



2025 Abuse Workshop at Nordic Domain Days in Stockholm

- **Date & Time:** 29 April 2025, 13.30 – 17.00 CEST
 - **Organizer:** eco's topDNS Initiative & iQ Global
 - **Target Audience:** Domain name registries, registrars, hosting providers, ISPs, cybersecurity experts, and other key stakeholders in the domain industry.
-

Executive Summary

The 2025 Abuse Workshop at [Nordic Domain Days in Stockholm](#), co-hosted by [eco's topDNS Initiative](#) & iQ Global, convened a cross-sector group of stakeholders across the Internet infrastructure ecosystem – including registrars, registries, hosting providers, and ISPs.

Building on discussions from the Internet Infrastructure Forum (IIF) in Amsterdam earlier in 2025, the workshop explored cross-industry collaboration as a key element to address the growing scale and sophistication of online abuse. Traditionally, registries, registrars, hosting providers and other infrastructure operators have worked in isolation – often pointing fingers rather than partnering to resolve incidents. At the IIF, participants urged to bridge these silos by first acknowledging the very different volumes and workflows each segment faces and understanding one another's constraints and capabilities to help all parties converge on a shared, effective response.

The workshop brought together diverse voices. Keith Drazek of Verisign stressed alignment between regulation and voluntary industry safeguards to build a resilient DNS ecosystem. Dennis Dayman from M3AAWG reiterated the long-standing value of global, cross-sector cooperation. Bertrand de la Chapelle of the Internet & Jurisdiction Policy Network called for proportional, jointly governed spaces beyond ICANN's DNS-only mandate, laying the groundwork for the IIF – a multi-stakeholder forum where registries, registrars, hosting providers, content platforms and others can exchange intelligence, coordinate takedowns and develop best practices.

Adam Eisner of CIRA shared how .ca keeps abuse low through practical residency rules, modest pricing and swift law-enforcement partnerships – yet acknowledged that manual



processes must evolve toward proactive, automated detection as threats and regulations escalate. Kristian Ørmen of Internetstiftelsen (.SE) demonstrated how delegating abuse-data validation to registrars – flagging domains with invalid WHOIS under new agreements—scales effectively, enabling registrars to verify or suspend suspect domains at speed while the registry focuses on priority incidents.

Mo Zaman and Ivan Hadzhiev from DMARC Advisor illustrated two DNS-centric threats: clients' outdated SPF records, which enabled 2.3 million spam messages before correction, and “dangling” CNAME records, which attackers re-registered to host massive phishing campaigns. Their experience underlines that robust decommissioning processes, strict change-control procedures and strong authentication are vital first lines of defense.

Under the IIF umbrella, four workstreams have been launched: harmonizing legal and regulatory approaches (notably in the EU), automating abuse workflows via APIs and structured notice formats, piloting phishing as a case study for cross-layer interventions, and improving responses to CSAM and non-consensual imagery through trusted notifier networks. The emphasis is on shifting from reactive removals to proactive prevention, sharing post-incident data to strengthen deterrence and build systemic resilience.

It was acknowledged that legal advisors sometimes hinder rapid collaboration, but that a robust legal framework - one that accepts measured risk - is indispensable for enabling timely information-sharing and joint action. Drawing on his own experience shepherding the Internet Infrastructure Forum's (IIF) legal and policy track, Rickert underlined the need to clarify constraints imposed by NIS2, the Digital Services Act, and privacy regimes so that organizations can confidently share non-personal data to mitigate abuse.

Operationally, Rowena Schoo of the NetBeacon Institute demonstrated how enriched, standardized reports—delivered through integrated threat feeds and APIs—can streamline abuse handling for both large and small operators. Theo Geurts of Realtime Register argued that consistent abuse indicators, rapid registrar vetting and automated feedback loops are critical to maintaining trust and efficiency. Speakers from Netcraft, iQ Global and DomainCrawler showcased AI-driven intake systems, conversational reporting agents and multilingual translation layers that convert unstructured reports into machine-readable schemas like XARF. By guiding reporters to supply complete evidence packages and notifying all relevant parties simultaneously, these tools promise to reduce manual burdens, eliminate duplicate efforts and accelerate mitigations.



