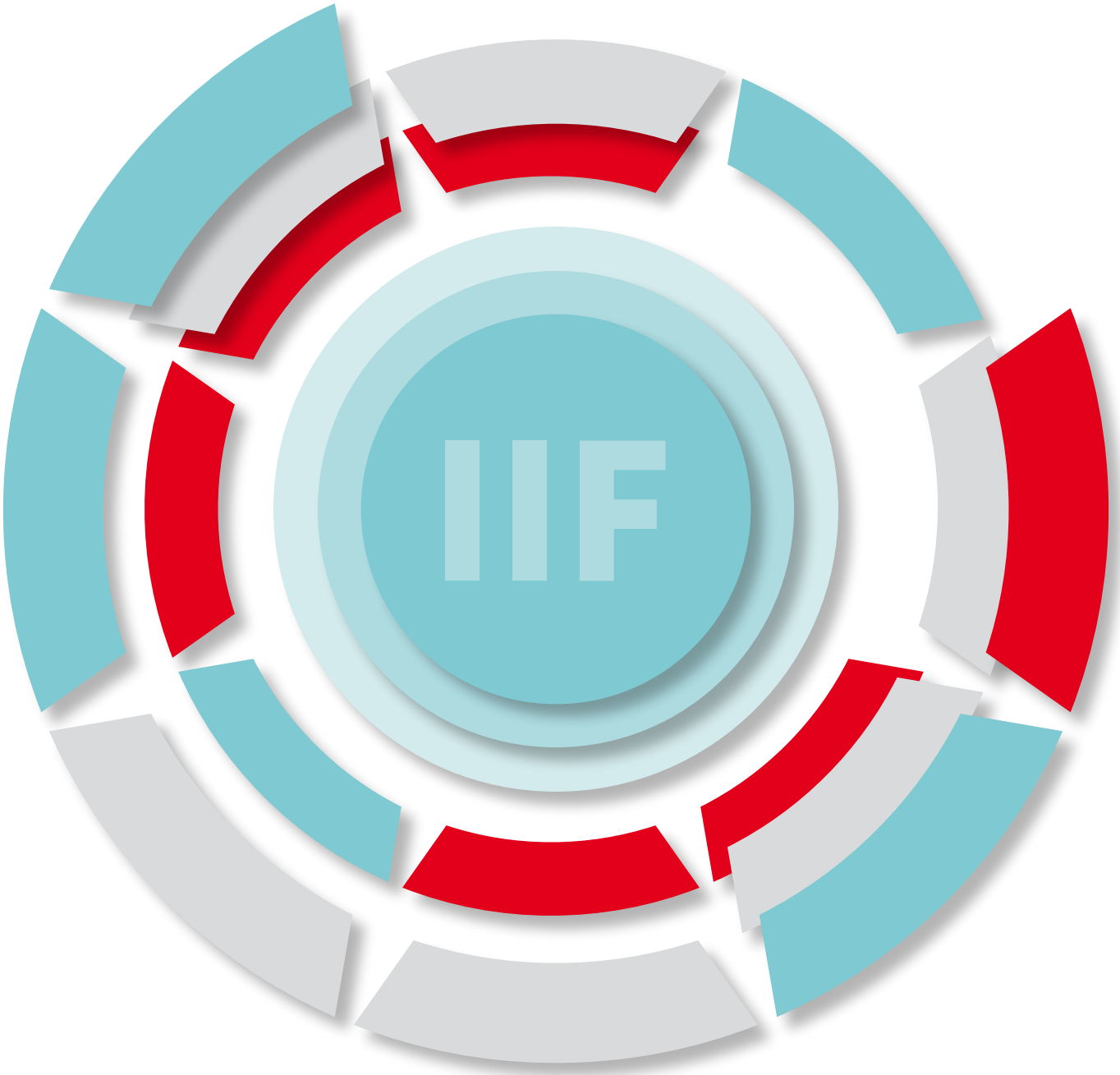
Groundwork for the Internet Infrastructure Forum (IIF)



topDNS

An initiative by eco

eco

ASSOCIATION OF THE INTERNET INDUSTRY

Table of Contents

Laying the Groundwork for the Internet Infrastructure Forum (IIF)

The Internet Infrastructure Forum (IIF) is a new initiative to bring together a diverse set of Internet infrastructure operators – including to improve coordination in combating online abuses.

eco – Association of the Internet Industry and its topDNS initiative invited participants to an exclusive preparatory feeder workshop in Frankfurt, Germany, on 5 November 2024 in advance of the formal founding of the Internet Infrastructure Forum (IIF) in February 2025.

