State of the DNS in 2022 Workshop in Brussels, 8 and 9 November 2022

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

VERISIGN

CentralNic Registry

.org

nic.at

CleanDNS

leaseweb

REALTIME REGISTER

Content

Preface

On 8 and 9 November 2022, eco – Association of the Internet Industry held a workshop in Brussels on DNS abuse. The workshop was attended by around 30 experts from various stakeholder groups, either in person or remotely.

On 31 January 2022, the European Commission published the Study on Domain Name System (DNS) Abuse. The study was extensively discussed within the domain name industry and beyond. The aim of the workshop was to take stock of the measures that have been taken against DNS abuse, which ones are in the making, and to discuss which measures should be focused on to mitigate DNS abuse best.

The workshop's aim was not to rehash previous comments on the study itself or the definition of DNS abuse. The focus of the workshop was on the 27 recommendations of the study, but these were only intended to serve as a starting point for discussion.

As the meeting was designed as a two-day workshop to allow for intensive debate, the number of participants had to be limited, and not all requests for participation could be granted.

With this report, we would like to offer the details of the discussion and the results for further discussion as a stimulus for action.

The issue of DNS abuse cannot be solved by a single category of actors or with a single measure. It will be a constant arms race with criminal actors that can never be won, but the damage can be significantly limited if all parties concerned live up to their respective roles and responsibilities and work together quickly and effectively.

The workshop was not intended to be a one-off event, but we would like to review the progress of the ongoing work and the commitments made by the various stakeholders again in the near future.

We would be delighted to start or continue the dialogue with you to advance the fight against DNS abuse.

Sincerely,

Thomas Rickert & Lars Steffen
eco – Association of the Internet Industry

Management Summary

On 31 January 2022, the European Commission published the Study on Domain Name System (DNS) abuse conducted by independent experts from Fasano Paulovics Società tra Avvocati and Grenoble INP-UGA Institute of Engineering. The study was extensively discussed within the domain name industry and beyond.

Also at the beginning of 2022, registries, registrars and hosting providers from the membership of the eco Association joined forces in the **topDNS initiative**. Since then, the stable, reliable, and secure operation of the DNS (Domain Name System) has been their common goal.

Against this background, the topDNS initiative organised a two-day "State of the DNS in 2022" workshop in Brussels on 8 and 9 November 2022. The goal of this workshop was to review the 27 recommendations from the study, potentially reframe the general ideas and suggestions and agree on actions and operationalisable solutions. However, neither the study itself nor the definition of DNS abuse was discussed in this workshop.

To enable a robust discussion about the roles, responsibilities and capabilities along the infrastructure intermediaries' value chain and who can do what by when, representatives from different sectors of the industry were present:

- Members of the European Commission (DG CONNECT, DG HOME, DG GROW).
- The authors of the Study on Domain Name System (DNS) abuse.
- Subject Matter Experts of CENTR, DNS Abuse Institute, International Trademark Association and the Internet & Jurisdiction Policy Network.
- gTLD & ccTLD Domain Name Registries.
- Domain Name Registrars & Resellers.
- DNS Service Providers.
- Hosting & Email Service Providers.
- Brand owners & experts on Intellectual Property.
- Staff members of eco – Association of the Internet Industry.

To facilitate the work of the participants, the recommendations were summarised and grouped into six segments:

- Registration Data Issues
- Exchange of Intelligence
- Preventative Measures
- Carrots & Sticks
- Enhancing Security
- Awareness Raising & Capacity Building

Each segment was introduced by a series of lightning talks to outline the respective recommendations and whether or how they have been addressed since the publication of the study. If yes, by whom and how? If not, what is missing or needs to be done to be successful, and how to prioritise different measures to balance efficiency and effort?

In this context, the following aspects were also discussed: Who can do what and what recommendations might need refinement based on new findings? The aim of the discussion was to develop proposed actions, priorities and methods that go beyond the scope of the study, where appropriate.

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:

- **Fast takedowns of malicious and compromised domain names are key.** But DNS abuse cannot be tackled with a single solution. There must be a well-orchestrated approach with concrete actions that enable people to work together towards a common goal.
- **There is often a chance to prevent abuse before it is reported.** There is a need for a trusted space for collaboration and intelligence information sharing among all parties involved. There are already initiatives in place. A discussion along the entire value chain is needed to identify the right ones for scaling. topDNS will prioritise the dialogue on this in 2023 with its partners to operationalise this crucial cornerstone.

- **Automation is indispensable in this context.** The effort of fighting abuse online has to be as quick and efficient as possible and kept at a reasonable level from a cost perspective. Also, the industry has to keep up with the malicious actors.
- **Building trust. Personal relationships between the actors involved is key.** It's a people business. topDNS and the eco Association will use their broad, cross-industry membership to bring together those who can make a difference by working together.
- **Improving abuse handling** by promoting adequate procedures for processing abuse reports.
- **Automatic responses to abuse reports** are the first step towards improving communication between actors and building trust.
- **Developing training opportunities for all actors along the value chain.** The topDNS initiative will offer educational support to newcomers in dealing with abuse in 2023.
- **Creating "Anti-Abuse Kits/Toolbox in a Box".** These training opportunities mentioned above will include recommendations of (non-)commercial tools for different intermediaries/target groups to guide through the first steps.
- **There is a chance to initiate a cultural change, for example by implementing current technical standards.** Abuse prevention/treatment/combating does not necessarily have to be a cost centre. In saturated markets, it is becoming increasingly interesting as a business model (network hygiene). The anti-abuse working group at the eco Association is already promoting this approach among its members and is always willing to share best practices.
- **Commercial incentives and reputation-based measures** have proven to support and accelerate development in this direction. Targeted approaches should be considered in favour of regulatory measures.
- **Building a schedule of roles and responsibilities** on who does what for all actors along the value chain. The contents and format of such schedule of responsibilities or agreements require further dialogue. The eco initiative topDNS has published an Abuse Table to provide guidance on which cyber threats are considered to be abuse of the Domain Name System – and which parties should be contacted first. This table will be further developed.

The participants agreed that there should be a public report based on the discussions and findings of the two-day workshop and a follow-up workshop in 2023.[1]

Out of these points, the following three topics have been identified as priority issues:

- **Trainings.**
- **Establishing a trusted space of collaboration including opportunities for automation.**
- **Building a schedule of roles and responsibilities to provide for co-operation and swift action by the various types of intermediaries.**

[1] Once a date has been fixed, the event details will be shared with the topDNS community. Interested parties are welcome to signal interest in being sent an event invitation by writing to topdns@eco.de.

Welcome and Introduction

Thomas Rickert welcomed the participants and introduced them to eco – Association of the Internet Industry and the topDNS initiative.[2]

Gemma Carolillo, Deputy Head of Next Generation Internet Unit, DG CONNECT, kicked off the workshop by sharing insights on the European Commission's take on DNS abuse. She recalled the preliminary discussions with eco where the context of the workshop was presented, in particular the idea to discuss with different actors what is currently being done and what will come in the future to fight DNS abuse. One of the interesting aspects of the eco Association for her is its diverse membership, which brings several actors that could contribute to prevent and fight DNS abuse to the table.

DNS abuse and its prevention and mitigation is of interest to several Directorates-General of the European Commission, as it is a cross-cutting issue for different services of the European Commission, such as DG HOME and DG GROW (IPR). Fighting DNS abuse is a key priority in several European Commission policies, and it is addressed at different levels with different instruments, for example with the Cybersecurity Strategy 2020, the reviewed Directive on Security of Network and Information Systems ("NIS2 Directive"), the EU toolbox against counterfeiting, while DNS is also covered in the Digital Services Act (DSA).

The European Commission decided to procure an independent study on Domain Name System (DNS) Abuse two years ago to address operators and policymakers. The aim was to gain more insight into the extent of the issue and to come up with recommendations for operators and policymakers to step up efforts in the prevention and fight against DNS abuse. Carolillo added that the comprehensive study was an offering with a broad scope and that she was interested in seeing what could be gained from the study, what progress could be made, and then assessing whether further policy intervention was needed. She concluded that DNS abuse is a global phenomenon and requires collaboration between many different players in the DNS ecosystem and that it would be important to explore strengthened collaboration between actors in the DNS ecosystem and beyond as vertical integration increases.