Despite the technical, legal and organizational challenges, the workshop concluded with broad agreement on three imperatives: adopt a shared data format (XARF or equivalent), stand up a neutral coordination hub to track actions and feedback, and pilot playbooks that define when and how hosting providers, registrars and registries should be alerted. By the next Nordic Domain Days, participants aim to demonstrate tangible improvements – wider standards adoption, faster takedowns and stronger cross-industry trust – validating the collaborative model as the future of online abuse response.



Context and Facilitation

The workshop was hosted and moderated by the following colleagues:

- **Thomas Rickert**, Director Names & Numbers
eco – Association of the Internet Industry
- **Lars Steffen**, Head of International, Digital Infrastructure & Resilience
eco – Association of the Internet Industry
- **Su Wu**, COO
iQ Global

Opening remarks by **Michael Halverson** of iQ Global emphasized the workshop's significance: *"This session has become a cornerstone – an important opportunity for us to share information and insights in the industry and to collaborate in the combat against DNS abuse."*

Expert Speakers

Official Speakers	Organization
Keith Drazek	VP of Policy & Government Relations, Verisign
Dennis Dayman	M3AAWG (Messaging, Malware, and Mobile Anti-Abuse Working Group)
Bertrand de La Chapelle	Executive Director, Internet & Jurisdiction Policy Network
Rowena Schoo	Director of Programs and Policy, Netbeacon Institute
Luke Wood	Infrastructure Partnerships Lead, Netcraft
Rickard Vikström	Founder, DomainCrawler
Theo Geurts	CIPP/E Privacy & GRC Officer, Realtime Register
Mo Zaman & Ivan Hadzhiev	Implementation Consultants, DMARC Advisor
Adam Eisner	Vice President, .CA and Registry Services, CIRA
Kristian Ørmen	Vice President, Registry Services, Internetstiftelsen



Key Themes and Discussions

Why Cross-industry Collaboration is Needed to Fight Abuse Across the Stack

Thomas Rickert emphasized the need for stronger cross-industry collaboration in combating online abuse. Historically, different segments – like registries and hosting providers – have operated in silos, often blaming each other rather than working together. While initial outreach efforts met resistance, there's now growing momentum toward bridging these gaps. Rickert highlights the importance of understanding each other's operational realities, noting stark differences in abuse report volumes and workflows. The goal is to find common ground and build a more unified and effective approach to tackling abuse across the internet ecosystem.

Rickert (eco Association) stressed the importance of a robust legal framework in the fight against abuse and reflected on the significant progress made in recent years. He spoke about the expansion of initiatives such as the NetBeacon Institute, which now has a broader scope than DNS abuse, including the hosting industry and other types of online abuse. Rickert also pointed out that while lawyers can sometimes limit collaboration, their role is essential in navigating legal complexities. He emphasised the need to take calculated risks in the pursuit of change: *"You might not have 100% solution or certainty with what you're doing. But if we want to collectively bring about a change, we need to move, not just analyse and find excuses as to why we can't do certain things."*

The diverse group of experts offered unique insights into the challenges and potential solutions for domain abuse management. For example, **Keith Drazek** (Verisign) pointed out the importance of aligning regulatory frameworks with industry self-regulation to effectively combat domain abuse. He highlighted that collaboration between policy and technical communities is essential for a resilient, long-term strategy, and asserted the need to balance oversight with industry-led initiatives to protect the DNS ecosystem.

Dennis Dayman, representing the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), emphasized the group's long-standing commitment to collaboration in fighting abuse, including the Internet Infrastructure Forum. He stressed that combating abuse requires global, cross-sector cooperation, regardless of region or technical background.

Bertrand de La Chapelle (Internet & Jurisdiction Policy Network) argued that a proportionate and coordinated approach is essential, especially when addressing abuses that straddle the line between technical and content-related issues. Historically,



DNS abuse discussions within ICANN were limited by its mandate. To address this, new collaborative spaces are needed that go beyond ICANN's remit and include actors across the entire digital ecosystem, such as hosting providers, infrastructure services, and abuse mitigation experts.

This led to the creation of the **Internet Infrastructure Forum (IIF)** – a multi-stakeholder initiative designed to bridge gaps in cooperation across different parts of the ecosystem. The IIF aims to create a trusted, operational space for actors dealing with abuse to coordinate, exchange actionable intelligence, and develop best practices. Content-related harms, are a central focus and require layered, synchronized action across DNS operators, hosting providers, and content platforms to effectively disrupt abuse cycles.

