# State of the DNS in 2025 Workshop in Brussels, 6 February 2025

## Report and Conclusions

Hosted by eco – Association of the Internet Industry

topDNS

An initiative by eco

eco

ASSOCIATION OF THE INTERNET INDUSTRY

We thank the members of the
topDNS Steering Committee for their support

# Content

Executive Summary . . . . . 4

Housekeeping rules . . . . . 7

Participants . . . . . 8

Introduction: Advancing DNS abuse mitigation . . . . . 9

1. Segment: Contract amendments – Is there a measurable impact? . . . . 10
   1.1 Lightning talks by ICANN, NetBeacon Institute, and CleanDNS . . . . . 10
   1.2 Contributions and main findings . . . . . 11

2. Segment: Automated vs. manual processing of abuse reports . . . . . 13
   2.1 Lightning talks by nic.at, SWITCH, and Realtime Register . . . . . 13
   2.2 Contributions and main findings . . . . . 14

3. Segment: Cultural change within the industry . . . . . 15
   3.1 Lightning talks by Abusix and sys4 AG . . . . . 15
   3.2 Contributions and main findings . . . . . 15

4. Segment: A Forum for Internet Infrastructure Operators to coordinate anti-abuse efforts . . . . . 17
   4.1 Lightning talks by Verisign and Internet & Jurisdiction Policy Network. . . . . 17
   4.2 Contributions and main findings . . . . . 18

5. Open Discussion: How can we get all stakeholders to play their part? . . 19

6. Summary of Findings & Conclusions . . . . . 20
   Contract amendments – Is there a measurable impact? . . . . . 20
   Automated vs. manual processing of abuse reports. . . . . 20
   Cultural change within the industry. . . . . 20
   A Forum for Internet Infrastructure Operators to coordinate anti-abuse efforts. . . 21
   Getting all stakeholders involved . . . . . 21

7. List of Appendices:. . . . . 22

# Executive Summary

The **topDNS Initiative** of **eco – Association of the Internet Industry** held a workshop on the "State of the DNS 2025" on 6 February 2025 to discuss the progress made by the domain name industry in the fight against DNS abuse. This followed on from the previous "State of the DNS 2022" workshop held in November 2022, with the results of this prior workshop published in a **comprehensive report**.

Overall, 2024 marked a turning point in the discussion of DNS abuse and online harms. In January, M3AAWG published the document "M3AAWG DNS Abuse Prevention, Remediation, and Mitigation Practices for Registrars and Registries". Moreover, in April, the contract amendments requested by domain name registries and registrars in contractual relationships (contracted parties) with ICANN to increase the level of abuse mitigation came into effect. From October 2024, the NIS2 Directive became the first piece of legislation to include the term "DNS abuse".

In the course of the "State of the DNS 2025" workshop, the topDNS Initiative discussed the status and progress of the following topics:

- Contract amendments - is there a measurable impact?
- Automated vs. manual processing of abuse reports
- Cultural change within the industry
- Creation of a Forum for Internet Infrastructure Operators to coordinate anti-abuse efforts
- Internet Infrastructure Operator Collaboration.

These items also included updates on those that were supported as priority actions by a number of participants during the State of the DNS 2022 workshop:

- Fast takedowns of malicious domain names
- Prevent abuse before it is reported
- Automation is indispensable in this contextEnhancing Security
- Building trust
- Automatic responses to abuse reports
- Developing training opportunities
- Initiate a cultural change
- Abuse prevention/treatment/combating does not necessarily have to be a cost centre
- Commercial incentives and reputation-based measures
- Building a schedule of roles and responsibilitie

In addition to addressing many of the issues covered in 2022, and in close collaboration with partners such as the **Internet & Jurisdiction Policy Network**, an **Internet Infrastructure Forum (IIF)** for operators had been developed to improve coordination of abuse prevention efforts among Internet infrastructure operators in their respective roles and capacities. These included registries, registrars, resellers, hosting, cloud and email service providers, content delivery network operators, etc. The **IIF** was held in Amsterdam on **March 18th. 2025.**

In preparation for the launch of the Internet Infrastructure Forum (IIF), eco – Association of the Internet Industry and its topDNS Initiative held an exclusive preparatory feeder workshop for its members on 5 November 2024 in Frankfurt, Germany, ahead of the formal founding of the IIF in February 2025. The results of this workshop have been published in a **comprehensive report.**

In order to have a robust discussion about the roles, responsibilities and capabilities along the value chain of Internet infrastructure providers – and who can do what and by when – various stakeholders and representatives from different segments of the industry were invited:

- Members of the European Commission representing different DGs
- Experts from ICANN Org, the Internet & Jurisdiction Policy Network, NetBeacon Institute (formerly known as the DNS Abuse Institute), Global Cyber Alliance, and the Forum of Incident Response and Security Teams (FIRST)
- Domain name registries & registrars
- DNS service providers
- Hosting & email service providers
- Staff members of eco – Association of the Internet Industry

Each segment of the workshop began with a series of lightning talks, providing an overview of the respective recommendations and assessing their progress since the "State of the DNS 2022" workshop.

In this context, participants explored the roles, capabilities and responsibilities of different stakeholders.

The workshop showed that, for most of the recommendations, there are already solutions, tools and people addressing and working on them. The following points seem to have been supported as priority actions by most, though not all, participants:

## Contract amendments – Is there a measurable impact?

- **ICANN's enforcement efforts:** For example, five-year retrospective of DNS abuse mitigation, including new tools such as Metrica and INFERMAL.
- **Mitigation trends:** Early data shows increased mitigation rates (from mid-80% to over 90%) following April 2024 amendments.
- **ICANN compliance actions:** Over six months, 192 investigations led to 2,700 domain suspensions and two breach notices. Research showing that policy changes typically take 9-12 months to show full impact.
- **Challenges in measurement:** Reports suggest increased abuse reporting does not always indicate higher abuse but improved detection.
- **Ongoing monitoring:** Future improvements needed in evidence collection, reporting accuracy, and enforcement effectiveness.
- **Registrar compliance:** The 20 registrars with the highest abuse volume accounted for 80% of incidents, but they were not necessarily the largest registrars.
- **Measuring of harm:** Participants acknowledged the difficulty of quantifying the harm, given the varied impact of phishing, malware and other threats.

## Automated vs. manual processing of abuse reports

- **Efficiency of automation:** While automation speeds up response times, manual intervention remains necessary to ensure accuracy and compliance with legal requirements.
- **Legal and trust issues:** Many abuse reports come from unreliable sources; law enforcement agencies often face jurisdictional limitations.
- **Threat intelligence:** Legal frameworks like in Switzerland leverage intelligence-sharing to prevent malicious registrations.
- **Data verification challenges:** The nature of identity verification frameworks is fragmented, lack of a centralised stolen passport verification system complicates identity checks.
- **Balancing security and usability:** Strict verification measures may deter legitimate users while failing to stop organised cybercriminals.
- **Called for continuous improvement:** Threat intelligence sharing, automation in data processing, and structured reporting methods to help streamline cybersecurity efforts across the industry.

