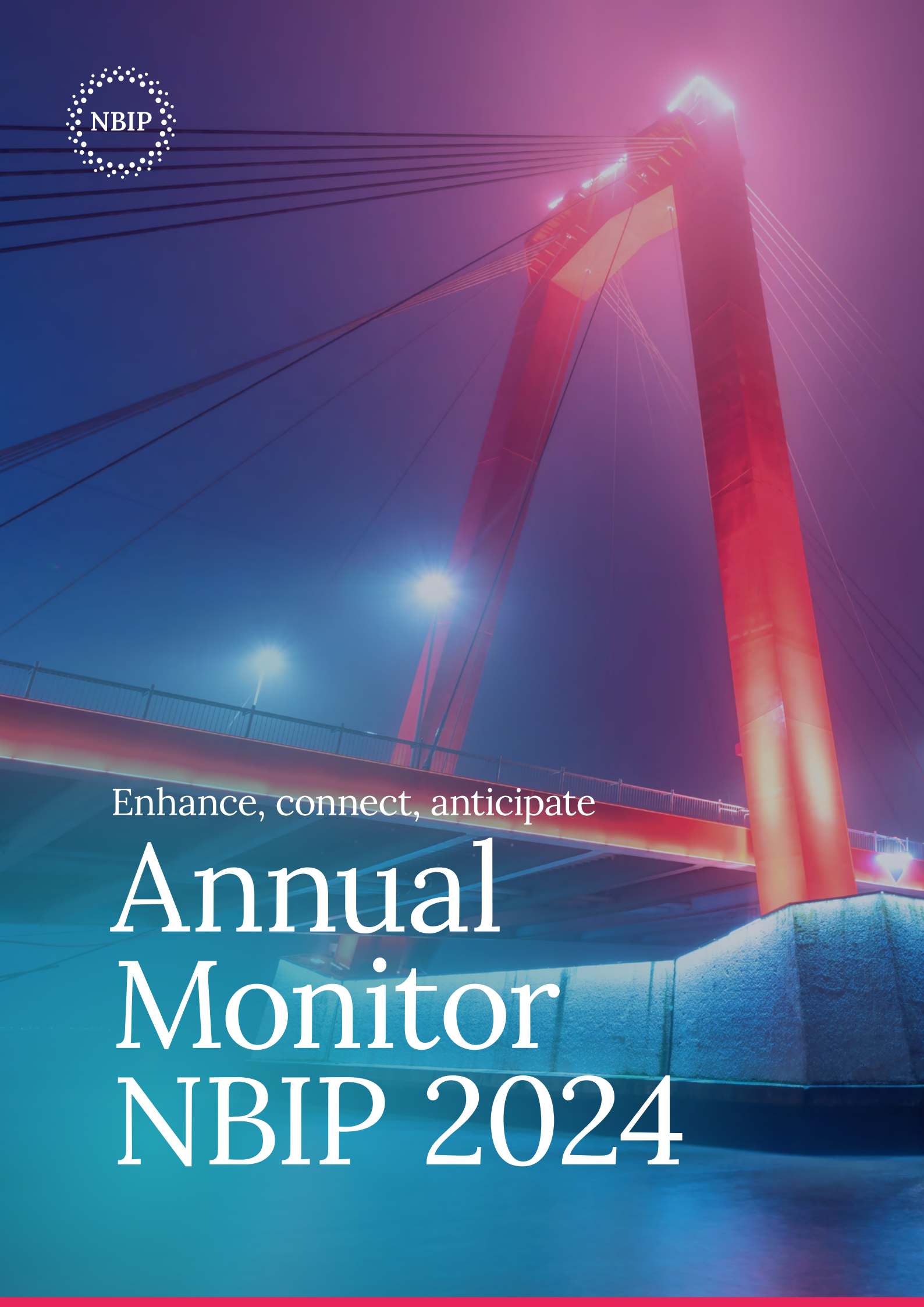


Enhance, connect, anticipate

Annual Monitor NBIP 2024

Colophon

Authors

Octavia de Weerdt
general director, NBIP

Wouter Pegtel
communications and public affairs manager, NBIP

Pim Kokke
communication specialist, NBIP

Contributors

Valerie Frissen
Rick Sulman

Design

Bijdevleet, Rotterdam

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

Table of Content

Preface

Octavia de Weerdt
General Director NBIP

2024 was an important year for NBIP, in which a solid foundation was laid for the future. That future is uncertain in some respects: the shifting landscape on the world stage places greater demands on the (cyber) resilience of our society and therefore also on NBIP. That resilience consists not only of preparedness in the face of threats, but also of Europe's ability to shape its digital autonomy.

Like many other organisations in our sector, NBIP has had to adapt to this new reality. Fortunately, in 2024 we worked hard to further develop a robust and stable organisation that provides its services and expertise to participants, partners and stakeholders in a relatively autonomous manner. This has created a solid foundation that can be relied upon even in an increasingly turbulent world.

This is necessary because Europe is embroiled in hybrid conflicts. As we wrote in early 2025 in our DDoS annual review for 2024, which is also included in this report, DDoS attacks are increasingly being used to disrupt Western democratic societies and sow fear. Unfortunately, attacks, hacks and theft of sensitive data are also commonplace in the broader cyber domain.

We must therefore be resilient to systematic attempts at disruption, sabotage and destabilisation. NBIP has therefore made significant improvements to its infrastructure in 2024 and created additional robustness in several areas. This is now an ongoing effort within the organisation, which is constantly being tailored to the needs of our participants and the (DDoS) threat landscape.

Now that virtually all major operational and strategic changes have been implemented (see also the previous NBIP Monitor), we are continuing to build on our mission: to provide shared facilities for digital infrastructure providers, enabling them to ensure their digital resilience and compliance with laws and regulations.

In 2024, we also focused on strengthening ties with our participants and partners. We revamped our corporate identity and implemented more accessible branding, including a redesign of our logo and a new website. In 2024, we launched a new format for participant meetings (Lunch & Learn) to enable more frequent face-to-face discussions. We spoke at events and in podcasts and shared our knowledge in the media at home and abroad. In addition, we have given our own event, NBIP NEXT, a new look and our ambition is to further expand this knowledge event around the core themes of NBIP.

Recently, consideration has also been given to how NBIP can contribute to the challenges we all face. Creating and strengthening the digital autonomy of the Netherlands and Europe has quickly become a very important theme. This ambition is widely endorsed and expressed, but it must result in concrete solutions sooner rather than later. NBIP contributes to this through various European projects, including IPCEI-CIS. We will continue to expand this contribution in the coming years, with the aim of establishing collective cyber resilience facilities for the digital infrastructure in the Netherlands and Europe.

Finally, in 2026, NBIP will celebrate its 25th anniversary. This is a special milestone for the foundation, and we can be proud of what we have achieved as an organisation for our participants and the sector. We have developed into the centre of expertise for DDoS and its mitigation, lawful interception and disclosure, threat intelligence and the fight against online abuse. This would not have been possible without the dedication and commitment of our participants, the board and, of course, the renewed NBIP team. It is very special to be able to lead this dedicated group of people who work every day to ensure a safe, reliable and open internet.

Summary

Annual Monitor NBIP 2024

Over the past year, NBIP has worked hard to further develop a robust and steadfast organisation that provides its services and expertise to participants, partners and stakeholders in a relatively autonomous manner. This has created a strong foundation that can be relied upon in an increasingly turbulent world.

Connection

There is strong momentum to strengthen Europe's strategic digital autonomy. NBIP plays a role in this as a developer and connector. In concrete terms, this means that NBIP develops solutions to increase the digital resilience of the digital infrastructure sector. In addition, NBIP participates in various European projects and partnerships and actively provides knowledge and expertise.