As outlined in the IIF Prospectus, the goal of this new forum is to:

- Connect infrastructure operators around their common coordination challenges, exchange experiences, share best practices, and develop new communication channels.
- Inform participants about the prevalence of different types of abuses, existing mitigation procedures and standards, and the distribution of roles and responsibilities.
- Develop cooperation mechanisms and workflows for abuse reporting and handling, to reduce the burden of dealing with abuses online.

This new forum will provide a dedicated space for infrastructure operators to work together to address online abuses that go beyond the limited mandate of ICANN, such as content-related abuses. By improving coordination and collaboration, the IIF aims to bolster the industry's reputation and reduce the need for additional regulation.

At the feeder workshop in Frankfurt, the participants discussed the various forms of abuse, including phishing, malware, and spam, and the role of the different providers and operators in prevention. The workshop initiated an exchange about common challenges and best practices and new communication channels.

A two-day meeting will take place in Amsterdam in February 2025, at which the founding of the forum will be formally concluded and the first workflows for combatting abuse will be defined.

Internet Infrastructure Forum Feeder Workshop, Frankfurt, November 2024

The feeder workshop brought together DNS providers, hosting and cloud service providers, ISPs and other Internet infrastructure providers. It was divided into several focus areas, accompanied by expert presentations and interactive discussion sessions. The event underlined the urgency of cross-sector cooperation to ensure trust in online services and to improve reporting of and response to online abuse.

The workshop addressed the current trends and challenges that Internet infrastructure operators face in relation to abuse and cyber threats. The rising prevalence of online abuse is placing an increasing burden on all stakeholders, as the frequency and complexity of abuse types continue to grow.

Different types of online abuse are most effectively mitigated at various levels of infrastructure. Therefore, it is crucial for different infrastructure operators to collaborate within their capacities to prevent and combat online abuse effectively.

The following companies and organisations took part in the feeder workshop:

- eco – Association of the Internet Industry
- Internet & Jurisdiction Policy Network
- Abusix
- Anexia
- German Federal Office for Information Security (BSI)
- German Federal Network Agency (BNetzA)
- Cloudflare
- Deutsche Telekom
- GoDaddy
- Google
- Hetzner
- IONOS
- KEVAG Telekom
- nGENn
- Public Interest Registry
- Spamhaus
- Swisscom
- SWITCH
- Team Internet
- Vodafone

Introducing the Internet Infrastructure Forum and its goals

Thomas Rickert, Director Names & Numbers, eco – Association of the Internet Industry **Bertrand de La Chapelle**, Executive Director, Internet & Jurisdiction Policy Network

Thomas Rickert and Bertrand de la Chapelle introduced the Internet Infrastructure Forum (IIF). The goal is to create a network that would connect Internet infrastructure stakeholders and enable them to work together to address abuse. Since ICANN has only a technical mandate and is limited to only part of the abuse issue, the forum's focus is on types of abuse that go beyond this, such as content-related abuse.

Efficiency through trust and collaboration: The goal is to create a common framework to improve response times and effectiveness in curbing abuse. Unfortunately, the general approach we are seeing today is to try tackling online abuse closer and closer to the root of the Internet infrastructure rather than going after the perpetrators involved in content-related harms and getting the respective content offline. The Quad9 case is just one of the latest examples of blocking at the infrastructure level, which is becoming a new but ineffective trend.

Who is best placed to tackle which type of abuse?
topDNS Abuse Table & FIRST DNS Abuse Techniques Matrix

What is online abuse? And how much?