## Cultural change within the industry

- **ISP and hosting challenges:** Internet Service Providers (ISPs) process millions of abuse reports daily, but there is no centralised enforcement mechanism.
- **Regulatory gaps:** Unlike ICANN-regulated registrars, ISPs and hosting providers lack binding compliance requirements.
- **Legal certainty:** Clarity, not more legislation, is essential. Despite existing regulations, providers too often remain indifferent to their obligations. For example, while the DSA provides a foundation, its definitions and reporting requirements are unclear and impractical for many providers.
- **The business case for abuse prevention:** Some businesses successfully reduced abuse through dedicated anti-abuse teams.
- **Reputation as a driver:** Companies with weak anti-abuse measures risk losing business partnerships.
- **Systemic barriers:** Many companies prefer absorbing the costs of abuse rather than investing in preventative measures.

## A Forum for Internet Infrastructure Operators to coordinate anti-abuse efforts

- **Purpose:** Designed to bring together registries, registrars, hosting providers and Content Delivery Networks (CDNs) to tackle online abuse collaboratively.
- **Separation from ICANN:** ICANN must not engage in content moderation, necessitating a new venue for discussions on content-related harms.
- **Early-stage development:** Industry players are exploring new information-sharing mechanisms and enforcement strategies.
- **Industry self-regulation framework:** Plans to engage notifiers, regulatory bodies and other Internet stakeholders to enhance accountability.
- **Challenges in coordination:** Legal and technical inconsistencies across hosting environments require a structured, industry-led approach.

## Getting all stakeholders involved

- **Financial incentives:** Suggestions included discounted pricing for smaller companies and registry fee reductions for low abuse registrars.
- **Shared responsibility:** Participants discussed whether abuse mitigation should be framed as a public good rather than just a business challenge.
- **Intelligence sharing:** Improved data-sharing mechanisms are needed but should avoid overwhelming companies with excessive raw data.
- **Bridging silos:** The need for a more integrated, ecosystem-wide approach to tackling abuse, rather than relying on fragmented, sector-specific solutions.

## Final takeaways

- **No single solution:** A multi-faceted approach combining incentives, compliance enforcement, and better coordination is necessary.
- **Industry collaboration is critical:** The success of anti-abuse efforts depends on joint participation from registries, registrars, ISPs, and regulators.
- **Moving forward:** More research, standardised enforcement mechanisms, and structured workstreams are needed to improve long-term abuse mitigation.
- **Shared responsibility:** Tackling online abuse should be seen as a shared public responsibility, rather than just a business challenge. The sheer scale of the problem has outstripped traditional law enforcement capabilities, leading to greater reliance on the private sector.

## Welcome

**Lars Steffen** from the eco Association welcomed the participants to the "State of the DNS 2025" workshop and introduced them to eco – Association of the Internet Industry and the topDNS Initiative.[1] As he noted, the group gathering at the workshop were primarily those who support the topDNS Initiative, which was founded in 2021.

In welcoming the full group, Steffen thanked all of the attendees for their participation and for the time they had dedicated to joining the workshop, whether in person or remotely. He noted how the workshop built on discussions from the previous gathering in 2022, providing an opportunity to update developments in the DNS ecosystem.

As Steffen emphasised, the workshop would cover key topics, including recent contract amendments and their impact, the evolving landscape of automated versus manual abuse management, cultural change within the industry, a Forum for Internet Infrastructure Operators, and Internet Infrastructure Operator Collaboration. Additionally, he highlighted how the workshop would reflect on insights from the recent Internet Infrastructure Forum (IIF) that had just taken place in Amsterdam, particularly regarding increased cooperation among intermediaries to mitigate abuse and online harm.

## Housekeeping rules

Regarding the housekeeping rules, Steffen suggested an open and productive dialogue under Chatham House Rule, ensuring a collaborative and insightful exchange of ideas. He also requested a recording of the meeting for internal use, to compile a summary for all participants. These guidelines were unanimously approved by the attendees.

[1] Information on the eco Association and the topDNS Initiative can be found in the eco slide deck (Annex 1)

# Participants

Participants were asked to share their expectations at the start of the workshop. Several participants expressly welcomed the initiative and stressed that they came to the table with an open mind. A summary of the main thoughts they shared follows in this report. The list of participants can be found below.

## On-Site Participants

- **Petra Arts**, Senior Manager Public Policy, Europe, Cloudflare
- **Martina Barbero**, Policy Officer, DG CNECT, European Commission
- **Gemma Carolillo**, Deputy Head of Next Generation Internet Unit, DG CNECT, European Commission
- **Mukesh Chulani**, GDD Programs Director, ICANN Org
- **Bertrand de la Chapelle**, Executive Director, Internet & Jurisdiction Policy Network
- **Keith Drazek**, Vice President of Policy & Government Relations, Verisign
- **Janos Drienyovszki**, Legal and Policy Officer, DG HOME, European Commission
- **Alejandro Fernández-Cernuda Díaz**, Director of Engagement, Internet Integrity Program, Global Cyber Alliance
- **Ajith Francis**, Director, Policy Programs, Internet & Jurisdiction Policy Network
- **Volker Greimann**, Head of Policy and Compliance, General Counsel - Online Division, Team Internet
- **Michael Hausding**, Competence Lead DNS & Domain Abuse, SWITCH
- **Klara Jordan**, Cybersecurity & Technology Public Policy and Government Relations, Verisign
- **Julija Kalpokiene**, Consultant, Internet & Jurisdiction Policy Network
- **Tobias Knecht**, CEO, Abusix
- **Patrick Ben Koetter**, Leader of the Anti-Abuse & Email Competence Groups, eco – Association of the Internet Industry, Member of the Board, sys4 AG
- **Chris Lewis-Evans**, Director of Governmental Engagement and Internet Abuse Mitigation, CleanDNS
- **Antonella Munisteri**, Policy Officer, DG Home, European Commission
- **Elena Plexida**, Vice President, Government and IGO Engagement / Senior Manager, Government and IGO Engagement, ICANN Org
- **Thomas Rickert**, Director Names & Numbers, eco – Association of the Internet Industry
- **Robert Schischka**, General Manager, nic.at
- **Lars Steffen**, Head of Digital Infrastructures, Resilience and International, eco – Association of the Internet Industry
- **Dimitris Zacharias**, Government and IGO Engagement Sr. Manager, ICANN Org

## Remote Participants

- **Leticia Castillo-Sojo**, Senior Director, Contractual Compliance, ICANN Org
- **LG Forsberg**, Chief Technology Officer, iQ Global AS
- **Theo Geurts**, CIPP/E Privacy & GRC Officer, Realtime Register B.V.
- **Rowena Schoo**, Director of Programs and Policy, NetBeacon Institute
- **Samaneh Tajaizadehkhoob**, Director, Security, Stability and Resiliency Research, ICANN Org

# Introduction: Advancing DNS abuse mitigation

**Thomas Rickert** of the eco Association opened the discussion by reflecting on the key issues identified during the previous workshop in 2022, and emphasised the need to assess progress and determine the next steps in **DNS abuse mitigation**. Rather than diving into extreme detail, he provided a structured update on industry developments, highlighting advancements in fast takedowns of malicious domains and preventive measures such as deferred delegation, which prevents high-risk domain names from entering the DNS.