[2] Information on the eco Association and the initiative can be found in the 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

- **Ajith Francis**, Director, Policy Programs, Internet & Jurisdiction Policy Network
- **Alejandro Fernández-Cernuda**, Director of Engagement, Global Cyber Alliance
- **Bertrand De La Chapelle**, Founder & Executive Director, Internet & Jurisdiction Policy Network
- **Gemma Carolillo**, Deputy Head of Next Generation Internet Unit, EC, DG CONNECT
- **Ivett Paulovics**, Lawyer & Partner, FASANO PAULOVICS Sta
- **Jordi Iparraguirre**, Innovation Manager, EURid
- **Lars Steffen**, Director International, eco – Association of the Internet Industry
- **Laura Polo**, Intern, INTA
- **Lori Schulman**, Senior Director Internet Policy, INTA
- **Maciej Korczynski, Ph.D.**, Associate Professor, Grenoble Alpes University
- **Patrick Hauss**, Directeur Général Délégué, CSC Digital Brand Services SAS
- **Patrick Koetter**, Head of Anti-Abuse & Email Working Groups, eco – Association of the Internet Industry
- **Peter van Roste**, General Manager, CENTR
- **Raquel De Haro Perez**, Blue Book Trainee, European Commission, DG GROW
- **Richard Leaning**, Director – Trust and Safety, Cloudflare
- **Robert Schischka**, CEO, nic.at
- **Rowena Schoo**, Director of Programs and Policy, DNS Abuse Institute
- **Susan Payne**, Head of Legal Policy, ComLaude
- **Theo Geurts**, CIPP/E Privacy & GRC Officer, Realtime Register B.V.
- **Thomas Rickert**, Director Names & Numbers, eco – Association of the Internet Industry
- **Tim Werner**, Legal & Policy Officer, European Commission, DG GROW
- **Velimira Nemiguentcheva-Grau**, Policy Officer Internet Governance, EC, DG CONNECT

Remote Participants

- **Brian Cimbolic**, Vice President, General Counsel, Public Interest Registry
- **Brian Cute**, Director, Capacity & Resilience Program, Global Cyber Alliance
- **David Lossignol**, Global Head Legal Brand Protection, Novartis
- **Enrico Biess**, Abuse Manager, Strato AG
- **Gavin Brown**, Technical Fellow & Registry Services Ambassador, CentralNic
- **Janos Drienyovski**, Policy Officer Fight against Cybercrime, EC, DG HOME
- **Jeffrey Bedser**, CEO, CleanDNS, Inc.
- **Keith Drazek**, Vice President of Policy & Government Relations, Verisign, Inc.
- **Klara Jordan**, Senior Director Public Policy and Government Affairs, EU, Verisign, Inc.
- **Polina Malaja**, Policy Director, CENTR

Framing the Issue

Three compact presentations kicked off the two-day workshop. First, Thomas Rickert introduced the methodology and expected outcomes of the workshop (a). Next, Bertrand de la Chapelle spoke about the difficulties of responding to DNS abuse (b), focusing on the limitations of DNS actors who only have a binary choice in their responses, namely taking down a domain name or allowing it to continue to resolve. To better understand the scale of the problem, Rowena Schoo then presented the DNSAI analysis of DNS abuse statistics (c). Finally, Thomas Rickert ended this section with a short plea not to be distracted by trying to define DNS abuse (d).

a) Methodology and Outcome – Thomas Rickert

Thomas Rickert, Director Names & Numbers, eco – Association of the Internet Industry, outlined some housekeeping rules for the two days and provided input and food for thought for the discussions ahead.

Setting the tone:

- Don´t rehash previous comments on the study, we want to make progress: Keep an open mind and make the most of our time.
- Perhaps the study will give us new ideas and inspire us.
- Many of us will be fine with being held accountable.
- There will be a transparent review of what we have achieved between now and around a year from now.
- We will publish a report after the workshop.
- If this proves worthwhile, another workshop will be held in 2023.
- To facilitate discussion, the 27 recommendations have been divided here into six segments.

Housekeeping rules:

- At the beginning of each section, volunteers will give lightning talks followed by a discussion among the participants.
- A rapporteur will summarise the discussion at the end of each segment.
- The moderation will be done by Bertrand de la Chapelle for one segment and Thomas Rickert, Bertrand de la Chapelle and Ajith Francis are the rapporteurs.
- The participants agreed on the Chatham House Rules (with the statements in the lightning talks being reproduced with the permission of the speakers).
- During each segment, the recommendations will be briefly outlined.

Food for thought:

- The study provides an excellent overview of the proposals made and discussed in various bodies. The recommendations are not weighted in the study, the uninitiated reader might think that all recommendations are equally important and effective. For example, there are four recommendations for DNSSEC, but DNSSEC may not be the silver bullet for the issue.
- Are there other measures that are not mentioned in the study?
- Where are the low-hanging fruits?
- What needs to be done to become more effective?
- What is still missing for the measures combatting DNS abuse to be successful, and which measures should be prioritised?
- What can we do to involve people and get them to invest in technology and human resources?

b) The Predicaments in Responding to DNS Abuse – Bertrand de la Chapelle

Bertrand de la Chapelle, Founder & Executive Director, Internet & Jurisdiction Policy Network, addressed some of the difficulties in responding to DNS abuse.

"DNS abuse" is now a widely used term and has been discussed for a long time. However, its definition is confusing. Many interpret "abuse" as covering any problem in the use of the Internet; from phishing and malware to hate speech and copyright infringement. DNS abuse is actually a shorthand for a more accurate and important question: **"When and under whose responsibility is it appropriate to act at the DNS level to address abuse online?"** We should not confuse this shorthand with the real question, lest we begin to see the DNS as the default tool to address any problem online.

Unfortunately, there is still a broad lack of understanding about the actual functioning of the DNS and the limited and blunt tools that action at this level of the stack provides. In this context, work by the Internet & Jurisdiction Policy Network (I&JPN) has highlighted the useful distinction between technical abuse (e.g., phishing, malware, botnets) and website content-related abuse (e.g., CSAM, hate speech, IP issues).

There are very different types of abuse, and we all have a collective interest in balanced measures to prevent and reduce them. The DNS is an important technical infrastructure. What role does – and should – the DNS and those who operate it play in fighting abuse on the Internet? Various approaches need to be combined to combat abuse on the Internet:

- Make it harder to happen (prevention);
- React and mitigate it (intervention);
- Prosecute offenders (investigation and enforcement) to go beyond the whack-a-mole arms race.

There is a diversity of tools related to:

- Registration data
- Action on the domain name itself (where there are four limited options: lock, hold, redirect, transfer)
- Mechanisms to strengthen DNS security channels at a technical level
- Escalation path (acting at lower levels of the stack, e.g., hosting providers level instead of registries or registrars)

Acting at the DNS level is more relevant for technical abuse than content-related abuse, where proportionate action is more difficult and complex globally.

De la Chapelle found the EU Commission study very interesting, in particular regarding the distribution of different types of abuse across different registries/registrars and regions. The issue of proportionality is crucial, and a delicate balance needs to be struck between registrants and operators regarding registration verification and efficiency. However, the different actors' capacity to evaluate abuse must be taken into account. Trusted Notifiers can play a role if they send quality notices after due diligence procedures.

- Operator responsiveness upon notification is an important metric.
- ccTLDs and gTLDs are different, and ccTLDs are usually regulated at a national level.
- Escalation paths need to be established between registries, registrars and hosting providers.

The key challenges that de la Chapelle sees are:

- Simplicity for users and abuse reporters
- Importance of co-operation between the different actors
- Workflows in dealing with abuse
- Relationships between the different actors

He concluded that it is important to strengthen co-operation mechanisms between the different actors in order to have the best tools and most efficient procedures in the future.

c) The Size of the Issue – Rowena Schoo

Rowena Schoo, Director of Programs and Policy, DNS Abuse Institute (DNSAI), presented an analysis of DNS abuse statistics to illustrate the scale of the problem.

The DNSAI Compass[3] initiative focuses on measuring unique domain names involved in phishing and malware. The methodology also measures whether mitigation has occurred and whether the domain in question is registered for the purpose of phishing and malware, or whether it is associated with a compromised website. The purpose of measuring DNS abuse is to increase our understanding of the problem and bring greater sophistication to community discussions. With the ultimate goal of reducing abuse in mind, mitigation should still take place at the appropriate level.

