



# NBIP Monitor

Renewal, insight, community & intensification



nationale  
beheersorganisatie  
internet providers

# Colophon

**Authors:**

Octavia de Weerdt, general manager, NBIP  
Wouter Pegtel, communications manager, NBIP

**Contributors:**

Ludo Baauw, Frans ter Borg,  
Frank Dupker, Kai Peters,  
Simon Kuhn, Michiel Cazemier  
All rights reserved. © 2024 NBIP

For more information, see [www.nbip.nl/en](http://www.nbip.nl/en).





# Table of contents

<b>Summary</b> .....	<b>4</b>
<b>Foreword</b> .....	<b>5</b>
<b>About NBIP</b> .....	<b>6</b>
<b>Mission and vision</b> .....	<b>7</b>
<b>Organizational structure</b> .....	<b>8</b>
<b>Organization chart</b> .....	<b>9</b>
<b>Board composition</b> .....	<b>10</b>
<b>Development services</b> .....	<b>13</b>
<b>Participant development</b> .....	<b>18</b>
<b>Tap service figures</b> .....	<b>19</b>
<b>Expected developments Tap Service</b> .....	<b>21</b>
<b>Expected developments NaWas</b> .....	<b>23</b>
<b>IPCEI-CIS participation</b> .....	<b>26</b>
<b>Knowledge center</b> .....	<b>28</b>
<b>Public affairs</b> .....	<b>29</b>

# Summary

The past two years were marked by a transition for NBIP that resulted in NBIP now running its services entirely in-house. In doing so, NBIP continues to focus on European expansion and innovation. In order to continue developing services, efforts have been made to acquire financing from European funds. Both Clean Networks and participation in a consortium within the framework of IPCEI-CIS (Important Project of Common European Interest - Cloud infrastructure and services) are European funded. Under IPCEI-CIS, NBIP will develop an open and distributed security platform.

## Participant development

In 2023, we were again able to record a steady growth in the number of participants for both Tap Service and NaWas.

In total, we were able to record 13 new participants, while 2 participants terminated their agreement in 2023. A detailed breakdown of the number of participants by service is included later in this report.

## An organization in development

Both NBIP's target group and range of services are broadening. Small and medium-sized hosting, cloud, and VoIP providers, other digital infrastructure providers, public sector organizations, and private sector service providers with a strong digital presence are finding their way to NBIP. And not only in the Netherlands, but also in Europe.

The reason is obvious: even organizations whose core mission was not originally to provide and facilitate digital services, are now so digitized that they offer their services almost exclusively digitally. Questions about availability and information security

are just as important to them as they are to digital infrastructure providers. For this reason, they also face new obligations from the legislature.

The fact that more and more organizations are finding their way to NBIP is therefore testimony to the success of NBIP's cooperative approach and its services. This is also reflected in the Tap service. Whereas NBIP has long performed this service primarily for providers with fixed networks, NBIP can now also offer its services to mobile virtual network operators (MVNOs). We also see interest in this from Europe. With the implementation of the e-Evidence regulation approaching, it is obvious that this interest will increase in the future.

In short, the foundation was laid to broaden NBIP's services and its efforts to service its traditional base. The foundation is now well-prepared for the range of upcoming legislation that imposes operational obligations on providers. Where it makes sense to organize services jointly, the feasibility and interest from the community will be explored.

## Future Vision

NBIP focuses on the further development of its services and infrastructure. In doing so focus is on development and innovation, collectively organizing digital resilience and operationally implementing compliance with (European) laws and regulations. By strengthening collaborations and sharing knowledge, NBIP wants to contribute to a safer digital Netherlands and Europe. The organization strives to maintain its position as a constructive and, where necessary, critical discussion partner for the government and other stakeholders in the field of Internet reliability, resilience and security to expand further.

# Foreword

Dear Reader,

It is a great pleasure to present to you the NBIP Monitor. This report is a bit different compared to previous annual reports we have published, as we have chosen to present a general overview of NBIP activities and its plans for the future. We will publish annual reports again starting next year. As many of you reading this report will know, the past few years mark a period of strategic and operational change for NBIP. These changes allow us to move into the future with a thriving, agile organization and services. This is necessary, because there is a lot coming at our participants. New laws and regulations and a polarized world make vigilance and resilience increasingly important.

## Eye on the future

NBIP's strength has always been in jointly organizing operational compliance with obligations arising from the law and strengthening resilience against cyber threats for participants. The starting point here is more than ever that participants stand strong together and from cooperation enable a more reliable and safe Internet for all.

This formula only seems to be becoming more relevant. Not only in the Netherlands, but also in Europe. A lot of legislation is coming our way from the EU that will lead to new operational obligations for digital infrastructure providers. NIS2 is one of the best known, but there is more in the pipeline. Data, online services and their security have become a matter of geopolitical and therefore European interest. The implications, especially at the operational level, are substantial.

It is at this interface—the translation of regulatory compliance into operational efforts—that we foresee NBIP's greatest added value in the coming years.

Where it is feasible and creates clear benefits, it makes sense to jointly organise digital resilience and operational compliance. This way we strengthen each other and account for the social impact our industry has. Both the Tap service offered by NBIP and the DDoS mitigation platform NaWas have become successful with this philosophy.

## Grip on one's own operation

One of the most profound changes in the past years was the completion of a transition that saw NBIP take full ownership of its services. This strategic decision, made several years ago to gain greater control over our core activities, has allowed us to significantly improve the operational efficiency and flexibility of our services.

This also laid the foundation for a future-proof organization. By building our own team of experienced employees and developing and strengthening knowledge internally, we now have an organization that is ready for the future. That future is more unpredictable than in the past 20 years. That is why it is good to seek each other out and face common challenges together. NBIP not only takes this in hand with its services, but increasingly also with knowledge sharing and other forms of support.

As general director of NBIP, I am proud of the achievements of our team and the support of our participants. I invite you to read further about the developments within NBIP and look ahead to the (near) future.



Enjoy reading!

**Octavia de Weerd**  
**General Director**  
**NBIP Foundation**



# About NBIP

**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, this so-called Tap 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 Tap 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 Tap 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

Internet abuse, industry-wide agreements that commit providers to the 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 evolution of NBIP over the years has also led to a broadening of its mission. Everything NBIP does is based on the belief that the Internet sector is stronger together for a cleaner, safer Internet of which everyone benefits.

Everything NBIP does is based on the belief that the Internet sector is stronger together for a cleaner and safer Internet.

# Mission and vision

**NBIP provides providers of digital infrastructure and digital services with facilities that are indispensable due to availability or legal requirements. These facilities are not always necessary and costly to acquire, operate and maintain. Therefore, it makes sense to jointly operate such services.**

By joining forces, knowledge and resources, participants collectively organize their digital resilience and operational compliance with laws and regulations. Thanks to this joint approach, both large and small providers have their affairs in order in an accessible and cost-effective manner.

