitigate and remove abuse and vulnerabilities in their network. Clean Networks also serves as a sectoral CSIRT.

Through these activities, NBIP has developed into a center of expertise for lawful interception and lawful disclosure, DDoS and its mitigation, and Internet abuse and detection and mitigation of security vulnerabilities in providers' daily operations. It works closely with various partners, including industry associations, government, coalitions and public-private collaborations at both national and European levels. One example of this is the Connect2Data project in collaboration with Connect2Trust. This project, realised with the support of the SIDN Fund, is intended for organisations that wish to receive threat intelligence about their networks from the National Cyber Security Centre (NCSC) or via intermediary organisations such as Connect2Trust and NBIP. By automating the collection of the required technical data, registrations become more up-to-date and straightforward, enabling significantly more relevant threat intelligence to be delivered.

NBIP is working at a European level on the development of new tooling and services to further strengthen the cyber resilience of the digital infrastructure. By participating in European projects under, for example, the Horizon Europe and Digital Europe programmes, or by contributing as part of a consortium under the IPCEI instrument of the European Commission, NBIP ensures a reliable internet also in the future.

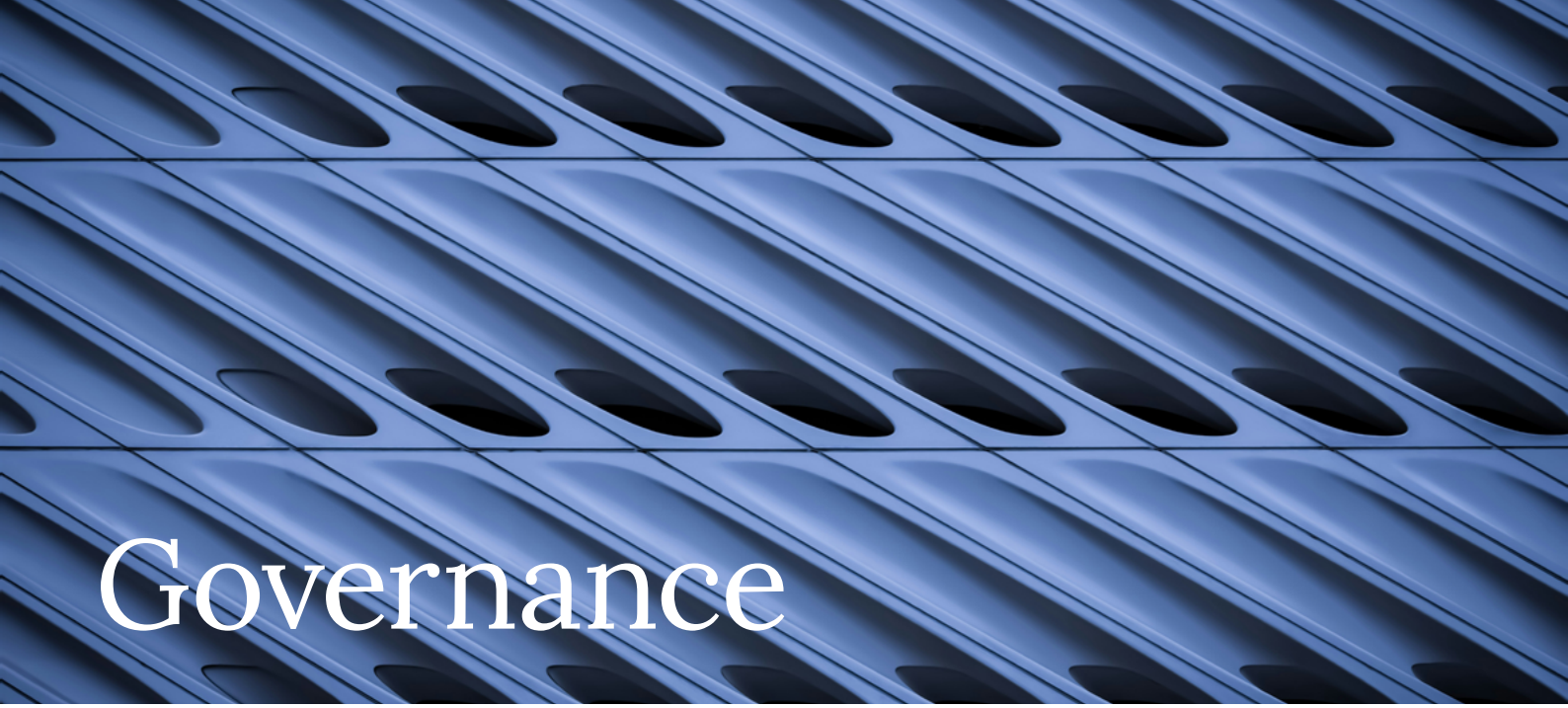
Mission & Vision

NBIP offers digital infrastructure providers collective compliance and cybersecurity services that are indispensable due to availability or legal requirements. By combining forces, knowledge and resources, participants jointly organise their digital resilience and operational compliance with laws and regulations.

"Stronger together for a resilient internet."

The services offered by NBIP are more efficient for participants to operate collectively than individually. Thanks to this joint approach, both large and small providers can keep their affairs in order in an accessible and cost-efficient manner.

The principle that cooperation helps to be stronger for a safer Internet is also at the basis of NBIP's non-profit set-up. NBIP provides professional services based on the idea that a secure Internet is a shared responsibility and therefore operates on a non-profit basis to achieve this goal. Our mission is reliable and resilient Internet, supported by a strong community of cooperating providers.