The priorities for DSNAI Compass are:

- **Transparency**: The methodology that collects, cleans, and aggregates the data must be as transparent as possible. To the extent that, should anyone wish to, they could replicate the process.
- **Credibility and Independence**: We aim to have an academically robust and independent approach, separate from commercial interests.
- **Accuracy and Reliability**: The goal of these reports is to enable focused conversations and to identify opportunities for abuse reduction. The data needs to be of high enough quality to serve as the foundation for meaningful changes to the ecosystem.

Granularity matters: When understanding this problem and thinking about the appropriate mitigation for the harm identified, it is important a report is well-evidenced. It is also important to be specific about the issue identified and which mitigation measure would be most appropriate (if any). For example, a domain that has been compromised for the purposes of phishing is typically not appropriately mitigated through DNS-level suspension.

[3] https://dnsabuseinstitute.org/dnsai-compass

d) How Definitions Stand in the Way of Being Productive – Thomas Rickert

Thomas Rickert, Director Names & Numbers, eco – Association of the Internet Industry, made the following points and pleas in his intervention:

- Let's not waste time on a war of definitions.
- We want to talk about real-time scenarios.
- Let´s talk about the intersection of content/trademark and technical abuse.
- Let's dive into substance.

He highlighted that, outside the industry, no one knows or uses the term DNS abuse. There are different views on DNS abuse in different communities:

- Discussions in the real world vs. ICANN world.
- ICANN's limited remit due to bylaws.
- If ICANN overreaches, there may be sanctions by the empowered community. The Board has to be careful.
- ICANN's remit creates tensions within the community.

Please see the table of abuse scenarios and parties to be approached, produced by the eco Association, in **Annex 2**.

In the subsequent discussion, the following points were raised by the participants:

- The discussion about definitions is instrumental and not closed.
- When you start with the issue, many parties push back and create their own definition.
- If you start with the consequences, you get a more comprehensive picture because you create distance from the actors.
- A definition needs to be accompanied by measures. The breakdown by granularity helps to assign measures to who has to do what.
- These measures can be matched with the means.
- The question of competencies and responsibilities is linked to the measures.
- The line between technical and content-based abuse is often blurred. Therefore, we should take the opportunity to have a discussion outside ICANN with many different stakeholders around the table.
- Low-hanging fruits need to be identified, as everyone agrees that bad things are happening.
- When we talk about preventive measures, it is really important that we also talk about processes and scales here and understand that not all solutions are suitable for all problems and that if we are open and creative, we can find workable solutions and have clean spaces.
- It is important to discuss how to build trust and to think outside the box; to discuss responsibilities, community building and circles of trust without lawyers in the room.
- Motivate people to talk to you and share information. Tools and platforms should come later.
- Invest in people and relationships, not in publications and tools.
- It is better to be overwhelmed by data and then get a tool than vice versa.

1 Segment – Registration Data Issues

1.1 Recommendations

This segment covers the following recommendations:

(1) Providing a scalable and unified way to access complete registration (WHOIS) information using RDAP to attribute abused and vulnerable domain names to their respective registrars and obtain their contact information.

(2) Publishing DNS zone file data similar to the Centralised Zone Data Service (CZDS).

(3) Email addresses for registrants and administrators by way of anonymised email addresses to contact and notify security vulnerabilities and abuses.

(4) Domain name administrators should maintain standard email aliases for given domain names (e.g. abuse, hostmaster, webmaster.

(5) A standardised (and potentially centralised) system for access to registration data.

(8) Registries, registrars and resellers should verify the accuracy of WHOIS data (KYBC, eIDAS).

1.2 Lightning talks by Realtime Register, CENTR, CentalNic and eco

- Theo Geurts, Realtime Register
- Peter van Roste, CENTR
- Gavin Brown, CentralNic
- Thomas Rickert, eco

In his lightning talk, **Theo Geurts** of Realtime Register described how abuse reports are processed from the perspective of the wholesale registrar. The introduction of automation has been key to speeding up processes and turning abuse handling into a business model. To reduce the overall volume of abuse reports, deeper investigations often uncover more abuses, which are shared with other stakeholders and security experts to mitigate them before they are reported. Idea: How to respond to abuse reports without waiting for the hosting provider? Resellers still struggle to deal with abuse reports due to a lack of knowledge and expertise, while attacks are becoming more complex and sophisticated.

Peter van Roste, CENTR, spoke about data accuracy, eID and KYBC in ccTLDs. ccTLD operators are very diverse in the way they are organised and in the legal frameworks in which they operate, leading to complexity in the ccTLD community. Therefore, there is a wide range of validation solutions due to the different legal frameworks in each country. Automation is key as manual verification is not scalable. The use of eID is still in its infancy. eID systems are available for interoperability and automation, but verification is still difficult and almost unfeasible. It is easy to check if an email is reachable, but it is a challenge to check if it belongs to a specific and correct identity. In the future, eID would be interesting for verification if it were more widely adopted.

Gavin Brown, CentralNic, spoke about the DNS zone file data. Every operator who has a contract with ICANN is obliged to publish this data. Any interested third party can get access. So we see uniformity in the gTLD space but more diversity in the ccTLDs. The majority of European ccTLDs do not publish zone data. The reasons for not publishing DNS zone file data are often to prevent abuse and to prevent disclosure of commercially sensitive information. The data allows bulk retrieval of domain registration data. Therefore, zone file data has been used for registrant spamming, renewal fraud, identity theft and targeted DDoS attacks.

As for the question of how to proceed, a possible solution could be a more decentralised system with user authentication. The remaining questions to be discussed concern the technical implementation and the assessment of the potential effort, impact, and consequences of such an approach.

Thomas Rickert, eco Association, said with regard to Recommendation No. 5, he hopes that we all advocate for the use of ICANN's new SSAD and sufficiently demand that ICANN puts resources into its development.

1.3 Contributions and main findings

It was mentioned in the group discussion that zone file data is useful for detecting malicious actors and investigating which domain names have been registered under a particular brand name. There is a real need for brand owners to have standardised access to zone file data. Also, updates every 24 hours are no longer considered sufficient as attacks are becoming faster and more complex and therefore require adaptation.

Regarding the verification of data, the examples of .dk, .eu and .cn were discussed. Some participants felt that data should be verified as much as possible using all available technologies. The participants agreed that a risk-based and commercially reasonable approach to data verification needs to be pursued as there is no one-size-fits-all solution. The .dk TLD, in particular, is characterised by intensive ID verification standards and high registration fees. Further, the Chinese TLD was mentioned as an example: As soon as the data of a domain name is not correct, it is immediately deleted. Website owners should also be contacted as soon as possible. On the other hand, it was also mentioned that despite intensive ID controls, .cn is the second most abused ccTLD in the world, according to Interisle, and criminals are apparently able to circumvent this process. This raised the question of whether the investment in further validation is efficient and worth the effort, and what exactly is to be achieved.

In this context, it was pointed out that a clear target must be defined. If only one part of the industry raises standards and hurdles, criminals will adapt and shift their activities to other providers. It was also suggested that the measures should be analysed more closely: In the case of .dk, it is perhaps difficult to say whether the high verification standards or the high prices lead to lower abuse rates. Perhaps the high price is already sufficient to deter criminals in terms of proportionality and effectiveness. In the case of malicious trademark registrations, it will always be a problem if the trademark is used at the subdomain level, which the registrar can never prevent in the first place.

A question was raised about how long an average investigation takes, as quick takedowns are key. Due to the different nature of cases, investigations can take anywhere from a few hours to months. The industry also faces an increasing number of commercial abuse providers with extensive resources. From a commercial perspective, it was also discussed to look at abuse prevention as a business model rather than a cost centre. With saturated markets, the situation has changed. Providers should calculate how much of their infrastructure and resources are absorbed by abuse and take this into account. There should be an interest in keeping reporting volumes low so that abuse helpdesks are of an appropriate size.

The group also discussed the use and disclosure of registration data. The question was raised of how accurate and useful this data is for investigators. Breached data or fake accounts are usually used for abuse. Since even breached and fake registry data passes many validation checks, host names and third-party information were mentioned as useful for investigations.

It was agreed that even with false, breached registry data, certain patterns of abuse can be detected. Logging IP addresses was also seen as useful. Bad actors try to hide behind VPNs and proxy services. Unfortunately, privacy tools and regulations are sometimes exploited by perpetrators to disguise their identity. As mentioned earlier, some communities within the industry already share data and information on infringement patterns on an informal basis.