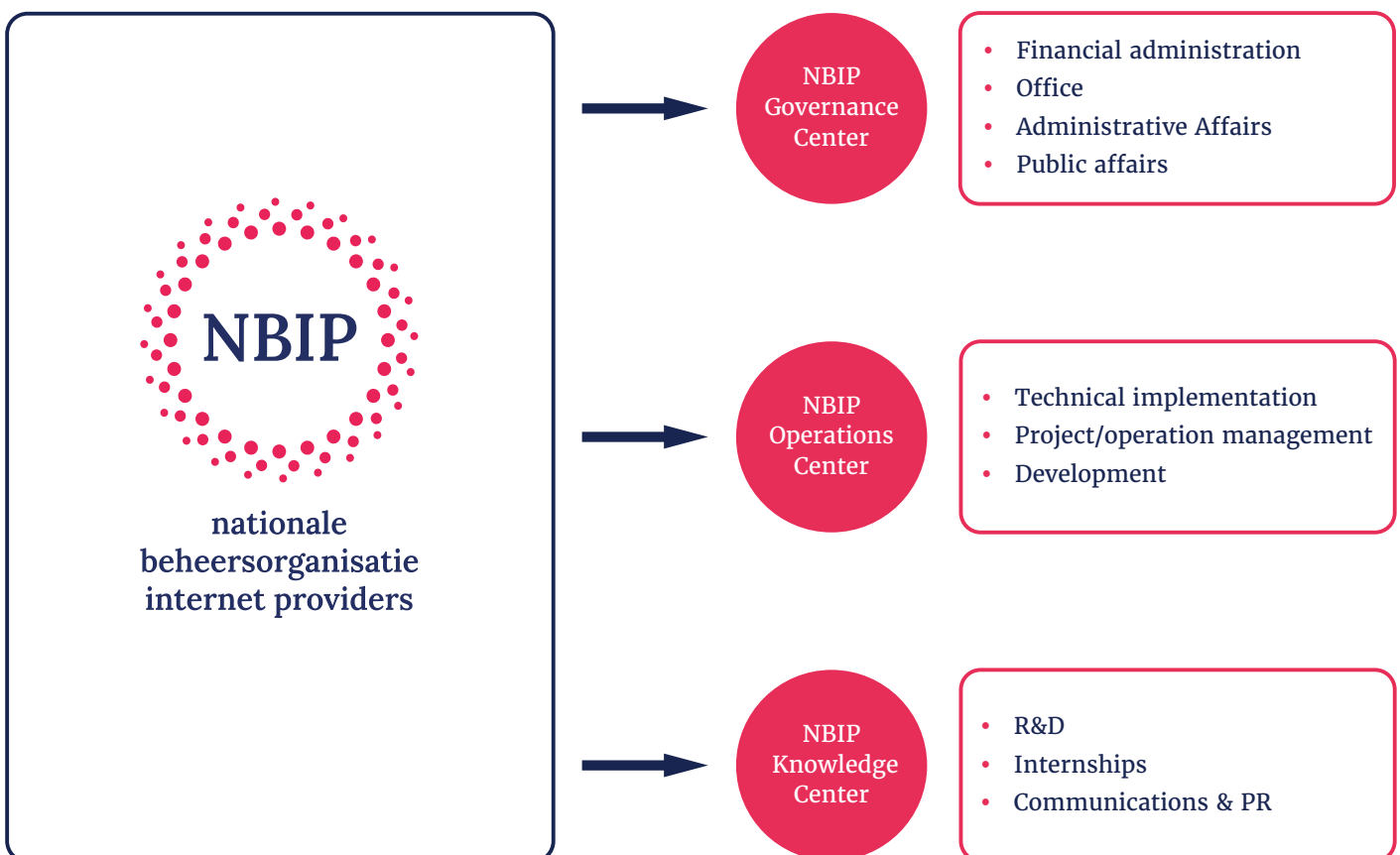
The principle that cooperation helps to be stronger for a safer Internet is also at the basis of NBIP's non-profit set-up. NBIP provides professional services based on the idea that a secure Internet is a shared responsibility, and therefore operates on a non-profit basis to achieve this goal. Our mission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



# Organizational structure

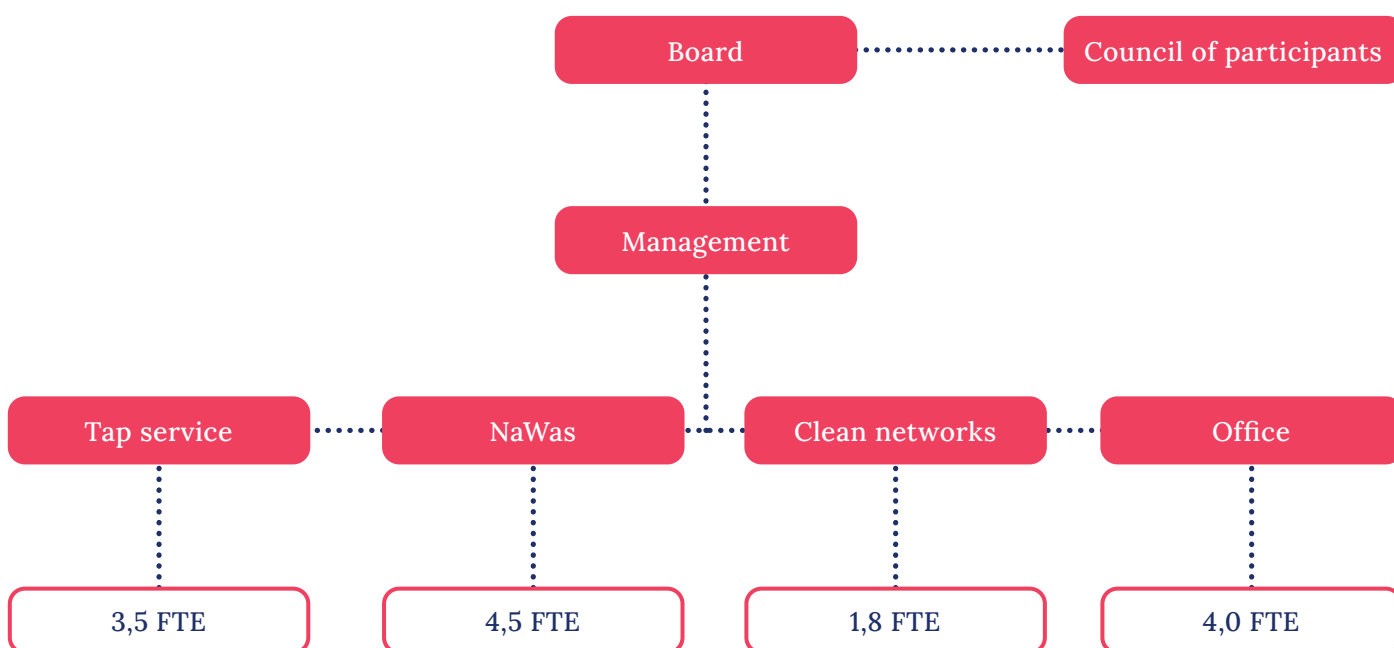
NBIP's services are delivered from an Operations Center, from which work is done daily to ensure the continuity of services to participants. The NBIP Governance Center, provides support services for NaWas, Tap Services and Clean Networks, including financial administration, administrative tasks and governance support.

The NBIP knowledge center's responsibilities include development of both knowledge, technology and partnerships. Externally, the knowledge center aims to inform both participants and the broader Internet community as well as government, media and the broader public about domains in which NBIP is active. These include technical information about DDoS mitigation, but also low-threshold explanations of how a DDoS attack works, or, for example, how to deal with bad hosters.





# Organization chart



**NBIP's board is composed of board members, each of whom comes from an individual participant of NBIP. The board is responsible for policy formation, financial control and accountability, prudent handling of the foundation and the interests of participants united in it.**

The Board is appointed by the Board of Participants, on which all NBIP participants have representation. They may, through the chairman of the Board of Participants critically question the board and provide solicited and unsolicited advice. The chairman of the Board of Participants has access to minutes of board meetings and one of the most important tasks is to put items on the agenda of the board on behalf of participants. By statute, the Board of Participants is the highest body within NBIP.

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

The general manager manages four operational departments: Tap Service, NaWas, Clean Networks and the Office, which houses support functions such as financial administration, project administration and management, communications & PR and public affairs. Each of these departments has at least one senior employee who leads the department independently but in close consultation with management as a cooperating foreman.

# Board composition



**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 can well understand 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.