In 2024, NBIP also devoted considerable attention to strengthening our connection with our participants and partners. The new Lunch & Learn meetings, where we engage with participants in discussions about the latest developments concerning our services and new legislation and regulations, contribute to strengthening this connection. In addition, we have also emphasised our expertise in DDoS attacks and their disruptive nature for society on several occasions in the media. The NBIP NEXT knowledge event was once again well attended last year, where we reflected on the tenth anniversary of the NaWas.

Strengthening

Connection goes hand in hand with strengthening our services. In 2024, we welcomed two new participants to the Lawful Interception and Disclosure Service, while the number of NaWas participants increased by eight. Last year saw a consolidation of the total number of NBIP participants. In a few cases, individual participants continued as a single participant. As a result, the absolute number of participants grew only slightly. However, the number of underlying networks served by NBIP did grow, but this is not directly reflected in the number of participants.

Development of Services

The most important development in 2025 and 2026 will be the technical implementation of eEvidence within the Lawful Interception and Disclosure Service. This new European directive and regulation ensures that Member States can request electronic evidence directly from providers operating in another Member State. NBIP has an excellent track record with our service, which means it is optimally prepared for the process changes. This also enables NBIP to support participants when they receive an eEvidence request.

NBIP focuses on shared, non-profit cyber resilience services for digital infrastructure

NaWas is also undergoing continuous development. For example, outdated equipment in the areas of routing, switching and mitigation layers have been replaced, increasing the stability and capacity of the NaWas. In addition, the capacity at various internet exchanges has also been increased.

The Code of Conduct for Combating Abuse, one of the pillars of Clean Networks, underwent a major update in October 2024. Changes were made to definitions and policy to bring them into line with the latest market developments and regulations. It was also decided that the Code of Conduct for Combating Abuse will now be reviewed annually, based on regulations, feedback and the experiences of the participants in the Code of Conduct.

Anticipate

The challenge for Europe to strengthen its strategic digital autonomy is broad and multifaceted. There is an undesirable dependence on non-European providers due to a lack of adequate European alternatives. That is why, on the one hand, we aim to develop concrete products and services in the field of digital resilience that provide participants with reliable, common alternatives to non-European services. On the other hand, NBIP wants to play a role in stimulating research, innovation and collaboration in the sector. An example of this is our participation in IPCEI-CIS (Important Project of Common European Interest on Cloud Infrastructure and Services) through the MISD consortium.

All this is done based on the belief that a safe and reliable internet is a shared responsibility. By combining forces, knowledge and resources, participants use NBIP to jointly organise their digital resilience and operational compliance with laws and regulations.

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.

The National Internet Providers Management Organization (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 service 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.

"The momentum is now there to strengthen European and national digital autonomy based on collective responsibility"

In conversation with

Valerie Frissen
Director SIDN Fund

Valerie Frissen is director of the SIDN Fund, which supports projects that contribute to a strong, open and free internet. She is also professor of Digital Technology and Social Change at Leiden University. In 2024, she received the Lifetime Achievement Award from the Internet Society Foundation for her services to the sector.

Can you provide a perspective on how the internet sector has changed since the beginning of this century, based on your various areas of expertise?

"That's always a bit difficult, because you tend to look at things through the lens you're currently wearing. From the perspective of the SIDN Fund, I think we now need to think carefully about how the internet is structured and whether that still works well. We designed it based on a number of core principles (openness and a safe haven for innovation) that we all still support because they have served us well in the past. But what we are now encountering is that the principles of the internet have also given space to parties that abuse those principles and have started to exhibit monopolistic traits.

This has had many negative social and economic effects. You can now also see that the discussion surrounding sovereign cloud has led to more explicit mention of our dependence on the services of a limited number of parties. This is economically unhealthy, but also socially unhealthy because the internet has become an integral part of our daily lives. As a result, we as users have become the raw material for the revenue model. Think of all the data about our behaviour that is used and how algorithms use it to steer us in all kinds of directions.

On the policy side and within the tech community, it has been assumed for too long that developments like these would regulate themselves. As a result, too little has been done to steer the process, which means that we are now lagging in Europe when it comes to regulation. This is necessary to a large extent, but it is very reactive. The sector may perceive this as "rigid regulation," and we often hear that it slows down innovation. But you could also argue that this is precisely our opportunity to do better for the next phase, for example, with all the AI developments, and to see responsible technology development as a source of innovation. That is what we are trying to contribute to with the fund."

Since 2015, more than 400 projects have been launched with support from the SIDN Fund. Which projects in the domain of an open, free and reliable internet stand out most to you?

"We have supported so many great projects that it is difficult to name just a few. It is good to know that we started with three objectives, one of which was to strengthen the internet itself. The projects we have carried out together with NBIP are excellent examples of this, because they were organised based on the collective spirit of the sector. This strengthens the sector, the internet and its users.

The second objective is to strengthen the position of the end user of the internet, with a particular focus on accessibility for users who are at risk of being left behind. A great project that falls between these two objectives is Publicroam. Publicroam is a Dutch initiative that originated from existing Wi-Fi roaming services in education (eduroam). Publicroam uses the same technology to provide citizens with secure, privacy-by-design Wi-Fi everywhere, without them having to use unsafe open Wi-Fi networks. Our educational programmes, such as HackShield, which "trains" children to become cyber agents in a gaming environment, are also part of the second objective and are a great and successful example of increasing digital awareness among children.

The third objective that the fund is committed to focuses primarily on the impact of the internet. Here, we want to reinforce the positive outcomes of the internet and counteract the negative ones by means of tools. In this area, we have supported projects that combat disinformation and social polarisation, for example. A good example of this is DuckDuckGoose, which focuses on detecting and exposing deepfakes."

What is the key to cooperation in strengthening our digital resilience?

"I think there needs to be cooperation between all parties, from the abstract policy level to the individual user level. Everyone must take responsibility from their own position. It is good that a lot is happening now on the regulatory front, with Europe taking the lead. This will naturally be reflected in national legislation. In addition, I think that the parties in the sector could work together even more and not just see each other as competitors. As the SIDN Fund, we also work a lot with other funds in joint calls that focus primarily on social impact. Individually, you can also increase your digital awareness of the services you use and start using alternatives more often. It is therefore a good time to sit down together and shape the responsibility we all have."

What can the Netherlands achieve in terms of digital resilience?

"The Netherlands has always been a country at the forefront of digital possibilities and access. This ensured that everything continued to run smoothly during the pandemic (2020-2022). We must certainly continue to look at the opportunities and what we are good at as a country. But what we should do much more, and this is very much part of the discussion on digital autonomy, is address the risks of our dependence on vital digital infrastructure. For example, the government can really play a role as a launching customer and, in its procurement policy, focus much more on what is needed for the future and set requirements for suppliers. This also applies to public sectors, such as healthcare and education, which rely heavily on the systems of a single provider. In this transition phase, you need to be stricter in your procurement conditions and ultimately move towards realising alternatives and investing in Dutch parties. This also requires knowledge on the part of the government."

Does the risk also stem from the level of knowledge on government side?

"I think the level of knowledge has improved in recent years, but the government wasn't really known for having this knowledge in-house. It was outsourced to large suppliers, which is quite risky because they try to get you into their systems and keep you there. If you can't assess for yourself whether that's what you really want, it becomes more difficult to get out."

How can we, as a society, sector and government, ensure that we do not fall back into old habits once the dust has settled in a few years' time?

"The difference with the past is that the geopolitical situation has changed. Security issues are completely different now that peace is no longer a given. That is why we now see the urgency of a secure and sovereign digital infrastructure much more clearly. And that is why it is important to take steps together now, because it is high on everyone's agenda. From a business perspective, it is interesting to consider the role of start-ups and scale-ups. In an open market, these successful pioneers will eventually be bought up by the big players. So, if you want a certain degree of digital autonomy in Europe and the Netherlands, you also need to look at how you can keep these parties and the vital services they provide autonomous."