There was also agreement that – without public access to registration data – it is very important to know who the registrar is. Since the registrar holds the customer relationship, they are also able to correlate the registration with the account holder's data. It has also been noted that inaccurate data has been entered into the public WHOIS in the past to avoid privacy issues and abuse. However, if the account data is invalid, the customer can be blocked. However, account and payment data are most likely correct. The argument was also made that with compromised domain names, even completely correct data does not help. It was noted that attackers will adapt as processes and requirements change. Therefore, some participants cautioned that regulation in the EU might lead to competitive advantages of registrars outside the EU.

In view of NIS2, multiple validations at the reseller, registrar and registry level must be avoided. It was also noted that thin registries cannot even validate at the registry level. Hopefully, the industry will agree on what kind of validation will be required, whether pre-validation or post-validation and whether things need to be re-validated after a certain period. There is also a need to address the implementation of NIS2 at the Member State level.

The question about anonymous abuse contacts at registrars and registries was answered to the effect that the contact forms on the websites of these bodies are the easiest and best way to process abuse reports. As soon as an anonymous email address becomes known, it is also abused. In this context, it was emphasised that trademark owners who send abuse reports need a reply to confirm that the abuse report has been received. It was also explained that the registrar is often the best party to contact first, as they often know best which party to contact next based on the customer data available. After lengthy discussions on accessibility at ICANN, web forms were identified as best practice. NetBeacon was also mentioned as a good way to send abuse reports.

There was a broad understanding of the need for standardisation and universal solutions, e.g., for abuse reporting, to be scalable and deliver results. There was also recognition of the cost to the whole ecosystem, as even the most sophisticated systems still need to be run by people. The final decision has to be made by people. That means money and investment – in people.

The UDRP (ICANN's Uniform Domain-Name Dispute-Resolution Policy) has been cited as an example of a good rights protection mechanism. But for many, especially those with large trademark portfolios, the UDRP is not the first port of call. The UDRP is usually used to clean things up, as many of these cybersquatting names are used for phishing, fraud, botnets and malware. According to some participants, much of the IP infringement is associated with technical misuse. It was also mentioned that the UDRP is aimed at something else.

It was also noted that those who want to do the right thing are also those who participate in discussions. But how can the bad actors be put in their place? Legislation will deal with the good ones because the bad ones don't care. It's about resources and expertise.

Expectation management in relation to the submission of abuse reports was also seen as important. The introduction of automatic response mechanisms was mentioned as a possible quick win. It was also argued that a "You didn't decide in my favour. That's why you didn't investigate" approach does not help. That would be a dangerous way to go because the investigation part is important.

Another solution proposed was the creation of spaces of trust and incentives to invest in combating abuse. There was also agreement that creating security is not a state but a process. We will never reach 0% DNS abuse; that will never be possible. The numbers will go down as more companies band together. There will always be those who do not comply with the law or enforce contracts. Laws and contracts must be enforceable. If the vast majority of operators follow all best practices, very few DNS operators will be left excluded from targeted action. Registrar hopping is widespread, and there is a need to take action against it. Currently, it is not yet possible to clearly identify the few bad actors. Some argue that legal and technical obligations should lead to a drastic decrease in abuse.

2. Segment – Exchange of Intelligence

2.1 Recommendations

This segment covers the following recommendations:
(6) A standardised abuse reporting system.
(7) The exchange of information between parties involved.
(21) CERTs should subscribe to feeds on open DNS resolvers and notify them to limit the number of open DNS resolvers.
(25) DNS Service providers should formally collaborate with Member State institutions, law enforcement authorities & Trusted Notifiers.

2.2 Lightning talks by DNS Abuse Institute, CleanDNS, eco, Internet & Jurisdiction Policy Network & nic.at

- Rowena Schoo, DNS Abuse Institute
- Jeffrey Bedser, CleanDNS
- Thomas Rickert, eco
- Ajith Francis, Internet & Jurisdiction Policy Network
- Robert Schischka, nic.at

Rowena Schoo, DNS Abuse Institute, presented DNSAI's NetBeacon (**https://netbeacon.org**) and the Registrar Stakeholder Group's Abuse Contact IDentifier (**https://acidtool.com**) as examples of what the industry is doing to facilitate the submission of abuse reports. ACID is a tool that facilitates the identification of the hosting provider.

NetBeacon aims to make reporting abuse easier for reporters by providing a central place and automatically addressing the report to the correct registrar. It provides a standard form to help reporters submit high-quality reports. It also aims to make the reports that registrars receive more actionable, as they are relevant, standardised, evidenced, and enriched with additional information. NetBeacon is currently sending reports to all gTLD registrars, with plans to begin incorporating ccTLDs in the future. NetBeacon was developed with support from CleanDNS.

Jeffrey Bedser, CleanDNS, presented an overview of what is tentatively called topDNS Hub, which is a trusted workspace and abuse aggregation tool for sharing information between different types of intermediaries to enable collaboration either through an API or a web interface. DNS abuse information can be submitted to the workspace and enriched with additional information, such as when an abuse report has been confirmed as valid by an individual. Since most criminal campaigns involve multiple domain names, registrars, web hosting companies and other intermediaries, the other parties involved can receive notifications and act on this information to take remedial action before an intermediary receives an abuse report from a third party. These measures include web hosting companies contacting their customers to repair the compromised web space.

The model is a central repository where, in the event of mitigated abuse, associated data such as the source IP address of the company that first registered or created the domain, the hosting company's user account, the host IP address, the name server and the reverse DNS domain are stored to provide key indicators of other activities carried out by the same operators.

Thomas Rickert, eco Association, complemented Jeff Bedser's presentation by saying that the validation of reports is a big problem. One problem is resources and the fact that reports are sent to multiple facilitators who all have to assess the same case, leading to inefficient use of resources and duplication of efforts. Also, due to the geographical IP address, sometimes the staff of a registrar do not see the same content as the victim concerned. In addition, a hosting company may not be able to verify reports if a customer whose web space has been compromised is using self-managed hosting.

A trusted collaborative environment such as topDNS Hub could be opened up to all affected parties, including brand owners whose brands are being misused for phishing, but who usually keep information about the misuse of their brands to themselves. Another envisaged feature is a list of domain names that are known to be abused, so that participating registrars know which domain names they would be better off not transferring. This will help to mitigate the problem of "registrar hopping".

Ajith Francis, Internet & Jurisdiction Policy Network, spoke on the topic of trusted notifiers. I&JPN's Muti Stakeholder Contact Group is working on the issue of DNS abuse and on a framework for trusted notifiers. He stressed that there is no formalised definition yet. There is, however, a broad consensus that the term "Trusted Notifier" should be used to cover either:

- Entities that have a formal agreement with a DNS operator or
- Law enforcement agencies with the legal authority to seize or suspend domain names in the operator's jurisdiction.

He explained that the relationship with trusted notifiers is different from that with so-called "trusted flaggers" in content moderation on online platforms. Francis emphasised the following issues: the difficult scaling of relationships between trusted notifiers and operators across jurisdictions; the trusted notifier's degree of expertise to investigate the actual reality and extent of abuse; the type of due diligence and the extent of evidence to be provided by the notifier; and liability considerations for the operator. While we see a growing number of agreements, there is still much work to be done on the above issues.

Robert Schischka, nic.at, spoke about working with CERTs and the role of open resolvers in DNS abuse. He recommended using the existing CERT networks that have been working for years to build trust. He stressed the importance of the accountability of trusted reporters.

Schischka questioned whether open resolvers are the main cause of malicious activity, saying this is an exaggerated claim. While open recursive resolvers have historically been used for attacks, there is a big shift to other protocols. In his opinion, unmanaged IoT devices are more of a problem. He went on to say that there is still a legitimate purpose for open resolvers, but there needs to be a distinction between intentionally managed open resolvers and those that are accidentally open and no one knows about. This, he sees as a growing problem. Schischka suggested taking a closer look at the companies that put equipment on the market in large quantities and making a regulation that they are responsible for the basic configurations.

2.3 Contributions and main findings

Today, the target groups of abuse have become smaller but much more specific.

Standardised reporting systems such as NetBeacon and ACID are to be welcomed and should be supported. There are already some trusted spaces, but they are not connected to each other. Many of them have their own interests but no common goal. There will never be a single platform, but there is a need to build bridges between the different efforts.