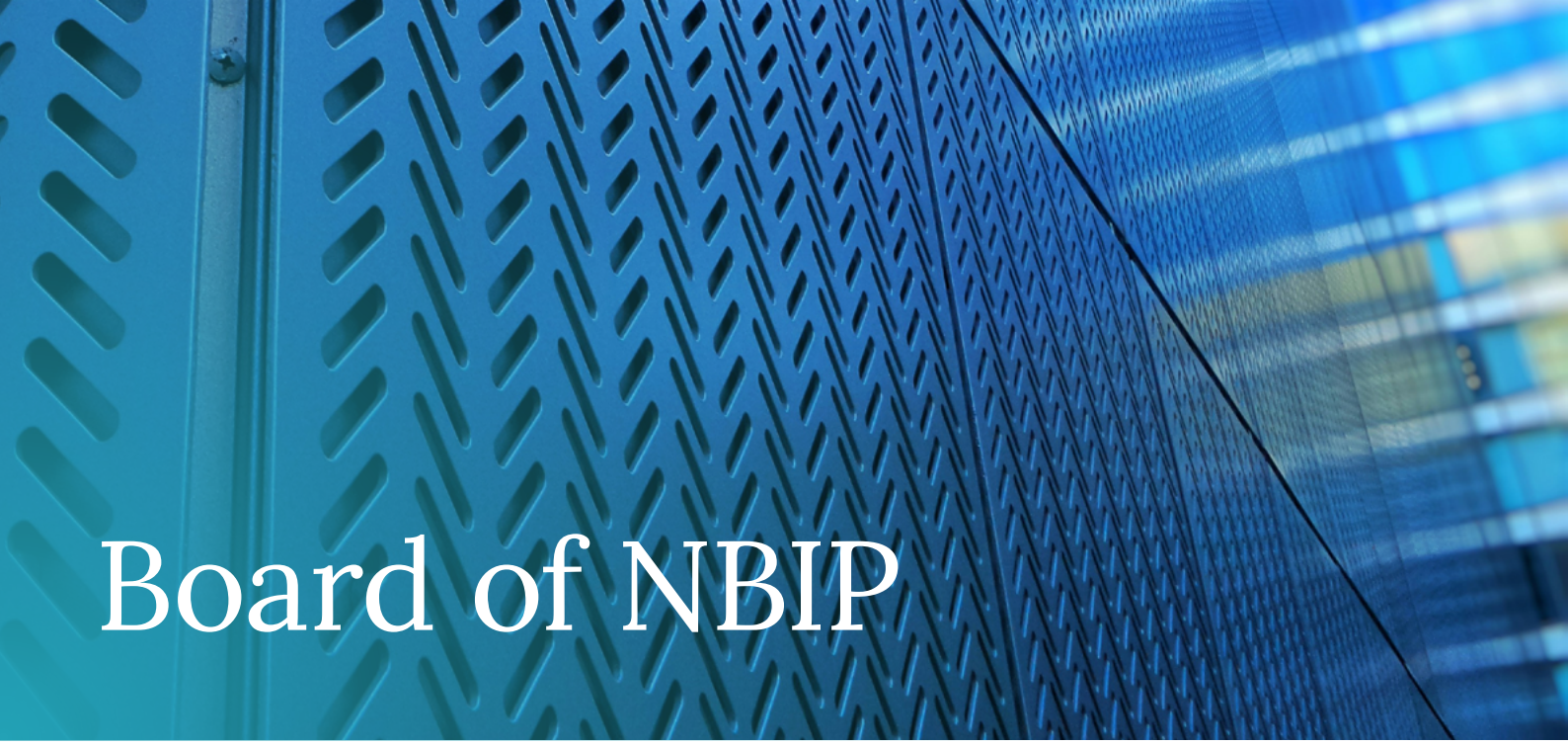
Governance

The NBIP board is composed of board members, at least half of whom are drawn from the ranks of NBIP participants. The board is responsible for policy-making, financial oversight and accountability, and for acting in the best interests of the foundation and the participants it represents.

In 2025, the board consisted of four members: a chairperson, a treasurer and two general board members, one of whom serves as vice-chairperson. In 2025, two vacancies arose, which the board advertised within the Council of Participants. These were the positions of secretary and general board member. Following the selection procedures, Jeroen Stevens (secretary) and Ruben van der Zwan (general board member) joined the NBIP board.

Board members are nominated by the Participants' Council, in which all NBIP participants are represented. They may, for example, through the chair of the Participants' Council, put questions to the board and provide advice, whether solicited or unsolicited. The chair of the Participants' Council may attend board meetings, has access to the minutes of those meetings and has, as one of their key tasks, the responsibility to put items on the board's agenda on behalf of participants. The board bears ultimate responsibility for all decision-making within the foundation.

The management team is responsible for implementing the policy as determined by the board and is accountable for the results achieved. The general director has autonomy within the established frameworks to carry out her remit. She leads the organisation, supported since 2025 by a four-member management team.



Board of NBIP

Ludo Baauw
Chair of the Board

Ludo Baauw is the chairman of the NBIP foundation. As chairman, he leads the board and, together with them, oversees the foundation's course. He is in close contact with the Council of Participants, other stakeholders, and partners in the industry. In his daily life, he is CEO of IMG (Intermax Group).

Rick Sulman
Vice Chairman

Rick Sulman is a general board member and vice-chairman of NBIP. As a board member, he plays a role in the organization's governance and is involved in overseeing ethical, transparent, and effective management. Rick looks after the interests of VoIP providers within the foundation. In his daily work, he is CEO of telecom operator Speakup B.V.

Jeroen Stevens
Secretary

Jeroen Stevens is the secretary at NBIP. He is committed to issues relating to digital resilience, business continuity and innovation within the sector. In his role as secretary, he closely monitors developments in the industry and contributes ideas on how NBIP can respond to these proactively.

Tjebbe de Winter
Treasurer

Tjebbe de Winter is the treasurer of NBIP. As treasurer, he oversees the financial health and stability of NBIP. With more than 25 years of experience in ISP technology and networks, he understands the technical considerations and consequences of the financial picture. Tjebbe is one of the founders and directors of Cyso Group.

Board of NBIP

Mike Janssen
Board Member

Mike Janssen is a general board member at NBIP. He is committed to a secure digital infrastructure. Mike focuses on strategic decision-making and strengthens collaborations to jointly address cybersecurity challenges such as DDoS attacks. Mike is CIO at ITQ and is involved in general and digital strategy there.

Ruben van der Zwan
Board Member

Ruben van der Zwan is a general board member at NBIP. He has over twenty years' experience in the sector. Ruben is committed to making the internet safer and more efficient. He also serves as CEO of Worldstream and Greenhouse Datacenters.