NBIP and the SIDN Fund collaborate in various areas, with Clean Networks being one of the projects that has received support from the fund. How do you view the collaboration between the two organisations?

"Very good. We can support individual projects with parties from your organisation and partly from our own supporters, but they are somewhat more difficult to mobilise. Therefore, an organisation as NBIP is an excellent partner for us, because we share the same common interest – strengthening the sector and digital infrastructure as a whole – and work together to stimulate innovation."

Mission and 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.

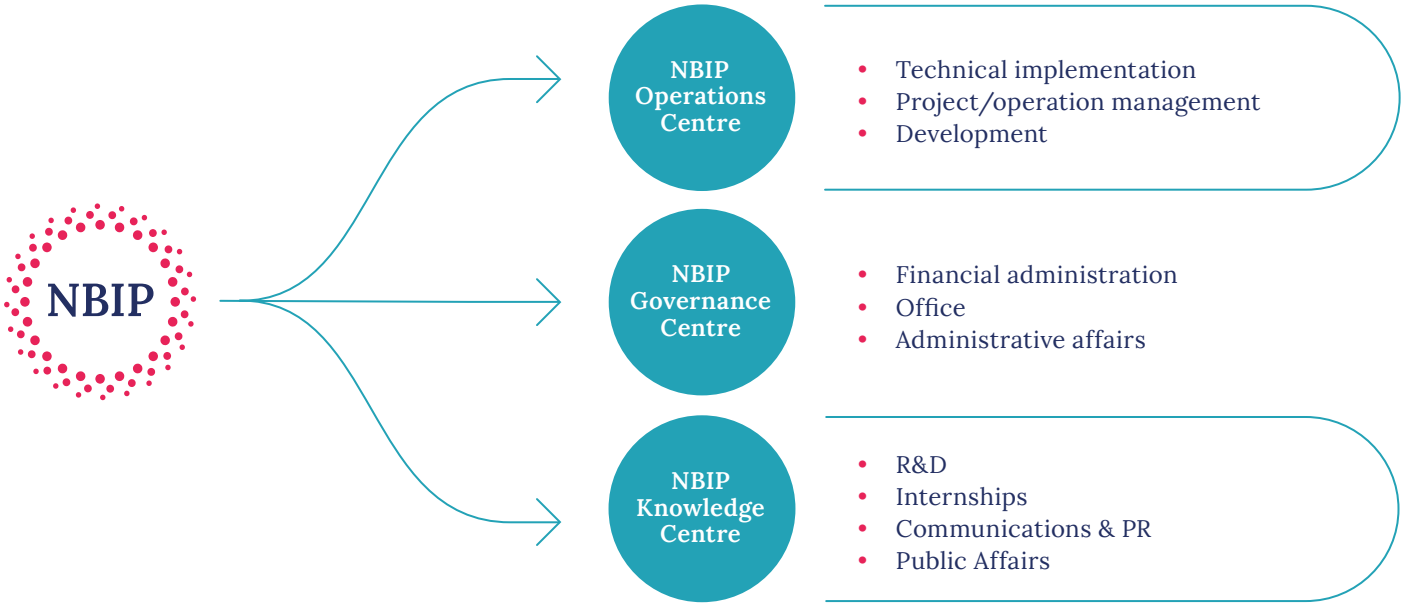
Organisational structure

NBIP's services are provided from its operations centre, which is the heart of the organisation. NBIP also has a governance centre, which handles management, finance and administrative matters, and a knowledge centre that serves both the internet community and the wider public.

The NBIP Governance Centre provides support services for NaWas, the Lawful Interception and Disclosure Service and the Clean Networks Platform, including financial administration, broader administrative tasks and management support.

The NBIP Knowledge Centre is committed to the development of knowledge, technology and employees.

The knowledge centre focuses on NBIP participants, the internet community and the government.
In addition, the Knowledge Centre increasingly serves as a point of contact and knowledge base for the media and the wider public in the areas in which NBIP is active. This includes position papers on digital autonomy, technical information on DDoS mitigation, background articles on cyber resilience and NBIP NaWas quarterly updates.



Governance

NBIP's board is composed of board members. The board is responsible for policy formation, financial control and accountability, prudent handling of the foundation and the interests of participants united in it.

In 2024, the board met five times. The board consisted of five members: a chairman, a secretary, a treasurer, and two general board members, one of whom serves as vice-chairman. This position was temporarily filled by the vice-chairman. In addition, the chairmanship of the Board of Members passed from Bernard Edelenbos, who held this role temporarily until a successor was found, to Frans ter Borg.

Board members are nominated by the Participants' Council, in which all NBIP participants are represented. Among other things, they can question the board through the chair of the Participants' Council and provide solicited and unsolicited advice. The chair of the Council of Participants may attend board meetings, has access to the minutes of those meetings and has as one of his or her most important tasks to put items on the agenda for the board on behalf of participants.

The NBIP management is responsible for the implementation of the policy as laid down by the board and is accountable for the results achieved. The general director is further autonomous within the set frameworks to carry out her assignment. The general director leads the organisation, supported by a management team since 2025.

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.

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.

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.

‘The Internet doesn’t stop at the border’

In conversation with

Rick Sulman
Vice Chairman and Board Member

Rick Sulman is vice-chairman of the board of NBIP and CEO of telecom operator Speakup B.V. Within NBIP, Rick is primarily responsible for overseeing ethical, transparent and effective governance within the organisation. In this interview, Rick briefly looks back and shares how NBIP will continue to position itself as an organisation within the digital infrastructure industry in the coming years.

In September 2020, you joined the NBIP board. How do you look back on the past few years?
“First of all, I personally find it important and enjoyable to contribute to the internet collective in the Netherlands. NBIP’s idea of working together as a sector to organise collective services for every provider, regardless of size, really appealed to me. In addition, VOIP parties, such as Speakup, were not very well represented within NBIP at the time. That is why I decided to run for the board. Over the past year and a half, we have been busy taking NBIP’s services in-house. This has been an incredibly important step for the organisation. Now that this transition has been completed, we are looking even more forward to the future.”

What are the goals and direction for NBIP in the coming period?
“The world of cybersecurity has changed significantly in recent years. Twenty-five years ago, for example, it was mainly hackers who occasionally caused trouble from their attic rooms. Now you see professional parties being hired by states to make the internet unsafe. The geopolitical situation has changed, and we as NBIP must anticipate this. The collective provision of operational services on a non-profit basis, for example, is something that happens very little or not at all in Europe. That is why we are looking to promote the collective philosophy of NBIP more widely in Europe.”

In your daily life, you are also CEO of telecom operator Speakup. From that position, how do you view the cooperation within the telecom sector in combination with the themes NBIP is dedicated to?
“The telecom world is quite opportunistic and particularly focused on the short term. A while ago, I attended a meeting in London with Octavia (de Weerdt, managing director of NBIP, ed.) organised by an overarching international VOIP organisation, of which Speakup is also a member. You notice that when there is a large wave of DDoS attacks, every organisation starts thinking about organising a solution to combat these attacks. During

> “The geopolitical situation has changed, and as NBIP we must anticipate this.”

that meeting, we explained how NaWas has been a widely embraced DDoS mitigation service within the sector for more than ten years. Unfortunately, the reality is that when there is less attention for DDoS attacks, the telecom sector tends to ignore the issue, even though there is enthusiastic response to the story surrounding NaWas. Raising awareness of the dangers of DDoS at a higher level is therefore a priority for the telecoms sector. That is why I try to invite as many companies from the sector as possible to come and listen when NBIP organises meetings and webinars.”

How can NBIP enhance its profile in Europe?