Rickert pointed out that commercial solutions, such as those offered by IQ, Domain Crawler, and CleanDNS, have significantly improved response times to illegal activity, providing both reactive and proactive measures to curb abuse. He noted that automation remains a central theme, with the industry recognising its essential role in managing abuse efficiently. However, Rickert highlighted the need to discuss in greater detail what automation means, in which areas automation should be used and further promoted, and in which areas manual intervention is required to ensure adequate and proportionate responses to abuse cases.

Trust was another key focus, particularly regarding who should be considered a reliable source of abuse reports and how to validate the information received. Rickert noted that automatic responses to abuse reports are now embedded in contract amendments, marking a significant step forward in regulatory compliance and enforcement. Additionally, he stressed the importance of training for registrars and industry professionals, highlighting eco's efforts through topDNS, which offers a collection of best practice webinars and educational videos to promote knowledge sharing.

Rickert highlighted some of the recent resources and initiatives developed since the last meeting. He encouraged attendees to explore the topDNS eco website's **video section**, where an inventory of recorded best practice webinars is available. These resources, he explained, serve as valuable tools for industry professionals looking to deepen their understanding of DNS abuse mitigation strategies. The initiative aims to share knowledge, highlight effective measures, and promote best practices across the industry.

He also emphasised the need for a cultural shift in how DNS abuse and harms online are tackled, citing increasing industry collaboration and initiatives that have prioritised abuse mitigation. He shared examples of how companies have transformed abuse mitigation from a cost centre into a commercially viable service, proving that proactive measures not only improve security, but also reduce operational burdens and improve reputation management.

In concluding his introduction, Rickert addressed the industry's efforts in defining clear roles and responsibilities for mitigating different types of abuse within the Internet infrastructure. He referenced **collaborative frameworks developed by eco** and **other industry organisations** like FIRST.org, ensuring that each stakeholder understands their role in addressing online threats.

Building on these themes of industry collaboration and progress, **Keith Drazek** of Verisign, one of the founding members of the topDNS Initiative, provided an overview of how these collaborative efforts have evolved into concrete actions. He traced the origins of these efforts back to May 2022 in Paris, where a key meeting of the Internet Jurisdiction Policy Network Domains Contact Group initiated structured collaboration among registries, registrars, and ICANN. At the time, the 2013 Registrar Accreditation Agreement only required registrars to acknowledge abuse notifications, without mandating action. Recognising that ICANN lacked the enforcement tools to tackle bad actors, responsible industry players voluntarily developed new contractual commitments to strengthen abuse mitigation.

By late 2022, contracted parties formally entered into negotiations with ICANN, reaching an agreement by March 2023. After a public comment period and a rigorous voting process, the amendments were officially approved and came into force on 5 April 2024, making them enforceable by ICANN Compliance. A significant milestone came when Verisign voluntarily incorporated these amendments into its .com and .net agreements, extending the new requirements to 175 million domain names and aligning legacy TLDs with broader DNS abuse obligations.

Drazek underscored the collaborative and voluntary nature of these efforts, calling them a major achievement. However, he emphasised that this was only the beginning. The next steps include monitoring compliance, evaluating the amendments' effectiveness, and considering further policy development within ICANN's framework. The industry remains committed to ongoing collaboration to ensure that these measures have a meaningful impact on reducing DNS abuse while continuing to strengthen the broader domain ecosystem.

# 1. Segment: Contract amendments – Is there a measurable impact?

## 1.1 Lightning talks by ICANN, NetBeacon Institute, and CleanDNS

- **Mukesh Chulani**, ICANN
- **Rowena Schoo**, NetBeacon Institute
- **Chris Lewis-Evans**, CleanDNS
- **Leticia Castillo-Sojo**, ICANN

Presenting a five-year retrospective of ICANN's DNS abuse mitigation efforts, **Mukesh Chulani** highlighted how ICANN first reorganised internally to create a cross-functional programme built on three pillars:

- providing trusted information,
- developing community tools,
- and enforcing contractual provisions.

During this period, ICANN launched the DNS ticker tool during COVID-19 (which identified over 200,000 suspicious domains) and, by late 2022, established a baseline definition of DNS abuse aligned with **SAC 115** guidance.

More recently, ICANN has launched two significant initiatives: the **ICANN Domain Metrica platform**, which improves upon the previous Domain Abuse Reporting system to track abuse metrics across registries and registrars, and the **Inferential Analysis of Maliciously Registered Domains** (INFERMAL) project, analysing maliciously registered domains. Chulani emphasised that these developments demonstrate ICANN's ongoing commitment to community engagement and continuous improvement in abuse mitigation strategies.

**Rowena Schoo**, representing the NetBeacon Institute, presented an analysis of how the gTLD contractual amendments have influenced DNS abuse mitigation, particularly in combating phishing and malware. Funded by **Public Interest Registry** (PIR), the NetBeacon Institute provides free tools and research to improve Internet safety. Schoo outlined the NetBeacon MAP project, which tracks unique malicious domain registrations to assess how effectively registrars are responding to abuse. Their methodology filters out duplicates and special cases, ensuring that mitigation efforts are accurately measured.

Their findings show that mitigation rates have increased, particularly following the April 2024 enforcement of the amendments and ICANN's breach notices in July and September. Prior to these compliance actions, mitigation rates were in the mid-80% range, but by late 2024, they had climbed above 90%, suggesting that enforcement measures are driving improved registrar behaviour. Schoo also highlighted that abuse does not correlate directly with registrar size, as the 20 registrars with the highest abuse volumes accounted for 80% of incidents – many of which were not the largest by number of domains under management.

While the early data is promising, Schoo cautioned that measuring DNS abuse mitigation remains complex and influenced by multiple factors. She emphasised the need for continued analysis, including trends at the TLD-level and enforcement patterns among registrars and registries. Future research will focus on interactive data visualisations to track long-term progress, and Schoo encouraged community engagement and feedback to refine the methodology and enhance DNS abuse mitigation efforts.

**Chris Lewis-Evans** of CleanDNS subsequently reported on the impact of DNS abuse amendments on the volume of abuse reports. He provided a registry-level perspective on DNS abuse mitigation, complementing Rowena Schoo's registrar-focused analysis. He underlined the challenges of obtaining reliable, consistent data, noting that different reporting sources can lead to varying interpretations. He pointed to ICANN's Compliance reports, which initially showed a spike in complaints after the amendments came into effect, followed by a stabilisation in reporting levels. Over the past six months, 2.3 million abuse reports were recorded, equating to 780,000 unique domain cases, with monthly abuse reports rising from 220,000 to 380,000. However, Lewis-Evans argued that this increase in reports does not necessarily indicate an increase in abuse, but rather that more incidents are being reported due to greater awareness and enforcement activity.