Markus de Brün, Senior Security Specialist, Federal Office for Information Security (BSI)

Markus de Brün described the different types of abuse that are currently challenging Internet infrastructure operators:

- **Phishing**: Phishing attacks, where criminals trick users into revealing confidential information, remain a widespread threat. The proliferation of phishing websites necessitates prevention and rapid detection. Differentiating between phishing and fraud is often challenging. The volume of phishing sites has decreased, but the quality has increased massively.
- **Malware**: Malicious software is increasingly being used to exploit or damage infrastructure. The variety delivered through different channels has also increased, putting operators' response times and defences to the test.
- **Botnets**: Combatting botnets – networks of infected devices used for malicious activity – is a complex challenge because they are often difficult to identify and operate on a large scale.
- **Spam**: Despite years of countermeasures, spam remains a significant source of abuse. The mass distribution of unwanted messages puts a strain on systems and requires specialised filtering and detection technologies.

When it comes to online abuse, it is often challenging to say what exactly and how much we see. There are neither universal nor clear definitions, also due to cultural and legal differences globally. Verifying abuse is sometimes hard, and public statistics are often created with intentions. This often unclear situation is not a good basis for the decision to block a domain.

As described with phishing, actors adjust to new measures:

- Instead of selling counterfeit products, more fake shops try to phish credit card details.
- Multi-factor authentication is growing, leading to more targeted attacks/requests for this data.
- Often domains are used for phishing for only a few hours – consider the reputation of the TLD that enables such registrations. Would it help to make domain registrations more expensive? In most cases, stolen credit card details are involved, hence the short lifetimes.
- 50% of all new domains are only online for 6 hours and, therefore, do not appear in blocklists.

Given the broad landscape of online harms, the question remains: Does it make sense to try to define the scope of the term 'DNS abuse'?

Costs and business case of abuse management

Oliver Werner, CEO, netcup GmbH
Tobias Knecht, CEO, Abusix

In their separate presentations, Oliver Werner and Tobias Knecht discussed the extent to which abuse management can be integrated as a business model, with a focus on automated systems that can help minimise manual processes and reduce costs.

A key point of discussion in these two sessions revolved around the financial impact of abuse management. While for most infrastructure providers, combating abuse is primarily a cost factor, Werner and Knecht both discussed ways in which this could create added value for the company. The structure and the right approach are more important than the costs. It doesn't have to be expensive if it's done cleverly.

- **Costs for abuse management and scalability**: The increasing threat situation means that companies have to make considerable resources available for defence and prevention. Smaller providers, in particular, are burdened by the cost of technologies and monitoring, which was cited in the discussion as a hurdle to effectively combating abuse. Better scalability, e.g. through standardised processes and automation, could help here.
- **Automation as cost reduction**: The use of automation solutions was highlighted as a key strategy for reducing the costs of abuse management. Rather than relying on manual processes, automated systems can deliver faster and more reliable results. Tobias Knecht from Abusix explained that they can help to minimise abuse while reducing the burden on resources. Some providers shared the size of their abuse departments to demonstrate that with the right strategy and level of automation, abuse management can be done at a reasonable cost.
- **Added value of abuse management**: The speakers discussed whether and how abuse management can be integrated into the business model. One approach is to offer additional security services that increase customer loyalty and trust. Participants agreed that effective abuse management not only offers legal and regulatory advantages, but also has the potential to act as a competitive differentiator.
- **Proactive approach**: More proactive measures, such as scanning one's own infrastructure, were considered to help rather than waiting for reports of problems on the won network.
- **Be uncomfortable**: Bad actors are well-organised and structured. We can take resources away from these bad actors by identifying the sources of spam, malware, and phishing. For hosting providers, whether the issue is spam or phishing is usually not a critical question; from their perspective, it involves a compromised system.
- **React more quickly**: Research shows that domains are typically used for only six hours by these malicious actors. Every website is vulnerable, and it is not the hosting provider's fault. If all hosting services took phishing sites offline within 24 hours it would significantly reduce abuse.