“If you look at NaWas, for example, it would be great to have different points of presence (PoPs) in even more European countries, so that traffic can be redirected even more easily. In addition, we have noticed that European authorities are very interested in the NBIP model as a foundation that offers operational services. It would be great to roll this out further and for NBIP to play a role in this. We have a lot of expertise in-house, which means we can make a difference, because the internet does not stop at the border.”

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 the 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 (Wet BOB), this special investigative power can only be used on the basis of these three titles:

1 There must be a 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 also 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.

Key developments

eEvidence

The implementation of eEvidence within the Lawful Interception and Disclosure Service will be tackled in the coming period. This new European directive and regulation ensures that Member States can request electronic evidence directly from providers operating in another Member State. From 18 August 2026, providers who receive a request must provide the requested data within 10 days, or in urgent cases within 8 hours. Currently, for requests of this kind from another Member State, providers have a maximum of 120 days to provide the data.

Within the Netherlands, the Ministry of Justice and Security is responsible for implementing eEvidence in national legislation. A decentralised IT system is currently being developed in Europe, with each Member State having a connection point for accessing, sending and receiving requests. It is important to note that there will be no European data storage. There will be national

> “All work is carried out in strict compliance with legislation and under strict safety measures.”

connection points for government and service providers. In addition, an eEvidence order can only be sent to providers via the Dutch national connection point.

NBIP has an excellent track record with its Lawful Interception and Disclosure Service, which means it is optimally prepared for the process changes. This also enables us to support participants when they receive an eEvidence warrant. In addition, we are involved in the technical committee during the implementation of eEvidence, where we contribute ideas within Europe about the practical implementation of the system. In this way, we are ensuring that our participants will soon be able to comply seamlessly with the new legislation.

ATKM

Since 2024, the Authority for Online Terrorist and Child Pornographic Material (in Dutch: ATKM) has been detecting and assessing online terrorist and child pornographic material. If the ATKM determines that online material is terrorist in nature, it can issue a removal order. Providers where such material is found must remove the material or make it inaccessible within one hour. If terrorist material is found online on multiple occasions at the same provider, the ATKM may issue an exposure order. The provider must then take measures to prevent terrorist material from reappearing online. In addition, the authority may impose sanctions, in the form of fines or a penalty payment, on providers who do not comply with the obligations laid down in the Terrorist Online Content (TOI) Implementation Act and the Administrative Law Approach to Online Child Pornography Act.

For small and medium-sized providers of digital infrastructure, this entails a great deal of responsibility, which is accompanied by the necessary additional organisational burden. In addition to the Lawful Interception and Disclosure Service, NBIP is therefore launching a helpdesk to supplement the Lawful Interception and Disclosure Service for its participants. This new helpdesk, which will operate on a notice and take-down basis, will ensure that (new) participants are supported in the event of any orders from the ATKM. In concrete terms, this will mean that NBIP can accept orders on behalf of participants and ensure that the participant takes urgent action.

Services

NaWas

The NaWas has been improved in various ways in 2024, with a strong focus on the reliability and continuity of service provision.

2024 was an anniversary year for NaWas, as the service celebrated its 10th anniversary. From a small-scale service developed by a few NBIP participants, it quickly grew to become a household name in the Dutch internet sector. It was a huge success: in 10 years, the platform grew to 130 participants in various European countries.

Over the years, various expansions of the NaWas were realised, both in terms of capacity and availability and additional services and functionality. However, the architecture of the NaWas has not changed significantly in those 10 years, simply because there was no need to do so.

In recent years, however, it has become increasingly clear that the DDoS landscape has changed significantly under pressure from geopolitical developments, among other things. Attacks have become more complex, longer-lasting and have had a greater impact across the DDoS landscape. Participants have made more frequent use of the NaWas and, in some cases, have had to deal with prolonged or repeated, advanced attacks that had to be countered.

Behind the scenes, work was therefore carried out on a major upgrade of the NaWas, with the ultimate goal of providing better service, improved redundancy and greater capacity. Improvements were also made to infrastructure management and analytics.

A large part of these plans was realised in 2024, including improved redundancy within the infrastructure and at the internet exchanges used by NaWas. In addition, an sFlow service has been made available to participants and internal monitoring has been greatly improved, with engineers being immediately notified of new prefixes routed through NaWas so that they can monitor in real time whether mitigation is successful.

The NaWas team has also been expanded, so that all the necessary expertise is now available in-house, from specialised knowledge of networks and BGP to the details of very diverse types of DDoS attacks and how to mitigate them. In addition, the support infrastructure has been updated so that questions and requests can be handled quickly and effectively via a dedicated channel.

Services

Clean Networks

Clean Networks consists of two pillars: a threat intelligence platform for digital infrastructure providers and a code of conduct that commits those providers to preventing and actively detecting and removing abuse in their networks.

The need for Clean networks

The misuse of systems and security vulnerabilities in the networks of digital infrastructure providers is a major source of illegality on the internet. We refer to this type of misuse as abuse. This refers to all activities in which providers' infrastructure is used and misused, for example to coordinate and carry out cyber attacks, steal data or offer illegal content.

One of the problems providers encounter in preventing abuse is that security vulnerabilities are not always known. It therefore helps if they are proactively informed about vulnerabilities in their network. It is also important for providers to implement policies that enable them to prevent abuse by malicious parties posing as legitimate customers or buyers. Clean Networks offers a comprehensive approach to abuse, from detection and notification to a code of conduct that enables providers to keep their policies and enforcement in order.

Clean Networks' comprehensive approach

Clean Networks offers digital infrastructure providers an effective and proven solution with broad support from the digital infrastructure sector to detect and combat abuse. Clean Networks' threat intelligence provides providers with automated notifications from a variety of sources of vulnerabilities, tailored to specific IP ranges within the provider's network. With this information, providers can take targeted action and preventively reduce the risk of abuse in their own network.

Clean Networks also helps to comply with laws and regulations such as the Digital Services Act (DSA) and Network and Information Security Directive 2 (NIS2) through its Code of Conduct for Combating Abuse. Part of this code of conduct includes a notice and takedown (NTD) policy and a know your customer (KYC) policy, designed on the basis of internationally accepted standards.

Code of Conduct for Combating Abuse

By signing the Code of Conduct for Combating Abuse, providers commit to taking measures to detect abuse in their networks and remedy security vulnerabilities. They also commit to a notice and takedown procedure, a "Know Your Customer" (KYC) policy and ensuring that abuse reports can be easily submitted. Signatories to the code of conduct receive the Clean Networks Quality Mark, which means they contribute to a safer digital Netherlands. This allows them to demonstrate that they are taking the necessary measures to prevent abuse, giving them a competitive edge in the market, as more and more organisations are including requirements for this in their procurement policies. The code of conduct also helps with compliance with the Digital Services Act (DSA) and the Cyber Security Act (Cbw/NIS2).

In October 2024, the Code of Conduct for Combating Abuse was updated. We made adjustments to definitions and policy to bring them into line with the latest (market) developments and regulations.

> “Providers who sign the Code of Conduct for Combating Abuse have a competitive edge in the market.”

It has also been decided that the Code of Conduct for Combating Abuse will now be revised annually, based on regulations, feedback and the experiences of the participants in the Code of Conduct. With each revision, the version number will be updated and the changes will be documented in the revision history. NBIP is the administrator of the Code of Conduct and is responsible for version management. New sections have also been added to the new version: Know Your Customer policy, Non-compliance and the signatories to the Code of Conduct.