# On behalf of the board

## Ludo Baauw

### Chairman of the Board


**Ludo Baauw is chairman of the board of NBIP and CEO of Intermax Group, which at the time this report went to press includes eight IT companies. He and the other board members ensure that NBIP stays on track in its linking function between ISPs, hosting providers, telecom companies and other providers of digital infrastructure and services.**

### What were the most important issues for the NBIP board in the past period?

“There were several important themes on the agenda. One of the main developments was the intensification of contact with participants. This manifested itself, among other things, in the search for a new chairman for the Council of Participants, which resulted in the appointment of Frans ter Borg.

In addition, the focus was on further professionalization of the organization. Concrete examples were the preparation for and start of two important projects, respectively: MISD (Modular Intergrated Sustainable Datacenter) under the banner of IPCEI-CIS and Clean Networks. The IPCEI CIS project aims to increase European autonomy and sovereignty in data and cloud infrastructure and services. MISD contributes to this by developing a concept and field lab for modern, efficient modular data centers for a distributed cloud infrastructure. In doing so, NBIP is building on its experience with the DDoS scrubbing center and exploring opportunities to develop secure-by-design open source solutions as an alternative to commercial equipment.

The Clean Networks program responds to increasing government demands on service providers, ISPs and telecom companies. Its goal is to remove vulnerabilities and abuse from networks as quickly as possible. We can play a crucial role



in this as NBIP. These projects illustrate NBIP's core philosophy: “Alone you go faster, but together you go further. They enable the organization to undertake initiatives that would not be feasible for individual participants.

And of course we implemented and further developed our tap services. Our more than 100 participants have all ‘outsourced’ their obligations under the Telecommunications Act to NBIP, and every day there is a dedicated crew of people working here who go out with ‘tap boxes’ where necessary to carry out the obligation on behalf of the participants securely, with the highest form of confidentiality, at the request of the police, judiciary or intelligence services.”

### NBIP took full control of its operations, retiring most third party dependencies. Why was this chosen and what did it achieve?

“After working intensively with external suppliers for more than 20 years, we made the strategic choice to start providing services completely independently. This choice was primarily driven by the significant growth of the organization and the increasing importance of our operations. We thus have more control over our operations and are less dependent on third parties. This is crucial, given the public relevance of our work. Moreover, the organization has now reached a scale where it is more cost-effective to perform certain activities internally.

This change has brought several benefits to the participants. First, there is now a more intense and direct contact between the participants and the NBIP office, making it possible to respond more quickly to the needs of the participants. In addition, we can now develop new features more flexibly and quickly because we have our own people with the

necessary expertise. Ultimately, it has helped to ensure that, despite increasing costs and inflation in the outside world, we have managed to keep rates for participants virtually the same.”

#### **What is the board’s vision for the coming years?**

“As a board, we have an ambitious vision for the future. A key focus is to leverage and share knowledge and expertise. We aim to replace equipment that is currently purchased commercially with open source alternatives. This is part of the effort to increase digital sovereignty for the Netherlands and Europe.

We also want to further develop as NBIP as a valued interlocutor for the government in the field of Internet security, with an emphasis on a joint, European approach rather than dependence on non-European parties. For example, NBIP’s unique model as a non-profit, community-based DDoS scrubbing center is gaining increasing interest from Europe. We want to build on and expand that position. The growth in the number of international participants underlines the relevance of this model. In the long term, we see opportunities for the development of a quality stamp or seal of approval. This could further enhance the value of NBIP participation for ISPs and telecom companies in their interactions with government and other stakeholders.”

#### **What makes the Internet sector as a community so strong and the work for NBIP so rewarding?**

“The strength of the Internet sector as a community lies in its collaborative approach to challenges that are too complex or costly for individual parties to address would be to take on alone. The NBIP acts as a connecting factor that provides the knowledge, resources and interests of its participants. This collaboration enables even smaller players in the market to comply with

increasingly stringent laws and regulations and to take advantage of advanced services such as the DDoS scrubbing service.

In this, we play an important role as a translator between government and industry, providing practical solutions to often complex requirements. Working for NBIP is particularly rewarding because it makes a tangible difference. Acting together gives the industry a strong voice towards government and other stakeholders. This enables us to represent the interests of our participants effectively and thus contribute to a safer and more stable Internet.”

#### **What are you proud of?**

“There are several aspects of NBIP’s work of which I am proud. First and foremost is the successful transition to an organization that fully self-manages and develops its services. Despite the complexity of this change, service delivery to our participants has continued uninterrupted. This is a great compliment to the entire team, led by Octavia de Weerd.

In addition, I am proud of our position as the first and largest non-profit DDoS scrubbing service in the world. This unique model attracts worldwide attention and demonstrates that a cooperative approach can be very effective in the Internet sector. But also our ability to attract top talent, even in a tight labor market, says something about our organization. The fact that experienced professionals choose NBIP because of our social impact underscores the relevance of our work.

Finally, I am proud of the strong community we have built. NBIP embodies the Dutch tradition of collaboration, similar to cooperatives in other sectors. This sense of community enables us to tackle big challenges and make a meaningful contribution to a safer and more reliable Internet for all.”



# Recent developments

## Tap service

**NBIP offers its participants comprehensive Internet security and legal compliance support. Through advanced technology and years of expertise, NBIP provides reliable tap services, state-of-the art DDoS mitigation and thorough threat intelligence analysis.**

### Overview of Tap Services

NBIP acts as a one-stop shop for participants in taking warrants intended for affiliated participants. In practice, this means that justice, police and intelligence agencies contact NBIP when they have a warrant for a participant in the Tap Service. NBIP then takes care of the technical, legal and administrative aspects of these requests. When an investigative agency issues a warrant, NBIP assesses its legality and handles the implementation of the tap. This process includes both the placement of tap systems and the management of the interception during the duration of the tap. This also applies to requests around the provision of data of various kinds. All this is done with strict compliance with the legislation and under strict security measures to ensure the confidentiality and integrity of the data.

NBIP offers its participants comprehensive support on Internet security and legal compliance.

### Notable developments

#### 1. Increase in connections and coverage:

NBIP continued to expand its tap services, with now more than 100 participants, including new ISPs and VoIP providers. This growth has been driven in part by tightened legislation and stricter controls by the National Digital Infrastructure Inspectorate (RDI), leading to increased demand for compliance solutions.

#### 2. Technical infrastructure and innovation:

A major milestone was the completion of bringing all core activities in-house. This included the redesign of the technical infrastructure and processes, so NBIP now has a dedicated taproom. This taproom is equipped with modern security systems and is 24/7 operational, which has significantly improved the response time and reliability of tap services.

#### 3. European cooperation and legislation:

NBIP has also been allowed to bring its expertise gained from the tap service to the European level. With the expected implementation of the new European e-Evidence legislation, which will allow the investigative services from other EU countries to request data directly from Dutch providers and vice versa, NBIP has played an active role in European Commission working groups to provide (technical) input.

#### 4. Expansion of services and education:

In addition to traditional tap services, NBIP worked to expand its portfolio of services, including the handling of various judicial claims and the link with the Central Telecommunications Research Information Point (CIOT). This expansion ensures that participants are fully compliant with all legal requirements and offers them an integrated solution for their obligations towards investigative agencies.

# NaWas

The National Washing service against DDoS attacks

**NBIP made significant strides with its NaWas service, a crucial part of their service portfolio aimed at protecting networks from Distributed Denial of Service (DDoS) attacks. This service provides an advanced solution to the growing threat of DDoS attacks, which can severely disrupt the availability and reliability of Internet services.**

## Overview of the NaWas DDoS scrubbing center

NaWas is designed to redirect Internet traffic affected by DDoS attacks to a secure environment where harmful traffic is filtered and only clean traffic is returned to its original destination. This not only protects providers' services but also those of their customers, ensuring continuity of service.