The resources required for effective abuse management

The increasing diversity and adaptability of threats require infrastructure operators to constantly adapt their protective measures. The discussion following Werner and Knecht's presentations emphasised the following aspects:

- **Complexity and adaptability of attacks**: Cybercriminals are flexible in their response to new defences, so they must be constantly updated and adapted.
- **Resource Expenditure**: Many providers feel that the resources required for abuse management can be a challenge, especially for smaller ones. Participants discussed ways to save resources through collaborative efforts, standardised tools, and efficient automation.
- **Shifting threats to content-related abuse**: Many forms of abuse are moving to the content level, requiring infrastructure providers to be more vigilant and responsive.
- **Changing rules & regulations**: The contract amendments at ICANN may just be the beginning. Over the past decade, IT security regulations have evolved significantly. The next revision of current regulations will most likely introduce even stricter obligations.

Regulatory and legal aspects for abuse management

Thomas Rickert, Director Names & Numbers, eco – Association of the Internet Industry

Another key topic was the role of new regulations, such as the Digital Services Act (DSA) and the NIS2 Directive, which place increasingly stringent requirements on abuse management. Thomas Rickert went through some of the challenges and opportunities that these regulations bring:

- **Responsibilities and liability**: Infrastructure and Internet Service Providers are increasingly under pressure to ensure that their platforms and networks are not used for illegal purposes. The challenge is to implement measures that ensure compliance and keep users safe.
- **Smart contracting**: Many contracts allow for a 24-48-hour response time; however, many malicious domains are only live for up to 6 hours. We need to adapt contracts to reality, e.g., through Acceptable Response Policies. Clean contracts can minimise liability risk.
- **Consensus policies**: An IIF with 'multistakeholder superpowers' could be the right place to work on these policies at a global level. Then we can help to shape the rules we agree to play by.
- **Promoting transparency**: Regulations often require more transparency and accountability in anti-abuse measures. This increases the pressure on operators to establish clear and comprehensible processes.
- **Coordinate the delivery of reports and response channels**: Regulatory requirements emphasise the importance of coordination and rapid response channels, which underscores the importance of standardised processes and reporting channels. We currently see too many 'one-size-fits-all' approaches but differentiated treatment of different types of abuse makes more sense.

Sharing is caring

Michael Hausding, Competence Lead DNS & Domain Abuse SWITCH, Forum of Incidents Response & Security Teams (FIRST)

Michael Hausding gave an overview of the historic development of the exchange of data about abuse.

1. **Founding Phase (up to 2000)**: The first Computer Emergency Response Teams (CERTs) emerged following significant incidents like the Morris Worm in 1988, establishing frameworks for information sharing and collaboration within the cybersecurity community.
2. **Formalisation and Trust Communities (2000-2010)**: The exchange of abuse data became more structured with the establishment of organisations such as the European Government CERT (EGC) and ENISA. This period focused on building trust within communities to facilitate sensitive information sharing.
3. **Development of Standards (2010-2020)**: Increased funding drove the creation of key standards for information exchange to enhance interoperability. Notable examples include the Common Vulnerability Scoring System (CVSS) and the Traffic Light Protocol (TLP), which allow for efficient data sharing and better understanding of threats.
4. **Cross-Sector Coordination (2020-Present)**: There is now an emphasis on breaking down silos and fostering collaboration among various sectors addressing online abuse. Regulations such as NIS2 and the DSA have led to the creation of Information Sharing and Analysis Centres (ISACs), and frameworks like the DNS Abuse Matrix are being developed to clarify roles and responsibilities among stakeholders in abuse response.

A further goal of the feeder workshop in Frankfurt was to encourage international cooperation and coordination among the various players in the Internet infrastructure sector. The complexity and diversity of the international fight against abuse show that a unified strategy is necessary but difficult to implement, due to several factors:

- **Cultural Differences in Defining Abuse**: One of the main problems of international cooperation is the different understanding of what constitutes abuse. Regional and cultural differences mean that definitions vary widely. Participants from different regions shared their specific challenges and discussed how to reach a global consensus.
- **Biggest challenge**: Threat actors take advantage of known weaknesses in combating abuse, including regulatory constraints, the speed of response (the average phishing campaign lasts 217 minutes, with most clicks occurring within the first four hours), and the resources available to them (attackers typically have the upper hand in this area).