At the Top-Level-Domain (TLD) level, he highlighted a specific case where reported abuse dropped initially after ICANN's first breach notices in July 2024, only to rise again in December, a well-known seasonal spike due to increased online activity during the holiday period. He noted that 50-60% of reported cases led to some form of mitigation, though not all reports required direct registrar or registry intervention. He pointed out that speed of response is crucial in reducing the harm caused by phishing and malware, as most attacks are effective within 48 hours. Therefore, he called for greater collaboration between registrars, registries, law enforcement, and industry stakeholders to align DNS abuse takedowns with crime prevention efforts.

Lewis-Evans concluded that the contract amendments have indeed led to measurable improvements, with higher mitigation rates and increased enforcement activity. However, he stressed the importance of refining abuse reporting mechanisms to improve data accuracy. He highlighted concerns over the quality of reports, with only 35% of phishing and malware cases providing sufficient evidence for immediate action, while 46% required further verification. While the amendments have driven positive change, Lewis-Evans indicated that more work is needed to reduce abuse volume, improve reporting efficiency, and ensure that mitigation efforts translate into a meaningful reduction in harm across the Internet ecosystem.

From her perspective, **Leticia Castillo-Sojo**, Senior Director at ICANN Contractual Compliance, provided insights into the enforcement of the DNS abuse mitigation requirements that came into effect on 5 April 2024. Over the first six months, ICANN launched 192 investigations against registrars and registries regarding DNS abuse, with the majority of cases involving phishing. Most reports came from cybersecurity experts and impersonated entities, leading to two formal Notices of Breach – one against a registry (.top) and another against a registrar, both of which are now undergoing remediation. Additionally, 154 cases were resolved informally, resulting in the suspension of over 2,700 abusive domains and the takedown of 350+ websites. Castillo-Sojo stressed that not all enforcement actions are publicly reflected since many registrars and registries take corrective measures before escalation.

To ensure long-term compliance, 16 contracted parties presented remediation plans to ICANN. These plans aimed to address systemic issues, such as insufficient training in handling DNS abuse reports. One registrar, for example, implemented a training programme to improve its abuse response procedures. Castillo-Sojo highlighted that ICANN is actively monitoring compliance and will evaluate the effectiveness of these measures over time. She also noted the significant difference in enforcement activity between registrars and registries, with 97% of investigations targeting registrars, reflecting their primary role in abuse mitigation.

ICANN has begun publishing monthly enforcement reports to provide greater transparency on DNS abuse trends. The first six-month report, released in November 2024, details compliance actions, including the reasons for case resolutions – 52% of cases resulted in domain suspensions, while 12% were mitigated through registrant intervention. Castillo-Sojo emphasised that the amendments have already led to more active enforcement and improved compliance behaviour, but ongoing monitoring and further refinements will be necessary to sustain long-term progress in DNS abuse mitigation.

## 1.2 Contributions and main findings

Based on these lightning talks, the panelists provided a comprehensive analysis of the impact of generic Top-Level-Domain (gTLD) contractual amendments on DNS abuse mitigation, exploring trends, enforcement actions, and challenges in measuring progress. The group discussion focused on registry-level data, highlighting the difficulties in achieving consistent and meaningful statistics. One panelist noted an initial spike in ICANN Compliance reports following the amendments, with reports stabilising afterward, while also cautioning that increased reporting does not necessarily indicate increased abuse, but rather reflects improved reporting mechanisms. Another presenter reinforced this point, emphasising that nearly half of abuse reports lack sufficient evidence, delaying mitigation efforts. This sparked discussions on how to improve the submission of evidence, possibly through standardised reporting formats, automated verification checks, and better education and training for reporters.

A key challenge discussed was the measurement of harm caused by DNS abuse. Participants acknowledged the difficulty of quantifying harm, given the varied impacts of phishing, malware and other threats. It was also suggested that harm might be inferred through financial estimates, such as the cost of a malware-related data breach. However, phishing remains complex to measure, with variables such as the type of target (e.g., personal vs. business accounts) influencing the severity. A question was then raised regarding the issue of establishing consistent baseline metrics, inquiring whether the amendments have led to measurable improvements or if the industry is still in the early stages of impact assessment.

ICANN's enforcement capabilities were also debated, with one participant detailing ICANN Compliance's first six months of enforcement. ICANN launched 192 investigations, issued two formal Notices of Breach, and resolved 154 cases informally, leading to 2,700 abusive domain suspensions. While compliance measures have increased, questions remain about whether ICANN now has the necessary tools to enforce DNS abuse obligations effectively. Some panelists felt that progress is being made, but long-term evaluation is needed to assess the amendments' full impact. An additional member further noted that seasonal trends and emerging scams complicate enforcement, with criminals adapting tactics based on market trends and global events.

Another recurring theme was the need for better coordination between registries, registrars and hosting providers. Group members noted that while registries are not required to notify registrars of abuse, greater collaboration could speed up mitigation efforts. One member pointed to **NetBeacon Reporter**, a project that sends abuse reports directly to registrars, registries and hosting providers simultaneously, as a potential solution to streamline action. Additionally, metrics such as "client hold" status were discussed, with one member highlighting that while it works well for gTLDs, it is not standardised in country code Top-Level-Domains (ccTLDs), making uniform tracking more difficult.

Looking forward, improving consistency of measurement and refining compliance processes emerged as key priorities. In citing research indicating that policy changes typically take 9-12 months to show full impact, it was suggested that more substantial results may be seen in the coming months. Several panelists agreed that alignment on mitigation metrics – such as tracking time-to-mitigation from blocklisting vs. registration dates – is necessary for accurate impact assessment. Participants also pointed to the need for industry-wide discussions on refining abuse tracking, particularly regarding sinkholing, which can take down malicious domains without triggering traditional suspension indicators.

Overall, while early data suggests progress in enforcement and mitigation, panelists acknowledged that further improvements are needed in evidence collection, reporting consistency, and measurement methodologies. The discussion reinforced that DNS abuse is an evolving challenge, requiring continuous collaboration between industry stakeholders, ICANN Compliance, and cybersecurity experts to ensure effective long-term impact.

# 2. Segment: Automated vs. manual processing of abuse reports

## 2.1 Lightning talks by nic.at, SWITCH, and Realtime Register

- Robert Schischka, nic.at
- Michael Hausding, SWITCH (.ch) & FIRST.org
- Theo Geurts, Realtime Register

**Robert Schischka** of nic.at emphasised the importance of distinguishing between different sources when handling domain abuse reports. While automated processes can help speed up responses, manual intervention remains necessary, especially from the perspective of ccTLDs, which operate under distinct legal frameworks separate from ICANN regulations. He highlighted the challenge of dealing with a flood of abuse reports, many originating from unreliable sources, including orchestrated efforts by malicious actors. Schischka shared an example where competing Russian cybercriminal gangs attempted to use fraudulent takedown requests to undermine each other. However, law enforcement agencies were reluctant to act due to jurisdictional limitations, underscoring the difficulty in addressing such issues without strong legal backing.