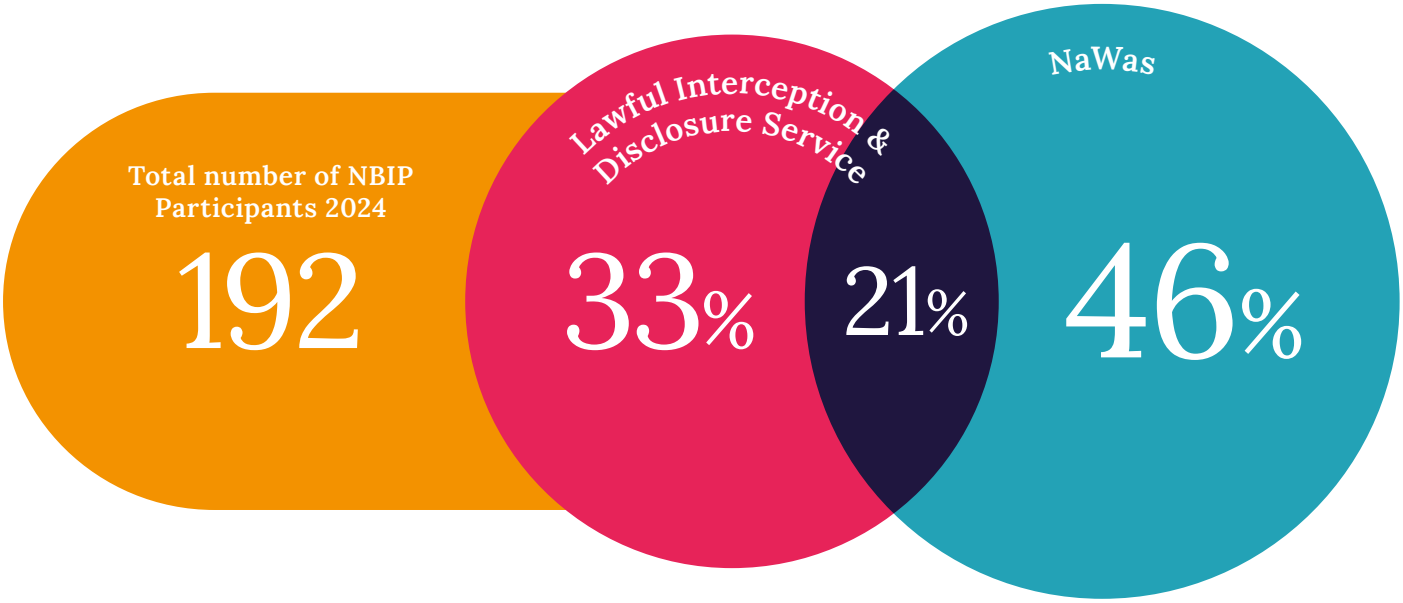
Representatives Code of Conduct In addition to NBIP, the following organisations actively contributed to the drafting of the Code of Conduct: Stichting Digitale Infrastructuur Nederland (DINL), Dutch Cloud Community (DCC), and Vereniging van Registrars (VvR).

Clean Networks was made possible in part by a grant from the European Union and funds from the Digital Trust Center and the SIDN Fund.

Participant development

In 2024, there was consolidation in the number of NBIP participants. The reason for this is that in a few cases, separate participants continued as a single participant. As a result, the absolute number of participants grew only slightly. The number of networks served by NBIP has expanded further.

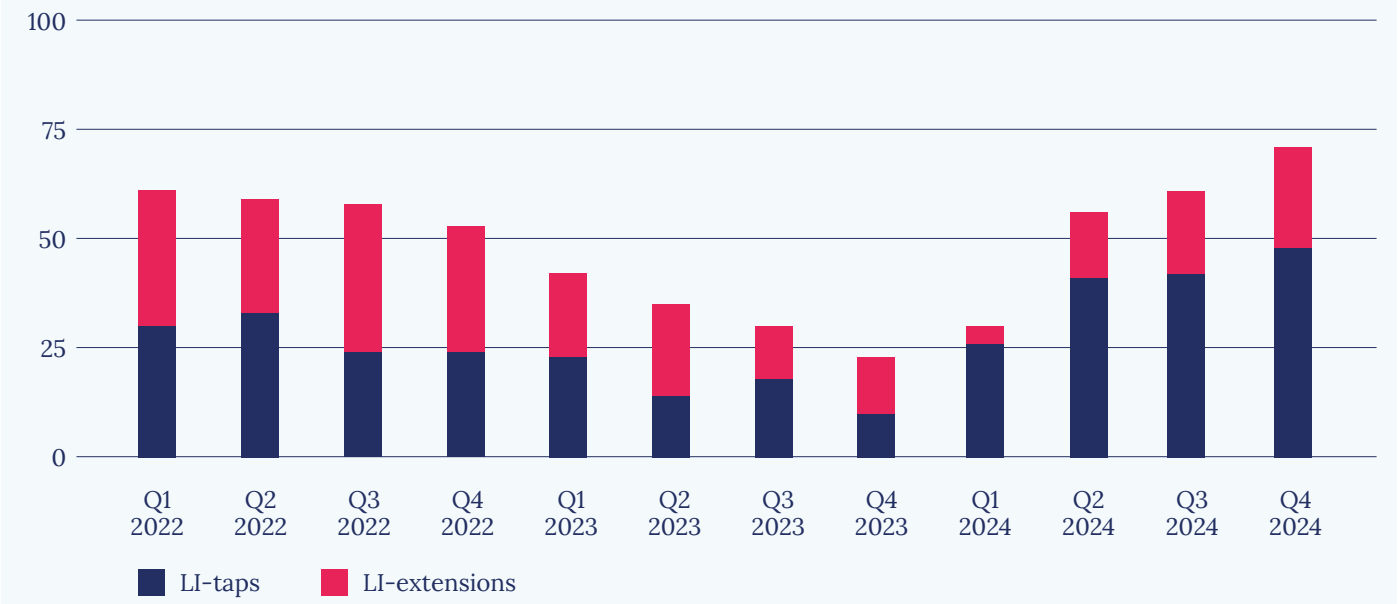
Organisations that benefited from both the Lawful Interception and Disclosure Service and NaWas are counted as one single participant in NBIP's total number of participants. At the end of 2024, NBIP therefore had 192 participants, of which 103 organisations participate in the Lawful Interception and Disclosure Service and 129 organisations to the NaWas. 40 organisations are participating in both services.



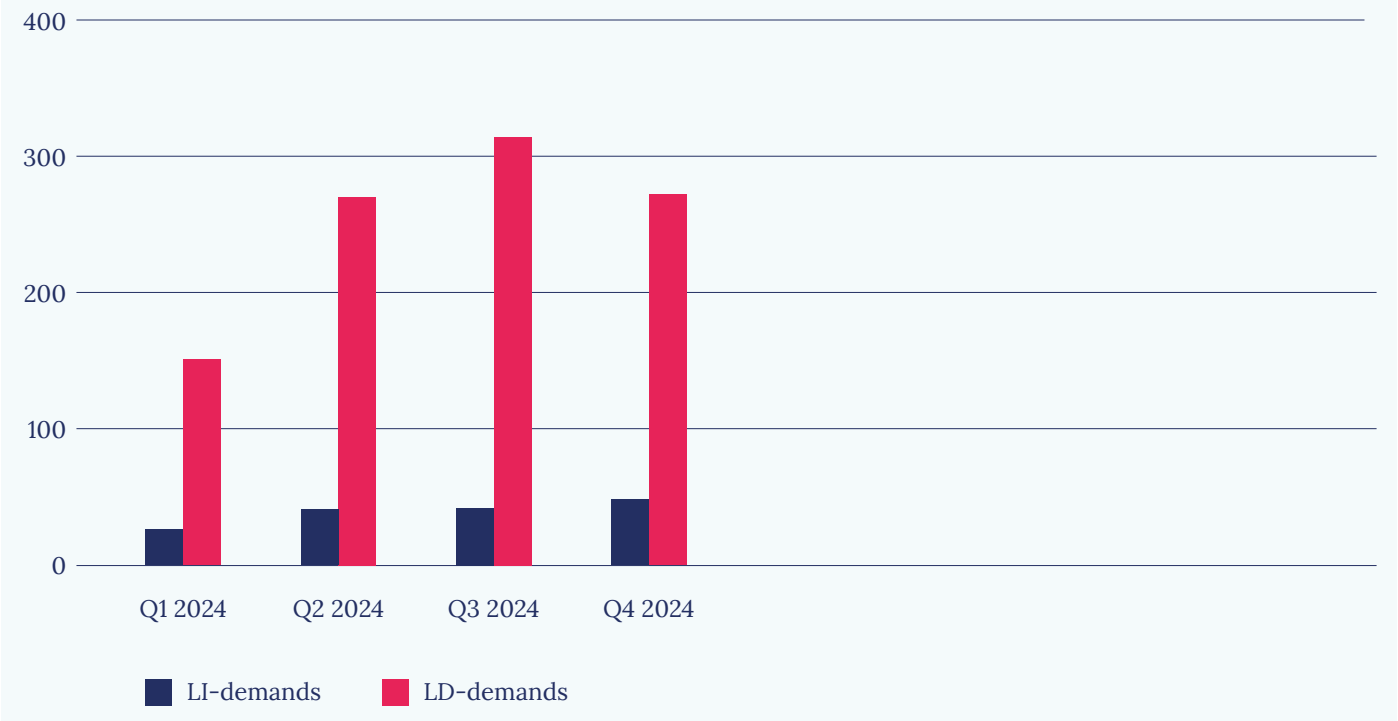
Lawful Interception and Disclosure Service