Relationships between trusted notifiers should be worked on. They are easier to establish in the case of technical abuse as they are less dependent on jurisdiction. However, for content abuse, there are problems due to the different jurisdictions and geographical scope. It was mentioned that the DNS is a very poorly equipped level to act on content abuse.

- Open resolvers not be abolished, but opportunities for communication with operators should be created.
- Sometimes there are thousands of compromised devices, and the amplification doesn't necessarily come from the protocol. It's like a big botnet with millions of clients, so it's like a game of whack-a-mole.
- A cultural change in the management of network operators is required, with network hygiene becoming an important factor.

Reputation becomes key at different levels. Blocking bad traffic is increasingly done at the network level. The Internet is no longer about filtering. It's about reputation-based systems. Commercial incentives to improve are key. These can be positive incentives or sanctions.

DNA abuse cannot be tackled with a single solution. It will be a cocktail of many approaches. There are different tools that can be used, which is good in terms of competition. Often high reputation goes hand in hand with places where there is regulation. It will always be an arms race. The abusers are always better equipped, financed and organised.

Most abuse is reported to infrastructure providers in two ways. One is via their abuse@ email address or their abuse@ form on their website. The other is via blacklists to which they subscribe to protect the network, and which are well-evidenced so that the parties can prove the abuse so that they can react to it.

There is a need to work with the cybersecurity companies to get the data that they have, that they collect, that they track, and that actually informs what domains are being used for abuse.

An important aspect is the connection to the tools and automation as well as the relationships between the different actors.

Automation is necessary to maintain the arms race. Good anti-abuse staffers are sometimes against automation because they do not want to lose their position.

The discussion on tools shows that a lot can be achieved, not necessarily by setting principles, new rules, or new commitments, but by concrete actions that enable people to work together. And that is one element because this is about sharing information. It is about sharing relationships, again in the sense that there is a common goal. The good actors of all parties should build what they accept and displace the bad actors.

At ICANN, the community became increasingly polarised between contractual and non-contractual interests. Pragmatism – it's not about perfection; it's about taking it one step at a time.

3. Segment – Preventive Measures

3.1 Recommendations

This segment covers the following recommendations:
(9) Similarity search tools or surveillance tools.
(10) Offering IPR holders services to preventatively block infringing domain name registrations.
(11) Predictive algorithms to prevent abusive registrations from being used by registries and registrars.
(16) The issue of free hosting and subdomains.

3.2 Lightning talks by Novartis, EURid, CleanDNS, nic.at

- David Lossignol, Novartis
- Jordi Iparraguirre, EURid
- Jeffrey Bedser, CleanDNS
- Robert Schischka, nic.at

David Lossignol, Novartis, reported that a growing number of brand owners feel left alone in the fight against abuse. As many proactive tools as possible should be used to automatically remove things that are at least likely to infringe. He urged all players to play their part and take responsibility as he sees the balance currently in favour of the bad guys. It was noted that the phrase “likely to hurt” is very vague.

It was also emphasised that automation is key at many levels, including for intellectual property rights holders. Currently, they feel that they just have to catch up and do not get answers from registries, registrars and other intermediaries. Many types of abuse are now automated; therefore, mitigation processes need to be automated as well. NetBeacon was seen as a good start in the right direction. It was also noted that there will be little chance of a uniform system in the market. Abuse reports need to be adapted to the different industry systems. It was explained that trademark owners can gain valuable insights from the zone file data to identify broader patterns of abuse.

Jordi Iparraguirre, EURid, explained EURid’s practice of preventive measures against DNS abuse. EURid performs a trademark match against the EUIPO database for each domain registration. In case of a match, the rights holder and the registrant are informed.

EURid’s APEWS system is an AI-based system check that is performed before the domain is delegated. In case of doubt, the delegation is delayed. The system includes automated and human checks that are redistributed for machine learning. Serious and suspicious cases are also immediately forwarded to cybersecurity experts and LEAs.

KYBC measures may ask registrants to confirm their identity. They receive an access code by email, which they can use to verify themselves on the EURid website. Again, suspicious domains are forwarded to LEAs, CERTs, GCA, GASA, etc. Iparraguirre also explained that EURid performs automatic content checks through APEWS. The system tries to find out if something deserves a human revision of the content. In the past, for example, fake shops had patterns of a similar look and feel.

All registered domains are checked within 24 hours. The system also checks some domains days and weeks later. The system also tries to find out if something deserves a human review of the content. Every day, the latest domains are automatically checked. Every domain is checked: scroll, analyse, look. Fake shops used to have a similar look and feel. Today they don’t. There are no regular checks of all 4 million domains, but targeted checks according to specific patterns, etc.

APEWS is still a prototype, but licensing might be possible in the future. EURid has started to cooperate with other registries that are also looking for abuse and it shares information about (allegedly) abusive domains that have been discovered.

Jeffrey Bedser, CleanDNS, gave an overview of the incentives for registrars to behave cleanly, using PIR’s QPI program as an example. The program measures various activity points between the registry and a registrar to determine how much discount that registrar earned per domain sold. One must bear in mind that the profit margins are meager.

He sees many different ways to incentivise, be it between registrars and hosting companies or registries and registrars through joint marketing efforts, discounts, etc. QPI also improves retention rates. The longer the domain name stays registered, the less relevant the additional costs/discounts are.

There are also programs to increase the quality of domain name registrations, like homonym blocking by Identity Digital, domain protected marks list by Identity Digital, and TruNames, to prevent maliciously registered domain names. Other market participants must be encouraged to offer comparable services.

Robert Schischka, nic.at, argued from the point of view of ccTLDs that trademark infringements only occur to a very small extent. More problematic are generic domain names that nobody notices and unknown niche brands that are only used for misuse much later. A well-known pattern is the misuse of existing names due to their reputation (drop catching). In addition, users are directed to abusive websites by online advertising because they do not pay enough attention to the domain name/URL.

To sum up, **Thomas Rickert**, eco Association, said that he thinks preventive measures are a good idea and asked the group if these services should be recommended. Or whether registries and registrars should be forced to become competitors of services that have existed for many years? He argued that if registrars and registries are forced to use all these fancy technologies, the industry might miss the point, at least when it comes to DNS abuse and trademark infringements. That is another matter, but that is not the core of this discussion. In his opinion, a well-established is a powerful tool as URS and UDRP are easily triggered.

3.3 Contributions and main findings

Some parties agreed that AI and/or predictive scripts are very helpful if users of the system are aware of false positives and handle them properly. In addition, certain types of abuse, e.g., fake shops, seem to change and adapt to learned patterns, which requires constant "learning". By analysing patterns in valid registrations, malicious registrations can be detected.

It was also mentioned that there is a trend to target smaller groups for abuse in order to stay below certain thresholds. All validation checks must also comply with data protection and data storage regulations. One issue to be discussed is the acceptance in the market for delayed delegations of domain names due to validation checks.

One contributor pointed out that the hopes of solving the problem through artificial intelligence were too high, but the tools were still good. This would be something for large registries with enough resources and staff.

The question was raised whether ICANN's Trademark Clearinghouse (TMCH) had been a success. In the discussion that followed, some problems related to the TMCH were raised. Some brands consider it a risk to be listed in the TMCH as a target for abuse. URS was seen as hardly used. It was felt that it does not have the impact hoped for.

Another aspect discussed was that the study says nothing about how to process reports quickly. It encourages the reception of information, but not how it should be processed to shorten the turnaround time. A usual response time of 48 hours adds up by the number of intermediaries. It was mentioned that the study on DNS abuse includes data about uptimes: Certain intermediaries fall into specific categories: 1 hour, 6 hours, 24 hours etc.

There are also examples of hosting providers giving their customers only one hour to respond to phishing. As mentioned earlier, dealing with abuse can be turned into a profit centre by offering abuse removal services to the client. It was also mentioned that it is worth thinking about contractual options to hold the customer responsible and accountable.

It was also acknowledged that some expense will have to be borne by brand owners. There will be costs for developing systems and creating clean spaces. This may also lead to higher prices for domain names.

From the perspective of the rights holder, it has been argued that there is indeed an overlap between intellectual property fraud and technical abuse. For some abuses, the domain name is not relevant; for others, it is. It was also suggested that more data and intelligence should be shared with and between trademark owners.

