WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

eco

**Comment on the Study on Domain Name System (DNS) Abuse (1st edition, manuscript completed in January 2022)**

Berlin, 10 May 2022

## I. Introduction

The eco Association welcomes the attempt by the European Commission and the authors to "analyze the scope, impact and magnitude of DNS abuse." The present "Study on Domain Name System (DNS) abuse" is one of the most comprehensive studies on this topic.

For more than 25 years, eco has been intrinsically motivated to make sure that abuse and illegal content are combated and that crimes are prosecuted. Cooperating with the various stakeholders in the process is as important to us as neutrality and transparency. The eco Complaints Office reports regularly on its experiences in combating illegal content online, proactively or on request (among others by participating in hearings, expert meetings, workshops).

The eco Names & Numbers Forum brings together more than 140 companies from the Domain industry. It represents representatives from all parts of the domain industry: ccTLDs, legacy & new gTLDs, registries, registrars & resellers, technical service providers, consultants and experts from the secondary market. The eco Complaints Office accepted a study workshop invitation and took the chance to inform about its working approach and successes. Therefore, we would like to take the opportunity to contribute our expertise to respond to some assumptions, recommendations, and results presented in the study and submit the following comment.

## II. Broad and inconsistent definition of DNS abuse

The study defines DNS abuse broadly as "any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity." This definition is more expansive than the working definition currently used by ICANN's registries and registrars and ICANN Org, which define DNS abuse as being "composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam when spam serves as a delivery mechanism for those other forms of DNS abuse." The latter is more appropriate to the scope and remit of ICANN as technical coordinator for the DNS, which does not include regulating content. However, the issue of DNS abuse is not limited to gTLDs, but concerns gTLD and ccTLD registries and registrars as technical intermediaries of DNS services.

The expansion of the scope of the definition does not help. It seems not only to ignore the ecosystem of different intermediaries such as hosting services, access providers etc. that operate and use the Domain Name System but

also their different roles and responsibilities that, in many cases, allow a more targeted approach against content abuse. The authors consider all illegal activities online to be DNS abuse. According to this broad definition, a fraudulent message sent via a messenger service or illegal postings on social media platforms, for example, would be considered DNS abuse. Under this logic, the registrar of the domain name used by the messenger service (e.g., “messengerservice.com”) might be considered to be liable and could be required to take the domain name offline. Without differentiating DNS abuse from other types of abuse, such as content abuse, it would be more sensible to discuss abuse on the Internet in general. The problem that we see with such a broad definition of DNS abuse is that many stakeholders involved in this discussion might think that every kind of abusive behavior on the Internet should be considered DNS abuse – that ICANN, registrars, and registries should solve.

At the same time, the study does not touch upon the existing intermediary liability framework in the European Union and the upcoming Digital Services Act. Both include principles of limited liability, set strict boundaries for monitoring obligations by intermediaries, and define notice and action procedures for hosting providers.

In addition to the phenomenon of ‘DNS abuse’, the effect thereof is defined in the study as follows: “DNS abuse disrupts, damages or otherwise adversely impacts the DNS and the Internet infrastructure, their users or other persons.” This definition of the effects caused by DNS abuse is inconsistent with the definition used by the authors. According to the study, content-related abuse does not have an impact on the infrastructure level and “mitigation is only recommended on the hosting level, not on the DNS level.” Types of abuse that cannot be handled on the DNS level should not be considered DNS abuse.

On this note, we appreciate the efforts of the study to distinguish different layers or thresholds for action to address DNS abuse. The distinction between maliciously registered and compromised domain names is key to quickly resolving abuse. We also strongly agree with the authors that DNS level action for certain types of DNS abuse, e.g., compromised domain names, can be “counterproductive” as it can create collateral damage, which victimizes the registrant and users of the domain name services.

Moreover, these cases require a proportionate approach involving other actors, e.g. the hosting provider or registrant, who are in a better position to address the alleged abuse, which may include removing pieces of content or patching software vulnerabilities at the hosting level. In contrast, registries and registrars only have the option of suspending a domain name, which can disable all the services connected to the domain name, e.g. website, email server, etc.

## III. DNS abuse in the NIS 2.0 Directive

Regarding the European Commission‘s proposal for a revised Directive on Security of Network and Information Systems, the NIS 2.0 Directive, the

authors acknowledge that the recent legislative proposal on cybersecurity measures will be the first legal instrument within the EU that introduces the term ‘DNS abuse’. However, the proposal, adopted by the European Commission and under discussion within the European Parliament and the European Council, does not yet provide a definition of DNS abuse, leaving an unnecessary and negligent lack of legal certainty.