He further discussed the complexities of trust in abuse reporting. While some trusted flaggers are legitimate, others may have biases or hidden agendas. He explained the dilemma between responding to takedown requests and adhering to contractual obligations, particularly when third parties demand quick action without assuming liability. Many takedown requests come from private companies expecting immediate response times, but without legal evidence or official backing, registries risk financial and legal consequences if they wrongly suspend a domain. He stressed that making qualified judgments in abuse cases is not straightforward, especially in areas like trademark disputes, hate speech in foreign languages, or cases where malicious actors change website content dynamically to evade detection.

In his conclusion, Schischka argued that while automation can enhance efficiency – especially in information sharing – fully automated decisions remain unfeasible unless liability is assumed by a trusted party. He accentuated how cybercriminals adapt their tactics to exploit registry procedures, citing examples where legitimate entities, including law enforcement and government ministries, mistakenly took down their own domains. Schischka also pointed out the inefficiencies in law enforcement's response times and the need for better collaboration between registries and authorities. Training for police, attorneys and judges could improve the handling of domain-related issues, as demonstrated in a successful yet short-lived initiative for addressing hate speech cases. Ultimately, he advocated for a balanced approach where technology aids decision-making, but human oversight remains crucial to prevent abuse and misjudgment.

**Michael Hausding** of SWITCH discussed how Switzerland's unique legal framework gives the registry direct responsibility for fighting cybercrime. Unlike in many other countries where registrars handle abuse reports, SWITCH receives and processes these reports, contacting registrants and registrars when necessary. He outlined the importance of threat intelligence sharing and distinguishing between threat intelligence data (patterns, tactics and indicators of compromise) and blocklists (immediate requests for takedown). By leveraging intelligence, SWITCH proactively detects malicious registrations, preventing domains from being activated if they show high-risk indicators. Hausding emphasised the benefits of collaborating with other European ccTLD registries, where shared intelligence helps identify threat actors migrating across different domain extensions. He also noted that open sourcing the .ch zone file increased the number of early warnings received from global researchers, particularly those outside of Europe.

Hausding also detailed how threat information reaches SWITCH, coming from data brokers, intelligence-sharing platforms (e.g., MISP, eCrimeX), national authorities and direct reports. He highlighted the challenges of using blocklists, explaining that many lists serve different purposes – some for email filtering, others for registries – and must be carefully evaluated to avoid false positives. He also discussed the automated and manual steps SWITCH follows when handling reports, such as verifying whether a domain is registered, delegated, resolving, and whether reported threats are accessible. The process involves semi-automated checks, but final takedown decisions remain manual to ensure accuracy and compliance with Swiss legal requirements. Hausding stressed that while automation improves efficiency, final actions still require human analysis, particularly in cases where cybercriminals use traffic redirection systems to obscure their activities. Ultimately, he called for continued improvement in threat intelligence sharing, automation in data processing, and structured reporting methods to help streamline cybersecurity efforts across the domain industry.

In his presentation, **Theo Geurts** of Realtime Register discussed the automation of cybercrime tracking using the Realtime Register Cybercrime Tracker, which processes data from reputation blocklists. Initially, the goal was simply to collect and analyse data, but it soon became clear that this information could be used to identify resellers with higher abuse rates, determine which TLDs are most and least abused, and assess the level of subdomain and URL abuse compared to domain name abuse. By automating data collection, the platform provided insights into the scale and distribution of abuse, revealing that URL abuse often outweighs domain abuse. Since many of the platform's resellers are hosting companies, they are in the best position to act on this information by addressing abusive content at the hosting level rather than relying solely on domain takedowns. Geurts highlighted how data-driven automation can enhance cybersecurity efforts by enabling targeted interventions rather than broad, often less effective, domain suspensions.

Geurts describes the evolution of their reputation blocklist system, which started with a dashboard solution offering video playback, API access, and email notifications for detected threats. To overcome the limitations of blocklists, which only provide domain names without context, they partnered with third-parties to obtain additional data, including screenshots, nameserver information and supplementary reports. The system allows resellers to manually review evidence through a dashboard or implement automated takedowns based on trusted sources like Google Safe Browsing. Looking ahead, they plan to expand automation capabilities for highly trusted reputation blocklist providers, particularly highlighting their strong relationship with third-parties, and integrate with NetBeacon Institute and CleanDNS APIs, enabling automated domain takedowns when reports meet specific parameters**.**

## 2.2 Contributions and main findings

The following discussion centred around the challenges of verifying identity documents in the context of domain registration and cybersecurity. One key issue raised was the lack of access to a centralised verification system for stolen passports, similar to how stolen credit cards are flagged in banking systems. As was noted, efforts to engage relevant authorities, including banks and financial regulators, are deemed to be unsuccessful, highlighting the fragmented nature of identity verification. While stolen passports are a common problem, an equally concerning trend is the use of passports from individuals unaware that their documents are being misused, such as students required to submit their passports for housing. Additionally, AI-generated forgeries make verification even more complex, as seen in cases where multiple passports with different photos but identical personal data were submitted for domain registrations. Without a reliable system to check the legitimacy of identity documents, distinguishing real applicants from fraudulent actors remains a significant challenge. Fortunately, ongoing discussions and collaboration between registries, law enforcement and technology experts offer hope for developing more efficient and secure verification methods in the future.

Another concern raised was the potential unintended consequences of stricter verification requirements. While increasing security measures aims to prevent fraud, it may also place a greater burden on legitimate individuals while failing to stop highly organised cybercriminals. A comparison was made to public transportation systems, where excessive security measures inconvenience law-abiding passengers while criminals find ways to evade detection. Participants stressed the need for collaboration between registries, law enforcement and verification systems to prevent abuse without disproportionately affecting legitimate users. A key takeaway was that clear legal frameworks are essential. Ultimately, cybersecurity efforts cannot solely rely on community-driven policies but require strong backing from law enforcement to ensure effective and enforceable solutions.

Participants highlighted significant advancements in the automation of abuse handling, with one attendee reporting that their organisation achieved response times under one minute for phishing and malware cases as of September 2024 through automated analysis and response systems. Automated interstitial warnings were introduced as an effective measure to protect users from phishing threats, while API-based reporting systems and specialised tools for trusted reporters were emphasised as key enablers for faster abuse response. While automation has greatly improved efficiency, attendees acknowledged the continued need for manual review to address false positives and refine automated processes. The discussion also covered how compromised websites can be automatically suspended and restored once secured, as well as the implementation of opt-in CSAM scanning tools for customers seeking proactive content moderation..

# 3. Segment: Cultural change within the industry

## 3.1 Lightning talks by Abusix and sys4 AG

- Tobias Knecht, Abusix
- Patrick Ben Koetter, sys4 AG

**Tobias Knecht** of Abusix provided insights into the evolution of abuse management within the Internet Service Provider (ISP) and hosting industry. Drawing from his 25 years of experience, he highlighted the sheer volume of abuse reports ISPs handle daily, with some companies receiving up to 500,000 abuse-related emails per day. Working alongside organisations like Shadow Server, Abusix processes and reports 8 to 10 million abuse cases every day, yet the overlap in reported abuse is surprisingly low: namely, less than 5% between major reporters. This suggests that the true scope of abuse remains vastly underestimated. While automation has improved abuse mitigation – some ISPs automate 95-98% of abuse handling – the lack of uniform enforcement mechanisms across ISPs and hosting providers remains a critical challenge. Unlike domain registrars, who now have compliance obligations enforced by ICANN, ISPs and hosting providers operate in a fragmented landscape without a central authority to ensure accountability.