- **Efficient and legally compliant transfer of data about abuse**: The sharing of data and threat intelligence has been identified as a key factor in efficiently combating misuse. However, data protection regulations often conflict with unrestricted data sharing. The workshop served to develop ideas for legally compliant yet effective sharing of abuse information, such as through the use of standardised formats and automated data transfer systems.
- **Communication gaps and coordination needs**: Many forms of abuse require transnational cooperation, but this is often hampered by communication gaps. Speakers emphasised the need for clear and rapid communication between stakeholders. Initiatives such as the Internet Infrastructure Forum could provide a platform to improve communication and facilitate closer cooperation.

Discussion: Best practices and standards for abuse management

Tobias Knecht, CEO, Abusix
Bertrand de La Chapelle, Executive Director, Internet & Jurisdiction Policy Network
Volker Greimann, General Counsel, Head of Legal and Policy, CentralNic Group

The next part of the feeder workshop was dedicated to specific technical and organisational approaches to combating abuse. Standardised processes and technologies were described as a promising strategy for detecting abuse at an early stage and combating it efficiently.

- **Automation as a key strategy**: The use of automation, particularly in the collection and processing of abuse reports, was highlighted as an important measure. Automated systems, such as MISP and XARF, enable providers to process large volumes quickly and in a structured manner, reducing response times and making more efficient use of resources.
- **Standardised complaint processes and reporting formats**: The need to handle abuse reports in a consistent and standardised manner was discussed. This included structuring them to include all relevant information and expedite the process. The use of clear standards and established complaint procedures promotes the efficient and consistent handling of abuse reports.
- **Tools and technical solutions for abuse management**: The workshop highlighted the importance of standardised tools and platforms to enable centralised processing of abuse data. Participants reported on the success of certain technical approaches and the benefits of standardised processes and tools. These include reducing manual processing and error rates in identifying and addressing abuse.

An open discussion on goals and strategies for combating abuse

Thomas Rickert, Director Names & Numbers, eco – Association of the Internet Industry
Bertrand de La Chapelle, Executive Director, Internet & Jurisdiction Policy Network

This section of the feeder workshop was an open discussion of long-term goals and strategies for combating abuse. The aim was to develop a vision for the coming years and discuss ways to achieve these goals through the creation of the Internet Infrastructure Forum.

We see technical DNS abuse on the one hand and significant content abuse on the Internet on the other hand which falls outside ICANN's responsibilities, including issues like copyright infringement. While it's possible to disrupt these issues online, that doesn't eliminate them entirely. The closer you are to the content, the more effectively you can take specific actions. Therefore, it is essential to have coordinated efforts among various stakeholders, as this conversation cannot take place within ICANN.

- **Networking among the participants**: A key conclusion was the necessity of enhancing networking among the various industry silos that exist within the diverse landscape of providers, which vary in size and form. This improved collaboration should facilitate the sharing of knowledge and best practices more effectively, ultimately contributing to increased efficiency.
- **Future-oriented cooperation and building a network**: The participants discussed the need for stronger networking within the industry to exploit synergies and share experiences. A comprehensive network that shares knowledge and best practices was seen as a key component in meeting the requirements of modern abuse management.
- **Development and promotion of common standards**: An important goal was to establish common standards and voluntary commitments for the industry. These could provide a voluntary but binding basis for obliging all providers to meet uniform security requirements and response times.
- **Regulation and voluntary self-commitment**: Another point of discussion was how the industry can achieve a voluntary commitment to combating abuse to prevent further regulatory measures. Through proactive engagement and adherence to voluntary standards, companies could build trust and demonstrate that they take the challenges of abuse management seriously.

There is currently no equivalent organisation to ICANN specifically for hosting providers and ISPs, which is a highly diverse landscape of providers, differing in shapes, types, and sizes. The Internet Infrastructure Forum aims to bring together DNS operators, hosting and cloud service providers, ISPs, and CDNs to foster collaboration and enhance information sharing. The role of the Internet & Jurisdiction Policy Network is to provide a space to connect, share and coordinate efforts to combat abuse.

This initiative represents an opportunity for stakeholders to develop common definitions and solutions (such as distinguishing between domain names and hosting) and to engage individuals who are eager to make progress. Numerous organisations, processes, and standards have been in place for many years; there is no need to reinvent the wheel with entities like FIRST or XARF already established. Instead, we should seek to understand the existing processes and explore how they can be refined.