## Notable developments

### 1. Expansion and redundancy:

One of the key milestones was the physical expansion of the NaWas infrastructure to Copenhagen. This expansion increases redundancy and provides more robust protection against DDoS attacks by leveraging multiple geographic locations. The choice of Copenhagen was strategic because of its strong connectivity and the presence of an active Internet community that demands local DDoS protection.

### 2. Technical developments:

NBIP invested in upgrading its technical infrastructure, including replacing outdated equipment with modern systems. One example is the replacement of the DDoS detection solution that NaWas deploys, which was

initiated in 2023. How to optimize NaWas' connectivity has also been explored. These upgrades improve the capabilities and efficiency of the NaWas, enabling faster and more effective mitigation of DDoS attacks. Improvements have also been made in load balancing and data sharing between different locations, further strengthening the resilience of the network.

### 3. European projects and collaborations:

NBIP has actively participated in applying for funding under European R&D projects aimed at, among other things, building secure, distributed edge cloud infrastructure in Europe. NBIP's focus here includes the development of edge cybersecurity solutions. This project, supported by European funding, will remain a major focus in the coming years. The goal is to create an open platform for DDoS detection and mitigation, for example, that can be used not only by NBIP, but by multiple European entities. This will promote the digital autonomy and reduce dependence on commercial, non-European providers.

### 4. Growth in participants:

The number of participants in the NaWas service has continued to grow by 2023, with now more than 130 affiliates. This growth is expected to continue in the coming years, in part due to the implementation of NIS2 and other legislation establishing requirements for the demonstrability of measures for availability of digital services and to limit the economic and social damage if these types of services are disrupted. The upgrades and expansions mentioned above also aim to create sufficient capacity ready for this growth.



# Clean Networks

**Clean Networks is an initiative that helps Internet, hosting and cloud providers keep their networks clean of so-called abuse. This reduces the abuse of security vulnerabilities so that cybercriminals have less opportunity to carry out their illicit activities.**

## Overview Clean Networks

Much abuse takes place in systems of Internet and hosting providers because they have large networks with often thousands of servers, where it is difficult to keep a good eye on the vulnerabilities that occur (with customers). In addition, there is a group of providers for whom this type of abuse is a blind spot. They are unconsciously incompetent.

Clean Networks therefore focuses on two aspects. On the one hand, it consists of an industry-wide code of conduct that providers sign. This commits them, among other things, to taking measures to detect abuse in their networks and fix security vulnerabilities. They also commit to a notice & takedown procedure, “know your customer” policy and good accessibility for abuse reports. Code of Conduct signatories differ positively from

similar parties that have not signed the code, by demonstrating that they detect and remove abuse from their networks. To make this distinction clear, they receive a certificate and eventually a seal of approval.

The second aspect of Clean Networks is technical in nature. The Clean Networks platform provides participants with automated notifications of vulnerabilities in their networks. In many cases, it offers perspectives to resolve these vulnerabilities. The platform thereby bundles threat information from various sources such as Shadowserver and CERT-Bund.

## Notable developments

Clean Networks continued to be developed in 2023 and 2024 after a successful launch in 2022. Efforts included improving the user experience and adding and automating notifications from additional sources. By the end of 2023, the platform provided information to participants from 25 sources. Looking ahead, Clean Networks aims to increase the number of signatories to the code of conduct significantly, as this is the only way to ensure the goal of a cleaner Internet is achieved. To this end, an intensive campaign will be launched to increase awareness and willingness to join Clean Networks.



# Interview Kai Peters

**Engineer NBIP**

Kai Peters is an Engineer at NBIP, specializing in technical aspects of the tap environment. With a broad background in ICT, ranging from help desk to system administration, his expertise contributes to the efficient and safe execution of complex technical projects of NBIP.

**What are you working on within NBIP?**

“I work on the technical part of the tap environment within NBIP. A major project we are working on is the move to a new system for live interception. We have built a completely new environment alongside the old one with the latest versions of the LI system, a different OS and new security features. In the new system, tap services can be fully automated even further through a message broker, making a lot of manual work a thing of the past. In addition, this increases efficiency and improves security.”

**What do participants notice about this?**

“Most participants will notice little of the transition to the new system because it is designed to run side-by-side. We will be running the same servers during the migration, but with different software that participants will not otherwise notice. The new system works more efficiently and securely. It ensures that data is processed faster and more reliably, which improves overall service.”

**What are the biggest challenges in tap service?**

“The biggest challenges in tap service revolve around the complicated, different networks and data security. Each participant has a unique network with different structures, making it difficult to find a good location to set up and run taps.”

*The new system works more efficiently and securely. It ensures that data is processed faster and more reliably, improving overall service.*



### How do you ensure data security during taps?

“The security of our tapping service is guaranteed in several ways. All data that is tapped is first encrypted before it is transmitted so that only authorized persons can access it. This keeps the data protected from unwanted access. In addition, there are strict access controls, and only a small number of people have access to the system. These people have signed a Certificate of Good Conduct (VOG) and a confidentiality contract. Even among themselves on the floor here, there is no substantive discussion of the taps. Moreover, nothing is stored on the hard drives of the systems at the participants. Once a system is shut down, all data that could refer to a tap disappears. Each data stream and target is encrypted with a unique key, so the data streams do not get mixed up.”

### What future developments can we expect for the tap service?

“One of the most important changes is the virtualization of tap servers. This means that the physical servers that are now at the participants’ premises can be replaced by virtual machines. This not only saves space and money, but also makes the system more flexible and easier to maintain.

### What are you most proud of in your work?

“I am most proud of how quickly I have been able to develop since working at NBIP. In a short period of time, I have significantly increased my knowledge of lawful interception and lawful disclosure, and the architecture of systems for these be able to delve deeper. Also, the fact that we overcame several technical challenges during the migration to the new system without any impact makes me proud.”

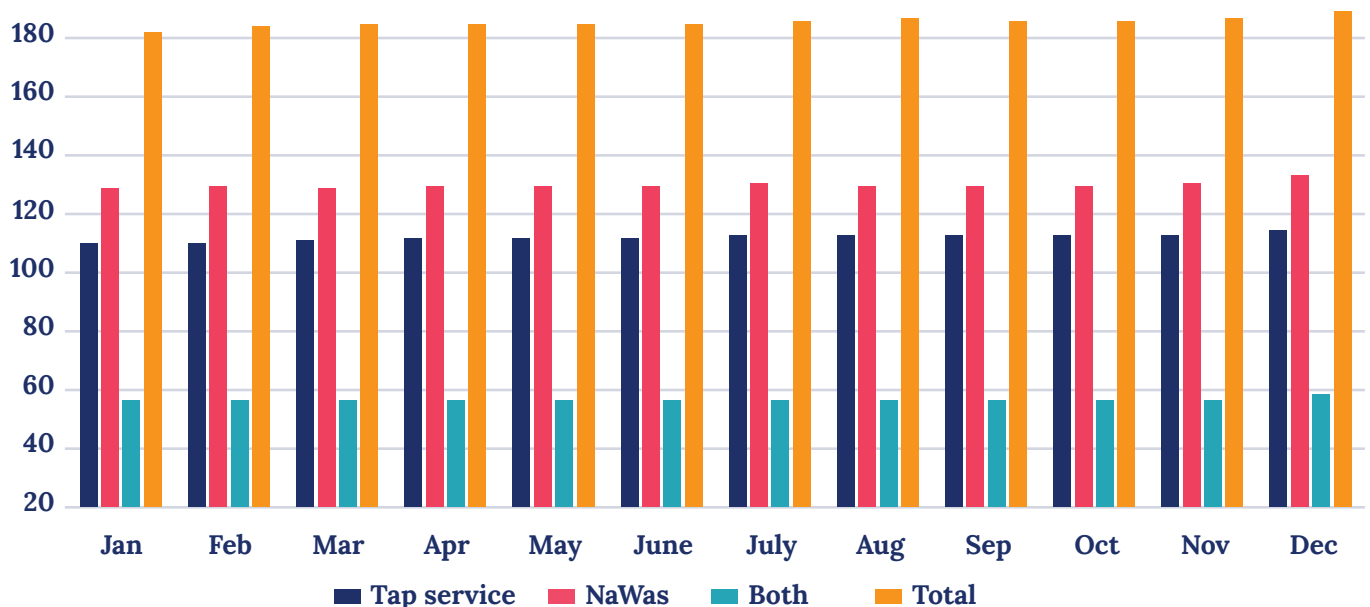


# Participant development

The number of NBIP participants continued to grow in 2023. The number of tap service participants grew by five, while the number of NaWas participants grew by nine. One participant cancelled participation to the Tap Service. Overall, the number of participants in the services grew by thirteen. Organizations that benefited from both the Tap