The absence of a definition in the European Commission’s proposal for NIS-2.0 and the introduction of a very broad definition of the term in a study commissioned by the Commission is a dangerous combination. This situation could lead to the impression the broad definition might be endorsed by the European Commission for future implementations of the NIS-2.0 directive because, under current EU legislation, there is no exact definition of DNS abuse that could be otherwise referred to.

Instead of just simply broadening the scope, eco advocates for initiatives to create legal clarity and security for intermediaries to take action. Governments – including the European Commission – are already involved in the Internet & Jurisdiction Policy Network to work in this direction. The promotion and adoption of the already developed toolkits would have a far more tangible impact than just working on new definitions for the same issue.

## IV. Methodology

- Data basis

Due to the very broad definition of DNS abuse, it is hard to compare the data used in the study to other data sets. Also, the decision by the authors to keep the sample size small makes it difficult to compare the data with other data sets. The 2.8 million reports and 1.6 million domain names that make up the sample used in the study is what members of eco see in just a single day of data.

This very small sample size makes it hard to argue that the data is statistically significant in any other period of time than a day. So, it is a very thin slice of data. Preferably, the dataset should have been at least 90 days, but ideally 180 or 365 days.

With this slim dataset, it is very difficult to predict trends or developments. Given that the selection of registries and registrars prominently used for malicious registrations and the hosting providers currently being hacked to compromise domain names is subject to trends, this would have been valuable and would have given much more meaning to the report.

The 2.8 million reports and 1.6 million domain names that have been used in the study are quite diverse and include URLs, IP addresses, hashes, and domain names.

Research by eco members on the dataset used for the study comes to the conclusion that hostnames and domains have been conflated. From eco’s perspective, Uniform Resource Locators (URLs) and IP addresses should

not be considered DNS abuse. This approach works under the study's broad definition. Still, we strongly disagree that this is the right path because domain name registrars and registries cannot deal with URLs, IP addresses, or subdomains on a technical level.

- Use of Reputational Block Lists to measure DNS abuse rates

The authors of the study recommend "that the abuse rates of TLD registries or registrars be monitored on an ongoing basis by independent researchers in cooperation with institutions and regulatory bodies…." While, in principle, this concept of monitoring abuse rates may sound reasonable, we believe the use of Reputational Block Lists (RBLs) as a means to measure DNS abuse is not the appropriate one.

Reputational Block Lists are an effective tool when used in the correct context; they were originally designed to protect networks and end users from security threats. In that context, they are liberal as to what is ingested and conservative as to what is removed. For security practitioners, RBLs are an effective and useful tool for helping an enterprise construct a defense security approach.

However, in the context of studying domain abuse, these RBLs were not designed nor intended to be used as a measurement tool. Understanding how RBLs are constructed, vetted, and assessed over time is important. Some RBLs are crowd-sourced — not evidence-based — and little is known about how reporters and individual reports are vetted.

- Access to and accuracy of WHOIS data & the ICANN multistakeholder model

The study seems to put an outsized emphasis on the importance of registration information (WHOIS data), conflating customer data with WHOIS data. NIS 2.0 proposes similar language related to the verification of domain registration data, which would be problematic for registries (and registrars) who do not have a direct relationship with the registrant data subject. The authors seem to have heavily bought into the belief that accurate and widely available WHOIS data will somehow prevent DNS abuse but provide little evidence to that effect. This approach disregards the EU General Data Protection Regulation (GDPR) and the interpretation of the Regulation by the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS). It is worthwhile noting that the Art. 29 Working Party reached out to ICANN as early as 2005 to raise concerns about the unlimited availability of registration data via the public WHOIS and the unlawfulness of that processing of personal data.

Access to data by legitimate access seekers such as law enforcement bodies is already adequately defined in the more appropriate Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (e-Evidence Regulation).

What also seems to be neglected is that registrars have a billing contact for every registered domain name. This contact information is verified through the billing process and provides a good starting point for investigations as required.

The study notes the inconveniences that redacted contact data causes to those with legitimate purposes for accessing registration data, but there is no mention of the illegitimate purposes previously unredacted data was used for or the harms to the data subject this caused. For example, domain registration contact data has often been used as a source for phishing and spam attacks. Because of this, users were trained to use invalid data for WHOIS records in the past. Most directories including personal data are not public in most countries for good reason.

Public WHOIS was a privacy issue. The issue is not that WHOIS data is no longer public but that it was in the past. There are no other products or services where buyers/owners are published in a globally accessible public database.

The authors of the study also call for a centralized system for the submission of registration data requests to ensure data accessibility. First of all, thick WHOIS registries already have this kind of information through EPP commands during the registration and updates of the registrant data. If a registry is aware of abusive behavior in relation to a domain name, the registry should request the registrar to take care of it. Secondly, Article 23 of the NIS-2 Directive counteracts the current multistakeholder policy development process at ICANN to develop a System for Standardized Access/Disclosure.