The initiative includes four major workstreams: examining legal and regulatory frameworks (particularly those emerging from the EU), improving automation in abuse handling (e.g., using APIs or structured notice formats), testing phishing as a cross-layer case study, and tackling CSAM and non-consensual imagery through improved engagement with trusted notifiers. The overarching goal is to move from reactive interventions toward preventative strategies. By sharing post-abuse intelligence, the forum hopes to strengthen deterrence mechanisms and foster greater systemic resilience.

Ultimately, the IIF's work is grounded in building trust among diverse actors who often face internal constraints and public pressure. Many abuse response teams operate under tight resources while simultaneously being criticized for doing too little. The forum aims to create a balanced, cooperative environment where infrastructure providers can act responsibly, transparently, and proportionately – laying the groundwork for a more sustainable, trust-driven model of internet governance.

From a further angle, **Rowena Schoo** (NetBeacon Institute) addressed the operational side of DNS abuse mitigation, focusing on the importance of accessible tools for reporting and response. Their service *NetBeacon Reporter* streamlines abuse reporting by enriching, standardizing, and routing reports to the right registrars and hosts. Integrated with threat feeds and APIs, the tool aims to improve report quality, expand harm categories beyond DNS abuse (e.g., smishing, fake webshops), and build trust-based collaboration. She noted the challenges faced by smaller operators and called for scalable, collaborative solutions that enable broader participation in combating abuse across the domain name space. Schoo highlighted alignment with the Internet Infrastructure Forum (IIF) as crucial to driving this ecosystem-wide effort forward.



Fighting Online Abuse: Legal and Policy Aspects

Thomas Rickert introduced himself as shepherd of the IIF’s legal and policy track, intended not to obstruct collaboration but to enable it by clarifying legal constraints and overcoming “excuses” that deter information sharing. At IIF’s inaugural meeting, participants pinpointed three priority areas: adapting to NIS2’s fragmentation challenges within its network-security mandate; improving the practicality of DSA transparency reporting through dialogue with legislators; and demystifying GDPR and similar privacy laws globally to agree on shareable, non-personal data for abuse mitigation. Rickert stressed that while risk aversion is natural, true progress demands calibrated risk-taking, collective action, and the creation of best-practice resources – potentially including pooled legal guidance – to empower more organizations to join the “good citizens club” of internet abuse fighters. He stressed that legal frameworks must enable, not inhibit, timely abuse response and collaboration.

Operational Aspects and Automation

Several speakers highlighted the need for better feedback mechanisms to manage domain abuse more effectively:

- Across the session, a key takeaway across was also the shared agreement on the need for **standardized data formats**, with XARF emerging as a leading candidate. Participants emphasized the importance of a flexible reporting ecosystem, where reports – whether via email, web form, or API – are translated into a machine-readable format, such as X-ARF. This led to the popular “translation layer” analogy, which suggests a unified schema bridging different input and output preferences. **Michael Duffy** (Excedo Networks) called for a universal format for abuse reporting.
- **Automated Feedback Systems:** Thomas Rickert suggested creating a centralized function to aggregate abuse information, providing stakeholders with real-time updates on which parties have taken action. This initiative aligns with the broader IIF goals of transparency and communication.
- **Standardization:** Theo Geurts (Realtime Register) highlighted the critical need for consistency in how abuse indicators are applied across the domain space. He argued that weak enforcement, due to high costs and backlogged legal systems, exacerbates online crime, and that registrars must focus on both **prevention** (e.g., stricter reseller vetting) and **mitigation**. For mitigation, he recommended

adopting automated abuse-reporting via APIs, enriching reports with threat intelligence and screenshots, and using standardized formats like **XARF** for swift takedowns – while building in safeguards and rapid false-positive recovery to balance efficiency with accuracy. Geurts also pointed out the challenges posed by the lack of standardized feedback mechanisms, which can impede effective communication and collaboration. Geurts urged for a global standardization of abuse reporting and response processes across all registries to improve cross-domain communication and ensure that abuse is mitigated more efficiently.

