



Study on Domain Name System (DNS) Abuse

Written for the European Commission by
Ivett Paulovics from FASANO PAULOVICS Società tra Avvocati and
Andrzej Duda and Maciej Korczynski from Grenoble INP-UGA
January - 2022

FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI



EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content and Technology
Directorate E — Future Networks
Unit E.3 — Next Generation Internet

Contact: Thomas de Haan

E-mail: CNECT-E3@ec.europa.eu

*European Commission
B-1049 Brussels*

Study on Domain Name System (DNS) Abuse

Manuscript completed in January 2022

1st edition

LEGAL NOTICE

This document has been prepared for the European Commission however it reflects the views only of the authors, and the European Commission is not liable for any consequence stemming from the reuse of this publication. More information on the European Union is available on the Internet (<http://www.europa.eu>).

PDF

ISBN 978-92-76-46586-7

doi: 10.2759/616244

KK-06-22-018-EN-N

Luxembourg: Publications Office of the European Union, 2022

© European Union, 2022



The reuse policy of European Commission documents is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Except otherwise noted, the reuse of this document is authorised under a Creative Commons Attribution 4.0 International (CC-BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

For any use or reproduction of elements that are not owned by the European Union, permission may need to be sought directly from the respective rightholders.

Table of Contents

1. Executive summary	6
2. Main findings and recommendations	10
3. Overview	19
4. Introduction	21
5. Objectives of the study, methodology and limitations	28
a. Objectives	28
b. Methodology	28
c. Limitations	32
6. Definition of DNS abuse	34
a. Definition of DNS abuse proposed by the authors and assessment of the role of the intermediaries in mitigating DNS abuse	34
b. Overview of the definitions used so far	39
c. International level	43
d. EU level	44
e. ICANN level	45
f. Other initiatives	49
g. Assessment of the definitions used by others, shortcomings and gaps	50
7. Magnitude of DNS abuse	53
a. Measurements carried out by the authors	53
b. Questionnaires conducted by the authors	54
c. Results of the secondary research on DNS abuse magnitude	59
d. Impact of DNS abuse and the sectors involved	83
8. Internet of Things (IoT) and 5G: impact on the magnitude and risks associated to DNS abuse	89
a. Internet of Things (IoT)	89
b. 5G	94
9. Regulatory framework of DNS abuse	100
a. Introduction	100
b. Domain registration information (WHOIS data)	101
c. Overview of the regulatory framework	106
d. International level	109
e. EU level	111
f. ICANN level	119
g. Other voluntary initiatives	131
h. Assessment of the regulatory framework, shortcomings and gaps	134
10. Good practices in mitigating DNS abuse	138
a. gTLDs	138
b. ccTLDs	148
c. Overview and assessment of gTLD and ccTLD good practices	162
11. Solutions and recommendations to mitigate DNS abuse	164
12. Acronyms and abbreviations	170

Appendix 1 - Technical Report (separate document)

1. Executive summary

The Domain Name System (DNS) is a hierarchical and decentralised naming system that translates human-friendly mnemonic domain names to numerical Internet Protocol (IP) addresses needed to route traffic across the Internet to the proper destination.

The EU's Cybersecurity Strategy for the Digital Decade (2020) has described the DNS as one of the key parts of the core of the Internet.¹ The European Commission's recent legislative proposal on cybersecurity measures (the Proposal for NIS 2 Directive) has also highlighted that upholding and preserving a reliable, resilient and secure DNS is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend.²

Malicious activities on the DNS have been a frequent and serious issue for years, affecting online security, causing harm to users and third parties and, thus, undermining their trust in the Internet.³ These activities are generally referred to as DNS abuse and comprise cybersecurity threats and the distribution of illegal and harmful materials. However, there is no consensus among stakeholders on the definition of DNS abuse and on what should be collectively done to prevent or fight DNS abuse.⁴ To date, the response to DNS abuse in terms of preventive and reactive measures includes a broad set of voluntary and prescriptive instruments, ranging from technical measures and contractual clauses, to cooperation between DNS operators and competent authorities, and to regulatory actions.⁵ However, past initiatives are fragmented⁶ and, as data shows, have not yet resulted in a significant reduction of DNS abuse.⁷

The European Commission commissioned the present study to assess the scope, impact, and magnitude of DNS abuse, as well as to provide input for possible policy measures on the basis of identified gaps.

The methodology of the study is based on three approaches: i) measurements, ii) questionnaires and in-depth interviews, and iii) workshops. Limitations in the measurements and assessment of the impact are thoroughly accounted for.⁸

The study adopts the following **definition of DNS abuse**:

Domain Name System (DNS) abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity.

¹ EU's Cybersecurity Strategy for the Digital Decade (2020) - <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>

² Recital 15 of Proposal for NIS 2 - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823>

³ Section 7

⁴ Section 6

⁵ Section 9

⁶ Section 9

⁷ Section 7

⁸ Section 5.c

To estimate the **magnitude of DNS abuse**, the authors have conducted primary⁹ and secondary research¹⁰. The measurements took place from March 2021 to June 2021 and concerned the overall health of the Top-Level Domain (TLD) ecosystems, as well as different types of intermediaries such as domain registrars, hosting providers and providers of free services (**Appendix 1 – Technical Report**).

The main findings of the measurements are:

- a) In relative terms, new generic Top-Level Domains (new gTLDs), with an estimated market share of 6.6%, are the most abused group of TLDs (Appendix 1 – Technical Report, Section 5, p. 26).
- b) Not all new gTLDs suffer from DNS abuse to the same extent. The two most abused new gTLDs combined account for 41% of all abused new gTLD names (Appendix 1 – Technical Report, Section 9.2, p. 32).
- c) European Union country code TLDs (EU ccTLDs) are by far the least abused in absolute terms and relative to their overall market share (Appendix 1 – Technical Report, Section 5, p. 26).
- d) The vast majority of spam and botnet command-and-control domain names are maliciously registered (Appendix 1 – Technical Report, Section 10.3, p. 41).
- e) About 25% of phishing domain names and 41% of malware distribution domain names are presumably registered by legitimate users, but compromised at the hosting level (Appendix 1 – Technical Report, Section 10.3, p. 41).
- f) The top five most abused registrars account for 48% of all maliciously registered domain names (Appendix 1 – Technical Report, Section 11.2, pp. 43-44).
- g) Hosting providers with disproportionate concentrations of spam domains reach 3,000 abused domains per 10,000 registered domain names (Appendix 1 – Technical Report, Section 12.3, pp. 48-49).
- h) The overall level of DNS security extensions (DNSSEC) adoption remains low. (Appendix 1 – Technical Report, Section 15.3, pp. 62-63).
- i) There are 2.5 million open DNS resolvers worldwide that can be effectively used as amplifiers in distributed denial-of-service attacks (Appendix 1 – Technical Report, Section 16.4, p. 70).

The DNS is not governed by any international treaty, nor are the ccTLDs that are specific for each EU Member State subject to harmonisation at the EU level. However, international, EU and national laws have significant impact on DNS operators. In Section 9 we analyze different frameworks involved in regulating the Internet and in particular the DNS at international, EU, the Internet Corporation for Assigned Names and Numbers (ICANN), and other voluntary initiative levels.

We gathered the data and inputs from stakeholders with two questionnaires: 1) the first one surveyed registries, registrars, hosting providers, other DNS operators, and 2) the second one surveyed intellectual property rightholders, practitioners, associations, business intelligence, and brand protection companies. The study also collected data from third parties and publicly available reports (secondary research), as well as evaluated the impact of DNS abuse.

Many stakeholders reported to the authors that the measures used by DNS service providers are not sufficiently effective in addressing DNS abuse. Moreover, there are several good practices adopted by intermediaries that ought to be expanded to other DNS service providers, in particular to gTLD and ccTLD registries and registrars. Although specificities in the regulation and practices of the ccTLDs exist and might depend on their national legal frameworks, the harmonisation through the adoption of good practices

⁹ Section 7.a-b and Appendix 1 – Technical Report

¹⁰ Section 7.c

available at the European and international market would enhance online security and EU citizens' and businesses' trust in the DNS and generally in the Internet.

Based on the analyses of measurements and available data, to **prevent, detect and mitigate DNS abuse**, the study proposes a set of **recommendations** addressed to a broad range of actors.

The most important recommendations are summarised below; the full list of the recommendations with explanation are available in Sections 2 and 11:

DNS metadata

- ccTLD registries should, in the same manner as gTLDs, provide a scalable and unified way of accessing complete registration (WHOIS) information using the Registration Data Access Protocol (RDAP) and consider publishing DNS zone file data through DNS zone transfer or a system similar to the Centralized Zone Data Service (CZDS) maintained by ICANN.