A policy development process at ICANN (EPDP on the Temporary Specification for gTLD Registration data) has recommended the establishment of a Standardized System for Access and Disclosure (SSAD), through which data disclosure requests would be processed. Diverging disclosure requirements that would need to be processed by registries and registrars would undermine the creation of such a centralized system, leading to the fragmentation and duplication of efforts.

The recommendation that “TLD registries, registrars, and resellers should verify the accuracy of the domain registration (WHOIS) data […] through possibly harmonized Know Your Business Customer (KYBC) procedures” and “eID authentication in accordance with the eIDAS Regulation” disregards the fact that half of the EU Member States do not have an eID scheme implemented. Furthermore, there is no procedure in place to scale this on the global level. Even if this approach would be feasible, in the vast majority of phishing and malware attacks, the criminal party does NOT own the domain name, but the domain names used are third-party domain names / compromised domain names. Therefore, the identification will not help to mitigate abuse in these cases.

The warranted immediate remedial action in these cases is the suspension of the domain name and for that, the ownership of the domain name is not relevant.

As mentioned above, we are concerned that the study and the European regulation of the processing of registration data will call the role of ICANN and of ccTLD registry operators into question. Through the Governmental Advisory Committee (GAC), the European Commission is actively following and is involved in these processes.

The study characterizes the work done by ICANN and the community as “unachieved” and “ineffective” and assumes the “reluctance or refusal by the majority of domain name registrars and registries to take action when the domains they service are used for IPR infringement. The same can be said for domain name registrars, with the majority being unresponsive to reports of DNS abuse based on IPR infringement.” However, the authors fail to reconcile ICANN’s efforts and achievements with its limited scope and remit. Case in point, hosting providers, whom the study acknowledges as important actors to act on cases of harmful content, do not have a contractual relationship with ICANN. Unlike gTLD registries and registrars, hosting providers are not subject to ICANN enforcement, and no comparable recommendations are suggested for them.

## V. Fact-based conclusions required

The study claims 44.3% of interviewed intellectual property stakeholders were not aware of “measures (mandatory, voluntary, proactive, reactive) put in place by the domain registries, registrars, hosting providers, and other DNS service providers to combat abuses involving domain names.”

Against the background of this significant lack of expertise by intellectual property stakeholders, the authors irritate with a number of strong and non-evidence-based statements that they claim to agree with:

> “NGOs, trade and industry associations reported to the authors that the measures used by DNS service providers are not sufficiently effective in addressing DNS abuse. While many providers’ terms of service foresee provisions that would enable those providers to take action against abusive activities, the most of them do not enforce the provisions and remain inert even in front of obvious abuses and well-founded abuse reports. They argued that the effectiveness of the measures deployed fluctuates according to DNS service providers. Those stakeholders also stated that domain registration information (WHOIS data) disclosure request forms and abuse reporting forms (if any) are not easily accessible, sometimes hidden and vary significantly between providers. Therefore, they pointed out that EU (statutory) rules should contain clear, strict, and harmonized provisions on DNS service providers’ accountability and should legally oblige them, in particular registries and registrars to have and make available a transparent domain name registration database, validate the data to include in that database by registrant identity verification (KYBC procedures) and that any suspicious, reported activity ought to be promptly addressed through harmonized and transparent notice-and-action procedures.

> Some stakeholders suggested strengthening the collaborations with authorities, hotlines, and trusted notifiers."

Without providing further details on the research (e.g., sample size, number of responses, statistical significance, error margins, etc.) or which questions have been asked, one might argue that this approach does not meet the required methodological requirements.

It should also be considered that this lack of knowledge might lead to a sizable number of incomplete abuse reports that cannot be processed and resolved. Therefore, eco supports the study´s recommendation to "encourage knowledge-sharing and capacity-building activities between all intermediaries and stakeholders involved in the fight against DNS abuse." Various registry operators have processes in place to address cases of confirmed abuse, whether technical or related to content.

eco also agrees with the recommendation that "DNS service providers should establish or improve collaboration with trusted notifiers which have proven expertise in determining the illegality of website content." For the latter, many registries are already working with trusted notifiers to help with the identification of domain names in connection with CSAM or illegal online distribution of opioids.

In this context, the authors again disregard the GDPR and the risks of liability that come along with it for domain name registries and registrars:

> "However, since May 2018, ICANN and domain name registration services have prioritized their own risks under the GDPR over the interests of parties legitimately policing unlawful online activity by restricting access to WHOIS data, which effectively shields the operators of illegal websites and creates an environment that allows DNS abuse to flourish. It impedes legitimate enforcement of intellectual property rights by rightholder groups against websites proliferating infringing content, causing substantial economic harm to rightholders."