He underscored the absence of mandatory enforcement mechanisms for ISPs and hosting providers, making it difficult to curb abuse effectively. He noted that some companies adopt "no-log policies", which prevent them from identifying malicious users even when faced with law enforcement requests. Despite regulations such as the Digital Services Act (DSA), many ISPs and hosting providers remain unaware of or indifferent to their obligations. The lack of enforcement allows bad actors to exploit loopholes, shifting operations to less regulated ISPs when faced with compliance measures. The contrast with the domain industry – where ICANN enforces stricter controls – demonstrates that regulation alone is insufficient without robust enforcement mechanisms to ensure compliance.

Knecht concluded that stronger enforcement, not just legislation, is essential to hold ISPs and hosting providers accountable. While the DSA provides a foundation, its definitions and reporting requirements are unclear and impractical for many providers. He advocated for an adapted enforcement model – similar to ICANN's approach but tailored to ISPs and hosting providers – to ensure that abuse reports are taken seriously, and appropriate action is taken. He stressed that even small to medium-sized ISPs making proactive changes have a measurable impact on reducing abuse, demonstrating that industry-wide enforcement could significantly disrupt malicious actors. Without enforcement, ISPs and hosting providers will continue operating in a cycle of inaction, allowing cyber threats to persist unchecked.

In his presentation, **Patrick Ben Koetter** of sys4 AG and Leader of the Anti-Abuse & Email Competence Groups at eco, focused on the evolution of anti-abuse measures within business platforms and the challenges companies face in addressing abuse effectively. He began by explaining the origins of the working group he leads, where members primarily operate business platforms and initially struggled to secure funding for abuse mitigation. The breakthrough came when they reframed anti-abuse efforts as a business case, demonstrating that investing in abuse prevention would ultimately save money and retain customers. By securing budgets, companies were able to develop internal tools to combat abuse, significantly reducing incidents and improving customer satisfaction. This internal control allowed them to take decisive action without external interference, ensuring a stable and secure platform environment.

The second phase involved collaboration with government entities to address abuse beyond individual platforms. As businesses implemented their own anti-abuse tools, they began engaging with authorities for cross-platform mitigation efforts, such as takedown operations and data sharing. This collaboration improved public perception and strengthened security measures but introduced new complexities, such as managing data sharing and regulatory compliance. Koetter highlighted that while this stage has proven effective, the current challenge lies in stage three: cross-platform collaboration between private entities. Unlike internal or government-driven initiatives, there is no established revenue model for businesses to justify investment in collaborative anti-abuse efforts. Companies struggle with the dilemma of spending resources on an issue that may not directly generate a profit. The presentation concluded by stressing the need for a clear business case, standardised communication, and trusted reporting mechanisms to facilitate effective cross-platform abuse mitigation.

## 3.2 Contributions and main findings

The discussion following the presentations by Tobias Knecht and Patrick Ben Koetter highlighted several key contributions and insights regarding anti-abuse efforts, business challenges and regulatory requirements. The scale of abuse incidents is staggering, with one server alone receiving 250-300 million spam incidents daily, plus an additional 500-600 million data points from other sources. Current monitoring captures less than 10% of total abuse, with 70,000-100,000 unique domain names being flagged in spam messages daily. This massive volume makes manual intervention impractical, underscoring the need for automation and collaboration. However, despite the availability of threat intelligence, many ISPs and hosting providers are reluctant to act, as there is no clear financial incentive to do so. Without a business case demonstrating profitability or cost-saving benefits, many entities remain disengaged from proactive measures to prevent abuse.

Another key issue discussed was the legal landscape surrounding abuse mitigation. While some jurisdictions enforce "coastal liability", meaning that companies are responsible for abuse on their platforms once they are aware of it, practical enforcement remains a challenge. The idea of filing millions of lawsuits or relying solely on legal action is impractical. There was broad agreement that while legal measures are necessary, they alone cannot solve the problem. Effective anti-abuse strategies require a combination of legal frameworks, corporate responsibility and market incentives that encourage action against cyber threats.

The business case for dedicated anti-abuse teams was another important point of discussion. Some businesses have successfully integrated anti-abuse strategies by creating dedicated teams to handle abuse, rather than leaving it to general customer support. One participant shared their success story of establishing a dedicated two-person team that focused solely on abuse management, allowing them to develop deeper expertise, create automated systems, and share intelligence with industry peers. This specialisation enables companies to gain deeper insights into cybercrime patterns and develop more effective solutions. The challenge, however, is convincing more companies – especially larger ISPs and hosting providers – that investing in dedicated abuse prevention is a sound business decision. While some smaller companies can benefit financially from anti-abuse initiatives, larger companies often see abuse management as a non-priority, as it does not significantly impact their revenue streams.

A significant debate emerged about the role of reputation in tackling abuse. Some participants argued that reputation serves as an alternative form of currency in the industry, with businesses increasingly considering the reputation of service providers when choosing partners. Companies known for negligent anti-abuse measures may lose business opportunities over time. However, scepticism remained, as some of the biggest players in the industry continue to thrive despite poor reputations regarding abuse management. The analogy of soft drinks – being widely recognised as unhealthy but still selling in massive quantities – was used to illustrate how reputation alone may not be enough to force industry-wide change.

Regulation was widely discussed as both a potential solution and a challenge. Some participants leaned toward regulatory intervention, arguing that without clear rules and enforcement, companies will not voluntarily act against abuse. Historical examples, such as the reduction in marketing spam following the introduction of double opt-in requirements, demonstrate how regulatory frameworks can successfully reduce certain types of abuse. The concern, however, is that overly rigid regulations might create unintended barriers, particularly for smaller companies that lack the resources to comply. Additionally, enforcement remains a challenge, as abuse is often a chain of events spanning multiple platforms and jurisdictions. The example of fraudulent credit card transactions was cited, where financial institutions often fail to act quickly enough to prevent cascading abuse incidents.

Finally, the discussion touched on the broader systemic challenges of abuse mitigation. The need for better collaboration between private companies, regulatory bodies and financial institutions was emphasised. Some participants suggested that penalties for inaction – such as financial consequences for credit card companies failing to verify transactions properly – could drive better behaviour. However, others pointed out that many companies find it cheaper to absorb collateral damage rather than invest in comprehensive anti-abuse measures. The conversation ultimately highlighted the complexity of the issue, requiring a multi-faceted approach that balances business incentives, regulatory measures and industry-wide cooperation.