Figures 2024

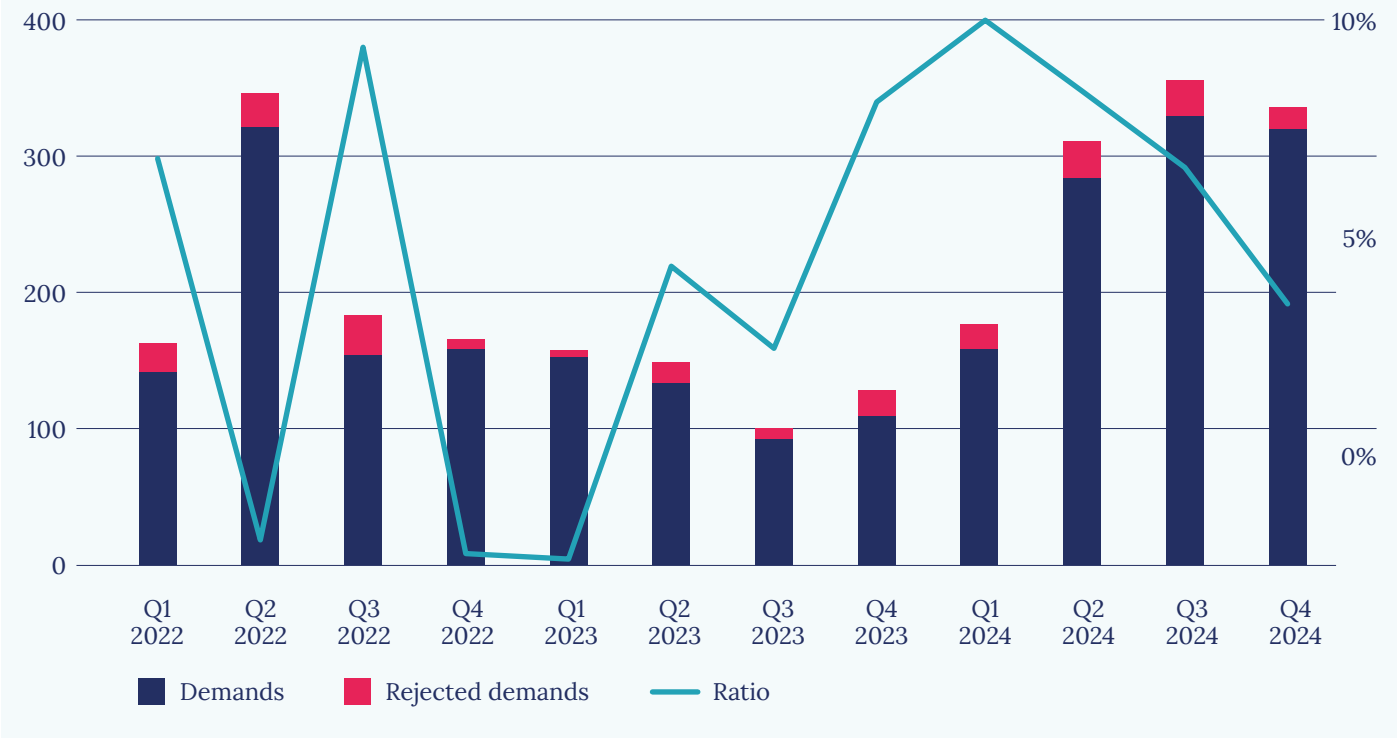
Total number of LI-taps and LI-extensions per quarter



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



Total number of demands versus rejected per quarter



NaWas

Figures 2024

NaWas Statistics 2024

1933
attacks mitigated

5.27
average number of mitigated attacks per day

353 Gbps
maximum mitigated attack size

Trends 2024

DNS Amplification attacks moved up in intensity. DNS amplification attacks moved from 5th in attack vectors at the first quarter of 2024, to being 1st for the rest of 2024.

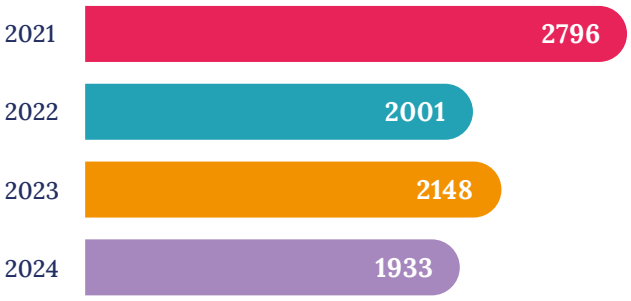
Decrease in the number of attacks towards the end of the year

NTP Amplification was a consistent top 3 attack vendor.

Top 5 attacks in 2024

1. DNS Amplification
2. NTP Amplification
3. TCP SYN Flood
4. IP low TTL Flood
5. UDP HTTP/3 QUIC Flood

Number of attacks per year



Clean Networks

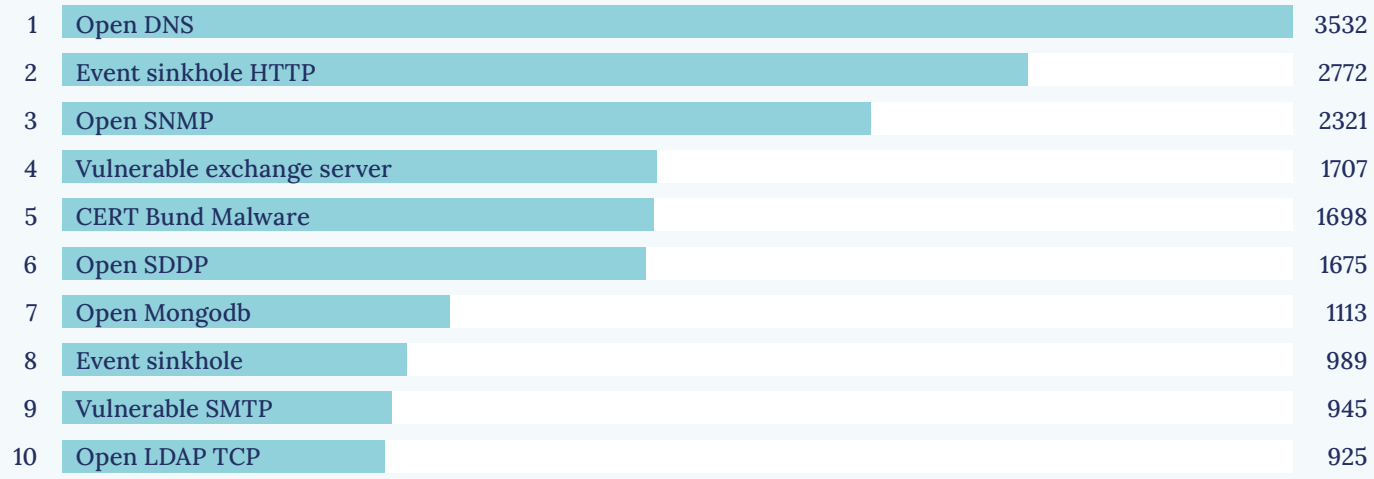
Figures 2024

Note

Through Clean Networks, NBIP disseminates information about security vulnerabilities and abuse to digital infrastructure providers. These reports are tailored to individual participants who have signed up for the Clean Networks threat intelligence feed, enabling them to take targeted action.