Other issues raised:

- Automation of workflows and detection tools is important. Equally important, however, is that the automation of decision-making must take place under human supervision.
- The question of delays between registration and delegation of domain names was discussed, whether this is good or not and, as such, accepted in the market.
- Handling of false positives when using AI.
- Different incentive programs in the market are already available.
- What is the chain of actions when abuse is detected? There is a group of actors that want to make a difference and are trying to move forward on a pragmatic basis.
- Roles, responsibilities and capabilities of all intermediaries involved need to be discussed.

4. Segment – Carrots & Sticks

4.1 Recommendations

This segment covers the following recommendations:
(12) Monitoring and reporting abuse rates, de-accreditations.
(13) Rewarding players with low abuse rates.
(14) Registries to maintain access to URL/domain blocklists, identify registrars with high/low abuse rates and provide incentive structures.
(15) Hosting providers should be monitored, abuse rate limits, incentive structures.

4.2 Lightning talks by Versign, PIR, CleanDNS, DNS Abuse Institute, nic.at:

- Keith Drazek, Verisign
- Brian Cimbolic, PIR
- Jeffrey Bedser, CleanDNS
- Rowena Schoo, DNS Abuse Institute
- Robert Schischka, nic.at

Keith Drazek, Versign, summarised and explained the joint letter by the contracted parties (Registries and Registrar Stakeholder Groups, RySG and RrSG) of 4 November 2022 as follows: The current ICANN Registrar Accreditation Agreement (RAA) did not truly create an obligation to act on and mitigate DNS abuse. Therefore, the contracted parties think it is time to take the initiative to work with ICANN to create these requirements. For the definition of parameters and new obligations, a GNSO Policy Development Process might be required. The defined goal is to give ICANN Org and the ICANN Compliance team the tools to hold bad actors to account. It is planned to conclude the contract negotiations by the ICANN76 meeting in Cancún in March 2023.

Drazek concluded that in combating DNS abuse, gTLD registries and registrars are only one part of the ecosystem, and the whole picture needs to be looked at, including CDNs, hosting providers and trusted registrants. He said it is important that there are a number of actors with unique roles, responsibilities and capabilities, and the community needs improved communication and collaboration between these actors, including hosting service providers.[4]

Brian Cimbolic, PIR, stressed that tools are needed to take action against actors who do not sit down at the table and that he is very encouraged by the promising letter. He said it is very important to give ICANN the tools to act against bad actors who do nothing. It's not about ICANN making decisions at a granular level about individual actions or contractor decisions.

The letter and its implications were then discussed. The most important arguments are listed below:

- The letter was seen as a very positive sign, but it is necessary to wait and see how the process will develop and what the concrete goals, measures and results will look like.
- This will be a kind of cementing of what is already done under the DNS abuse framework, which many registries and registrars have signed on a voluntary basis, but now it will have a legal basis.
- It is seen as problematic that most discussions at ICANN are based on assumptions and old data.
- Threatened actors are considered to be much more advanced than actors in the ICANN space, including among contractors, and therefore have more resources and experience than others. The question was raised of how to support the less well-equipped actors.
- Accreditation will become even more complex and complicated in the future.
- It will be crucial for the contract amendments to be powerful so that ICANN Compliance will have the capacity and skills to act.
- The need to respond will make a difference. This is an area where contracts should not be too prescriptive. Some don't believe that the method of interruption needs to be prescribed or predetermined for a contractual clause to be truly enforceable.
- Concerns were raised about whether a GNSO PDP was the best mechanism to agree on concrete actions related to specific threats, but it was also argued that the ICANN multi-stakeholder process needed to be followed to achieve broad industry and community consensus.
- More educational work is needed to balance the different levels of knowledge and expertise within the industry, and to investigate DNS abuse and take the right actions. Therefore, topDNS is working on educational formats for registrars, registries, etc.
- There was also agreement that other intermediaries, such as hosting providers, need to be included in this multi-stakeholder dialogue.

[4] An overview of the parties' recent letter to ICANN can be found at: https://www.icann.org/en/system/files/correspondence/heineman-demetriou-to-marby-04nov22-en.pdf

Cimbolic also gave an overview of the QPI incentive program at PIR, which has been running since 2019. In the past, most incentive programs in the industry were independent of the underlying quality of registrations. Instead, QPI monitors six different matrices such as renewal rates, website usage, SSL certificates, DNSSEC activation, etc., leading to a healthier ecosystem, rewarding good behaviour and enabling low abuse rates. Today, 50% of all registrations at PIR are done through the system. PIR has seen a significant decrease in abuse rates over the last three years. QPI is a good business opportunity for PIR and participating registrars: + 4% on renewals, discounts for registrars. QPI is an example of several similar incentive programs, e.g., at SIDN (.nl) or Traficom (.fi).

Theo Geurts, Realtime Register, added that introducing incentives at SIDN was a turning point for DNSSEC adoption among registrars. Incentives help turn abuse management into a business model for registrars. A commercial incentive is extremely helpful in changing this. The profit margins for some TLDs are meager. Dealing with a single DNS abuse report can incur costs that can never be recovered. Gavin Brown added that CentralNic will offer QPI on its platform from 2023.

Jeffrey Bedser, CleanDNS, spoke next about raising awareness. One of the beauties of topDNS is that the initiative takes the conversation beyond registrars and registrars and reaches out to other intermediaries along the value chain, such as hosting companies, content delivery networks, etc., where the problem exists at all levels of the stack.

A disadvantage of incentive programs such as the aforementioned QPI is that they can only address the problem of malicious registrations. To tackle compromised domain names, more standardisation is needed to enable a more comprehensive approach across the industry. Paper SSC115 addresses the need for interoperability. NetBeacon is a piece of the puzzle as it provides a common point of contact for abuse reports. It also opens the channel for incoming reports and data from victims, those who disclose abuse. NetBeacon wants to encourage users to send reports and make it as easy as possible for them to send them.

Regarding blocklists, Bedser explained that they are good indicators of problems, but are not evidence. Therefore, from the operator's point of view, they will not take action against domain names that have not been evidenced to be part of an abuse activity. More and more services are coming onto the market offering services to smaller businesses that do not have the internal resources, skills or knowledge to help with this type of problem. Very affordable solutions are quickly eroding the excuse not to act.

Rowena Schoo, DNS Abuse Institute, also emphasised that real-time blocklists (RBLs) were originally designed for network protection, not for DNS abuse mitigation. They have a higher tolerance for false positives, are URL-targeted, often require deduplication and the removal of "special domains", e.g., Google Docs. A lot of manual clean-up work is required to make RBLs useful for registrars and registries.

4.3 Contributions and main findings

In the discussion that followed, some participants felt that focusing only on malicious domain registrations could be a mistake, but that a balance needs to be struck to adequately deal with the harms arising from compromised domain names. Different standards might be needed for different types of abuse. The creation of an "anti-abuse toolbox/hub" was discussed.

In the context of tools and data sharing, the importance of a legal framework for data sharing (e.g. GDPR) was also highlighted. The CERTs appreciated the NIS and the NIS-2 for the legal clarification of data sharing. For NIS-2, it remains extremely important that individual national implementations are clear and precise on this point. As before, the General Data Protection Regulation (GDPR) is often misused as an excuse for not sharing data. A clarification, that the exchange of data to fight abuse is done on a legal basis, is of importance.

Other issues raised:

It was noted that the accreditation arrangements for registrars and registries so far did not sufficiently specify the obligations to act. The aim of the negotiations is to find new formulations and instruments to facilitate compliance. Supported by an additional community policy development process, the community will consider what these commitments and policies might actually look like. ICANN needs to have the tools to take systematic action against those actors who systematically fail to combat DNS abuse. The question was also raised as to whether there is a skills gap in compliance at ICANN and whether there is a need to engage in resource building. It is about providing tools to take action against certain malicious actors who do not necessarily act in good faith and do not punish what they do in particular.

The intention is a multi-stakeholder process that brings people together that have a role to play to agree on what those measures might look like. There also needs to be a balance between the risk of imposing measures while, at the same time, maintaining the scope for good faith action on the part of operators. Knowledge gaps were also raised, particularly with operators and the role of the registrar, training the registrar to identify and mitigate abuse.

The group also looked at some incentive programs, such as the Quality Performance Index and how it has reduced abuse rates while causing a surge in renewal rates.