Internationally inconsistent rules and regulations should not be an excuse for not caring. The industry must strive to define common goals and expectations, including managing those expectations.

There is still significant work to be done. Each stakeholder must clarify their responsibilities: What does each party want to be accountable for? Who can fulfill which roles? We need to outline what actions can and should be taken and identify tasks that can easily be addressed by others. Additionally, we need to consider the most effective ways to report these efforts. It should also be straightforward for users to address and report instances of abuse.

Summary and next steps

Thomas Rickert, Director Names & Numbers, eco – Association of the Internet Industry
Bertrand de La Chapelle, Executive Director, Internet & Jurisdiction Policy Network

In the final part of the workshop, the most important findings of the day were summarised, and possible next steps were discussed. The participants agreed that a long-term strategy is required to meet the challenges of abuse management. Closer collaboration, a clearly defined process for dealing with different forms of abuse, and increased automation in abuse management were identified as key strategies.

Creating a dedicated space in the form of the Internet Infrastructure Forum will bring together the relevant industry actors sharing the objective of improving coordination in anti-abuse efforts among Internet infrastructure operators. Recent discussions with key players have clearly confirmed their interest in joining such an effort to break down silos.

A two-day meeting will take place in Amsterdam in February 2025, at which the founding of the forum will be formally concluded and the first workflows for combating abuse will be defined.

Regular meetings and collaborative projects will further develop and implement the strategies formulated during the feeder workshop. The participants are committed to applying the strategies and best practices in their companies. They also emphasised the importance of transparent communication and proactive engagement in building trust within the industry and with users.

This new Forum will allow infrastructure operators to:

- Connect around their common coordination challenges, exchange experiences, share best practices, and develop new communication channels between them and with other stakeholders.
- Be informed about the prevalence of abuses, existing mitigation procedures and standards, and, according to their respective capacities, the distribution of roles and responsibilities.
- Develop cooperation mechanisms and workflows for abuse reporting and handling, to reduce the human and financial burdens of dealing with abuses online.

By pursuing these objectives, the IIF hopes to create a more robust and collaborative ecosystem for combating online abuse, ultimately enhancing the safety and trustworthiness of the Internet.

Why you should join the Internet Infrastructure Forum (IIF)

There are many compelling reasons for industry actors to join the IIF. Here are eight reasons why you should participate.

1. Minimising Liability Risks:

- The current legal landscape regarding online abuse is complex and evolving, with regulations like the Digital Services Act (DSA) and NIS2 Directive placing increased responsibility on infrastructure providers.
- The IIF offers a **platform to collaborate** on developing acceptable response policies and model contracts that can help minimise liability risks, especially in relation to content-related abuse.
- By working together, industry actors can establish clear expectations and responsibilities, potentially influencing policy development and avoiding stricter, less flexible regulation in the future.

2. Improving Coordination and Efficiency:

- Currently, dealing with online abuse often involves a fragmented, siloed approach, leading to delays and inefficiencies.
- The IIF aims to break down silos, allowing for **better coordination across different industry segments** (registrars, hosting providers, ISPs, etc.).
- This can lead to **faster response times** for dealing with abuse, particularly important for time-sensitive issues like phishing campaigns that often last only a few hours.

3. Sharing Best Practices and Reducing Costs:

- Many companies struggle with the costs of abuse management, especially smaller providers who lack the resources for sophisticated systems.
- The IIF offers a venue for sharing **cost-effective strategies** and developing **standardised tools** for tasks like automated abuse report handling.
- This can help smaller players keep up with the evolving threat landscape without facing unsustainable financial burdens.

4. Shaping Industry Standards and Avoiding 'One-Size-Fits-All' Solutions:

- Overly broad, 'one-size-fits-all' regulations fail to account for the nuances of different abuse types and the varying capabilities of providers.
- The IIF can serve as a platform for the industry to proactively develop its own **voluntary commitments and standards**, tailored to the specific challenges of different abuse scenarios.

- This can help avoid overly burdensome or ineffective regulations being imposed from outside.