In 2023, we shared **21256** notifications about a total of **803764** IP addresses. In the past year, there were **8367** notifications concerning a total of **254132** IP addresses. It is important to note that in 2023, we collaborated with an external organisation, which meant that IP addresses of non-participants were also included.

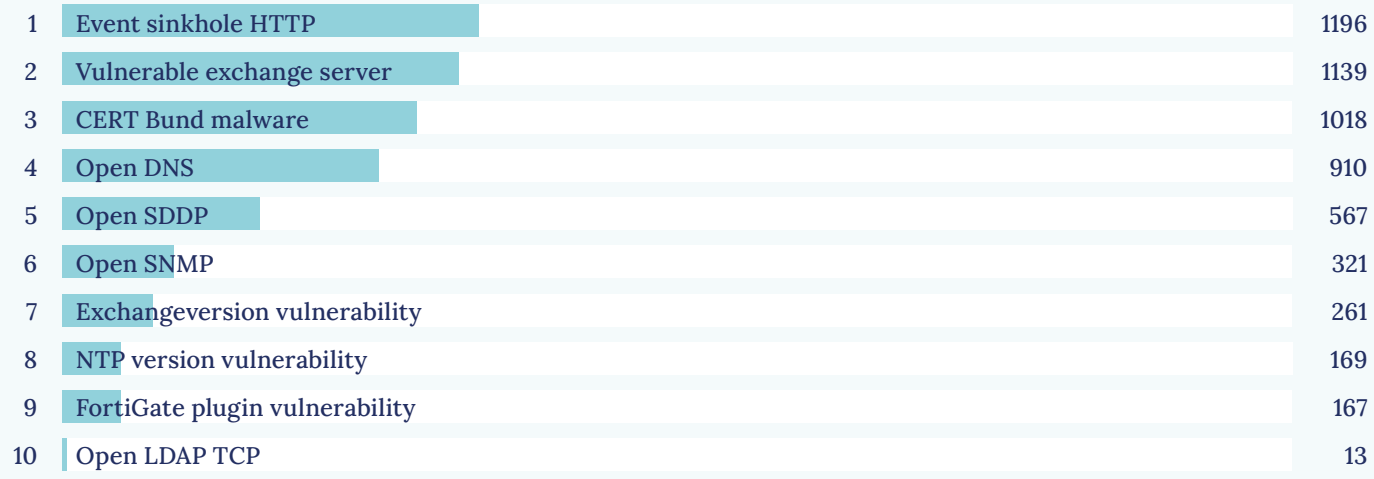
Top 10 Threat Types (measured in number of notifications) 2023



Total number of notifications (2023) — **21256**

Total number of IP addresses (2023) — **803764**

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



Total number of notifications (2024) — **8367**

Total number of IP addresses (2024) — **254132**

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 to NBIP's public affairs activities is always to bring practical challenges in complying with legislation and regulations that affect participants to the appropriate consultation tables. Because NBIP is also operationally active with its services, it can paint a clear picture of how legislation and policy ultimately have an impact in daily practice. We do this structurally in four areas.

DDoS Protection

Within the Netherlands and Europe, NBIP positions itself as the (inter)national knowledge centre for protection against DDoS attacks. Thanks to our many years of knowledge, extensive experience and the NaWas, we can be of great value to policymakers. That is why we actively share knowledge about the nature and scope of DDoS attacks, effective protective measures and the role of various parties in the digital ecosystem.

Digital resilience in digital infrastructure

Due to increasing digitisation, digital resilience has become an important issue that is higher on the agenda of many organisations. Sectoral cooperation is therefore crucial for digital resilience in the Netherlands and Europe. NBIP uses its expertise in the field of DDoS protection, abuse prevention and SOC operations to strengthen digital resilience. Joint responsibility among all parties in the value chain is key to this, with NBIP also advocating for space in the market to build innovative and practical solutions.

Abuse prevention

NBIP focuses on developing best practices and policy advice on combating abuse and bad hosting in the Netherlands and Europe. Therefore, through our insights in this domain, we aim to help policymakers develop effective measures without limiting the open and innovative nature of the Internet.

Operational compliance with laws and regulations

Over the past 25 years, NBIP has been one of the few parties in the Netherlands and Europe to build up independent expertise in the operationalisation of the enforcement of claims and orders from authorities for providers of digital infrastructure. We use this knowledge to ensure the operationalisation of these cases for digital infrastructure in the most pragmatic way possible.

Column

Cyber resilience is a collective cause

By Octavia de Weerdt

DDoS attacks are becoming an increasingly serious threat. In 2025 alone, we saw attacks that affected European Parliament elections and public services and infrastructure, shut down provincial and municipal websites, and became increasingly complex. To remain resilient, we need to take a different approach to this problem.

Arms race in a hybrid battle

DDoS attacks are part of a new normal characterised by a hybrid conflict between different geopolitical power blocs. They are now being used strategically to disrupt free, democratic societies in Europe. Not surprisingly, the intelligence agencies recently sounded the alarm about this.

This is not to say, incidentally, that recent attacks have all had this intention. This is known about some attacks; others not so much. But we do know that the motives of attackers often lie in retaliation and the disruptive effect of attacks, and that they often link these motives to developments in the geopolitical arena. With this, DDoS attacks have long since ceased to be “mischief” or “digital vandalism”, but are part of a broader, global struggle.

DDoS and the protection measures that are taken, moreover, have the dynamics of a classic arms race. Defences that are adequate today may be insufficient or obsolete tomorrow. This dynamic makes it virtually impossible to achieve 100% protection. And it is a big task to keep up to date in terms of knowledge and technology to repel these kinds of attacks.

Dependency

It stings in this respect that we in Europe have made ourselves largely dependent on non-European-made DDoS protection. Because in this area too, as for many other online services, it is only a handful of mainly US companies that control almost the entire market. If we feel that the government has made itself vulnerable by hosting sensitive data at US cloud providers, we should also ask ourselves whether we should not organise our resilience against cyber-attacks such as DDoS differently.

After all, European countries have every interest in organising their digital resilience. With their knowledge, technology, and on their soil. This is of great importance for the digital sovereignty and strategic autonomy of Europe and thus also the Netherlands.

> *"Without our own European knowledge and technology, our digital resilience remains vulnerable."*
>
> ***Octavia de Weerdt***

It is therefore obvious to seek much more cooperation, both within the Netherlands and within Europe. This is already happening in the Netherlands in the anti-DDoS coalition, in which government and critical sectors work together on their resilience against DDoS attacks. For example, a methodology has been developed there to exchange characteristics of attacks via a so-called Clearing House, as a result of which attacks can be better recognised and repelled by organisations that have access to this Clearing House.