A number of points were also made about the need to raise awareness of DNS abuse outside of premises and to distinguish between malicious registrations, which are currently targeted by most DNS abuse organisations, and the need to also focus on compromised domains.

5. Segment – Enhancing Security

5.1 Recommendations

This segment covers the following recommendations:
(17) DNSSEC for ccTLDs.
(18) Registrants should have easy access to DNSSEC
(19) Discounts for DNSSEC use.
(20) ISPs running DNS resolvers should configure DNSSEC validation
(21) Security Community to measure and educate about DMARC, SPF.
(23) IP source address validation for incoming and outgoing traffic.

5.2 Lightning talks by eco, CentralNIC, CENTR, CleanDNS:

- **Patrick Koetter**, eco
- **Gavin Brown**, CentralNic
- **Peter van Roste**, CENTR
- **Jeffrey Bedser**, CleanDNS

Patrick Koetter, eco Association, gave a presentation on DNSSEC against the background of the study on DNS abuse, which highlighted DNSSEC as a measure to avoid cache poisoning. Because even if you use encryption, you have to know that you are talking to the proper authority.

Today, he said, the DNS is a highly distributed database that not only serves name resolution but also covers many other purposes. The DNS has evolved into an identity provider, but it does not provide the level of security we need. DNSSEC is one of the cornerstones of the modern Internet.

A lively debate showed that participants were in favour of DNSSEC and its implementation. However, there were different views on the simplicity or complexity of its implementation at the registrar level. For the sake of completeness, Patrick Koetter also explained SPF, DKIM and DMARC. Nowadays, all companies use platforms that have just one IP address. Against this background, the mechanisms for building up reputation for an IP do not work as they do with SPF. DMARC could help, but it is not yet widely used. Therefore, he recommended that the authors of the study call for a wider implementation of SPF, DKIM and DMARC in future studies and publications. DMARC is seen as helpful against phishing. The authors of the DNS abuse study admitted that DKIM was not sufficiently considered in the study.

Gavin Brown, CentralNIC, made a cost-benefit assessment of DNSSEC implementation from the registrars' point of view. He described the scope of cache poisoning as small. In the context of DNS abuse, it does not help to prevent and contain it. For registrars offering DNSSEC, it was described as vulnerable, costly and complex to implement, citing examples of recent outages due to DNSSEC failure. The question was raised as to what the value of incentives for DNSSEC should be.

According to **Peter van Roste**, CENTR, Malta has confirmed next year's launch of DNSSEC as the last EU ccTLD. There are only 6 TLDs left without DNSSEC support in the whole of Europe.

Jeffrey Bedser, CLeanDNS, addressed the recommendation on IP source validation. He explained that there can be no DNS without IP addresses. But the domain name system is not the IP address. IP addresses can be helpful for the best practice of validating geo-locations, but not for combating DNS abuse.

Thomas Rickert, eco Association, reported that IP source validation is part of the standards set by the industry working groups after the introduction of NIS and that it can be assumed that this requirement will continue under NIS2 – at least in Germany. It is also part of the Mutually Agreed Norms for Routing Security (https://www.manrs.org), which also addresses this very issue. The problem, however, is that this is an altruistic measure that you have to take, as you, as a network operator, do not benefit from it yourself but let others benefit from it.

5.3 Contributions and main findings

In this discussion on the implementation of different standards, it was also mentioned that this has already been promoted in the Cybersecurity Strategy 2020 by the European Commission, which will establish a monitoring platform for different standards that will provide more insights on the current uptake of key Internet standards across the EU.

It was also mentioned that, for example, the adoption of HTTPS was driven by Google ranking. Further adoption of standards will always be a combination of improved tools and commercial incentives against a background of cost-benefit analysis. SWITCH and SIDN were also mentioned as best practices to incentivise DNSSEC implementation. However, it was also acknowledged that the underlying mechanisms do not work for every organisation.

Other issues raised:

- Consideration of the technical and cost-based perspective on DNSSEC.
- Today, the DNS is a highly distributed database with many different functions such as verification, validation of senders, etc.
- The use of DNSSEC, considered a cornerstone of the modern Internet, has no negative impact on business but is a challenge for users' tools and knowledge and is expensive to support as a service.
- There is a clear intention of the EU to support the uptake of standards at the policy level, including IPv6, DNSSEC, email security like SPF and DMARC, HTTPS, etc. Aligning incentives for adoption might be considered.

6. Segment – Awareness Raising & Capacity Building

6.1 Recommendations

This segment covers the following recommendations:

(24) The harmonisation/approximation of the practices of ccTLDs by the adoption of the good practices available.

(26) Awareness-raising and knowledge-building activities to make the consumers, IPR holders, or other affected parties aware of existing measures tackling DNS abuse.

(27) Knowledge-sharing and capacity-building activities between all intermediaries and stakeholders involved in the fight against DNS abuse.

6.2 Lightning talks by CENTR, CleanDNS, eco, nic.at:

- **Peter van Roste**, CENTR
- **Jeffrey Bedser**, CleanDNS
- **Thomas Rickert**, eco
- **Robert Schischka**, nic.at

Peter van Roste, CENTR, explained that one of the most important tasks and goals of CENTR is the exchange of best practices and ideas. To this end, CENTR conducts working groups, surveys, meetings, and calls. These efforts include (test) projects to cooperate on DNS abuse, e.g., by sharing data on maliciously registered domains, although there are some legal difficulties regarding data protection.

There are also projects and test environments to verify registration data, e.g., based on eID. It is still open as to how eID will be implemented in all 27 Member States of the European Union. It is often very helpful for ccTLDs to have cooperation agreements with their local governments for sector-specific security policies, and the sharing of best practices and soft policies, such as with Covid-19-related measures.

Thomas Rickert, eco Association, explained that topDNS will promote the exchange of information and expertise. The initiative is currently working on a curriculum for training for hosting and email service providers, contracted parties and LEAs. The curriculum will include recommendations on open-source and commercial tools. The group also provided comments on the DNS abuse study and hosted a workshop at the Nordic Domain Days in Stockholm in May 2022, where the Stockholm recommendations were compiled:

1. Publish an anti-abuse policy covering DNS abuse and contact details for abuse reports.
2. Have staff that is trained to process DNS abuse reports.
3. Try to find out if there are DNS abuse issues with your customers.
4. Be responsive to abuse reports.
5. Pass on reports you cannot handle to a party that is better placed to take action.
6. Explore opportunities for the exchange of intelligence.
7. Use tools. They provide data, insights, and guidance.
8. Act swiftly if the issue requires urgency.
9. Let proportionality guide your actions.
10. Be part of the solution, not the problem.

6.3 Contributions and main findings

In the discussion that followed, it was reiterated that standards for evidence across the industry are key to automation and scalability. It was also pointed out that collaboration with LEAs is extremely important and needs to be expanded. There is a constant need to learn from each other with data and information in order to collaborate effectively. Often, especially on substantive issues, key liability and law enforcement expertise is required. There are still gaps in knowledge that need to be filled and relationships of trust built. In addition, clear instructions from LEAs are more helpful than asking intermediaries for favours.

In the context of cooperation with LEAs, it was mentioned that there is – and will always be – a constant need for education, as good law enforcement resources are often poached by the industry sooner or later. The constant expansion of the Internet will also lead to more reports of abuse in the future. Policymakers and rights holders still have an incorrect picture of what can and cannot be done, e.g., that blocking IP addresses is not useful. LEAs in the upcoming GNSO PDP need to be heard through the RAA at ICANN so that the work is not just based on assumptions. It was also explained that the topDNS initiative is already on track to provide training for registrars to investigate DNA misuse in the near future.

Another recommendation was added with transparency reports that give an overview of what intermediaries are actually doing to fight abuse online.

From the perspective of some participants, it was argued that trademark owners are still in the situation where abuse reports often go unanswered. INTA explained that it provides training and materials to its members to improve the quality of reports and target different intermediaries. The WHOIS toolkit was presented to explain how to obtain and access information. As before, the need for trusted spaces to share information was emphasised. Based on the DNS abuse study, rights holders see contracted parties in a position to act next if hosting providers do not respond.

The contracted parties present expressed their understanding for the frustration of trademark owners, especially in the context of phishing. They pointed out that, e.g., CENTR and I&J already provide excellent content on how to deal with this. Nevertheless, IP infringements are often difficult to assess without more detailed investigations. Therefore, relationships with expert organisations are vital to curbing content misuse. Somebody saying that he is not the right party to take action does not mean that these issues are not important.