- **Artificial Intelligence (AI) and Data Aggregation:**

- **Michael Halvorsen** (iQ Global AS) brought up the very important point of user-friendliness for the end user. He argued that email remains a low-friction reporting channel for senders, but acknowledged its unstructured nature is a burden for receivers. They proposed leveraging AI as an intermediary: an AI assistant could parse incoming emails, automatically request missing evidence or clarifications, and only forward fully-formed reports to backend systems. This approach maintains email's ease of use for reporters while ensuring receivers obtain the structured data they need.
- **Luke Wood** (Netcraft) emphasized the strain on small abuse teams – receiving up to 600 reports daily – and the need for standardized, automated reporting methods, noting Netcraft's use of XARF and its newly launched API to replace unreliable email and form submissions. Wood also described how trusted partners have granted “kill switch” privileges, allowing Netcraft to immediately disable abusive content at scale, underscoring both the industry's reporting challenges and evolving solutions.
- **Su Wu** (iQ Global AS) highlighted how AI can drastically improve abuse handling by transforming static reporting forms into interactive, conversational intake systems that guide reporters, automatically build rich evidence packages, and format them to each recipient's preferences. She described using AI-driven workflows and “abuse agents” to triage incoming reports – automatically closing clearly invalid cases, prioritizing high-risk ones, and routing them appropriately – thereby reducing human workload by up to 80%. Finally, Su noted AI's strength in pattern recognition for proactive abuse identification, enabling earlier intervention in the domain lifecycle while reserving human review for the more ambiguous, high-stakes cases.



- **Rickard Vikström** (DomainCrawler) called for expanding abuse-fighting collaboration beyond Europe to a truly global scale, starting with overcoming language and communication barriers that prevent reporters from reaching the right contacts at non-English-speaking hosts and registrars. He stressed the need for a universal, multilingual reporting format and processes to help reporters identify which individual or team actually cares about and can act on a given abuse case.

He also highlighted the inefficiency of “scattergun” reporting – where a single abuse incident is sent to multiple parties – which creates duplicate workloads and confusion. He advocated for building feedback loops into reporting systems so that once one provider takes down the abusive content, all other stakeholders are notified, preventing redundant reports and streamlining the mitigation process.

Discussion

The group agreed that the focus should shift from debating reporting channels (email vs. web form vs. API) to ensuring **reports are as easy as possible to submit** while still delivering **structured, actionable data**. Email remains a low-friction option – especially for lay users – but AI or intermediary services (e.g., NetBeacon) can prompt reporters for missing evidence and translate incoming messages into standardized formats like XARF. Professional reporters need scalable APIs to handle high volumes, whereas individual end users benefit from a simple “send email and get a confirmation” experience.

Crucially, participants highlighted the emergence of a **two-sided marketplace** of notifiers and receivers bridged by **intermediary platforms** that aggregate, enrich, prioritize, and dispatch abuse notices. This ecosystem approach accommodates everyone – from solo reporters to brand-protection teams—by offloading complexity to specialized intermediaries, fostering **trust, uniform standards**, and **feedback loops** so that once one actor mitigates an abuse, others are automatically informed. This model promises to balance ease of reporting with the operational needs of varied recipients and to scale with evolving regulatory demands.



The Role of Information Sharing in Domain Abuse Management

Information sharing plays a critical role in improving the speed and accuracy of responses to domain abuse. Two models of information sharing were discussed:

1. **One-to-One Sharing:** Bertrand de La Chapelle highlighted the importance of direct communication between stakeholders when an abuse case is identified. This would ensure that all parties involved take appropriate action to resolve the issue, including registrars, registries, and hosting providers.
2. **Large-Scale Data Sharing:** De La Chapelle also explored the possibility of aggregating abuse data from multiple sources to identify broader abuse patterns. While this approach holds promise, privacy concerns were raised, emphasizing the need for careful management of sensitive data.

Phishing and Other Malicious Online Activities

Mo Zaman and **Ivan Hadzhiev** (DMARC Advisor) illustrated two prevalent DNS-related abuse scenarios. First, **Mismanaged DNS** - exemplified by a client's outdated SPF record that included shared-host IPs, which attackers exploited to send 2.3 million spam messages before the record was corrected. Second, **DNS Dangling/CNAME Takeovers** – where forgotten CNAME records (e.g., pointing to decommissioned Azure resources) allowed criminals to rent the same hostnames and launch large-scale phishing campaigns, with hundreds of thousands of messages sent from dozens of IP ranges.