Council of Participants

Frans ter Borg
Chairman

NBIP participants are represented on the Council of Participants. They meet at least once a year for the general participants' meeting. The Participants' Council provides both solicited and unsolicited advice to the NBIP board. The chair of the Participants' Council is Frans ter Borg. Frans is the founder and CTO of Quanza.

Services

Lawful Interception and Disclosure

NBIP acts as a central point of contact for warrants of authorized government agencies. In practice, this means that authorized government agencies contact NBIP if they have a request for a participant of the Lawful Interception and Disclosure Service of NBIP. NBIP takes care of the technical, legal and administrative aspects of these requests.

Providers of public electronic communications services or networks must be able to provide data about customers or install wiretaps if requested to do so by authorities that are legally authorised to do so. In the Netherlands, the legal basis for this is laid down in Chapter 13 of the Telecommunications Act.

The powers of investigative services are described in the Code of Criminal Procedure, Book I, Articles 126m to 126nb. Like the intelligence services, investigative services, such as the police, are allowed to tap and analyse various forms of online data traffic.

Article 126m of the Code of Criminal Procedure establishes telephone and internet tapping as a special investigative power. According to the Special Investigative Powers Act (in Dutch: Wet BOB), this special investigative power can only be used based on these three titles:

1 There must be suspicion that a crime has been committed (Title VI a);
2 There must be reasonable suspicion that crimes, as described in Article 67(1) of the Code of Criminal Procedure,
   - are being planned in an organised context
   - or committed which, given their nature or connection with other crimes planned in that organised context
   - or committed, constitute a serious breach of the legal order (Title V).
3 There must be indications that a terrorist offence is being committed (Title V b).

NBIP receives the warrants on behalf of the affiliated participant and checks whether the content of the claim has been drawn up in accordance with the legal requirements. If this is the case, NBIP ensures on behalf of the relevant participants that the warrant is settled. If a warrant does not meet the requirements, NBIP rejects the requests and informs the applicant.

All activities carried out by NBIP in accepting, processing and executing warrants are performed in strict compliance with the law and under strict security measures to ensure the confidentiality and integrity of the data.

Dossier: eEvidence

The forthcoming legislation on e-evidence will ensure that, in principle, from 18 August 2026, competent judicial authorities from EU Member States will be able to request direct access to electronic evidence (e-Evidence) from digital service providers in other European Member States. Providers will then be required to provide the requested information and/or data within 10 days (currently: 120 days) and, in some urgent cases, within 8 hours. The number of warrants to providers is expected to increase.

The background of eEvidence

According to the European Commission, in more than half of all criminal investigations, authorities now submit requests to obtain electronic evidence ('e-evidence'). This includes emails, chat messages and account information. This is also referred to as historical data. However, obtaining this data is a lengthy legal process if it is stored on servers located in other European countries. That is why the European Commission has proposed a regulation and a directive under the heading of eEvidence. Both have been adopted by the European Parliament. The directive must be transposed by Member States by 2026, and the regulation will enter into force across the EU on 18 August 2026.

What does eEvidence consist of?

The Regulation is directly applicable, which means that it does not need to be transposed into national law but comes into force directly in the Member States. This will take effect on 18 August 2026.

The Regulation establishes the legal basis for competent authorities to access data stored within a Member State. This falls under the European Production Order. It also stipulates that service providers must respond within 10 days, or within 8 hours in urgent cases. At present, a time limit of 120 days still applies to production orders, whilst the mutual legal assistance procedure has a period of ten months.

The preservation order prevents a provider from deleting electronic evidence whilst the disclosure order is still pending.

Who will the eEvidence legislation apply to?

The eEvidence legislative package will apply to providers offering the following services:

- electronic communications services
- internet domain names and IP numbering
- communication, storage and processing services, including social media platforms, hosting platforms and gaming services.

eEvidence in practice

An eEvidence platform is being developed in Europe, with a single point of contact in each Member State for accessing, sending and receiving requests. This platform will be used by both the applicant and the provider.

eEvidence & the Lawful Interception and Disclosure Service

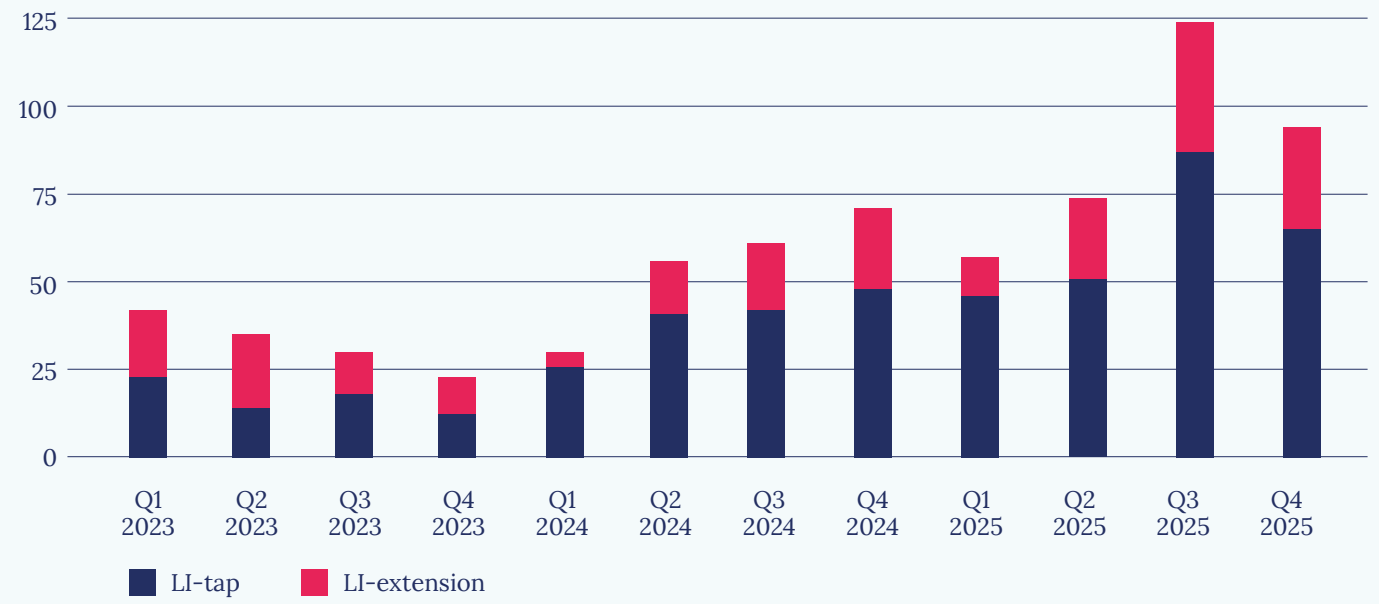
NBIP anticipates that eEvidence will lead to an increase in the number of lawful disclosure orders. Providers offering services in other Member States must be prepared for eEvidence and able to process such orders. To this end, they must, among other things, register and specify in detail the services they provide. It is expected that more parties will register with NBIP to comply with eEvidence. For this reason, our service is being organised in such a way that eEvidence orders for NBIP participants will also be processed in the future. The approach is, on the one hand, to utilise the existing operational and legal expertise in the field of lawful disclosure within NBIP to ensure participants become compliant quickly and effectively.