## VI. Selected recommendations

- Financial Incentives, Abuse Rates Monitoring

The study recommends financially rewarding registries and registrars to raise barriers to abuse. It is not clear as to how this recommendation could work within the existing contracted parties' agreements and whether such measures could be effective in curbing abuse. While the carrot-and-stick approach might sound good in principle, we believe that more analysis is required to determine the appropriateness of such a system. This analysis should consider, at a minimum, the different business models and the multi-jurisdictional reality of the industry.

Many hosting providers already charge penalty fees for customers that do not patch their hosting with the latest version of PHP, WordPress, etc. Instead of subsidizing hosting companies, it would be easier to scan servers,

see if they are up to date, and issue penalties when they are not patched. The recommendation also remains unclear about the source of funding for the incentives.

- Mandatory Collaboration

The study recommends " requir[ing] the DNS service providers to collaborate with EU and Member States' institutions, law enforcement authorities (LEA) and so-called trusted notifiers or trusted flaggers." We kindly suggest that the authors clarify the meaning of "requiring" the DNS service providers, e.g., registries and registrars, to collaborate with the EU and various other entities. We are supportive of good faith collaboration, but we discourage mandatory collaboration.

Another item that needs clarification is the issue of scale and legal framework of potentially hundreds of entities wanting to report DNS abuse incidents to a registry or registrar. Typically, registries and registrars do not have the expertise to investigate certain types of abuse, e.g., IPR infringement or other content-related issues. Therefore, it would be irresponsible to set expectations that these issues would be resolved at the DNS level.

As the study describes, DNS abuse type 3, "abuse related to domain names distributing malicious content", in most given examples should be mitigated on the hosting level, not on the DNS level.

- Publication of zone file

The authors also recommend that "in the same manner as gTLDs, ccTLD registries should consider publishing DNS zone file data through DNS zone transfer or a system similar to the Centralized Zone Data Service (CZDS) maintained by ICANN." At first sight, this is not a bad recommendation. However, not only security professionals and law enforcement authorities have access to the CZDS but also criminals. Plus, such information will encourage unwanted practices like drop-catching of domains (i.e. monitoring domain names that are becoming available and registering them in split seconds to monetize them) and more. The use of zone files in the fight against DNS abuse should, therefore, be accompanied by a review of the requirements established by ICANN for gTLDs in connection with granting access to zone files. At present, a registry has almost no justification to not grant access due to the contractual requirements. Access should be limited and in accordance with applicable laws. However, we do not share the view that the publication of zone files will impact the mitigation of DNS abuse in any way, shape, or form.

- Maintain standard email aliases

The recommendation that domain name administrators should also maintain standard email aliases for given domain names (e.g., abuse, hostmaster,

webmaster) so that they can be contacted directly in the event of vulnerabilities and domain name abuse does not add any value. Also, it offers an easy way for attackers to send unwarranted communication to exactly these addresses. However, contactability is a requirement, and there are web forms in place to contact registrants. The domain name administrator is usually the hosting provider or the registrar and can be easily contacted. Interested parties should stop advocating restoring public WHOIS for hosting details and start using other available services, e.g., https://dnslytics.com or https://cybertoolbelt.com.

Note that such recommendations would need further work to be operationalized as there is no enforcement mechanism to make the publication of such contact details an industry standard.

- Allowing intellectual property rights (IPR) holders to preventively block infringing domain name registrations

The recommendation that “TLD registries are encouraged to offer, directly or through the registrars or resellers, services allowing intellectual property rights (IPR) holders to preventively block infringing domain name registrations” is worth exploring in further detail because it removes the registry or registrar from the process of determining whether a string is a trademark or not. The existing TMCH was built for exact matches only. There is a risk that such a matching system might create a considerable number of false positives (e.g. “my-amazon-vacation2022.com” would most likely be blocked) and result in over-blocking, considering that IPRs are not all-encompassing and other legitimate uses of matching domain names may be prevented. Such blocks further carry the risk of limiting free speech in the form of legitimate gripe-sites.

Prioritizing IPR enforcement over other potentially legitimate uses of domain names with the same string (typically non-business-related uses) would endanger human rights such as freedom of expression. The DNS is a general-purpose naming system for all human activities, not a commercial promotion system only. Thus, any preventative measures need to be assessed with utmost caution.

- Predictive algorithms to prevent abusive registrations

Predictive algorithms to prevent abusive registrations by TLD registries and registrars are already in use by a growing number of registries. This measure only helps with malicious rather than compromised domain registration.

**About eco:** With over 1,000 member companies, eco is the largest Internet industry association in Europe. Since 1995, eco has been instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. eco's key topics are the reliability and strengthening of digital infrastructure, IT security, and trust, ethics, and self-regulation. That is why eco advocates for a free, technologically-neutral, and high-performance Internet.