To combat these risks, they recommended strengthening **prevention and mitigation** practices: implementing rigorous **decommissioning processes** for retired DNS records; enforcing **strong user authentication**, role-based access, and password policies for DNS management; and establishing formal **change-control procedures** to ensure DNS records are reviewed and updated. These measures help close the gaps that attackers exploit in shared infrastructure and forgotten DNS entries.

Adam Eisner (CIRA) explained that .ca's relatively low abuse rates stem from a combination of practical policies and strong partnerships rather than any "magic bullet." Key factors include a Canadian-nexus residency requirement that filters out many bad actors, a modest but responsive abuse team bolstered by threat feeds from CIRA's free Canadian Shield DNS firewall, and quick internal review processes. Close relationships with Canadian law-enforcement and regulators – who know the domain ecosystem well – also enable swift, cooperative action on abuse.



Eisner noted that CIRA’s affordable, non-promotional pricing (no deep discounts) further discourages bulk malicious registrations. However, he acknowledged that these manual and policy-based measures are only a starting point: increasing regulatory demands, ICANN contractual obligations, and evolving cyber threats mean CIRA must move toward more automated, proactive abuse detection and mitigation tools. He stressed the importance of maintaining constructive dialogues with authorities to stay ahead of enforcement and technological developments.

Kristian Ørmen (Internetstiftelsen) explained how the registry shifted much of the abuse-fighting workload onto registrars by leveraging incorrect registrant data as a clear, enforceable trigger. Rather than wading into content disputes, .SE flags domains with invalid or obviously fake WHOIS details – information any third party (including abuse monitors) can report – and under updated registrar agreements, registrars must verify or deactivate those domains within set deadlines. This approach scales more easily than debating “what is abuse,” since registrars can quickly confirm data accuracy and act without lengthy policy discussions.

Ørmen acknowledged that as criminals begin supplying valid-looking data (e.g., correct company names with only an email tweak), the method will grow more complex, especially for non-Swedish registrants. .SE combats this with dedicated data analysts who continuously scan for anomalies – currently preparing to notify registrars about over 30,000 domains with suspect data – and prioritize cases tied to clear abuse. While not a silver bullet, rigorous WHOIS validation coupled with automated registrar notifications has proven an effective first line of defense against domain-based abuse.

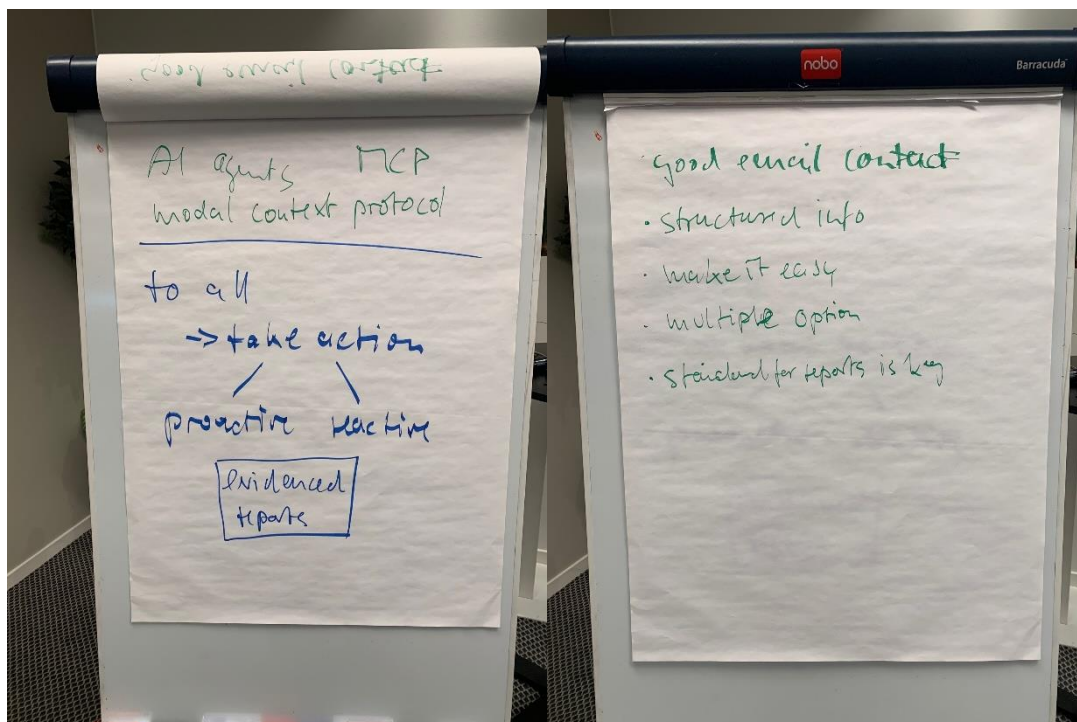
Centralized Coordination, Reporting, and AI Integration