At the same time, newly acquired experience and legal knowledge will be shared with participants in a working group to be set up specifically for this topic. Naturally, the common, non-profit approach, with due regard for the interests of both participants and stakeholders, remains the primary guiding principle here.

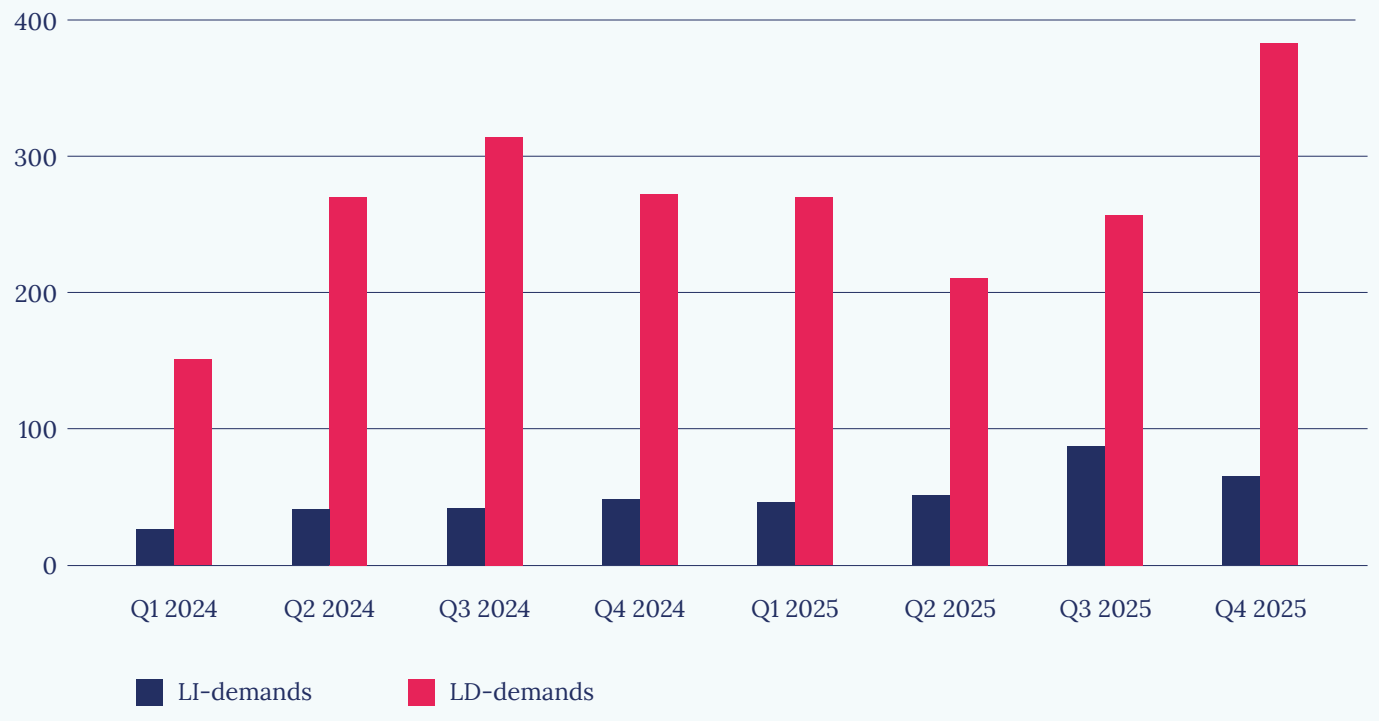
Lawful Interception and Disclosure

Figures 2025

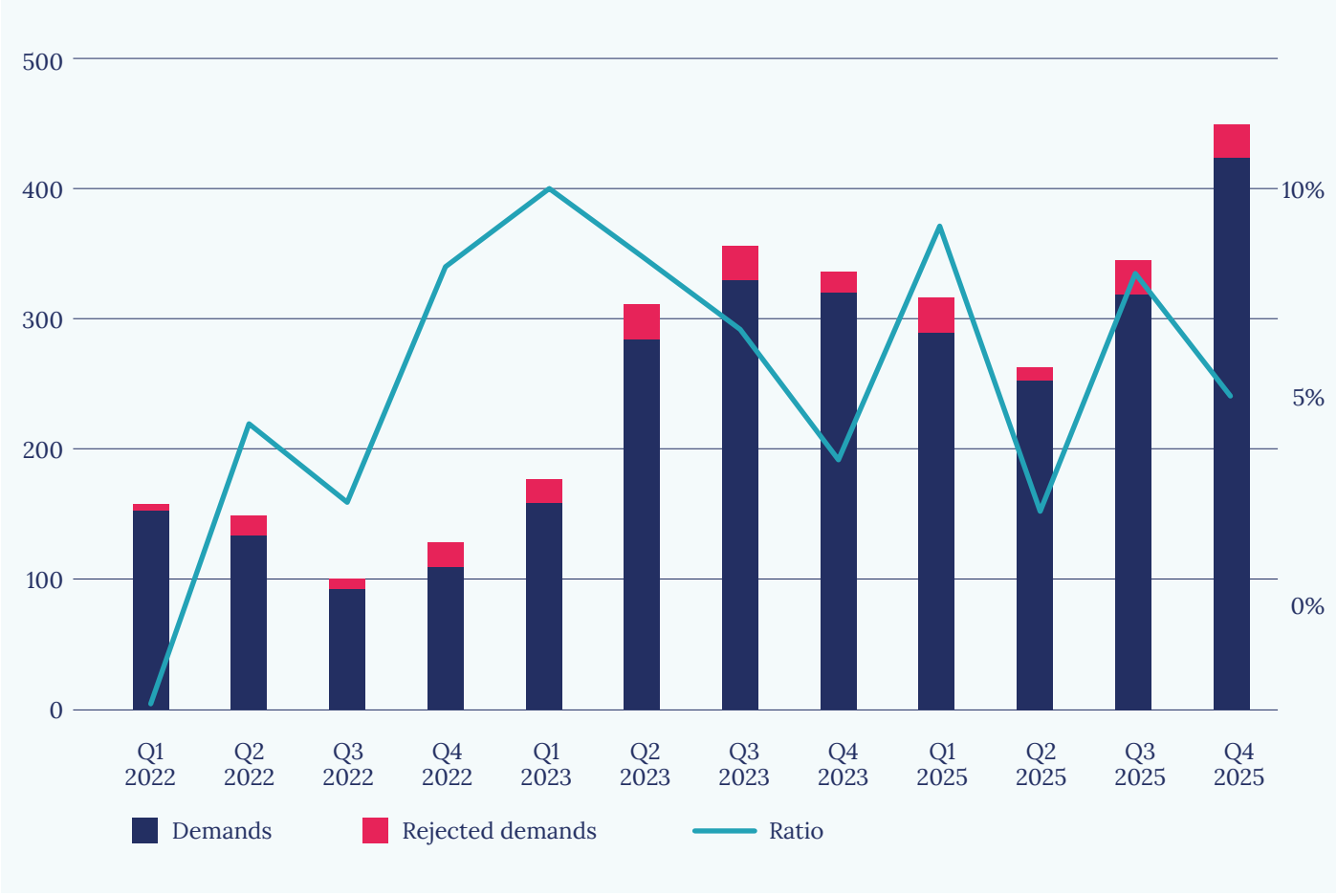
Total number of LI-taps and LI-extensions per quarter



Total number of LI-demands versus LD-demands per quarter



Total number of demands versus rejected per quarter



Services

NaWas

NaWas is a collective 24/7 DDoS mitigation service for providers of digital infrastructure and services. The service's non-profit structure enables providers of all sizes to protect themselves against DDoS attacks at a relatively low cost.

In 2025, our ambition to offer this shared service more widely across Europe took further shape. We have entered a partnership with ERA-IX, making NaWas immediately available on the ERA-IX platform in several European countries.

Furthermore, the NaWas infrastructure has been further optimised and its capacity expanded. Following a successful beta phase, Splitflow 2.0 (sFlow) was launched at the end of 2025 as an add-on for participants. With Splitflow 2.0, participants can track the progress of the attack, know when it has ended, and gain improved insights. A GRE tunnel has also been added to NaWas as an add-on. This is particularly relevant for providers such as VoIP providers that are not connected to an internet exchange. They now have an alternative for receiving clean traffic back from NaWas during a DDoS attack.

NaWas

Figures 2025

NaWas statistics 2025

5865
mitigated attacks

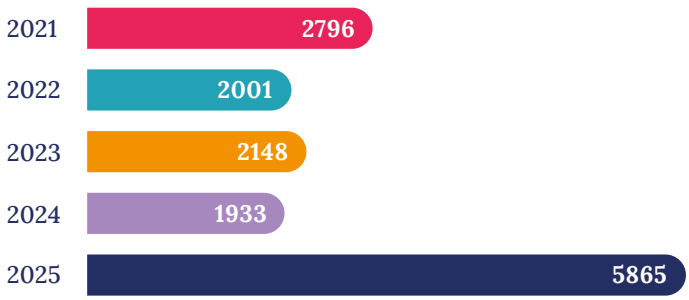
16.07
average number of mitigated attacks per day

305 Gbps
maximum mitigated attack size

Top 5 attacks in 2025

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

Number of attacks per year



NaWas

Figures 2025

Trends 2025

1

Increase in prolonged attacks, spread over several day