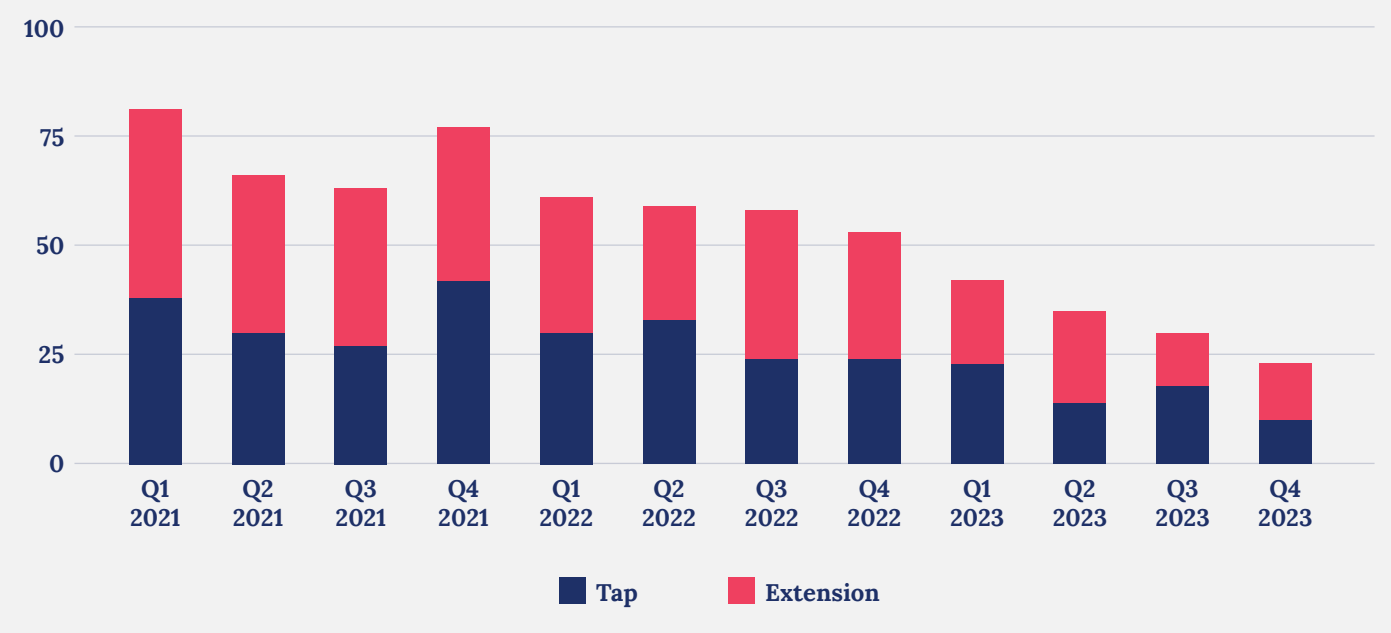
Service and the NaWas use, are counted as a single participant in NBIP's total number of participants. Viewed this way, at the end of December 2023, NBIP had 190 participants, of which 104 organizations participate in the Tap service and 129 organizations participate in the NaWas. There are 43 organizations participating in both services.

	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
<b>Tap service</b>	101	101	102	103 (+1)	103	103	104 (+1)	104	104	104	104	106 (+2)
<b>NaWas</b>	122	123 (+1)	123	123	123	123	124 (+1)	123 (-1)	123	123	124 (+1)	127 (+3)
<b>Both</b>	41	41	41	41	41	41	41	41	41	41	41	43 (+2)
<b>Total</b>	182	184	185 (+1)	185	185	185	186	187	186 (-1)	186	187	190 (+3)