Contact information and abuse reporting

- Email addresses of registrants and domain name administrators, otherwise not visible in the public WHOIS, could be displayed as anonymized email addresses in the public WHOIS.
- Domain name administrators should maintain standard email aliases for domain names to report abuse.
- Standardized systems, both for access to registration data (WHOIS data), as for abuse reporting should be set up.

Prevention, detection, and mitigation of DNS abuse

TLD registries, registrars, or resellers, depending on their role, should:

- verify the accuracy of the domain registration (WHOIS) data, among others through harmonised Know Your Business Customer (KYBC) procedures and eID authentication;
- be encouraged to develop and offer similarity search tools or surveillance services to enable third-parties to identify domain names that potentially infringe their rights;
- offer services allowing intellectual property rights (IPR) holders to preventively block infringing domain name registrations;
- be encouraged to use predictive algorithms or other methods to prevent abusive registrations;
- be identified with respect to the concentration and rates of DNS abuse in their ecosystems;
- have abuse rates being monitored on an ongoing basis by independent researchers in cooperation with institutions and regulatory bodies;
- have their accreditation revoked if their abuse rates still exceed predetermined thresholds within a given time period;
- be financially rewarded for lower abuse rates through a reduction in domain registration fees.

Hosting providers should:

- be identified with respect to the concentration and rates of DNS and hosting infrastructure abuse in their ecosystems;
- have abuse rates being monitored on an ongoing basis by independent researchers in cooperation with institutions and regulatory bodies, and their abuse rates not exceed predetermined thresholds;

- be encouraged to develop and use technical solutions that effectively curb hosting and content abuse;
- employ advanced prevention and remediation solutions to quickly curb abuses of hosting infrastructure and subdomain names.

Protection of the DNS operations and prevention of related DNS abuse

- TLD registries and registrars should sign TLD zone files (registries) and domain names (registrars) with DNS security extensions (DNSSEC), facilitate its deployment according to good practices, and be offered discounts for DNSSEC-signed domain names.
- Internet Service Providers (ISP) operating DNS resolvers should configure DNSSEC validation.
- National governments and CERT teams should intensify notification efforts to reduce the number of open DNS resolvers (and other open services) to prevent distributed reflective denial-of-service (DRDoS) attacks.
- The security community should intensify efforts to measure the adoption of email security standards preventing domain spoofing.
- Network operators should deploy IP source address validation protecting the Internet against IP spoofing, distributed reflective denial-of-service (DRDoS) and DNS infrastructure attacks.

Awareness, knowledge building, and mitigation collaboration at EU level

- Harmonise ccTLD operation by adoption of good practices.
- Require DNS service providers to collaborate with EU and Member States' institutions, law enforcement authorities (LEA), and trusted notifiers.
- Encourage awareness-raising and knowledge-building activities to make affected parties aware of existing measures tackling DNS abuse.
- Encourage knowledge-sharing and capacity-building activities between intermediaries and stakeholders involved in the fight against DNS abuse.

2. Main findings and recommendations

The objective of the study is to assess the scope, impact and magnitude of DNS abuse, as well as to provide input for possible policy measures on the basis of identified gaps.

The methodology of the study is based on three approaches: i) measurements, ii) questionnaires and in-depth interviews, and iii) workshops.

To estimate the magnitude of DNS abuse, the authors have conducted real-time measurements of DNS abuse between March 2021 and June 2021. They concerned the overall health of the TLD ecosystems, as well as different types of intermediaries such as domain registrars, hosting providers and providers of free services, and other services.

The analysis and research conducted by the authors show that the existing typologies of DNS abuse, the terminologies and the definitions have much in common and partly overlap. However, consensus on a global and comprehensive DNS abuse definition is still missing. Therefore, the authors of the study conclude that, in order to effectively fight the DNS abuse phenomenon, a broader approach ought to be adopted regarding the DNS abuse definition that considers the great deal of overlap between different categories, and can keep up with the development of the technology and adaptable to the everchanging threat landscape.

As a consequence, we adopt the following definition:

Domain Name System (DNS) abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity.

DNS abuse exploits the domain name registration process, the domain name resolution process, or other services associated with the domain name (e.g., shared web hosting service). Notably, we distinguish between:

1. **maliciously registered domain names:** domain names registered with the malicious intent to carry out harmful or illegal activity
2. **compromised domain names:** domain names registered by bona fide third-party for legitimate purpose, compromised by malicious actors in order to carry out harmful and illegal activity.

The following three categories of actors are involved in DNS abuse:

1. **the abuser / attacker** – the registrant of the maliciously registered domain name or the actor compromising a legitimately registered domain name (e.g., by exploiting vulnerable websites)
2. **the abused party** – Internet users and/or third parties affected by the abuse causing physical, psychological, or economic harms such as minors in case of child sexual abuse material (CSAM), consumer victims of online scams and frauds, intellectual property rights (IPR) holders, etc.

3. **the intermediaries** – DNS operators (notably TLD registries and registrars) and information society service providers (ISSPs)¹¹, including providers of hosting, access, and online platforms operators, as well as regular Internet users of the misused infrastructures that facilitate the distribution of illegal content. They should also be considered as victims (unless they are willingly facilitating malicious activities), because DNS abuse affect their reputation and impose economic costs related to abuse handling. At the same time, this third group of actors plays a key role in effective abuse prevention and mitigation.

DNS abuse can be categorized into **three main types that can also appear combined**:

- Type 1** Abuse related to **maliciously registered domain names**
- Type 2** Abuse related to the **operation of the DNS** and other infrastructures
- Type 3** Abuse related to domain names **distributing malicious content**¹².

Each abuse incident, regardless of the attack type (e.g., phishing, malware distribution), should be considered separately, as it might require mitigation actions by different intermediaries and at different levels (hosting and/or DNS level).

The distinction between the three types helps us to identify relevant entities and levels responsible for mitigation measures and/or best positioned to put them in place:

1. Abuse related to **maliciously registered names (Type 1)** is usually best addressed at DNS level by resellers (if any), registrars, and registries with the following proper remediation path:

Domain reseller (if any) → registrar → TLD registry (at DNS level)

2. **Malicious content** can be distributed using a maliciously registered domain name (**Types 1 and 3**) or it can be distributed using a compromised domain name (**Type 3**), where the domain under which the malicious content is made available is registered by an unaware third-party, which uses it legitimately.

2.1 In case of illegal/harmful content distributed using a **maliciously registered domain name (Types 1 and 3)** (e.g., typosquatted domain name serving phishing content), the following remediation path is to be followed in order to effectively mitigate this abuse:

**Hosting reseller (if any) → hosting provider (at hosting level)
AND**

Domain reseller (if any) → registrar → TLD registry (at DNS level)

Mitigating abuse only at the hosting or DNS level will prevent access to malicious content but will not block *all* elements of the malicious infrastructure. Therefore, both levels have to be involved in the mitigation of this kind of abuse.

¹¹ Providers of any information society service defined by the [Directive \(EU\) 2015/1535](#), any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: i) ‘at a distance’ means that the service is provided without the parties being simultaneously present; ii) ‘by electronic means’ means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; iii) ‘at the individual request of a recipient of services’ means that the service is provided through the transmission of data on individual request.

¹² This type of abuse may take advantage of maliciously registered or compromised domain names.

2.2 While it is also possible for the reseller (if any) / registrar / TLD registry to take action in case of malicious content hosted on a **compromised domain name (Type 3)**, addressing abuse at the DNS level can be counterproductive, as it can cause collateral damage to legitimate registrants. In this case, the site operator, the hosting provider (and where it exists, its reseller) are well positioned to take action to curb the abuse. The remediation path is as follows:

Site operator → registrant (if different from site operator) → hosting reseller (if any) → hosting provider (at hosting level)

Mitigating abuse at the hosting level includes removing malicious content from the hacked website and patching the vulnerability. Site operators are best positioned to mitigate abuse in case of so-called unmanaged dedicated servers that they are in complete control and are responsible for their hosting servers and software. Hosting companies are best positioned to mitigate abuse in case of so-called managed shared hosting as they maintain the operating system and application infrastructure.

3. All entities related to the DNS infrastructure (registrars, registries, resellers, operators of authoritative name servers, and DNS resolvers) are concerned with the abuse related to DNS operations (**Type 2**). This type of abuse is to be addressed **at DNS level**.