A key trend in 2025 was that an increasing number of attacks were of a longer duration. In some cases, these attacks were spread over several days and involved multiple hosts within the same network. This involved a type of attack known as a 'carpet bomb'. In 'carpet bombing', attacks are carried out on multiple IP addresses rather than a single IP address. These attacks often have a 'low-and-wide' effect. At first glance, it appears that a single IP address can handle the data traffic, as the limit (e.g. 20 Mbps) is not exceeded at the individual level. However, when the entire network is factored into the total, it can still be severely impacted. Awareness of this type of attack is particularly important for organisations with a public infrastructure and a large footprint. This is because such attacks can cause prolonged operational pressure.

2

More attacks that resemble normal traffic

In 2025, NaWas mitigated a greater number of attacks that resembled the normal traffic of the service targeted by the attacks. One example of this was UDP traffic passing through SIP gateways, which closely resembled expected telephone signalling. DDoS attackers adapt their methods accordingly by blending in with expected telephony signalling. This makes detection and filtering more difficult for providers offering real-time communication services or other specialised, internet-focused services.

3

Web applications remain the most targeted attack vector, with an increase in HTTP/3 and QUIC attacks

Web applications remain the most targeted attack vector for attackers. Furthermore, HTTP request flooding remains the most used attack vector in 2025. There was also an increase in attacks on HTTP/3, based on the QUIC protocol, in 2025. Attackers are targeting the application layer (layer 7) and keeping pace with the modern protocols used by websites, APIs and digital platforms.

Services

Clean Networks

Clean Networks comprises two pillars: a threat intelligence platform for digital infrastructure providers and a code of conduct through which those providers commit to preventing and actively detecting and removing abuse on their networks.

By 2025, project management had been further professionalised to effectively steer the Clean Networks initiative within an increasingly complex regulatory landscape. The focus was on the structural organisation of work packages, intensive coordination with stakeholders and a fundamental review of content considering NIS2 and the Digital Services Act (DSA). We also actively contributed to national policymaking, such as the exploratory study into tackling 'bad hosting' in collaboration with the Ministry of Justice and Security.