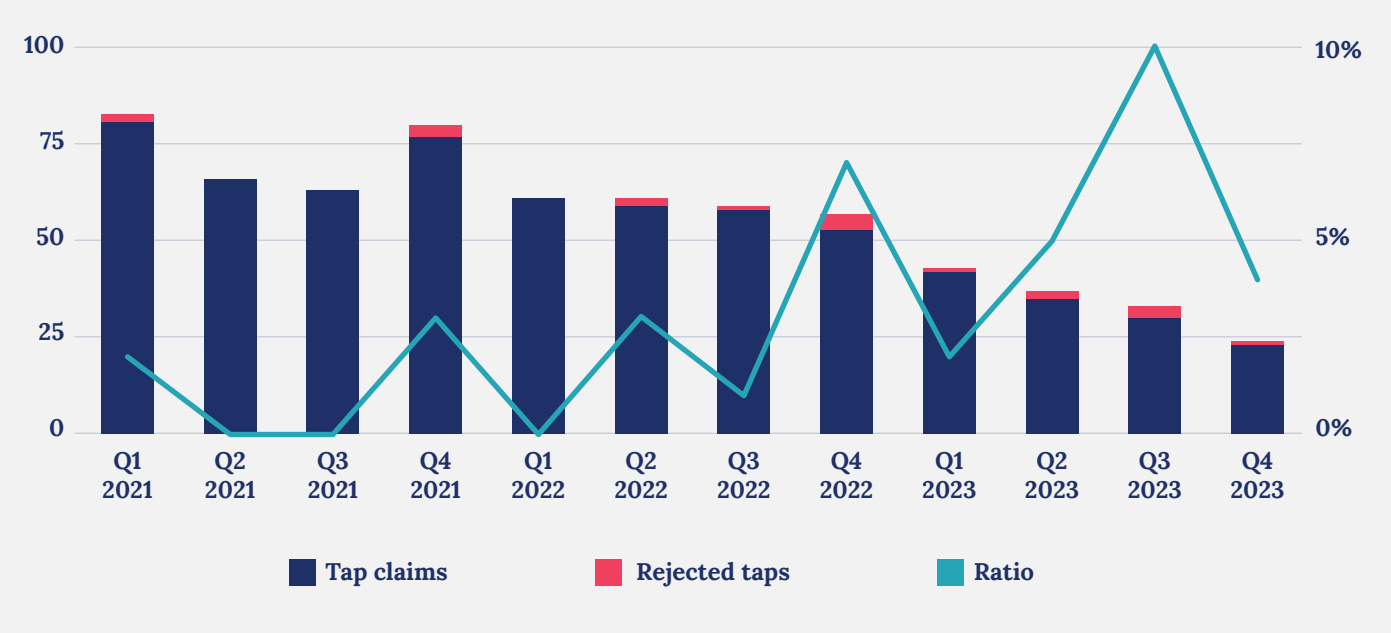


# Tap service figures

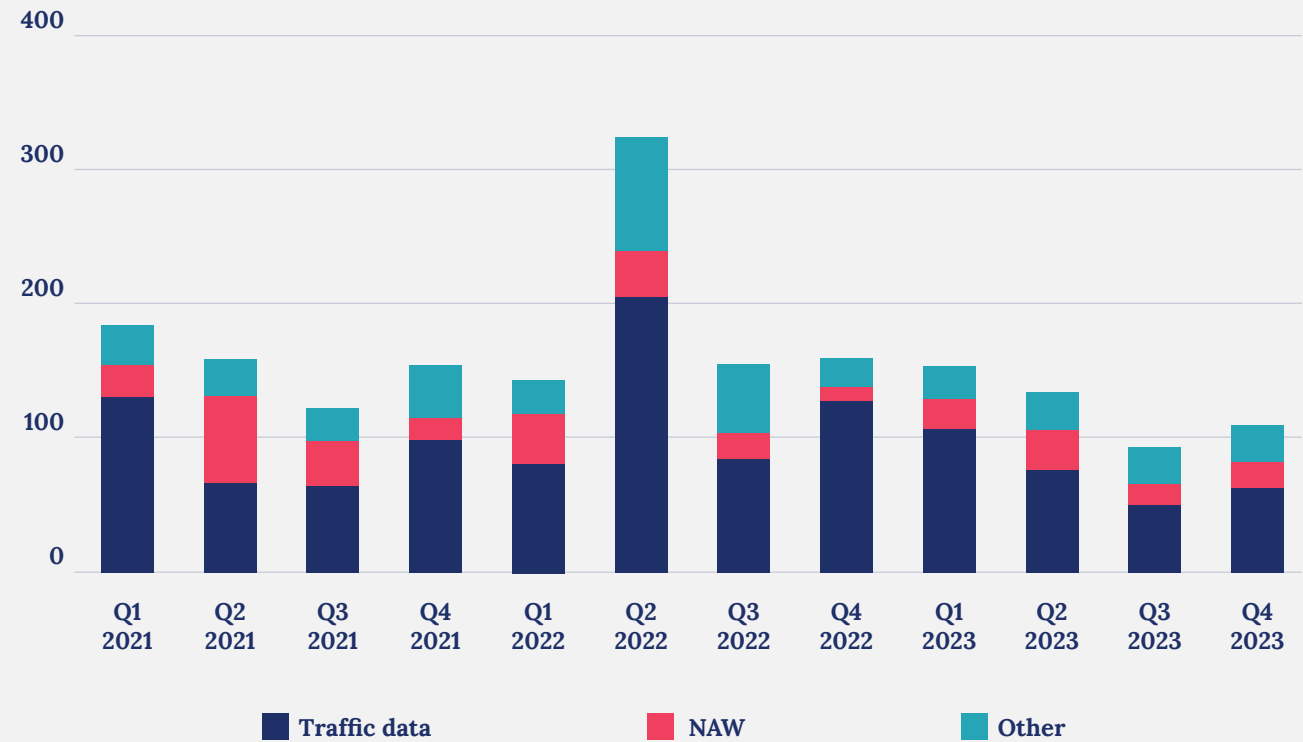
Taps and renewals per quarter



Tap claims versus dismissed



Other by quarter



Claims versus rejected





# NaWas figures 2023

Below you will find NaWas DDoS statistics for 2023.  
The 2024 statistics will be made available in the 2024 Annual Report.

2023	Quarter 1	Quarter 2	Quarter 3	Quarter 4
< 1 Gbps	205	146	140	212
1 - 10 Gbps	410	213	300	376
10 - 20 Gbps	26	26	35	43
20 - 40 Gbps	20	13	15	28
> 40 Gbps	15	10	15	19

2023	Quarter 1	Quarter 2	Quarter 3	Quarter 4
< 15 min	337	200	293	361
15-60 min	242	121	124	204
1-4 hours	71	51	49	78
> 4 hours	26	36	39	35

# Expected developments tap service

**In the coming years, NBIP's focus is on a transformation and expansion of the tap service, with innovation and European regulations are central. The term "Tap Service 2.0" symbolizes this evolution, which is no longer just about executing (tap) claims, but a broader service that responds to growing and changing regulatory and legislative demands.**

One of the core components of this transformation is the development of a more comprehensive counter. This counter can serve as a central point where warrants from authorities come in and are reviewed before being executed. This counter will be expanded to efficiently handle multiple queries coming from different organizations with varying mandates. This expansion aligns with the requirements of the Dutch online Terrorist material and CSAM Authority (ATKM) and e-evidence legislation, among others. This will allow NBIP to better support its participants in meeting new obligations arising from laws and regulations.

The e-evidence regulation and associated directive harmonize the process for digital search requests. This means that NBIP must provide an infrastructure ready to handle a large number of queries, not only from national, but also from international, European authorities. The challenge here is to create an approachable and efficient system that directly meets the needs of providers such as Internet service providers. The commitment to a decentralized system should ensure that these queries can be processed more quickly and easily, leading to increased efficiency and better compliance.

In addition to the practical implementation of new regulations, NBIP is also focused on strengthening its infrastructure and services. This includes developing new technologies and adapting to developments such as 5G and 6G, which bring new challenges and opportunities.

# Expected developments NaWas

**NaWas will continue to be developed as a Dutch service in Europe, with ongoing improvements to its architecture and infrastructure. Using the recent expansion to Copenhagen as an example, NBIP focuses on strengthening and broadening its services in the area of DDoS mitigation and network resilience. This vision is based on three main pillars: digital sovereignty and autonomy, “Made in Europe,” and a distributed, open platform.**

Digital sovereignty and autonomy emphasize the importance of European independence in technology and cybersecurity. Outsourcing knowledge, technology and applications to parties outside the EU, increasingly constitutes a security and continuity risk. This is, of course, inseparable from the geopolitical landscape, which has changed rapidly in recent years. Europe-wide, a movement toward digital sovereignty and autonomy is underway in parallel with similar movements in other areas such as energy. A multipolar world is emerging in which both economic and technological choices and developments are directly related to the geopolitical balance of power.

In practice, for NBIP this means that the commitment to a reliable and clean Internet has the implication that further development of the NaWas takes place in a European context. The first steps in that regard were taken several years ago. In this context, NBIP aims to position NaWas as a robust component of European cyber resilience. By participating in European projects and partnerships, NBIP aims to contribute to a more secure and self-sufficient digital Europe.

The concept of Made in Europe plays a leading role here. The NBIP strives to develop technologies and solutions that are manufactured in Europe and comply with European standards and values. This means that the NaWas must not only be technologically advanced, but also in line with the legal and ethical standards in place in Europe. By using open source technologies and working with European partners, NBIP aims to ensure that NaWas is not only effective, but also transparent and reliable.

A distributed, open platform is the third pillar of the future vision for NaWas. This entails spreading the NaWas infrastructure across multiple locations in Europe, which increases the robustness and resilience. By using a distributed network, NaWas can better respond to attacks and disruptions, providing a higher level of protection to participants. In addition, an open platform allows for greater collaboration and knowledge sharing, leading to continuous improvement and innovation within the service.

Another important aspect of the future vision is to strengthen cooperation with small Internet service providers and hosting companies in Europe. By supporting them in complying with increasingly stringent European regulations, NBIP wants to ensure that they too have access to the resources and knowledge needed to ensure cyber resilience. This means that NaWas is not only a service for large players, but also a reliable and affordable option for smaller companies that often have limited resources to protect themselves.



# Interview Simon Kuhn

## Head of Engineering

Simon Kuhn is Head of Engineering at NBIP. He started at NBIP late last year and has a broadly defined role that includes both operational tasks as strategic planning and systems architecture. His team consists of five engineers, including himself, who work to modernize and improve infrastructure and services of NBIP. Prior to joining NBIP, Simon worked at Amazon Web Services and Vodacom (South Africa) in various roles, among others.