# 4. Segment: A Forum for Internet Infrastructure Operators to coordinate anti-abuse efforts

## 4.1 Lightning talks by Verisign and Internet & Jurisdiction Policy Network

- Keith Drazek, Verisign
- Bertrand de la Chapelle, Internet & Jurisdiction Policy Network

**Keith Drazek** of Verisign introduced the Internet Infrastructure Forum (IIF) as a new platform designed to bring together Internet infrastructure operators, including registries, registrars, web hosts and Content Delivery Networks (CDNs), to collaborate on mitigating online abuse. The idea emerged from discussions at the Internet Jurisdiction Policy Network meeting in May 2022, where it became clear that while ICANN and contracted parties focus on technical abuse – such as phishing, malware and botnet control – there was a missing voice in the conversation: web hosts and content providers. These entities are often in a better position to take targeted action against harmful content rather than resorting to broad domain takedowns, which can cause unintended consequences. The IIF was conceived as a venue separate from ICANN, allowing these stakeholders to communicate, share information, and develop best practices for handling both technical and content-related abuse, while maintaining their respective responsibilities and technical capabilities.

As Drazek noted, the IIF seeks to become a long-term framework for industry self-regulation, interfacing with notifiers, regulatory bodies and other Internet stakeholders. Unlike ICANN, which is legally restricted from content moderation, the IIF provides a space for discussions on tackling content-related harms, fostering self-regulation and collaboration among key players. The forum is still in its early stages, having successfully convened industry participants to explore new information-sharing mechanisms and cooperative strategies. Ultimately, the goal is to create a structured, industry-led approach to mitigating abuse, ensuring that infrastructure providers work together more effectively to combat online threats while maintaining a free and open Internet.

**Bertrand de la Chapelle** of the Internet & Jurisdiction Policy Network also discussed the evolution of the IIF as a necessary platform for addressing content-related harms beyond the scope of ICANN's DNS abuse policies. He highlighted those efforts to combat DNS abuse date back to 2012, with years of stalled progress due to definitional debates over what constitutes abuse. As he pointed out, the breakthrough came when stakeholders moved beyond semantic disagreements and established a minimum standard for addressing phishing, malware and botnets through ICANN's compliance mechanisms. However, he indicated that DNS takedowns alone are often insufficient because malicious sites can still be accessed via alternate domains or IP addresses, requiring intervention at the hosting level. Since ICANN is legally prohibited from engaging in content moderation, he recommended a clear need for a separate, neutral space where hosting providers, CDNs, and other infrastructure operators can coordinate on tackling website-based abuse.

As he also quoted, the IIF was created as an independent, multi-stakeholder initiative to improve cooperation, information sharing and enforcement mechanisms across the broader Internet infrastructure landscape. Unlike registries and registrars, which operate under ICANN's governance, hosting providers are seen to lack a centralised structure, making coordinated action difficult. The IIF therefore aims to fill this gap by facilitating dialogue between hosting providers, CDNs, public authorities and other stakeholders with registries and registrars to create best practices and industry-driven solutions for abuse mitigation. As he stated, recent exploratory meeting with 50 participants from Europe and the U.S. revealed strong interest in formalising cooperation, particularly in reducing redundant enforcement actions (such as the "whack-a-mole" effect of repeated takedowns without addressing the root issue). From his perspective, participants recognised the need for automation, data sharing and bridging the silos between DNS operators and hosting providers to increase the speed and efficiency of abuse mitigation efforts.

While still in its early stages, de la Chapelle pointed out that the IIF seeks to become a long-term framework for industry self-regulation, interfacing with notifiers, regulatory bodies and other Internet stakeholders to improve enforcement capabilities without overburdening responsible actors. One of the key challenges he identified is the balancing effective anti-abuse measures with minimising unintended burdens on legitimate businesses and users. As he noted, the IIF aims to develop guidelines, codes of conduct, and scalable solutions that enable infrastructure operators to proactively combat abuse while maintaining an open and resilient Internet. De la Chapelle emphasised that while industry-led action is essential, public authorities may eventually need to engage to ensure that enforcement mechanisms remain effective against bad actors. The IIF thus represents a critical step in fostering greater coordination and accountability within the broader Internet infrastructure ecosystem.

### 4.2 Contributions and main findings

The follow-on discussion on the Internet Infrastructure Forum (IIF) highlighted both the enthusiasm for collaboration among different industry stakeholders and the complexity of coordinating efforts across different layers of the Internet infrastructure stack. Participants noted that while key industry players understand their own responsibilities, they often lack visibility into the capabilities and constraints of others, which has historically hindered collaboration on abuse mitigation. Key challenges identified included legal barriers, data-sharing restrictions, and inconsistencies in technical implementations, such as differences in hosting environments – from shared servers to dedicated hosting and co-location services. Understanding these technical distinctions is regarded as essential for ensuring that abuse mitigation strategies are targeted, proportionate and effective.

A key takeaway was the need for a more integrated, ecosystem-wide approach to combating abuse, rather than relying on fragmented, sector-specific solutions. As it had been noted, the ICANN community has long struggled with responsibility-shifting, where different entities defer action to others rather than addressing abuse collectively. However, as abuse cases increasingly span multiple levels of the infrastructure stack, it has become clear that isolated interventions are insufficient. Many participants referenced the Digital Services Act (DSA) as a useful framework for defining responsibilities, even for entities not directly bound by it. There was broad agreement that clearer expectations for ISPs, hosting providers and registrars would improve enforcement, although concerns were raised that regulatory uncertainty has left many companies hesitant to act for fear of misinterpreting their obligations. The discussion reinforced that effective abuse mitigation requires a concerted effort, ensuring that all relevant stakeholders work together in accordance with their respective roles, responsibilities and capabilities, rather than shifting responsibility.

Looking ahead, there was strong support for regular engagement and structured workstreams, rather than limiting discussions to one-off or annual meetings. A number of participants emphasised the importance of identifying internal "evangelists" within major organisations who can champion these initiatives across different business units. The immediate focus will be on breaking down into specialised workstreams addressing narrowly defined abuse mitigation challenges, with the goal of building consensus before publishing key outcomes. Lessons from successful industry-led initiatives – such as the Global Cyber Alliance's project **MANRS** on mutually agreed routing security – suggest that measurable, self-regulated frameworks can prevent overreach from external regulators while ensuring effective enforcement. To achieve this, it is perceived that the IIF will prioritise automation, improved data-sharing mechanisms and trust-building across stakeholders, laying the groundwork for a more cohesive and proactive approach to mitigating online abuse.

## 5. Open Discussion: How can we get all stakeholders to play their part?

The final discussion covered several key points around bridging silos and ensuring that all stakeholders actively contribute to mitigating online abuse. Participants explored challenges related to financial incentives, shared responsibility and improving coordination, recognising that a business-as-usual approach is unlikely to be sufficient..

### Incentives and pricing models:

- Participants discussed potential pricing models to make abuse-fighting services more accessible, especially to smaller companies that struggle with the costs of security intelligence and enforcement. Ideas included discounted or subsidised pricing models to lower financial barriers.
- Examples were given of registries offering fee reductions to registrars with low abuse levels, serving as an incentive to improve security practices. The group considered whether ICANN could introduce similar incentive structures at a broader level.
- However, there was some scepticism about whether financial incentives alone would be sufficient to drive meaningful change, particularly for large industry players whose business models are not significantly impacted by small financial adjustments.