Thomas Rickert summarized the discussion by noting that no single reporting channel fits every use case: end users may best be served by AI-enhanced web forms or chatbots that guide them to submit complete reports, professional reporters can leverage direct APIs, and email remains necessary for many interactions – provided recipients publish clear, dedicated contacts and use machine-readable standards. **Atro Tossavainen** (Koli-Löks) stressed the importance of “being liberal in what you accept and conservative in what you send,” echoing Postel’s principle, and suggested documenting a nuanced, scenario-based set of preferred channels and practices.

Bertrand de la Chapelle emphasized the importance of flexible “intermediaries” that can translate between multiple report submission methods (email, web form, API, various languages) and recipients’ preferred intake formats. He proposed a matrix-based

approach where reporters choose their easiest format and recipients their system-friendly format, while intermediaries handle conversion according to a shared underlying standard—ensuring interoperability without forcing a single channel on all users.

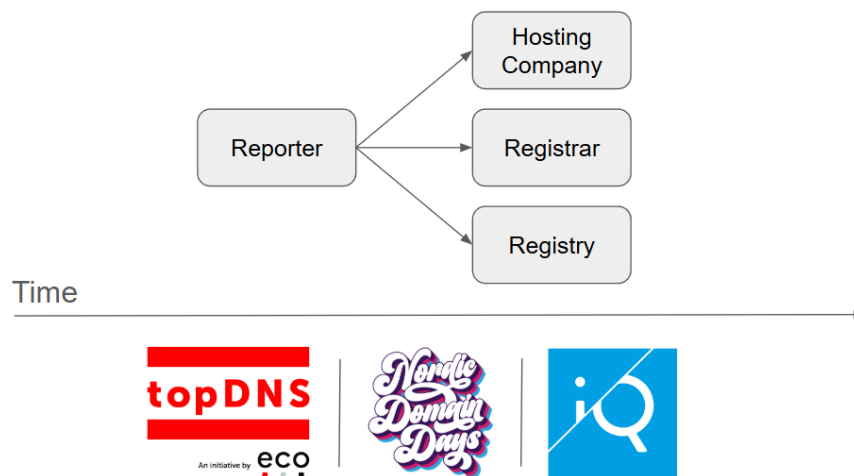
Michael Halvorsen noted that standardizing reporting formats simplifies data exchange, and falling integration costs – thanks to low-code tools and AI – will make API adoption much easier. They contrasted human-oriented channels (email, forms) with machine-to-machine APIs, then highlighted the rise of AI “agents” that’ll automate reporting: these agents can use email or APIs but increasingly favor emerging protocols like MCP (Mobile Context Protocol), suggesting we should ensure compatibility with such new, AI-driven interfaces.



Several workshop participants endorsed a “report to all” strategy – simultaneously alerting hosting providers, registrars, and registries – so that registries can immediately identify and suspend any related malicious domains, and registrars can swiftly disable clusters of phishing sites. They noted that hosting may be obscured by reverse proxies, making rapid safe-browsing notifications critical to blocking URLs before they propagate. In practice, a **hybrid, proportional approach** works best: professional reporters push standardized feeds (e.g., XARF) to all relevant parties, while end-user reports might go only to the most directly responsible platform (social media, e-mail host, etc.). Crucially, each recipient should receive a tailored, actionable report rather than a generic “cc,”

preventing notification fatigue and ensuring that each actor knows precisely what remedial steps to take.

Reporting: All at once?