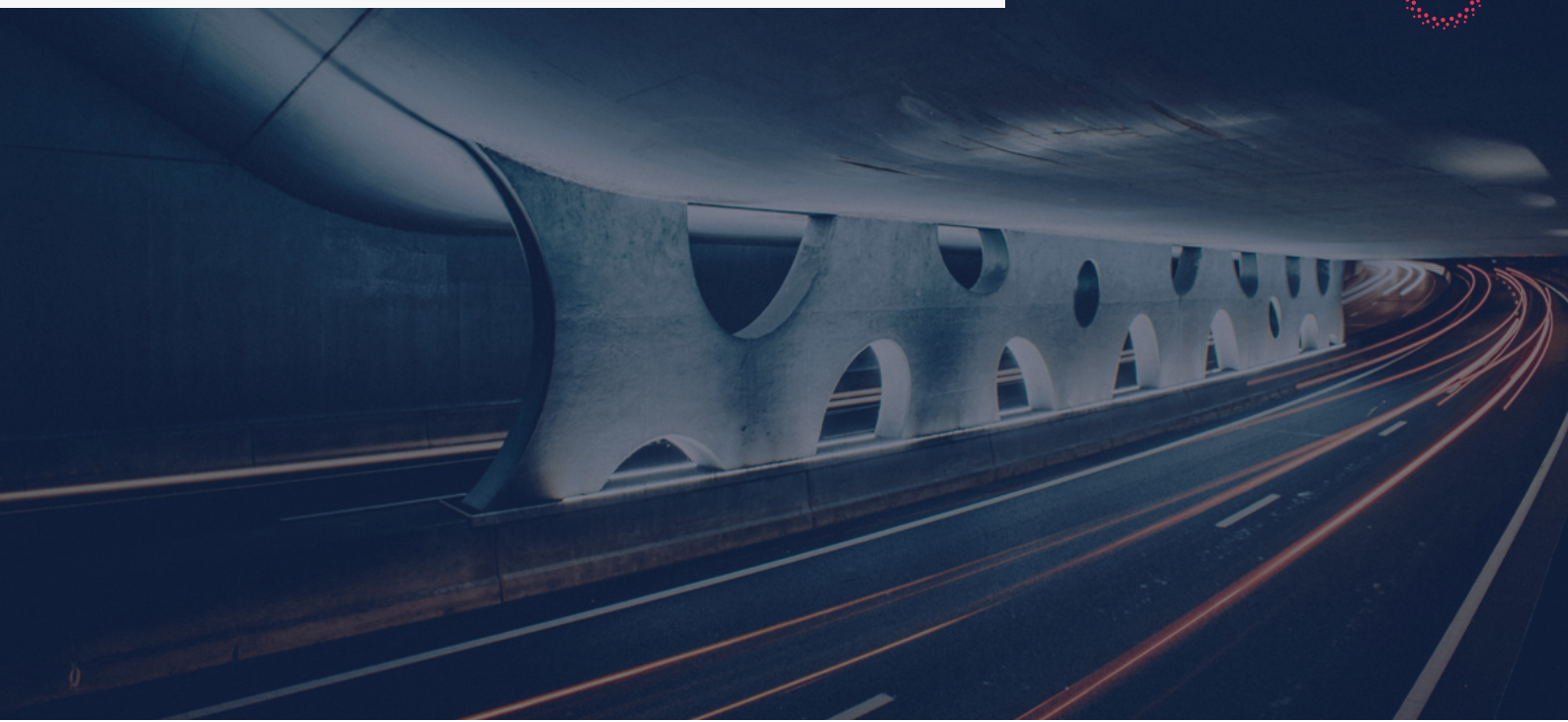
**Can you talk a little more about the modernization of the NaWas architecture?**

“When I joined NaWas, we had a very functional service, but we wanted to make some innovations to it. We then focused on major renewal, including the equipment itself, to provide greater flexibility, visibility and resilience. We made a significant change in architecture that, while not immediately noticeable to our participants, allows us to introduce new opportunities. For example, we are looking at /32-host protection, which is currently beyond our architectural capabilities. This modernization helps keep NaWas in line with the needs of our participants. It also allows us to keep up with recent developments in mitigation.”

**What exactly does this /32 host protection entail?**

“/32 host protection allows participants to single out specific hosts for mitigation, while allowing the rest of the network traffic within that subnet to continue unaffected and uninspected. This is a solution to what we call the “noisy neighbor” scenario. Right now, when participants send their network traffic to us, the entire network goes through our mitigation, which can affect services that were not actually the target of the attack. With /32 host protection, we can apply very aggressive mitigations to the specific IPs under attack without worrying about these policies affecting other legitimate traffic. This not

*We have made a fundamental change in the architecture that allows us to introduce new capabilities.*



only improves the experience of participants, but ensures also for more efficient use of bandwidth in our mitigation environments and reduces the load on our support infrastructure.”

#### **What are NaWas’ ambitions in terms of European expansion?**

We have traditionally been a single point-of-presence (PoP) service with our Amsterdam PoP, which admittedly now has two locations for data center redundancy. We expanded this with a PoP in Denmark, which we linked to Amsterdam. This multi-PoP infrastructure provides interesting opportunities for us. As soon as we are ready for that, we will certainly look at whether we can take the Danish PoP and replicate it at different locations in Europe. The advantage of these edge locations is lower latency for clean traffic, especially when the source and destination are in the same region. This expansion will allow us to provide better service through the actual mitigation closer to our participants, benefiting latency-sensitive applications such as voice or gaming.”

#### **What does the IPCEI-CIS program entail and what role does NBIP play in it?**

“The IPCEI-CIS (Important Project of Common European Interest on Cloud Infrastructure and Services) is the first IPCEI in the field of cloud and edge computing. IPCEI is a European initiative aimed at promoting innovation and collaboration to strengthen strategic chains and increase Europe’s technological sovereignty. This particular project is about developing Europe’s first interoperable and openly accessible data processing ecosystem, the multi-provider continuum from cloud to edge. As you can imagine, cybersecurity is of great importance in this. NBIP is involved in the cybersecurity aspect based on security by design. Our role is to ensure that security is built into all R&D projects from the beginning and not seen as an add-on. As a nonprofit organization with a mission to make the Internet more secure, NBIP is well positioned to contribute to this project aimed at developing technology that the market alone would not pursue because of cost.”

# Security by design: participation in IPCEI-CIS

**NBIP is a participant in the Modular integrated sustainable data center (MISD) consortium working on a field lab for a modular edge data center for a European cloud infrastructure.**

NBIP participates in the IPCEI-CIS (Important Project of Common European Interest on Cloud Infrastructure and Services) through the MISD consortium. Seven organizations participate in this consortium, each with its own specialization, with NBIP accounting for cybersecurity.

The goal of MISD 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 realized within the project come together in a validated, distributed setup in a field lab. The run time of the project is 5 years, from 2024 to 2029.

## **Role NBIP**


NBIP is focused on developing an open security platform integrated into the modular edge data center being developed within the project. The intention is to design the next generation of European data centers secure by design, so that resilience is organized where it belongs, namely where the applications, computing power and data reside.

A key objective for NBIP's involvement in the IPCEI-CIS is to create a testbed. This testbed serves as a controlled environment where new ideas and technologies can be in cybersecurity can be tested and optimized before they are rolled out. It allows participants to put their innovative concepts into practice and evaluate how effective they are in countering cyber threats. This process of testing and validation is essential to ensure that the final products and services meet the high standards prevailing in Europe.

A guiding principle in this process is “security-by-design,” which means integrating security into the design and development of systems and technologies from the beginning. By implementing security-by-design, security is not treated as an afterthought, but as a fundamental part of the product, resulting in more robust and better protected solutions.

Within the IPCEI-CIS, NBIP is also working to develop decentralized mitigation techniques. This means that instead of relying on a centralized infrastructure, a network of distributed systems is established that can collectively respond to cyber attacks. This approach increases the resilience and flexibility of defense mechanisms, significantly reducing the likelihood of attack success.