In Europe, in addition, as part of the multi-billion programme Important Projects of Common European Interest – Cloud Infrastructure and Services (IPCEI-CIS), digital resilience (security by design) is being worked on where it matters most, namely in tomorrow's digital infrastructure at Europe's geographical borders.

But while useful and important, both examples do not solve the challenges we face today. For that, something else is needed first.

Shift in thinking

We must be realistic: as long as many organisations have to manage their resilience against DDoS attacks individually, our society will remain vulnerable. Therefore, a change in thinking is necessary. We have been stuck for too long in a mindset where individual responsibility for organisations' digital resilience dominates. The new Cyber Security Act proposes and enforces a different approach to cybersecurity, but it applies only to a limited group of organizations. Consequently, we will need to consider this issue from the perspective of collective responsibility. Commercial interests are thereby placed below the broader societal need for stability through the continuous availability of critical online services. And, importantly, it involves standing firm against those who attempt to disrupt our societies and way of life. We should not be naive about that.

By collaborating on initiatives that boost our collective resilience, we ensure that individual organizations remain afloat. We must develop, share knowledge, and organize our resilience efforts within a Dutch and European context, avoiding dependencies outside our European sphere. This is only achievable if we rethink our approach to DDoS and further organize ourselves collectively. In this way, the new normal can be seen not as a threat but as a crucial step toward a digitally sovereign and resilient Netherlands and Europe.

NBIP & Europe

There is strong momentum to strengthen Europe's strategic digital autonomy. NBIP plays a role in this as a developer and connector. In concrete terms, this means that NBIP develops solutions to increase the digital resilience of the digital infrastructure sector. In addition, NBIP participates in various European projects and partnerships and actively provides knowledge and expertise.

The challenge for Europe to strengthen its strategic digital autonomy is broad and multifaceted. There is an undesirable dependence on non-European cloud providers due to a lack of adequate European alternatives. At the same time, there are also dependencies in other areas that are undesirable and could be used as geopolitical leverage, for example in the field of security solutions, threat intelligence and information about vulnerabilities and abuse.

NBIP endorses the urgent need for Europe to have its own cloud infrastructure and is therefore participating in IPCEI-CIS, as described above. However, the need for our own, Made in Europe cybersecurity and cyber resilience solutions is just as great, as these solutions must keep our data and systems secure. In this area too, excessive dependence is undesirable.

These problems can only be solved if successful sectoral and cross-sectoral partnerships can be forged and the government provides both policy and financial resources to reduce our digital dependence on non-European parties.

In practice, this means that the EU's current commitment to multi-annual programmes to improve and expand Europe's own cyber capabilities is the most important way to create and stimulate this type of cooperation. But more is needed. On the one hand, NBIP aims to develop concrete products and services that provide participants with reliable alternatives to non-European services. On the other hand, NBIP wants to play a role in stimulating research, innovation and collaborations in the sector.

NBIP & Europe:

IPCEI-CIS / MISD

NBIP participates in the IPCEI-CIS (Important Project of Common European Interest on Cloud Infrastructure and Services) through the MISD consortium. Seven organisations participate in this consortium, each with its specialisation, with NBIP handling the cybersecurity aspect.

In short: what is MISD?

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

The role of NBIP

NBIP focuses on developing an open security platform that is integrated into the modular edge data centre. The aim is to design the next generation of European data centres to be secure by design, so that digital resilience is organised where it belongs, namely where the applications, computing power and data are located.

Over the past year, we have taken the first steps towards setting up a test bed. This test bed serves as a controlled environment where new ideas and technologies in the field of cyber security can be tested and optimised before they are rolled out. It offers participants the opportunity to put their innovative concepts into practice and evaluate how effective they are in countering cyber threats.

In addition, NBIP has initiated the development of decentralised mitigation techniques. This means that instead of relying on a centralised infrastructure, a network of distributed systems will be set up that can respond jointly to cyber attacks.

On the soapbox

In 2024, NBIP shared its knowledge with the general public in various ways. For instance, we gave several presentations at home and abroad about our services and projects. In addition, we shared the latest developments around DDoS attacks at various media outlets.

Articles, Interviews & Podcasts

Threat Talks — *DDoS Attacks on European Elections*

Data Center Dynamics (DCD) — *The Edge in Action*

ComputerWeekly — *Dutch working to promote cooperation in Europe to keep internet safe*

Angry Nerds — *Tappen as a Service*

All the Cyber Ladies

AG Connect — *Concerns about cyber attacks and vulnerable computer networks are justified, but it is better to focus on solutions.*

AG Connect - *Dutch invention for extra DDoS protection almost live*

Presentations

DKNOG14 in Kopenhagen

European Peering Forum

Beyond 125 Years 'Securing our World's Digital Future and beyond'

Women4Cyber Conference 'Beyond Borders' – *The changing DDoS-landscape in geopolitical context*

Green Data Center Conference – *Modular Integrated Sustainable Datacenter*

Retrospect: Third edition of

NBIP NEXT

For the third time, NBIP organised its annual knowledge event NBIP NEXT in 2024. The event is an excellent opportunity to share practical knowledge about all the activities that help participants get their digital resilience and compliance in order.

More than 150 visitors registered for the event at Castle De Hooge Vuursche in Baarn. Traditionally, the participants' meeting took place in the morning, during which NBIP's Board of Participants met. The afternoon programme was divided into two tracks: laws and regulations in practice (Track 1) and DDoS mitigation (Track 2, English).

The afternoon's plenary was opened by Octavia de Weerdt, general director of NBIP. During this opening, she reflected on the 10th anniversary of the NaWas, highlighting some of those people and organizations that were involved from the beginning.

The afternoon programme featured a variety of speakers, including Jair Santanna (former principal researcher at Northwave Cybersecurity) and Arda Gerkens (board chair of the ATKM). Bibi van Alphen (legal & public affairs adviser Freedom Internet) kicked off the afternoon programme with a detailed story about the court case that Freedom, among others, fought in Europe because of internet blockades that ISPs have to enforce since 2022.

Cyber Security Act (NIS2)

During NBIP NEXT the obligations imposed by the Cyber Security Act (NIS2) were also discussed, including the obligation to report incidents, the registration obligation for NIS2 entities, and the duty of care. Matthijs van Amelsfort (director National Cyber Security Centre, NCSC) and Esther Paalman of the Ministry of Economic Affairs discussed some of the obligations, but also the way of cooperation between government and industry under the new legislation.

There was also an extensive focus on the latest developments in DDoS and DDoS mitigation. This included a look back at 10 years of DDoS attacks and an insight into a number of cases that occurred within NaWas in 2024. There was also an update from the academic research on DDoS and the international approach to booters to which the National Police is contributing.

Sector cooperation crucial for cyber resilience

After the afternoon programme, visitors were briefly addressed by Matthijs van Amelsfort. The NCSC has a number of important tasks in implementing the cyber security law, including incident response and sharing threat information.

As 10,000 entities will fall under the NCSC as of the Act, including a significant amount of digital infrastructure providers in the Netherlands, the message of that cooperation between the industry, including through NBIP and the NCSC, remains crucial to make and keep the Netherlands cyber resilient.

Sign up for NBIP NEXT 2025

On Wednesday 26 November and Thursday 27 November, NBIP is organising NBIP NEXT for the fourth time. Due to the growing need for knowledge sharing on European cyber resilience, DDoS mitigation, and abuse fighting, we are now organising a two-day event. The first day will focus on laws and regulations and DDoS mitigation in cooperation with the Anti-DDoS Coalition. The second day will focus on European cooperation and strategic autonomy. This year, NBIP NEXT will also take place at Castle De Hooge Vuursche.

Don't want to miss the event?
Click here to register yourself ↗

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 NBIP NaWas, the largest non-profit DDoS mitigation service 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