It was also argued that it is not a good idea to blame registrars and registrars. Abuse helpdesks often monitor suspicious domain names manually. For hosting providers offering shared hosting environments, reporting only an IP address is often not helpful. Web space hacking and compromised domain names are also monitored, and affected customers are notified immediately. If a hosting provider does not respond, try to hold them accountable, but do not blame DNS providers instead. For certain types of content abuse, e.g., fake shops, it is often not easy to confirm and verify the abuse. There are collaborations with trusted partners and reporters that help with some of these types of abuse.

Other issues raised:

Some participants emphasised the lack of clarity not only about the roles and responsibilities of actors but also the lack of clarity about obligations. Work still needs to be done on the working procedures between the actors in the identification process. It was also stressed that law enforcement and trusted notifiers still need to be involved more closely in these discussions.

A need for training and sharing of best practices with law enforcement agencies was also identified. Further points of discussion were the transmission of evidence, transparency reporting and documentation. In this context, it was pointed out that the information provided in transparency reports must be meaningful.

7. Summary of Findings & Conclusions

7.1 Collection of impressions and priorities from participants

The participants were asked to speak about:

- Which measures should take priority.
- Which measures can be implemented quickly.
- Potential cost implications.

Gemma Carolillo, DG CONNECT, went first to state:
Policy measures and regulations define the scope of responsibility of operators and help provide legal certainty. For example, NIS2 now provides a legal framework for DNS operators regarding domain name registration data with a clear set of obligations. Also the Digital Services Act, which considers DNS operators as intermediaries, provides the operators with the liability exemption for the information transmitted or accessed (on the basis of respect of basic due-diligence obligations) and establishes that they can receive orders from competent authorities to take action against illegal content.

It is very important that DNS operators and the other different layers of the stack, including hosting providers, now work out a scheme for roles and responsibilities. The scheme should provide for notifications and communication channels. This would really be a big step forward to ensure that both those who suffer harm and those who are willing to contribute in the form of notifications know what happens to reported incidents and to ensure that there is meaningful follow-up, i.e. that people are not inundated with notifications to which they cannot respond.

Based on the questions received, she clarified that the European Commission does not necessarily intend to commission another study on the topic of DNS abuse, but it will continue to monitor the situation to see what progress is made and assess whether policy intervention is needed or not. ;

For the European Commission, however, it is particularly important that a division of labour is sought and that agreements between the parties are clear, enforceable and effective. At this stage, no particular format is prescribed, it is to be seen what can be achieved through voluntary agreements, such as a code of conduct, or contractual agreements.

Other participants commented as follows:

- An anti-abuse kit in a box would be a great idea.
- eco's topDNS initiative is working on training for staff in the abuse departments and the LEA. These training materials will include a list of tools to be used, both open-source tools and commercial tools that can be used.
- Generic abuse policies are required.[5]
- People who are dealing with abuse should get in touch with each other and tell each other what they have identified as abuse so that others can pick up on this and look for it as well.
- People who are starting to do something about abuse should be trained by people who have already dealt with abuse so that they can become productive more quickly.
- The Trust & Safety Professionals Association (https://www.tspa.org) should be considered. Perhaps this concept should be extended to Europe.
- Trust is key and needs to be built. It needs to be created before we start automating. Existing initiatives should be examined.
- We need to ensure that there is less inbound abuse, e.g., by using DMARC, IPv6.
- DNSSEC should be supported by those who are able to do so.
- The suggestion that new domain registrations should go live with email functionality disabled by default and that it needs to be 'manually switched on' was raised but was met with concern from registrars.
- The eco Association is working on a tool to empower users: a topDNS scam adviser website in German and English in 2023.
- LEAs should be at the table next time, as the people behind the scams need to be held accountable. However, expectations should not be too high due to jurisdictional issues and problems of evidence. It may be possible to catch the stupid criminals, but not the clever ones.
- A trusted space for collaboration between registries, registrars, hosting companies, CDNs, mail providers, rights holders, CERTs and LEAs is needed. eco offers to continue work on such a space (topDNS Hub).
- Existing projects like NetBeacon and ACID should be promoted.
- There should be a list of "bad" domain names that registrars can share so that they do not "transfer" these names to avoid hopping between registrars.
- The competitive aspect should be eliminated, and co-operation encouraged.
- Operators should track what abuse they see, share information about it and take action that will have the greatest impact.
- There are responses to almost all issues and measures on all recommendations. However, most of these measures are not applied industry-wide or across silos. Therefore, it is important to promote projects such as QPI, APEWS, etc., to ensure that they are publicised and implemented by more actors. eco offers to host a webinar series on all these best practices to create a repository of material that everyone can refer to.
- Low-hanging fruits may have a quick impact, but criminals will then carry out more sophisticated attacks that require more sophisticated responses and more budget. We need to be prepared for this.
- ICANN's pilot project SSAD or WHOIS Disclosure System should be supported.
- Regarding the validation and verification of registration data, participants prefer a risk-based approach.

7.2 Conclusions and main findings

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:

- **Fast takedowns of malicious and compromised domain names are key.** But DNS abuse cannot be tackled with a single solution. There must be a well-orchestrated approach with concrete actions that enable people to work together towards a common goal.
- **There is often a chance to prevent abuse before it is reported.** There is a need for a trusted space for collaboration and intelligence information sharing among all parties involved. There are already initiatives in place. A discussion along the entire value chain is needed to identify the right ones for scaling. topDNS will prioritise the dialogue on this in 2023 with its partners to operationalise this crucial cornerstone.
- **Automation is indispensable in this context.** The effort of fighting abuse online has to be as quick and efficient as possible and kept at a reasonable level from a cost perspective. Also, the industry has to keep up with the malicious actors.

[5] The DNSAI has a range of materials on its website, including a generic policy against abuse: https://dnsabuseinstitute.org/generic-abuse-policy-for-registrars-and-registries/

- **Building trust. Personal relationships between the actors involved is key.** It's a people business. topDNS and the eco Association will use their broad, cross-industry membership to bring together those who can make a difference by working together.
- **Automatic responses to abuse reports** are the first step towards improving communication between actors and building trust.
- **Developing training opportunities for all actors along the value chain.** The topDNS initiative will offer educational support to newcomers in dealing with abuse in 2023.
- **Creating "Anti-Abuse Kits/Toolbox in a Box".** These training opportunities mentioned above will include recommendations of (non-)commercial tools for different intermediaries/target groups to guide through the first steps.
- **There is a chance to initiate a cultural change, for example by implementing current technical standards.** Abuse prevention/treatment/combating does not necessarily have to be a cost centre. In saturated markets, it is becoming increasingly interesting as a business model (network hygiene). The anti-abuse working group at the eco Association is already promoting this approach among its members and is always willing to share best practices.
- **Commercial incentives and reputation-based measures** have proven to support and accelerate development in this direction. Targeted approaches should be considered in favour of regulatory measures.
- **Building a schedule of roles and responsibilities** with agreements on who does what for all actors along the value chain. The eco initiative topDNS has published an Abuse Table to provide guidance on which cyber threats are considered to be abuse of the Domain Name System – and which parties should be contacted first. This table will be further developed.

The participants agreed that there should be a public report based on the discussions and findings of the two-day workshop and a follow-up workshop in 2023.

Out of these points, the following three topics have been identified as priority issues:

- **Trainings.**
- **Establishing a trusted space of collaboration, including opportunities for automation.**
- **Building a schedule of roles and responsibilities to provide for co-operation and swift action by the various types of intermediaries.**

Thomas Rickert closed the workshop by thanking the participants and especially Lars Steffen, eco Association, who ensured that the preparation and the workshop ran smoothly.

List of Appendices:

Annex 1: **eco slide deck introducing eco, topDNS and the workshop**

Annex 2: **eco table of abuse scenarios and parties to be approached**

topDNS

An initiative by eco

eco – Association of the Internet Industry
Lichtstr. 43h, D-50825 Cologne, Germany
phone: +49(0)221/700048-0
fax: +49 (0)221 / 700048-111
info@eco.de, https://international.eco.de
@eco_de, @ecoverband

eco

ASSOCIATION OF THE INTERNET INDUSTRY