To illustrate the types of DNS abuse, we give the following examples of common DNS abuse cases along with the right level of mitigation actions:

Example	Abuse Type 1: related to maliciously registered domain name	Abuse Type 2: related to the operation of the DNS	Abuse Type 3: related to domain names distributing malicious content
Maliciously registered domain name serving phishing content	mitigation action at the DNS level		mitigation action at the hosting level
Compromised website serving phishing content			mitigation action at the hosting level
Compromised website used to distribute (deliver) malware			mitigation action at the hosting level
Maliciously registered domain name used to distribute (i.e., to deliver) spam	mitigation action at the DNS level		
Maliciously registered domain name (e.g., algorithmically generated domain name - DGA) used for malicious command-and-control (C&C) communication (between compromised hosts and a malicious actor)	mitigation action at the DNS level		
File sharing system abused to distribute child sexual abuse material (CSAM)			mitigation action at the hosting level
Maliciously registered domain name used to distribute child sexual abuse material (CSAM)	mitigation action at the DNS level		mitigation action at the hosting level

DDoS attack against a DNS server		mitigation action at the DNS level	
DDoS attack against a web server using DNS open resolvers as amplifiers/reflectors		mitigation action at the DNS level	
Hijacked domain name (e.g., cache or zone poisoning)		mitigation action at the DNS level	

To estimate the magnitude of DNS abuse, the authors have conducted primary¹³ and secondary research¹⁴.

The primary research, consisting among others in real-time measurements of DNS abuse, took place from **March 2021 to June 2021** and concerned the overall health of the TLD ecosystems, as well as different types of intermediaries such as domain registrars, hosting providers and providers of free services, and other services (**Appendix 1 – Technical Report**).

For the purpose of the study, over 2.7 million malicious URLs and 1.68 million unique abused domain names were analyzed.

The key findings of the authors' measurements are:

1. Overall health of TLDs

- In relative terms, new generic Top-Level Domains (new gTLDs), with an estimated market share of 6.6%, are the most abused group of TLDs. In the second quarter of 2021, 20.5% of all abused domain names representing phishing, spam, botnet command-and-control, and malware distribution combined were registered in new gTLDs (Appendix 1 – Technical Report, Section 5, p. 26).
- However, not all new gTLDs suffer from DNS abuse to the same extent. The two most abused new gTLDs combined account for 41% of all abused new gTLD names (Appendix 1 – Technical Report, Section 9.2, p. 32).
- European Union country code TLDs (EU ccTLDs) are by far the least abused in absolute terms, relative to their overall market share. Only 0.8 percent of all abused (maliciously registered and compromised) domain names were registered under EU ccTLDs (Appendix 1 – Technical Report, Section 5, p. 26).

2. Malicious vs. compromised domains: where does the abuse occur?

- The vast majority of spam and botnet command-and-control domain names are maliciously registered (Appendix 1 – Technical Report, Section 10.3, p. 41).
- About 25% of phishing domain names and 41% of malware distribution domain names are presumably registered by legitimate users, but compromised at the hosting level (Appendix 1 – Technical Report, Section 10.3, p. 41).
- When looking at compromised domain names, it emerged that for highly used TLDs such as European ccTLDs, there is a higher incidence (42%) of hacked websites. In TLDs with lower usage rates such as new gTLDs, attackers have a much stronger tendency to register directly the domains they intend to use for their malicious activities (Appendix 1 – Technical Report, Section 10.3, p. 42).
- TLD registries and registrars can prevent malicious registrations (proactive measures) and mitigate maliciously registered domains (reactive measures) at the DNS level. However, they have no control over the hosting infrastructure (unless

¹³ Section 7.a-b

¹⁴ Section 7.c

- they also provide a hosting service) (Appendix 1 – Technical Report, Section 11, p. 42).
- e) The top five most abused registrars account for 48% of all maliciously registered domain names (Appendix 1 – Technical Report, Section 11.2, pp. 43-44).
 - f) Hosting providers with disproportionate concentrations of spam domains reach 3,000 abused domains per 10,000 registered domain names (Appendix 1 – Technical Report, Section 12.3, pp. 48-49).
 - g) Phishers make heavy use of free subdomain and hosting providers because they incur no cost, which makes them practical for serving malicious content. These services are less suitable for distributing spam and botnet command-and-control (Appendix 1 – Technical Report, Section 13, pp. 53-54).

3. Adoption of DNS security extensions and email protection protocols

- a) The overall level of DNS security extensions (DNSSEC) adoption remains low. In a large sample of 227 million domain names, only 9.4 million domains have all the required DNSSEC resource records. 98.1% of these are correctly signed and have been correctly validated (Appendix 1 – Technical Report, Section 15.3, pp. 62-63).
- b) As for EU ccTLDs, .cz (59%), .se (55%), .nl (51%), and .sk (48%) have the highest percentage of domain names signed with DNSSEC. These ccTLD registry operators provide price incentives and technical support for DNSSEC adoption (Appendix 1 – Technical Report, Section 15.3, pp. 63-65).
- c) There are 2.5 million open DNS resolvers worldwide that can be effectively used as amplifiers in distributed denial-of-service attacks (Appendix 1 – Technical Report, Section 16.4, p. 70).
- d) In large sample of 247 million domain names, more than 60% of domain names are without Sender Policy Framework (SPF)¹⁵ and 97% of domains are without Domain-based Message Authentication, Reporting and Conformance (DMARC)¹⁶ records that prevent email spoofing, one of the techniques used in Business Email Compromise (BEC)¹⁷ scams (Appendix 1 – Technical Report, Section 17.3, pp. 74-75).

The DNS is not governed by any international treaty, nor are the ccTLDs that are specific for each EU Member State subject to harmonisation at the EU level. However, international, EU and national laws have significant impact on DNS operators. In Section 9 we analyze different frameworks involved in regulating the Internet and in particular the DNS at international, EU, ICANN, and other voluntary initiative levels.

Many stakeholders reported to the authors that the measures used by DNS service providers are not sufficiently effective in addressing DNS abuse. Moreover, there are several good practices adopted by intermediaries that ought to be expanded to other DNS service providers, in particular to gTLD and ccTLD registries and registrars. Although specificities in the regulation and practices of the ccTLDs exist and might depend on their national legal frameworks, the harmonisation through the adoption of good practices available at the European and international market would enhance online security and EU citizens' and businesses' trust in the DNS and generally in the Internet.

¹⁵ Sender Policy Framework (SPF) is an email authentication protocol designed to detect forging email sender address known as domain or email spoofing.

¹⁶ Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a protocol that extends SPF and gives the domain name owner the ability to protect their domain from unauthorized use (email spoofing).

¹⁷ Business Email Compromise (BEC) is a type of scam involving the hacking, spoofing, or impersonation of a business email address. The victim of a BEC attack receives an email that appears to come from a trusted business.

Based on the primary and secondary research conducted to measure the DNS abuse phenomenon (Section 7), and the extensive analysis of the regulatory framework (Section 9) and the good practices (Section 10), the authors propose the following set of **27 recommendations to prevent, detect and mitigate DNS abuse**¹⁸:

A. Better DNS metadata (for identifying resources and their attribution to intermediaries)

1. Likewise gTLDs, ccTLD registries should provide a **scalable and unified way of accessing complete registration (WHOIS) information** (in compliance with data protection laws), using the Registration Data Access Protocol (RDAP)¹⁹, necessary to attribute abused and vulnerable domain names to their respective registrars and obtain their contact information (Appendix 1 – Technical Report, Section 6, p. 27).
2. 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 ICANN²⁰ (Appendix 1 – Technical Report, Section 5, p. 26).

B. Contact information and abuse reporting

3. The **email addresses of registrants and domain name administrators** that are not visible in the public WHOIS could be displayed as anonymized email addresses to ensure the ability to contact domain owners and administrators directly to notify security vulnerabilities and abuses (Appendix 1 – Technical Report, Section 18.4, p. 79).²¹
4. With no direct contact with domain name registrants and administrators via the public WHOIS database, 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 (Appendix 1 – Technical Report, Section 18.4, p. 79).
5. A **standardized (and potentially centralized) system for access to registration data (WHOIS data)**²² should be set up, identifying the minimum information necessary to process disclosure requests. The reaction time to such requests shall be clearly defined (Section 9.b).
6. The study also recommends to set up a **standardized (and potentially centralized) system for abuse reporting**²³, identifying the minimum information necessary to process such report. The receipt of abuse reports is to be acknowledged. The reaction time to such reports shall be clearly defined and the abuse reporter should be provided with information on the actions taken (Sections 9.f-g). The DNS service providers shall provide for an appeal proceeding against their decisions to a third neutral party (Sections 9.f-g and 10.a).
7. The study encourages the **exchange of information on threats** between parties involved (e.g., Computer Emergency Response Teams – CERTs, security organisations) **using collaborative platforms** such as Malware Information

¹⁸ Section 11 contains a table providing detailed overview of the types of abuses to be addressed, the actors involved, and the actors that should take action.

¹⁹ gTLD registries and ICANN-accredited registrars are required to implement RDAP service since August 2019 - <https://www.icann.org/rdap>

²⁰ <https://www.icann.org/resources/pages/czds-2014-03-03-en>

²¹ This recommendation is without prejudice to current legislation on data protection (GDPR) and the and upcoming legislation that requires to make contact information accessible to legitimate access seekers for cybersecurity purposes (Proposal for NIS2 Directive).