The idea of a centralized abuse coordination function received broad support:

- **Improved Coordination:** A central hub would allow all actors to see who has taken action on abuse reports – reducing duplication and closing communication gaps.
- **Policy Facilitation:** This function could also promote standard-setting and accountability across the industry.
- **Transparency and Feedback Loops:** Stakeholders stressed that actions taken must be visible to others. Shared dashboards or reports could help establish trust and track outcomes.

The success of combating DNS abuse hinges on building robust cross-industry coordination mechanisms, enabling stakeholders to share information and resources effectively. This concept was reinforced throughout the discussions, highlighting that centralized coordination is vital for a more organized and effective approach.

In parallel, **AI integration** emerged as a key enabler. **Thomas Rickert** and **Lars Steffen** from eco Association noted the growing importance of AI in analyzing unstructured abuse



reports, identifying emerging threats, and improving scalability. AI could help detect patterns, triage reports, and provide real-time actionable insights.

Challenges and Best Practices

Ongoing challenges

- **Inconsistent Implementation:** The lack of consistent implementation across top-level domains (TLDs) remains a key challenge, with many participants noting the varying abuse response times and procedures that impede coordinated efforts.
- **Slow Response Times:** Fragmentation within the industry results in delayed action.
- **Complex Abuse Cases:** Increasing sophistication of abuse tactics requires more nuanced and adaptable solutions.

Best Practices









- **Increased Transparency:** Stakeholders should implement transparent feedback systems so everyone is aware of actions taken.
- **Standardization:** Standardizing reporting processes, feedback mechanisms, and action timelines would ensure consistency and improve collaboration.
- **Continued Collaboration:** Industry-wide collaboration, facilitated by organizations like the IIF, remains critical to solving the problem of domain abuse. By sharing information, knowledge, and best practices, stakeholders can create a more effective and cohesive response.

Conclusion and Takeaways

The workshop focused on improving how internet infrastructure actors handle abuse reports (e.g., phishing), particularly around reporting, responsibility, evidence sharing, and coordination.

The workshop successfully laid the groundwork for continued collaboration. As **Lars Steffen** (eco Association) noted, *“Hopefully we can continue those discussions in the work tracks of the IIF, but also next year at Nordic Domain Days.”*

In closing, Steffen summarized a number of the workshop's key messages:

-  **Broader, simultaneous reporting to all relevant actors:** All stakeholders should receive reports updates simultaneously to ensure consistent action and transparency.
-  **AI and Automation:** AI tools and machine learning should be explored further as a critical tool to process reports (e.g., phishing emails), accelerate pattern recognition across abuse types, automatic evidence parsing, and extract structured intelligence. This would help maintain pace with evolving threats and enable smarter processing to scale with complexity and volume.
-  **Need for Feedback Loops and Transparency:** Multilateral communication must replace isolated actions – everyone should see what has been done and by whom, both for transparency and accountability. Proposals included dashboards, visible domain status (like clientHold), and better use of EPP status codes.
-  **Centralized Collaboration Ecosystems:** There is a pressing need to create a shared reporting ecosystem of cross-industry platforms among infrastructure intermediaries to allow coordinated responses and communication between operators.
-  **Create Standardized Abuse Reporting Formats:** Ensure that all stakeholders are aligned on reporting formats and practices, including standardized clearing mechanisms, whether centralized or federated. Participants suggested systems like extended XARF formats with trustable assessments and jurisdictional/legal context.
-  **Division of Roles:** Participants discussed the need to distinguish between reactive action (e.g., hosting company removing content) and proactive action (e.g., registrars investigating linked domain registrations).
-  **Evidencing Abuse Reports:** A challenge is that abuse reports often lack preserved evidence, especially if content is removed before others can verify it. Participants discussed centralized or federated “clearing house” approaches for storing evidence and assessments.
-  **Technical and Administrative Action:** Topics such as dangling DNS were complemented by calls for better governance and process clarity. Some companies already have internal tools (e.g., iQ's real-time status sharing), but there's no industry-wide standard yet.

The call to action is to remain engaged: measure progress, report back on what worked or didn't, and hold each other accountable at future meetings. By [Nordic Domain Days](#)



[2026](#), the community hopes to showcase tangible improvements – perhaps a widely adopted reporting standard, or statistics showing faster abuse takedowns – as proof of concept that this collaboration makes a difference.

Resources & Further Reading

- 🔍 topDNS website: topdns.eco