Technical implementations

The technical foundations for data analysis have been further developed, with a focus on supporting abuse reports and the methodological development of the sector benchmark. This activity is highly operational in nature, comparable to the abuse follow-up processes, and involves the continuous improvement of existing analytical methodologies. The emphasis was on improving the internal data structure, validating legitimate information sources and setting up scalable reporting architecture. Work was carried out on a Proof of Concept (PoC) for the combination of MISP and AbuseIO. In addition, exploratory steps were taken towards automatic compliance validation, such as checking for references to Acceptable Use Policies (AUPs) and notice-and-takedown procedures in the context of the forthcoming implementation of the Dutch Cybersecurity Act. This act is the Dutch implementation of the European NIS2 Directive.

Clean Networks has continued to develop as an operational platform for abuse follow-up, fulfilling its role as a strategic information hub. As part of the NBIP's CSIRT working method, reports concerning vulnerabilities, abuse and breaches of code of conduct and notice-and-take-down obligations were received, assessed and, where necessary, forwarded to participants. In parallel, work was carried out to improve the reporting structure, validation logic and reporting formats. Informal checks were also carried out on references to abuse policies, AUPs and NTD procedures.

In addition, the abuse follow-up has been linked to work on the new codes of conduct and preparatory actions towards automated compliance validation. The reporting structure was strengthened as an integral part of Clean Networks as a coordinating platform for abuse response within the Netherlands.

> “Providers that sign the Code of Conduct on Abuse Prevention have an edge in the market.”

Market positioning

Over the past year, we have continued to invest in positioning Clean Networks within the Dutch and European markets. We have actively participated in industry events, including CloudFest, the Anti-Abuse Network, meetings organised by the Dutch Cloud Community (DCC), ATKM coordination, and the working groups on bad hosting and trusted notifiers. Partnerships have been established with, amongst others, Connect2Trust, SIDN, VvR, DCC and TU Delft. Clean Networks has also contributed to drawing up the blueprint for the Cyber Resilience Network, specifically within the ‘Information Sharing’ function.

Furthermore, the duration of the Clean Networks project has been extended until 31 December 2027. This was necessary due to the delayed initial grant award and the time required to recruit specialist staff. Preparations have also begun for the publication of Code of Conduct 3.0, the benchmarking process with TU Delft and the technical foundation of the Clean Networks platform. These steps mark the transition to an implementation phase in 2026 and 2027.

The Clean Networks initiative has been made possible thanks to a grant from the European Union and grants from the Digital Trust Centre and the SIDN Fund.

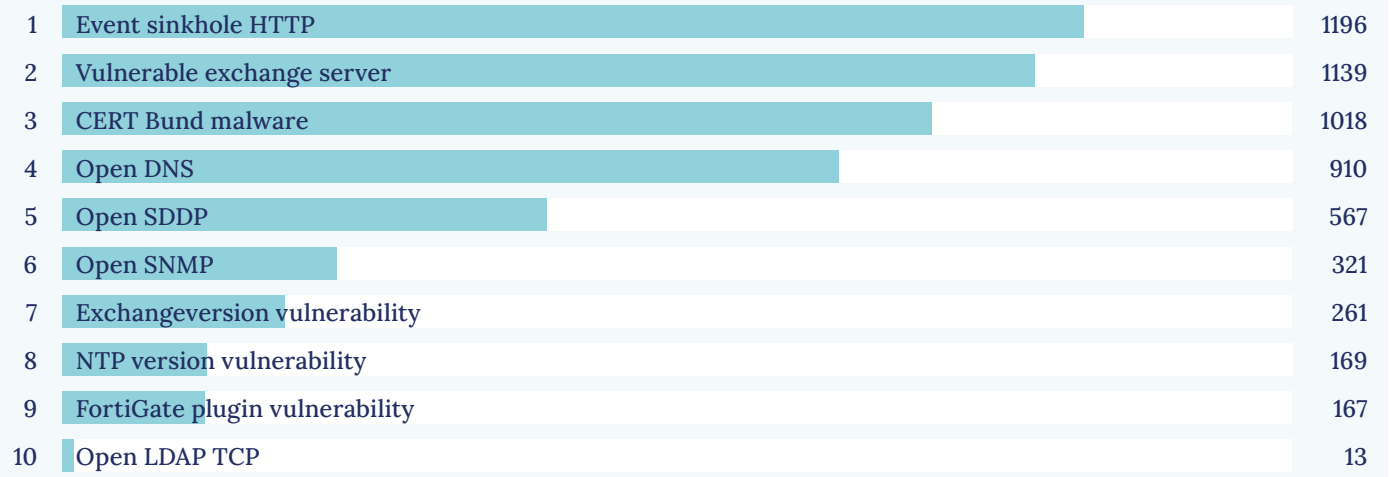
Clean Networks

Figures 2025

Clean Networks provides information about security vulnerabilities and abuse to digital infrastructure providers. These alerts are tailored to individual participants who have subscribed to Clean Networks' threat intelligence feed, enabling them to take targeted action.

In 2025, we shared **18,553 notifications** relating to a total of **287,007 IP addresses**. In 2024, there were **8,367 notifications** relating to a total of **254,132 IP addresses.**