²² ICANN is working on a similar system (SSAD) described in Section 9.b.

²³ A similar system has been proposed by ICANN's Second Security, Stability, and Resiliency (SSR2) Review Team Final Report (Recommendation 13), 2021: <https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf> (see also in Section 9.f)

Sharing Platform (MISP) to report and mitigate abuse in a more effective and timely manner.

C. Improved prevention, detection, and mitigation of DNS abuse Type 1

8. TLD registries, registrars, and resellers should **verify the accuracy of the domain registration (WHOIS) data**. The identification of the registrants could be implemented through possibly harmonised Know Your Business Customer (KYBC) procedures. In case of registrants from the EU, KYBC could be carried out through eID authentication in accordance with the eIDAS Regulation²⁴ ²⁵, as amended by the forthcoming Regulation on the European Digital Identity²⁶. KYBC procedure shall use cross-checks in other publicly available and reputed databases (Section 10 and Appendix 1 – Technical Report, Section 9.2, p. 35).
9. TLD registries are encouraged to **develop or improve existing similarity search tools or surveillance services** to enable third-parties to identify names that could potentially infringe their rights (Section 10 and Appendix 1 – Technical Report, Section 11.2, pp. 44-45).
10. 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** (similar to services already existing on the gTLD market²⁷) (Section 10 and Appendix 1 – Technical Report, Section 11.2, p. 45).
11. The use of **predictive algorithms to prevent abusive registrations** by TLD registries and registrars is also encouraged (Section 10).
12. The study recommends 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 (e.g., ICANN, European Commission, European Union Agency for Cybersecurity – ENISA or national authorities). Abuse rates should not exceed predetermined thresholds. If thresholds are exceeded and the abuse rates do not improve within a given time period, accreditation may be revoked (Appendix 1 – Technical Report, Section 9.2, p. 37).
13. **TLD registries and registrars with lower abuse rates may be financially rewarded**, e.g., through a reduction in domain registration fees, to align economic incentives and raise barriers to abuse (Appendix 1 – Technical Report, Section 9.2, p. 37).
14. TLD registries are also encouraged to:
 - **maintain access to existing domain/URL blacklists**
 - identify the **registrars with the highest and lowest concentrations and rates of DNS abuse** in their ecosystems
 - propose incentive structures to **encourage their registrars to develop methods to prevent and mitigate malicious registrations** effectively (Appendix 1 – Technical Report, Section 11.2, pp. 45-46).

D. Improved detection and mitigation of DNS abuse Type 3

15. In a similar manner with respect to the TLD registries and the registrars, **the abuse rates of hosting providers should be monitored** on an ongoing basis by independent researchers in cooperation with institutions and regulatory bodies (e.g.,

²⁴ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

²⁵ <https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS>

²⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281>

²⁷ [Donuts' Domain Protected Marks List \(DPML\)](#), [Trademark Clearinghouse's \(TMCH\) TReX](#), [Uniregistry's Uni EPS](#), [ICM Registry's AdultBlock](#), [club Registry's club Trademark Sentry](#)

European Commission, European Union Agency for Cybersecurity – ENISA or national authorities). Abuse rates should not exceed predetermined thresholds. Incentive structures should be studied to induce hosting providers to develop technical solutions that effectively curb hosting and content abuse (Appendix 1 – Technical Report, Section 12.3, p. 52).

16. Since free services (e.g., free hosting and subdomains) are commonly exploited in phishing attacks, their operators should **employ advanced prevention and remediation solutions to quickly curb abuses of subdomain names and hosting infrastructure**. They should proactively detect suspicious domain names containing keywords of the most frequently targeted brands and names and work closely with the most heavily attacked companies and develop trusted notifier programs (Appendix 1 – Technical Report, Section 13, p. 55).

E. Better protection of the DNS operations and preventing DNS abuse Type 2

17. Similar to gTLD registries²⁸, the registry operators of ccTLDs should be required to **sign TLD zone files with DNS security extensions (DNSSEC)** and facilitate its deployment according to good practices (Section 10 and Appendix 1 – Technical Report, Section 15.3, p. 60).
18. To facilitate the implementation of DNSSEC, domain administrators (registrants) should have **easy access to DNSSEC signing of domain names within the TLD**. TLD registries should require all registrars that offer domain names in the TLD to support DNSSEC signing for registrants (Section 10 and Appendix 1 – Technical Report, Section 15.3, p. 62).
19. As an incentive to the deployment of DNSSEC, TLD registries might **offer discounts for DNSSEC-signed domain names** (Section 10 and Appendix 1 – Technical Report, Section 15.3 p. 63).
20. Internet Service Providers (ISP) that operate DNS resolvers should configure **DNSSEC validation** to protect end users from cache poisoning attacks and ensure the integrity and authenticity of domain name resolutions (Appendix 1 – Technical Report, Section 16, p. 67).
21. National Computer Emergency Response Team (CERT) teams should subscribe to data sources that identify open DNS resolvers. National governments and CERT teams should intensify **notification efforts to reduce the number of open DNS resolvers** (and other open services), which are among the root causes of distributed reflective denial-of-service (DRDoS) attacks (Appendix 1 – Technical Report, Section 16.4, p. 71).
22. Security community should intensify efforts to continuously **measure the adoption of the Sender Policy Framework (SPF)²⁹ and Domain-based Message Authentication, Reporting, and Conformance (DMARC)³⁰** protocols especially for high-risk domain names and raise awareness of the domain spoofing problem among domain owners and email service providers. Correct and strict SPF and DMARC rules can mitigate email spoofing and provide the first line of defence against Business Email Compromise (BEC)³¹ scams (Appendix 1 – Technical Report, Section 17.4, p. 76).

²⁸ <https://www.icann.org/en/announcements/details/domain-name-system-security-extensions-now-deployed-in-all-generic-top-level-domains-23-12-2020-en>

²⁹ Sender Policy Framework (SPF) is an email authentication protocol designed to detect forging email sender address known as domain or email spoofing.

³⁰ Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a protocol that extends SPF and gives the domain name owner the ability to protect their domain from unauthorized use (email spoofing).

³¹ Business email compromise (BEC) is a type of scam involving the hacking, spoofing, or impersonation of a business email address. The victim of a BEC attack receives an email that appears to come from a trusted business.

23. Network operators should deploy **IP source address validation (SAV)**³² not only for outgoing but also for incoming traffic at the edge of a network. It provides an effective way of protecting closed DNS resolvers from different external attacks against DNS infrastructure, including possible zero-day vulnerabilities within the DNS server software (Appendix 1 – Technical Report, Section 19, p. 80).

F. DNS abuse awareness, knowledge building, and mitigation collaboration at EU level

24. At EU level, the study recommends the harmonisation/approximation of the practices of ccTLDs by the **adoption of the good practices** available at European and international level (Section 10).
25. The study recommends to require the **DNS service providers to collaborate with EU and Member States' institutions, law enforcement authorities (LEA) and so-called trusted notifiers or trusted flaggers**. Where informal collaborations exist, they are to be further strengthened and formal processes are to be set up for the parties to interact (Section 10).
26. The study encourages **awareness-raising and knowledge-building activities** to make the consumers, IPR holders, or other affected parties aware of existing measures tackling DNS abuse (Section 10).
27. The study encourages **knowledge-sharing and capacity-building** activities between all intermediaries and stakeholders involved in the fight against DNS abuse (Section 10).

³² Source Address Validation (SAV) verifies that a packet has been sent from a valid source address.

3. Overview

The study is structured as follows:

Section 4 – Introduction

This section presents the main concepts of DNS, the estimation of the size of the registration market, and the overview of the DNS ecosystem.

Section 5 – Objectives of the study, methodology and limitations

In this section, we present the study objectives and the methodology based on three approaches: i) measurements, ii) questionnaires and in-depth interviews, and iii) workshops. We discuss the methods of conducting measurements and their limitations. In addition to evidence and data gathered from a variety of sources, the study builds upon an appropriate mix of qualitative and quantitative techniques including real-time measurements (**Appendix 1 – Technical Report**), questionnaires, in-depth interviews with key stakeholders, and the organisation of two workshops with a selected number of leading experts.

Section 6 – Definition of DNS abuse

This section gives the definition proposed by the authors and provides examples of the recurrent abuse types. As the DNS encompasses a large ecosystem of different types of intermediaries that maintain the technical DNS infrastructure and hosting, this section also discusses the role of intermediaries in addressing abuse depending on both the type of abuse and the services they provide. Furthermore, this section analyses other approaches and terminologies related to DNS abuse at international, EU, and ICANN levels, identifying the flaws, shortcomings and gaps.