The decentralized system allows for a faster and more effective response to threats, which is critical at a time when cyber attacks are becoming more sophisticated and frequent.

### **Broader interest, good for participants**

In the broader context of the IPCEI-CIS, NBIP strives to contribute to overall cybersecurity in Europe. This includes collaboration with other European parties to share best practices, joint establish research projects and jointly work on solutions that strengthen Europe's digital autonomy and sovereignty.

For participants, participation in this project has the advantage of enabling NBIP to work more efficiently and in a more structured manner on further development of its infrastructure. As a result, the service will not only improve, but will also follow the market very closely and may even be able to take the lead in some aspects. It also helps to raise NBIP's profile in Europe. This can have all kinds of benefits, including further economies of scale and entrances to the right bodies to further solidify the interests of participants in Europe.



# Knowledge center

**NBIP's knowledge center is designed to share both subject matter and general knowledge.**

On the one hand, very specific expertise is shared, for example when it comes to DDoS, abuse prevention or lawful interception. On the other hand, the knowledge centre has a public function. Both participants, stakeholders and collaborative partners as well as media administrators, politicians and other interested parties can turn to NBIP for information. The intention is to further develop the knowledge centre's activities in the the coming years.

The knowledge center is primarily a platform for information exchange and cooperation. By regularly publishing articles, reports, white papers and case studies, NBIP provides valuable insights that participants can use to improve their own security strategies. In addition, the knowledge center organizes events, workshops and webinars where industry experts share their knowledge and experiences.

Another important aspect of the knowledge center is regulatory compliance support and legislation. NBIP helps participants understand what new laws and guidelines apply to them, and how to comply. This includes guidance on

the implementation of compliance measures and providing tools and resources to facilitate compliance. This support allows participants to better prepare for audits and inspections, and minimize their risk of non-compliance.

In addition, NBIP is committed to making access to European grants and funding easier for its participants. Many smaller Internet providers and hosting companies face the bureaucracy and complexity of European subsidy applications. NBIP wants to play a facilitating role in this with its knowledge center by sharing knowledge and experience, and by supporting participants with applications. This will make it easier for them to take advantage of available resources and realize their own cybersecurity projects.

Finally, the knowledge center is also actively involved in cybersecurity research projects and innovations. By working together with academic institutions, research organizations and other industry partners, NBIP remains at the forefront of technological developments. Participants benefit from these research efforts by access to the latest insights and technologies, which they can apply to improve their own services and security measures.

# Public affairs

**NBIP's public affairs activities are likely to intensify in the coming years. There are a number of reasons for this. NBIP is in close contact with, among others, the Ministry of Justice and Security, the Ministry of the Interior, the National Cyber Security Center (NCSC), Digital Trust Center (DTC), the National Digital Infrastructure Inspectorate (RDI), the Public Prosecutor's Office (OM), National Police and several European government organizations.**

In addition, NBIP participates in sectoral initiatives, coalitions and consultations, including the anti-DDoS coalition, the Anti Abuse Network (AAN) and the Digital Infrastructure Netherlands Foundation (DINL). NBIP is in close contact with the various industry associations in the sector. NBIP also hooks up with partnerships and coalitions at the European level.

From DINL, in which the core of the Dutch digital infrastructure is represented, interest representation is also done on behalf of NBIP for its base. NBIP does not lobby actively itself, but does provide solicited and unsolicited input on legislative proposals, regulations and policy.

NBIP is close to the fire and its input is valued by stakeholders. As a result, NBIP is able to convey the concerns and practical challenges of participants to the appropriate consultation tables. Because NBIP is also operationally active, it is able to paint a clear picture of how legislation and policy ultimately impact daily practice. The ability to land such information in the right place is seen as very valuable by all involved.





# On behalf of the Participants

## Frans ter Borg

**Chairman Board of Participants**

Frans ter Borg has been the chairman of NBIP's Council of Participants since April 2024, where he is committed to representing the interests of participants. With a long career in the Internet sector and as founder of Quanza in 2001, Frans has extensive experience in network and infrastructure solutions. He has previously held board positions with the Dutch Cloud Community (DCC) and foundation Digital Infrastructure Netherlands (DINL), where his work included policy issues around security and Internet infrastructure.

Since April 2024, you have been the new chairman of NBIP's Board of Participants. What made you decide to take on this role?

There had been a vacancy for some time, and I think it is important that the voice of the participants is properly reflected in what happens within NBIP. I felt called to do this.

Can you tell a little more about yourself and what makes you suitable for this position?

“My career in the Dutch Internet sector dates back to 1996, which has given me in-depth knowledge of hosting, telecom and cloud services. Through my company Quanza, I have developed specific

expertise in core Internet infrastructure, which ties directly into NBIP's activities. My board experience, gained during my seven-year term at the Dutch Cloud Community and DINL and my chairmanship of CITA (Cloud IT Academy), has familiarized me with important issues around security and policy and education in the industry. This new role at NBIP is a great opportunity to also work on the operational side and get a feel for what those policies are all about.”

You've taken over from Bernard Edelenbos, who held this role for nearly 10 years. Are his shoes hard to fill?

“Although Bernard's shoes are obviously hard to fill because of his years of experience, I bring a slightly different approach. I am originally perhaps a little more of a techie, which allows me to look at solutions for both the business and the organization from a different perspective.”

What is your ambition in this role and what themes are important to you?

“I want to strengthen contact with the participants, have more interaction and be able to properly bring the wishes and challenges of the participants to



the board. So that action can be taken on them in a good way and solutions can be built for them. On the DDoS side of the NBIP it would be nice if a structure could be built where there are indeed more international locations at which filtering can take place to share the load. This could also be of interest to foreign participants. I also want to focus on developing technology myself. By building out your own technology and making it open source, you make the Internet as a whole more secure. In the long run, this can be done at lower cost, which in turn benefits the participants.”

#### **What makes the Dutch Internet sector such a great community?**

“In the Dutch Internet sector, the we-feeling is very much developed. That’s what makes the Dutch Internet sector special. Organizations such as the Dutch Cloud Community, DINL and the NBIP reinforce this in specific sub-areas. There is a willingness to spar with each other about problems and give a peek at each other’s work. After all, we all have the same problems, so let’s learn from each other. There’s a piece of friendliness in it that I recognize much less in other sectors.”

#### **What makes NBIP special as an organization?**

“The NBIP is one of the unique organizations of ‘Internet Netherlands’ that was really created from collectivity. We all have the same problem, such as DDoS attacks, and together we try to solve it. Sometimes the cost comes before the benefit, but in the end we all create something beautiful and efficient. This collective nature is quite unique, especially internationally. In other countries, these kinds of initiatives are often more commercial in nature.

NBIP is not just about the individual, but about the collective. We invest in the collective, knowing that it will come back to us later and we will all benefit. That’s what makes NBIP truly special.

What I also want to have mentioned is that the organization has had a tough race over the past year and a half with taking the services in-house. That has created a lot of workload. NBIP, and by that I mean the management, staff and board, have really pulled off a feat there, and I think we as participants should really appreciate that, how much work has been done there with such a small team.”

# About NBIP

The Nationale Beheersorganisatie Internet Providers (NBIP) foundation was founded in 2001 as an implementing agency for tap commands in the Telecommunications Act. Today, NBIP has become the center 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 with services that are efficient to operate. Participants can jointly use expensive or complex facilities that they do not need all the time through NBIP. The best-known example of this is NaWas, the world's largest non-profit DDoS scrubbing centre used by more than 130 organisations in 10 European countries.

Over the years, NBIP has become a fixture in the Dutch and increasingly also the European internet landscape. With more than 200 participants, an international presence and involvement in strategic European development projects, it has been proven that NBIP's philosophy also works in practice. Digital infrastructure providers as well as public and private partners know how to find their way to NBIP.



nationale  
beheersorganisatie  
internet providers