5. Accessing and Sharing Threat Intelligence:

- Cybercriminals constantly adapt their tactics, making it essential for industry actors to stay informed about the latest threats.
- The IIF can facilitate the sharing of Cyber Threat Intelligence (CTI), including information on attack techniques, trends, and specific indicators of compromise.
- This can help companies improve their defences and proactively address emerging threats before they become major problems.

6. Leveraging Existing Expertise and Resources:

- Effective solutions for many abuse problems already exist, the challenge lies in making these solutions more widely known and adopted.
- The IIF can help **bridge this gap** by connecting companies with existing expertise and promoting the use of established best practices and technical solutions.

7. Building Trust and Improving the Industry's Reputation:

- Public trust in the Internet is being eroded by the prevalence of online abuse.
- The IIF, by demonstrating a commitment to collaborative action, can help **restore this trust** and show that the industry is taking the problem seriously.
- This can enhance the reputation of individual companies and the industry, making it a more attractive space for users and investors.

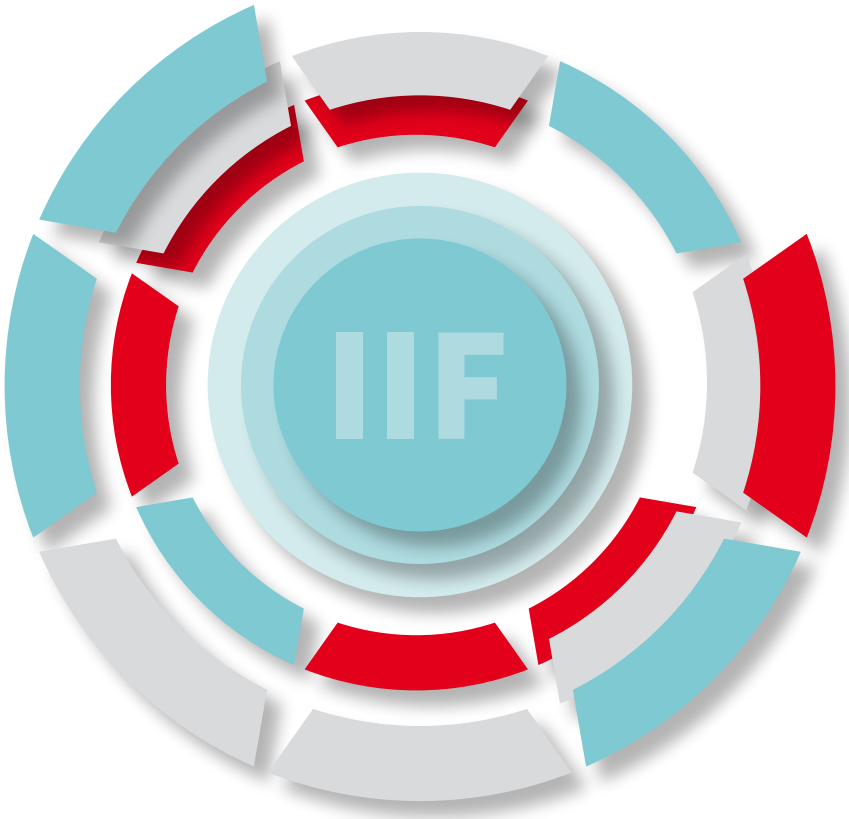
8. Influencing the Global Policy Landscape:

- While initially focused on European stakeholders, the IIF has ambitions to become a global forum.
- By developing successful models for addressing abuse, the IIF can **influence policy discussions internationally**, potentially shaping how online abuse is tackled globally.
- This offers companies the opportunity to set the rules of the game rather than simply reacting to regulations imposed by others.

The IIF presents a compelling opportunity for industry actors to address the shared challenge of online abuse. By working together, companies can not only protect themselves and their users but also help shape a safer and more trustworthy Internet for everyone.


Vorbereitungsworkshop

Groundwork for the Internet Infrastructure Forum (IIF)



eco – Association of the Internet Industry
Lichtstrasse 43h, D-50825 Cologne, Germany
phone +49 (0) 221 / 70 00 48 – 0
fax +49 (0) 221 / 70 00 48 – 111
info@eco.de
international.eco.de

topDNS

An initiative by eco

eco
ASSOCIATION OF THE INTERNET INDUSTRY