Section 7 – Magnitude of DNS abuse

In this section, we present the results of real-time measurements carried out by the authors (the details appear in the **Technical Report** annexed to the present study as **Appendix 1**), as well as the data and inputs from stakeholders gathered with two questionnaires: 1) the first one surveyed registries, registrars, hosting providers, other DNS operators; 2) the second one surveyed intellectual property rightholders, practitioners, associations, business intelligence and brand protection companies. We also include data collected from third parties and publicly available reports (secondary research), as well as the impact of DNS abuse and the involved sectors.

Section 8 – Internet of Things (IoT) and 5G: impact on the magnitude and risks associated to DNS abuse

This section explores the relation of IoT and 5G networks with DNS abuse. The advent of IoT contributes to the increase of security risks related to the DNS abuse and the adoption of the Internet protocols in the 5G core may expose mobile networks to new threats.

Section 9 – Regulatory framework of DNS abuse

In this section, we analyse different frameworks related to the Internet and the DNS including: private and public law regulation, private-public arrangements, self-regulation, and technical code at international, EU, and ICANN levels.

Section 10 – Good practices in mitigating DNS abuse

In this section we identify and review DNS industry good practices.

Section 11 – Solutions and recommendations to mitigate DNS abuse

This section provides an overview of the recommendations for mitigation of DNS abuse categorized according to the types of abuses to be addressed, the actors involved, and the actors that should take action to mitigate DNS abuse.

Section 12 – Acronyms and abbreviations

This section contains the acronyms and abbreviations most frequently used in the study.

Appendix 1 – Technical Report

This appendix presents the details of the results of real-time measurements carried out by the authors on different aspects of the DNS operation.

4. Introduction

The **Internet** is the global system of interconnected computer networks, often described as a network of networks.

The **Internet Protocol (IP)** is the principal communication protocol underlying the Internet that allows networks of devices to communicate with each other. IP addresses are unique numbers assigned to every device connected to the Internet. Thus, among other functions, IP addresses are used to identify and locate devices connected to the Internet and to route IP packets to their intended destinations.³³

The **Domain Name System (DNS)** is part of the application layer of the Internet on which the proper functioning of the Internet critically depends.³⁴ DNS is a hierarchical and decentralised naming system that translates human-friendly mnemonic domain names to numerical IP addresses.³⁵ In particular, the DNS is a distributed database where the nodes of the database are **name servers**. The naming system is hierarchical. Each domain has at least one **authoritative name server** that publishes information about that domain and the name servers of any domains subordinate to it. At the top of the domain name hierarchy is a group of root name servers. When looking up a domain name to retrieve a numerical IP address, the DNS works as a distributed directory service. The process called **domain name resolution** starts with a query sent to a **root name server**, which starts a recursive resolution process that will end up with a query to the authoritative name server that returns an IP address for the domain name.³⁶

A domain at the top of the naming hierarchy of the DNS is the **Top-Level Domain (TLD)**, called also extension or suffix. TLDs are separated into two groups: 1) generic Top-Level Domains (gTLDs), and 2) country-code Top-Level Domains (ccTLDs). gTLDs include general purpose TLDs, such as .com, .net, .org, etc., often referred to as legacy domain names, as well as over 1.200 new generic TLDs (new gTLDs), such as .online, .shop, .lawyer, .pizza, introduced in the root zone gradually starting from 2013.³⁷ ccTLDs are reserved for use by countries, territories, and geographical locations identified in the ISO 3166-1 country codes list, such as .eu for the European Union, .fr for France and .jp for Japan. Since 2009, ccTLDs may apply for internationalised domain names (IDN) in scripts other than US-ASCII, such as Arabic, Chinese, Cyrillic. The new gTLD program also allowed the addition of IDN gTLDs in the root zone, such as شبكة (web in Arabic), 游戏 (game in Chinese), сайт (site in Russian).

³³ The Internet Protocol has two addressing schemes: version 4 (IPv4) and version 6 (IPv6). IPv4 was developed in the early 1980s. It uses 32-bit address space providing 4.3 billion unique IP addresses that has already been fully allocated to Internet service providers (ISPs) and users. IPv6 is the next generation of IP with a 128-bit address space, providing 340 undecillion addresses.

³⁴ A brief description of how DNS works can be found at the website of the Internet Corporation for Assigned Names and Numbers (ICANN) - <https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en> and the Council of European National Top-Level Domain Registries (CENTR) - <https://www.centri.org/education/the-dns.html>.

³⁵ “The Domain Name System (DNS) helps users to find their way around the Internet. Every computer on the Internet has a unique address - just like a telephone number - which is a complicated string of numbers called its IP address (IP stands for Internet Protocol). IP addresses can be hard to remember. The DNS makes using the Internet easier by allowing a familiar string of letters - the domain name - to be used instead of the arcane IP address. For instance, you only need to type <https://icann.org> to reach our website, instead of the IP address 192.0.43.7” - <https://www.icann.org/en/icann-acronyms-and-terms/domain-name-system-en>.

³⁶ Schwemer, S., Mahler, T. & Styri, H. (2020). Legal analysis of the intermediary service providers of non-hosting nature - <https://op.europa.eu/en/publication-detail/-/publication/3931eed8-3e88-11eb-b27b-01aa75ed71a1/language-en/format-PDF/source-179885922>

³⁷ Delegated strings: <https://newgtlds.icann.org/en/program-status/delegated-strings>

According to **Verisign**, the registry operator of .com and .net, at the end of Q1 2021, there were 363.5 million **domain name registrations** across all TLDs, of which 207 million gTLD registrations and 156.5 million ccTLD domain name registrations. Total registrations decreased by 3.3 million or 0.9% year over year. The .com and .net TLDs had a combined total of 168 million domain name registrations, of which 154.6 million .com and 13.4 million .net domain names. The new gTLD registrations were 22.8 million (6.3% of the total TLD registrations), a decrease of 9.5 million registrations or 29.3% year over year. The largest TLDs by number of reported domain names were .com, .cn, .tk, .de, .net, .uk, .org, .nl, .ru and .br. As of 31 March 2021, there were 308 ccTLD extensions delegated in the root zone, including IDN. The top 10 ccTLDs were .tk, .cn, .de, .uk, .nl, .ru, .br, .fr, .eu and .it, representing the 64.3% of all ccTLD domain name registrations. The most registered new gTLDs were: .xyz, .online, .top, .site, .club, .vip, .icu, .shop, .app, .work.³⁸

According to the **Council of European National Top-Level Domain Registries (CENTR)**, at the end of 2020, the **global market** was estimated at 354 million domains split between ccTLDs (38%) and gTLDs (62%). 92% of the gTLDs were held by the top 10 gTLDs. The median growth of European ccTLDs in 2020 reached a 6-year high of 4.4%. The underlying reason for the surges in demand is considered to be linked to the COVID-19 pandemic-related lockdowns across Europe and the need of many businesses to move from offline to online. The high demand also highlights the importance of ccTLDs to European businesses and citizens as a means of getting online. The growth of the European ccTLDs continued in 2021 and at the end of Q1 was 4.9%. As for content, over a sample of European ccTLDs CENTR data showed that 25% of domains queried were broken or had no functioning content (e.g. HTTP/DNS errors, timeouts etc). A further 16% led to a registrar holding (parked) page. These figures tended to be higher for gTLDs. Based on web scans, 43% of gTLD domains queried were broken or had no functioning content (e.g. HTTP/DNS errors, timeouts etc). A further 22% led to a registrar holding (parked) page.³⁹

Figure 1: Global market share by registrations (source CENTR)

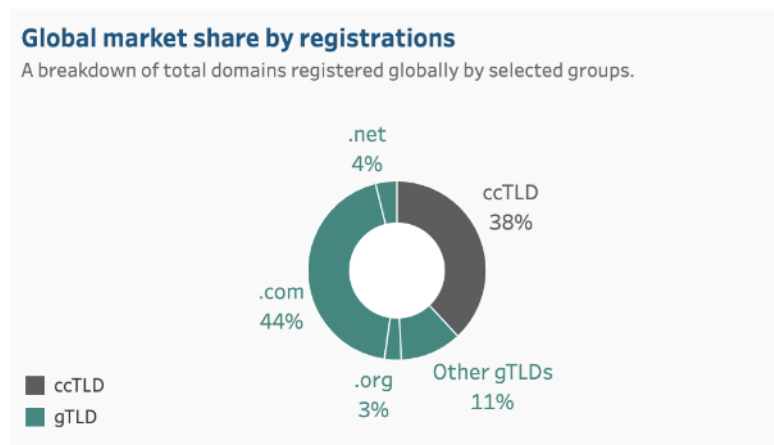
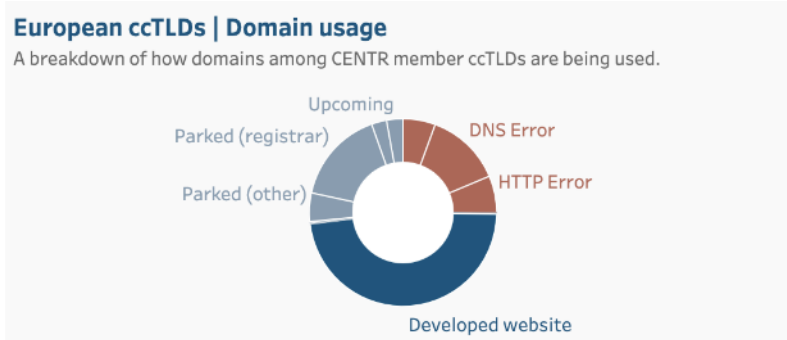