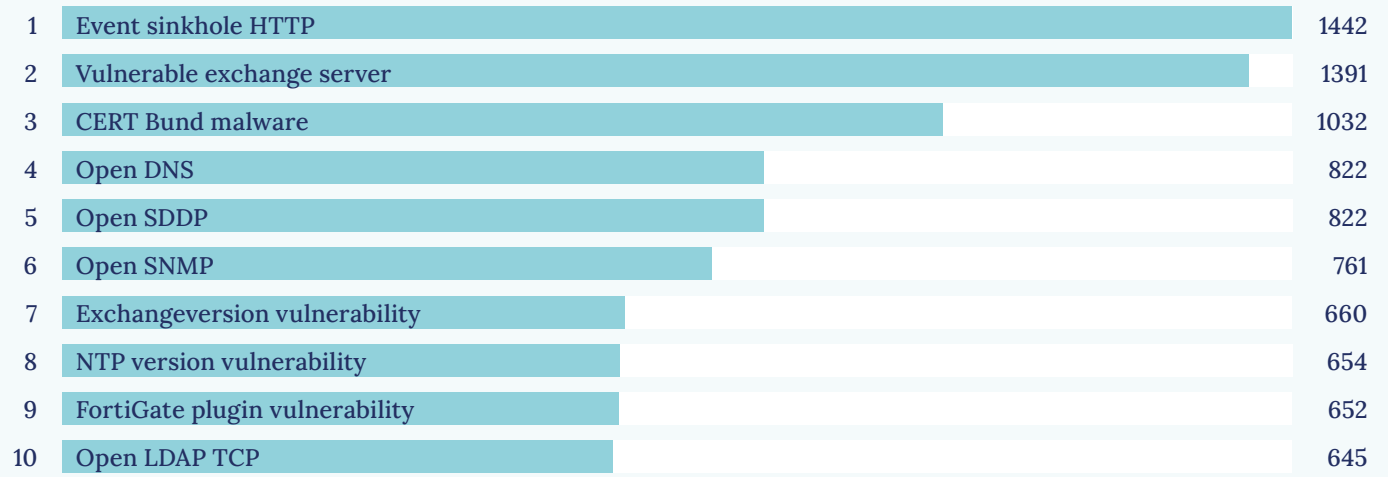
Top 10 Threat Types 2024 (measured in number of notifications)



Total number of notificaties (2024) — **8.367**

Total number of IP addresses (2024) — **254.132**

Top 10 Threat Types 2025 (measured in number of notifications)



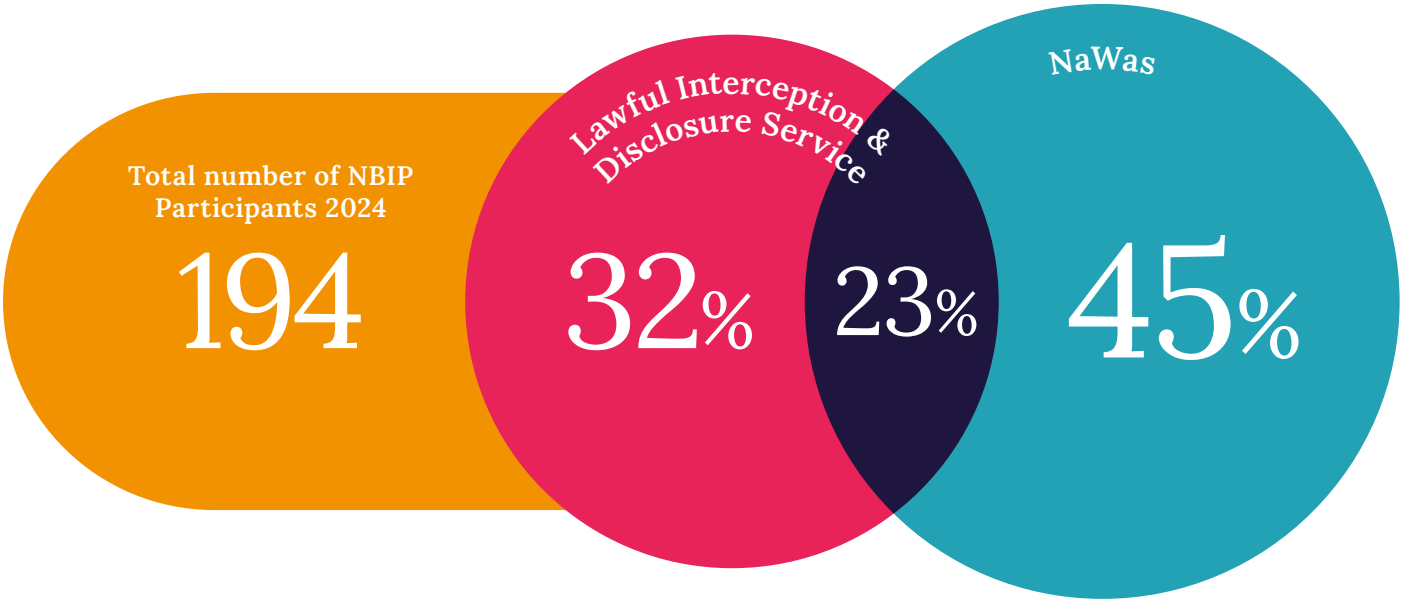
Total number of notificaties (2025) — **18.553**

Total number of IP addresses (2025) — **287.007**

Participant Development

In 2025, there was a slight consolidation in the number of new participants. At the same time, we also see that participants who use the Lawful Interception and Disclosure Service or NaWas are choosing to subscribe to both services. For example, one Lawful Interception and Disclosure participant decided to start using NaWas in 2025, and there were five NaWas participants who now also use the Lawful Interception and Disclosure Service.

We are seeing growing interest in the Lawful Interception and Disclosure Service from MVNOs and MVNEs. Interest in NaWas is also on the rise. This is due to the increasing emphasis on European-based DDoS solutions, an area in which NaWas has proven its worth in the sector for 10+ years. By the end of 2025, NBIP had over **194** participants, of whom **107** organisations were participating in the Lawful Interception and Disclosure Service and **131** organisations in the NaWas. There are **44** organisations participating in both services. Organisations that use both the Lawful Interception and Disclosure Service and the NaWas count as a single participant in the total number of NBIP participants.



Public affairs

NBIP is keen to contribute to issues that are important to its participants and to a safe and reliable internet. NBIP does this by providing its views, both solicited and unsolicited, on legislative proposals, regulations and policy, and by participating in various public-private partnerships. NBIP, together with AMS-IX, SIDN and SURF, is a member of the umbrella organisation Digital Infrastructure Netherlands (DINL).

The approach underpinning NBIP's public affairs activities is always to bring the practical challenges faced by participants in complying with legislation and regulations to the attention of the relevant decision-makers. As NBIP is also operationally active through its shared services, it can provide a clear picture of how legislation and policy impact day-to-day business. We do this systematically across four key areas.

- Digital resilience and digital autonomy in digital infrastructure
- Operational compliance with laws and regulations
- DDoS protection
- Abuse prevention

NBIP is not, by its very nature, a trade association, but provides operational services for the benefit of its members. By combining public affairs activities with these services, NBIP can highlight the interests of its members more effectively to political stakeholders.