### Shared responsibility and the public good:

- A key theme was whether online abuse mitigation should be seen as a shared public responsibility, rather than just a business challenge. The sheer scale of the problem has outpaced traditional law enforcement capabilities, leading to greater reliance on the private-sector.
- Some participants emphasised that abuse prevention should be framed as a moral and social obligation, even if the direct business case is not always clear.
- The discussion also touched on the outsourcing of enforcement to the industry, raising concerns about companies being expected to act as investigators and enforcers without public funding or support. Participants explored how the "public good" aspect could be better integrated into industry initiatives without placing an excessive burden on businesses.

### Improving information sharing and coordination:

- Participants discussed ways to improve sharing of information and intelligence and coordination between different industry players to enable more effective and timely abuse mitigation.
- Services such as **NetBeacon Reporter** were highlighted as positive steps in providing standardised reporting mechanisms and improving the flow of security data between registries, registrars and hosting providers.
- However, there was caution against simply "dumping" data on companies, which can lead to information overload. Instead, the focus should be on tailoring reports to meet the specific needs of each entity, ensuring they receive actionable information, evidence and intelligence rather than excessive raw data.
- Jurisdictional and regulatory challenges were also identified as barriers to sharing information and intelligence, as companies must navigate differing legal requirements across regions.

The final discussion reinforced that there is no single solution to the challenge of online abuse. Instead, a multi-faceted approach is needed – combining financial incentives, shared responsibility and improved coordination. While some progress has been made, participants generally agreed that existing models may not be sufficient, and that new strategies and collaborative frameworks – to which the IFF could contribute to as a platform for discussion and development – will be required moving forward.

# 6. Summary of Findings & Conclusions

The workshop showed that, for most of the recommendations, there are already solutions, tools and people addressing and working on them. The following points seem to have been supported as priority actions by most, though not all, participants:

## Contract amendments – Is there a measurable impact?

- **ICANN's enforcement efforts:** For example, five-year retrospective of DNS abuse mitigation, including new tools such as Metrica and INFERMAL.
- **Mitigation trends:** Early data shows increased mitigation rates (from mid-80% to over 90%) following April 2024 amendments.
- **ICANN compliance actions:** Over six months, 192 investigations led to 2,700 domain suspensions and two breach notices. Research showing that policy changes typically take 9-12 months to show full impact.
- **Challenges in measurement:** Reports suggest increased abuse reporting does not always indicate higher abuse but improved detection.
- **Ongoing monitoring:** Future improvements needed in evidence collection, reporting accuracy, and enforcement effectiveness.
- **Registrar compliance:** The 20 registrars with the highest abuse volume accounted for 80% of incidents, but they were not necessarily the largest registrars.
- **Measuring of harm:** Participants acknowledged the difficulty of quantifying the harm, given the varied impact of phishing, malware and other threats**.**

## Automated vs. manual processing of abuse reports

- **Efficiency of automation:** While automation speeds up response times, manual intervention remains necessary to ensure accuracy and compliance with legal requirements.
- **Legal and trust issues:** Many abuse reports come from unreliable sources; law enforcement agencies often face jurisdictional limitations.
- **Threat intelligence:** Legal frameworks like in Switzerland leverage intelligence-sharing to prevent malicious registrations.
- **Data verification challenges:** The nature of identity verification frameworks is fragmented, lack of a centralised stolen passport verification system complicates identity checks.
- **Balancing security and usability:** Strict verification measures may deter legitimate users while failing to stop organised cybercriminals.
- **Called for continuous improvement:** Threat intelligence sharing, automation in data processing, and structured reporting methods to help streamline cybersecurity efforts across the industry.

## Cultural change within the industry

- **ISP and hosting challenges:** Internet Service Providers (ISPs) process millions of abuse reports daily, but there is no centralised enforcement mechanism.
- **Regulatory gaps:** Unlike ICANN-regulated registrars, ISPs and hosting providers lack binding compliance requirements.
- **Legal certainty:** Clarity, not more legislation, is essential. Despite existing regulations, providers too often remain indifferent to their obligations. For example, while the DSA provides a foundation, its definitions and reporting requirements are unclear and impractical for many providers.
- **The business case for abuse prevention:** Some businesses successfully reduced abuse through dedicated anti-abuse teams.
- **Reputation as a driver:** Companies with weak anti-abuse measures risk losing business partnerships.
- **Systemic barriers:** Many companies prefer absorbing the costs of abuse rather than investing in preventative measures.

## A Forum for Internet Infrastructure Operators to coordinate anti-abuse efforts

- **Purpose:** Designed to bring together registries, registrars, hosting providers and Content Delivery Networks (CDNs) to tackle online abuse collaboratively.
- **Separation from ICANN:** ICANN must not engage in content moderation, necessitating a new venue for discussions on ontent-related harms.
- **Early-stage development:** Industry players are exploring new information-sharing mechanisms and enforcement strategies.
- **Multi-stakeholder engagement:** Plans to include law enforcement, regulators, and industry partners to enhance accountability.
- **Challenges in coordination:** Legal and technical inconsistencies across hosting environments require a structured, industry-led approach.

## Getting all stakeholders involved

- **Financial incentives:** Suggestions included discounted pricing for smaller companies and registry fee reductions for low abuse registrars.
- **Shared responsibility:** Participants discussed whether abuse mitigation should be framed as a public good rather than just a business challenge.
- **Intelligence sharing:** Improved data-sharing mechanisms are needed but should avoid overwhelming companies with excessive raw data.
- **Bridging silos:** The need for a more integrated, ecosystem-wide approach to tackling abuse, rather than relying on fragmented, sector-specific solutions.

## Final takeaways

- **No single solution:** A multi-faceted approach combining incentives, compliance enforcement, and better coordination is necessary.
- **Industry collaboration is critical:** The success of anti-abuse efforts depends on joint participation from registries, registrars, ISPs, and regulators.
- **Moving forward:** More research, standardised enforcement mechanisms, and structured workstreams are needed to improve long-term abuse mitigation.
- **Shared responsibility:** Tackling online abuse should be seen as a shared public responsibility, rather than just a business challenge. The sheer scale of the problem has outstripped traditional law enforcement capabilities, leading to greater reliance on the private sector.

Thomas Rickert concluded the workshop by expressing gratitude to all participants and giving special thanks to Lars Steffen from the eco Association for his efforts in ensuring the seamless preparation and delivery of the event.

## 7. List of Appendices:

Annex 1: eco slide deck

Annex 2: topDNS Abuse Table

Annex 3: dotmagazine "State of the DNS"

Annex 4: ICANN slide deck Timeline

Annex 5: ICANN slide deck Enforcement

Annex 6: NetBeacon Institute slide deck

Annex 7: NetBeacon Institute handout

Annex 8: CleanDNS slide deck

Annex 9: nic.at slide deck

Annex 10: SWITCH slide deck

Annex 11: sys4 slide deck

topDNS

An initiative by eco

**eco – Association of the Internet Industry**
Lichtstr. 43h, D-50825 Cologne, Germany
phone: +49(0)221/700048-0
info@eco.de, https://international.eco.de
@ecoverband

eco

ASSOCIATION OF THE INTERNET INDUSTRY