Figure 2: European ccTLDs domain usage (source CENTR)

³⁸ https://www.verisign.com/en_US/domain-names/dnib/index.xhtml

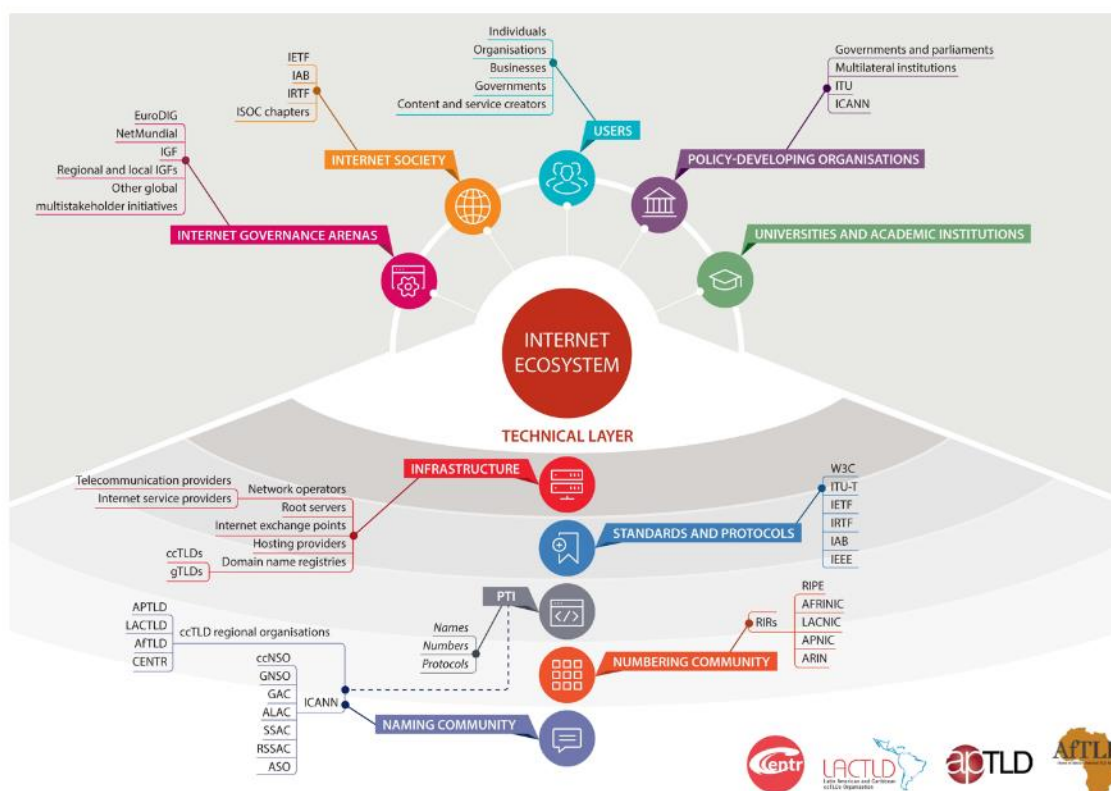
³⁹ <https://stats.centr.org/stats/global#europe>



As of 30 June 2021, the total number of **.eu domain name registrations** was 3,731,298 with an average renewal rate of 85.6% and 212,228 new registrations in Q2.⁴⁰ End-users of the .eu TLD include individuals, businesses from different industry sectors⁴¹ and other entities, as well as EU institutions, agencies, and bodies. In June 2021, from a random sample of 100,000 domain names, EURid found that more than 80% of domains had active web services, and 15% were DNSSEC signed. Out of those names, more than 44% resolved into a structured website.

The DNS is part of a large **ecosystem** composed of several public and private actors operating on a national, regional, and international level and of a wide community of stakeholders.

Figure 3: Internet governance ecosystem (source CENTR)



⁴⁰ EURid Quarterly Update. Q2 2021 Progress Report - https://eurid.eu/media/filer_public/b2/fe/b2fe65b5-7ae0-43ce-9c01-7e6c29ea16b0/quarterly_report_q2_2021.pdf

⁴¹ EURid's .eu website categorization - <https://eurid.eu/en/news/uptake-of-eu-use-for-the-trade-and-it-sectors/>

The **Internet Corporation for Assigned Names and Numbers (ICANN)** is an international private law organisation, specifically a non-profit public benefit corporation, set up on 18 September 1998 under California law. It is a key actor in Internet governance.⁴² Its mission is to ensure the stable and secure operation of the Internet's unique identifier systems.⁴³ It

⁴² Other actors include the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), the Internet Engineering Steering Group (IESG), the Internet Research Task Force (IRTF), the World Wide Web Consortium (W3C), the Internet Society (ISOC), etc., elaborating in particular technical or organizational specifications and procedures about the Internet (e.g., Request for Comments – RFC of IETF).

⁴³ ICANN Bylaws, Section 1.1 Mission:

“(a) The mission of the Internet Corporation for Assigned Names and Numbers (“ICANN”) is to ensure the stable and secure operation of the Internet's unique identifier systems as described in this Section 1.1(a) (the “Mission”). Specifically, ICANN:

(i) Coordinates the allocation and assignment of names in the root zone of the Domain Name System (“DNS”) and coordinates the development and implementation of policies concerning the registration of second-level domain names in generic top-level domains (“gTLDs”). In this role, ICANN's scope is to coordinate the development and implementation of policies:

For which uniform or coordinated resolution is reasonably necessary to facilitate the openness, interoperability, resilience, security and/or stability of the DNS including, with respect to gTLD registrars and registries, policies in the areas described in Annex G-1 and Annex G-2; and

That are developed through a bottom-up consensus-based multistakeholder process and designed to ensure the stable and secure operation of the Internet's unique names systems.

The issues, policies, procedures, and principles addressed in Annex G-1 and Annex G-2 with respect to gTLD registrars and registries shall be deemed to be within ICANN's Mission.

(ii) Facilitates the coordination of the operation and evolution of the DNS root name server system.

(iii) Coordinates the allocation and assignment at the top-most level of Internet Protocol numbers and Autonomous System numbers. In service of its Mission, ICANN (A) provides registration services and open access for global number registries as requested by the Internet Engineering Task Force (“IETF”) and the Regional Internet Registries (“RIRs”) and (B) facilitates the development of global number registry policies by the affected community and other related tasks as agreed with the RIRs.

(iv) Collaborates with other bodies as appropriate to provide registries needed for the functioning of the Internet as specified by Internet protocol standards development organizations. In service of its Mission, ICANN's scope is to provide registration services and open access for registries in the public domain requested by Internet protocol development organizations.

(b) ICANN shall not act outside its Mission.

(c) ICANN shall not regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide, outside the express scope of Section 1.1(a). For the avoidance of doubt, ICANN does not hold any governmentally authorized regulatory authority.

(d) For the avoidance of doubt and notwithstanding the foregoing:

(i) the foregoing prohibitions are not intended to limit ICANN's authority or ability to adopt or implement policies or procedures that take into account the use of domain names as natural-language identifiers;

(ii) Notwithstanding any provision of the Bylaws to the contrary, the terms and conditions of the documents listed in subsections (A) through (C) below, and ICANN's performance of its obligations or duties thereunder, may not be challenged by any party in any proceeding against, or process involving, ICANN (including a request for reconsideration or an independent review process pursuant to Article 4) on the basis that such terms and conditions conflict with, or are in violation of, ICANN's Mission or otherwise exceed the scope of ICANN's authority or powers pursuant to these Bylaws (“Bylaws”) or ICANN's Articles of Incorporation (“Articles of Incorporation”):

(A)

(1) all registry agreements and registrar accreditation agreements between ICANN and registry operators or registrars in force on 1 October 2016, including, in each case, any terms or conditions therein that are not contained in the underlying form of registry agreement and registrar accreditation agreement;

(2) any registry agreement or registrar accreditation agreement not encompassed by (1) above to the extent its terms do not vary materially from the form of registry agreement or registrar accreditation agreement that existed on 1 October 2016;

(B) any renewals of agreements described in subsection (A) pursuant to their terms and conditions for renewal; and

(C) ICANN's Five-Year Strategic Plan and Five-Year Operating Plan existing on 10 March 2016.

has responsibility for IP address space allocation, protocol identifier assignment, gTLD and ccTLD system management, and root server system management functions.