Developments in 2025

In 2025, progress was made regarding NBIP's public affairs activities. The team now includes a member dedicated to public affairs. Together with the director, they are working to implement the strategy set out based on the aforementioned issues on which NBIP is actively engaged.

In addition, concrete actions have been taken on the four issues. For example, cooperation with the National Cyber Security Centre (NCSC) has been intensified. Another highlight of our public affair's activities was the invitation to the V-100 (Accountability Day) in the House of Representatives. On this day, one hundred citizens who have direct contact with one or more public bodies are invited each year. The number 100 represents the hundred citizens invited by the House to critically review the ministers' annual reports and question the ministers on these matters.

NBIP has also shared its views on the supervision surrounding the upcoming eEvidence Regulation and accompanying directive.

Position paper: 'Strategic digital autonomy and the government-wide cloud policy'

In recent times, it has rapidly become clear that there are significant risks associated with our digital dependency. The fact that access to widely used cloud services can be used as a means of geopolitical pressure is just one example of this. This dependency therefore creates unnecessary and risky dependence. Concrete steps must therefore be taken immediately to reduce this dependency.

For this reason, the position paper 'Strategic digital autonomy and the government-wide cloud policy' was presented last year to Members of Parliament Barbara Kathmann and Jesse Six Dijkstra. The position paper was produced through a collaboration between various companies and organisations.

The aim of the position paper is to present a vision for the implementation of cloud policy within the government. Based on this vision, the following three concrete actions have emerged:

1 Create a new category of cloud services for sensitive government data, essential government services and critical physical infrastructure, subject to additional procurement requirements relating to digital strategic autonomy.
2 Promote freedom of choice and fair competition in the cloud market by making data portability and interoperability mandatory for non-critical cloud services and by implementing robust exit strategies. This also prevents the risk of vendor lock-in, where migration to another supplier is virtually impossible due to complexity and/or high costs.
3 Continue to emphasise the coordinating role within the government regarding the procurement policy for cloud services. This role is crucial to implementing a successful cloud policy in the long term.

NBIP in Europa

NBIP plays a key role as a developer and facilitator in strengthening Europe's strategic digital autonomy. In practical terms, this means that NBIP develops solutions to enhance the digital resilience of the digital infrastructure sector. In addition, NBIP participates in various European projects and partnerships and actively contributes knowledge and expertise.

One of the main reasons for this positioning is the growing awareness of the undesirable dependence on non-European cloud providers and their services in Europe. The lack of 'Made in Europe' solutions is therefore a major challenge. At the same time, there are also dependencies in other areas that are undesirable and could be used as a means of exerting geopolitical pressure, for example in the field of security solutions, threat intelligence and information on vulnerabilities and abuse. In the latter area, NBIP has already taken steps with Clean Networks to support participants in combating abuse.

IPCEI-CIS: MISD

NBIP recognises the urgent need for Europe to have its own cloud infrastructure and is therefore participating in IPCEI-CIS through the Modular Integrated Sustainable Datacenter (MISD) project. Within this project, seven organisations are participating in a consortium, each with its own area of specialisation. NBIP is responsible for the cybersecurity aspect of the project.

The aim of the Modular Integrated Sustainable Datacenter (MISD) project is to develop a new modular, sustainable and secure-by-design concept to be deployed in locations close to end-users (edge computing). The innovations and developments realised within the project are brought together in a validated, distributed setup in a field lab. The project will run for 5 years (2024 to 2029).

Over the past year, the testbed has been further developed as a controlled environment for testing new cybersecurity applications. In addition, the groundwork laid in 2024 for decentralised mitigation techniques has been further developed. The first successful tests have also been conducted.

Membership of the European Cyber Security Organisation (ECSO)

Over the past year, NBIP has become a member of the European Cyber Security Organisation (ECSO). The ECSO is a pan-European, non-profit public-private federation. Since 2016, this federation has been committed

to strengthening Europe's resilience in the field of cybersecurity and strategic autonomy. More than 300 organisations across 30 countries are now members of the federation. The decision to join the ECSO fits seamlessly with NBIP's mission to share our expertise in lawful interception/disclosure, DDoS mitigation, and threat intelligence even more actively across Europe. Furthermore, the knowledge gained within the ECSO can be used for the benefit of NBIP participants.

Participation in eEvidence Technical Committee within the European Commission

For the practical implementation of eEvidence, a European platform is used for accessing, sending, and receiving preservation and disclosure orders. As previously described in this Annual Monitor in the eEvidence Dossier section, both the applicant and the provider use this platform.

The European Commission established a technical committee to develop this platform. This committee comprises government bodies from across Europe responsible for the implementation of eEvidence, as well as industry experts, with the aim of building a reliable and user-friendly portal. Drawing on its expertise in lawful disclosure, NBIP has been involved from the outset and has contributed to the technical design of the platform.

On the soapbox

In 2025, NBIP shared its expertise in a variety of ways, both within and outside the sector. For example, we gave multiple presentations in the Netherlands and other European countries about our services and projects. We also had the opportunity to highlight NBIP's mission in various media outlets.

Presentations

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

Articles, 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)* ↗

About NBIP

Foundation NBIP was established in 2001 as an implementing body for interception orders arising from the Dutch Telecommunications Act. Today, NBIP has grown into the centre of expertise for DDoS mitigation, lawful interception and threat intelligence analysis for internet, hosting and cloud providers in the Netherlands and Europe.

NBIP's mission is to help digital infrastructure providers meet their operational compliance requirements with services that can be operated efficiently. Participants can jointly use expensive or complex facilities that they do not need all the time via NBIP. The best-known example of this is the National Washing Facility (NaWas), the largest non-profit DDoS scrubbing centre in the world, used by more than 130 organisations in nine European countries. Over the years, NBIP has grown to become an established player in the Dutch internet landscape.

With around 200 participants, an international presence and involvement in strategic European development projects, NBIP's philosophy has proven to work in practice. Both digital infrastructure providers and public and private partners know how to find their way to NBIP.

For more information and current developments, visit www.nbip.nl/en

NBIP
nationale beheersorganisatie internet providers