ICANN performs the actual technical maintenance work of the Central Internet Address pools and DNS root zone registries pursuant to the Internet Assigned Numbers Authority (IANA) function contract with the National Telecommunications and Information Administration (NTIA) of the United States Department of Commerce (DOC) dated 9 February 2000, renewed and amended several times. The contract regarding the IANA stewardship functions expired on 1 October 2016, formally transitioning the functions to the global multistakeholder community within ICANN.

ICANN is based on a multistakeholder model and a consensus-driven decision making according to its Bylaws. The Bylaws require that ICANN engages with several review teams, supporting organisations and advisory committees. The policy development process is led by the Generic Names Supporting Organization (GNSO)⁴⁴ and are adopted by the Board of Directors. Consensus policies are policies that accredited registrars and gTLD registries are required to follow. ICANN's agreements with these parties (ICANN-contracted parties) require compliance with stated procedures and with consensus policies.⁴⁵ ICANN Bylaws also require a periodic assessment of the security, stability, and resiliency (SSR) of the DNS.⁴⁶

Stakeholders at ICANN include: gTLD registries and registrars, ccTLD registries, regional Internet registries that manage the regional distribution of Internet number resources including IP address and autonomous system numbers, the thirteen root name server operators, commercial interests – including those representing large and small businesses, intellectual property interests and providers of internet and other communications services; non-commercial interests – including non-commercial users and not-for-profit organizations, governmental interests – including national governments, multi-national governmental organizations, and treaty organizations (gathered in the Governmental Advisory Committee – GAC with key role in providing advice to ICANN on issues of public policy, and especially where there may be an interaction between ICANN's activities or policies and national laws or international agreements⁴⁷), distinct economies, technical experts from industry and academia, and representatives of Internet users worldwide.⁴⁸

Figure 4: ICANN multistakeholder model (source: ICANN)

(iii) Section 1.1(d)(ii) does not limit the ability of a party to any agreement described therein to challenge any provision of such agreement on any other basis, including the other party's interpretation of the provision, in any proceeding or process involving ICANN.

(iv) ICANN shall have the ability to negotiate, enter into and enforce agreements, including public interest commitments, with any party in service of its Mission”

- <https://www.icann.org/resources/pages/governance/bylaws-en/#article1>.

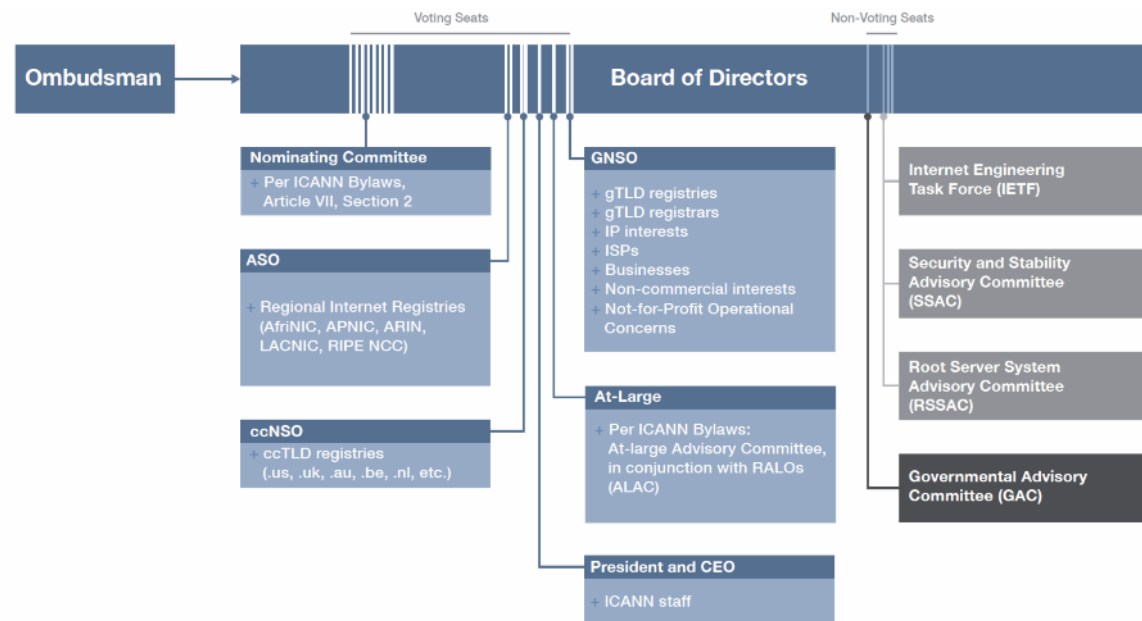
⁴⁴ <https://gnso.icann.org/en/about/council>

⁴⁵ <https://www.icann.org/resources/pages/registrars/consensus-policies-en>

⁴⁶ ICANN Bylaws Section 4.6(c)(i): « *The Board shall cause a periodic review of ICANN's execution of its commitment to enhance the operational stability, reliability, resiliency, security, and global interoperability of the systems and processes, both internal and external, that directly affect and/or are affected by the Internet's system of unique identifiers that ICANN coordinates ("SSR Review").* » - <https://www.icann.org/resources/pages/governance/bylaws-en/#article4>

⁴⁷ <https://gac.icann.org/>

⁴⁸ More details on ICANN's multistakeholder model at: <https://www.icann.org/community>



The governance of the gTLD namespace by ICANN is contractual, with a network of contracts, between, respectively, ICANN, registries, registrars, data escrow providers, and eventually between the registrants and the registrars with which they deal.⁴⁹ The management of the ccTLD namespace varies from informal to formal contracts between some countries or territories and ICANN. Some countries/territories also have statutory regulation of their ccTLD (e.g., the European Union for .eu).

The EU's Cybersecurity Strategy for the Digital Decade has recently described the DNS as one of the key parts of the core of the Internet.⁵⁰ The Directive on measures for a high common level of security of network and information systems across the Union (NIS Directive) defines the DNS as a hierarchical distributed naming system in a network which refers queries for domain names.⁵¹ The European Commission's recent Proposal for NIS 2 Directive has proposed to update the definition into a hierarchical distributed naming system which allows end-users to reach services and resources on the internet.⁵² The importance of the DNS is recognised in both the NIS Directive and Proposal for NIS 2 Directive. The latter proposal has indeed highlighted that upholding and preserving a reliable, resilient and secure DNS is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend.⁵³

While the reliability, resilience and security of the DNS are of paramount importance for the effective functioning of the economy and society, **malicious activities on the DNS** have been a frequent and serious issue for years, affecting online security, causing harm to users and third parties and, thus, undermining their trust in the Internet, which need to be addressed.⁵⁴ These threats and malicious activities are generally referred to as **DNS abuse**.

⁴⁹ <https://www.icann.org/en/registry-agreements?first-letter=a&sort-column=top-level-domain&sort-direction=asc&page=1>

⁵⁰ EU's Cybersecurity Strategy for the Digital Decade (2020) - <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>

⁵¹ Article 4(14) of Directive (EU) 2016/1148 on measures for a high common level of security of network and information systems across the Union (NIS Directive) - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148>

⁵² Article 4(13) of Proposal for NIS 2 - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823>

⁵³ Recital 15 of Proposal for NIS 2 - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823>

⁵⁴ Section 7

Furthermore, the interplay between the DNS and new technological developments such as **the Internet of Things (IoT)**⁵⁵ or **5G** might exacerbate these threats, not only by linking them to physical infrastructures beyond the virtual world, but also by multiplying the potential sources of vulnerability of the DNS.⁵⁶

A part of the Internet ecosystem where publishers can host or exchange information without revealing their identities or locations is the **dark web**. Although the dark web uses the IP protocol, it uses encryption and the Onion Router (TOR) to protect users from surveillance and traceability. The dark web does not use the DNS to resolve domain names. Instead it uses TOR's hidden service names, delegated from .onion, a special-use TLD. Due to the anonymity, privacy, and characteristic to defeat traffic analysis, TOR networks and dark web in general attract users wanting to keep their activities or marketplaces secret and untraceable. Such marketplaces offer a wide range of illegal goods and services, such as illegal drugs, weapons, counterfeit goods, stolen credit cards or breached data, digital currencies, national identity cards or passports, malware, spam campaigns to distributed denial-of-service (DDoS) attacks, etc. As mentioned, dark web visitors do not use the public DNS to resolve .onion names to IP addresses – instead, resolution occurs using the entirely separate TOR hidden service protocol. This protocol helps services make their existences known and helps clients find services, while preserving the anonymity and the location (IP address) of both client and service. Since the dark web does not use the DNS, it is out of scope of this study to analyze it in details.

To date, the response to DNS abuse, in terms of **preventive** and **reactive measures**, includes a wide-ranging set of voluntary and prescriptive instruments, ranging from technical measures and contractual clauses, to cooperation between DNS operators and competent authorities, to regulatory actions.^{57 58 59 60 61 62} However, past initiatives have not yet resulted in a significant reduction of DNS abuse.⁶³

Moreover, the **definition of DNS abuse** differs among different categories of stakeholders and there is no consensus on **what should be done collectively** to prevent or fight DNS abuses, including inside and outside the ICANN community.

Against this backdrop, the **European Commission** commissioned the present study to assess the scope, impact, and magnitude of DNS abuse as well as to provide input for possible policy measures on the basis of identified gaps. The focus is on the European market and regulatory framework but, given the global nature of the phenomenon, the study also assesses, as far as possible, the broader DNS market and governance framework.

⁵⁵ ICANN Security and Stability Advisory Committee (SSAC) 28 May 2019: <https://www.icann.org/en/system/files/files/sac-105-en.pdf>

⁵⁶ <https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis>

⁵⁷ <https://www.icann.org/resources/pages/framework-registry-operator-respond-security-threats-2017-10-20-en>

⁵⁸ http://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf

⁵⁹ <https://eurid.eu/en/register-a-eu-domain/apews/>

⁶⁰ <https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html#specification11>

⁶¹ <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en>

⁶² <https://www.icann.org/octo-ssr/daar>

⁶³ Section 7

5. Objectives of the study, methodology and limitations

a. Objectives

The overall objective of the study is to provide the European Commission with the comprehensive **assessment of the DNS abuse phenomenon and how to address it**.

The main objective can be further refined in the following sub-objectives:

1. The study aims at **defining and measuring the DNS abuse phenomenon, identifying and categorising recurring types of abuses**, whether these are related to the exploitation of the DNS infrastructure, such as in the case of cybersecurity threats, or to the distribution of harmful or illegal content. The study provides **a broad definition of DNS abuse** taking into consideration the different abuse categories, their magnitude and their impact. The study also assesses **the role of all the involved actors** including those at the international level in addressing DNS abuse.
2. The study provides a brief description of the **impact of DNS abuse on the European economy and society**, also in comparison to the international level. The study provides an overview of the sectors that are affected the most. Furthermore, the study explores the possible **impact of technological developments (such as IoT and 5G)** on the magnitude and risks associated to DNS abuse.
3. The study provides a comprehensive **overview of the existing policies, applicable laws, and relevant industry practices to address DNS abuse**, whether related to the DNS infrastructure or to the distribution of harmful or illegal content. Considering the international dimension of the phenomenon, this mapping exercise covers the European market, as well as policies adopted at the international level, in particular in the framework of ICANN. The study assesses the **effectiveness of those measures and identify possible gaps and shortcomings**.
4. On the basis of the previous analysis, the study provides **recommendations for improvements** in the different categories of remedies to address DNS abuses to guide possible future policy development.

b. Methodology

The study is based on both **primary and secondary research**.

Evidence and data were gathered from a variety of sources, such as relevant individual stakeholders, trade associations, experts, academics, public or government bodies and published studies as well as other publications, such as reports and academic journals. These sources included relevant data/statistics and documentation available from these institutions and organisations (non-exhaustive list): European Commission; Eurojust; European Union Agency for Cybersecurity (ENISA); European Union Intellectual Property Office (EUIPO); Europol; European Intellectual Property Prosecutors Network (EIPPN); Interpol; Federal Bureau of Investigation (FBI); Council of Europe; Organisation for Economic Co-operation and Development (OECD); Internet Corporation for Assigned Names and Number (ICANN); Internet Watch Foundation (IWF); INHOPE; Council of European Top-Level Domain Registries (CENTR); eco – Association of the Internet Industry; Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG); EURid (.eu); other European ccTLD registries (.be, .dk, .fr, .nl, .no, .pt, .uk, etc.); gTLD registries (Verisign Inc., Public Interest Registry – PIR, Donuts Inc., etc.); other intermediaries (UNR, Com Laude – Valideus, Leaseweb Global B.V., OVHcloud); World Intellectual Property Organisation (WIPO); International Trademark Association (INTA); European Communities

Trade Mark Association (ECTA); Alliance for Safe Online Pharmacies (ASOP); Internet & Jurisdiction Policy Network (I&JPN).

In the context of **primary research**, an appropriate mix of qualitative and quantitative techniques were used, which included the conduction of real-time measurements (**Appendix 1 – Technical Report**), questionnaires and in-depth interviews with key stakeholders, and the organisation of two workshops with a selected number of leading experts.

The authors conducted two questionnaires. One questionnaire was addressed to the main registries and a representative sample of the main registrars providing services in the EU (both gTLDs and ccTLDs). The other questionnaire was addressed to a representative sample of stakeholders other than registries and registrars. The questionnaires were accessible online or sent by email to representatives of the registries and registrars and other stakeholders (nearly 1,500 addressees). The authors conducted 20 in-depth interviews with key experts and institutions involved in DNS management and abuse prevention. Furthermore, the authors organised and held two workshops (on 12 March 2021 and 12 July 2021) in close cooperation with the Commission, with the participation of EU institutions and agencies, European and international law enforcement authorities, DNS operators, trade and industry associations, cybersecurity experts, academics, and other relevant stakeholders. The workshops were dedicated to discuss the definition of DNS abuse, its types, its magnitude and parties' role and measures to address it.

Below, the detailed description of the methodology used for the **measurements** conducted by the authors (**Appendix 1 – Technical Report**).

The authors first collected the list of abused domain names and URLs and the complete list of all domain names for certain TLDs, or the large sample of domains for the TLDs that do not make their zone files available. To estimate the **prevalence and persistence of DNS infrastructure and content abuse**, the authors used sixteen distinct blacklists generously provided by six blacklist providers: Spamhaus, SURBL, ABUSE.ch, the Anti-Phishing Working Group (APWG), PhishTank, and OpenPhish. They represent URL, fully-qualified domain name (FQDN)/IP address or domain name blacklists of spam, malware distribution, command-and-control (C&C), phishing, and IPR infringement. For the purpose of the study, over 2.7 million incidents (almost 2.17 million involving domain names) and 1.68 million unique abused domain names were analysed.

To calculate the **abuse rates per different actors** involved in the domain name registration and hosting, and the deployment of DNS security technologies, the authors first needed the list of domain names for each TLD. Two sources of data were used: i) zone files whenever available and ii) active web content crawling. Using the approaches, over 251 million active domain names for generic TLDs, new gTLDs, European Union country-code TLDs, and non-EU ccTLDs have been identified.

The methodology for finding information regarding different types of DNS abuse, vulnerabilities, and security technologies relies on active gathering of the following data: i) 'A' resource records to calculate the reputation metrics for hosting providers, ii) registration information using RDAP/WHOIS protocols to calculate the reputation metrics for domain registrars iii) TLD sizes to express the "overall health" of TLD ecosystems iv) information about the deployment of DNSSEC ('DS', 'DNSKEY', and 'RRSIG' resource records), v) open DNS resolvers, and, vi) SPF and DMARC entries in 'TXT' records to measure the deployment of email security extensions.

To measure the **deployment of DNSSEC**, the authors actively collected three DNS resource records for each domain in their database: 'DNSKEY', 'DS', and 'RRSIG'. If the 'DNSKEY' and 'DS' were present, the authors attempted to validate DNSSEC chain using

their recursive (validating) resolver. If the validation succeeded, the domain name was correctly signed.

To measure the **deployment of the Sender Policy Framework (SPF) and Domain based Message Authentication, Reporting and Conformance (DMARC)**, the authors collected SPF records (as part of DNS TXT resource records) of enumerated domains using the ZDNS tool. Then, for those domains with SPF records, they emulated the `check_host()` function as described in RFC 7208 to evaluate the validity and configurations of the records. The next step was to collect the DMARC rules, which exist in the TXT resource records of the `_dmarc` subdomains of the registered domains (e.g., `_dmarc.example.com`). Finally, DMARC rules were evaluated to check their strictness in accepting (delivering to the end-users) and/or rejecting the incoming forged emails.

To identify the **risks of launching reflective DDoS attacks (DRDoS)** through misusing open DNS resolvers, the authors actively scanned for them in IPv4 and IPv6 address spaces and analysed their distribution across organizations and countries. Scanning requires sending DNS requests to end-hosts and inspecting the received responses. The response codes (RCODE) defined in RFC 1035 signal whether the DNS server processes incoming requests. If the query resolution is successful, open resolvers send back the responses to end clients along with NOERROR status code.

The Technical Report (**Appendix 1**) presents several results of the domain name abuse measurements and analysis: i) distribution of the malicious resources and abuse rates per TLDs, ii) distinction between compromised and maliciously registered domain names, iii) registrar reputation metrics based on domain names categorized as maliciously registered, iv) and reputation metrics for hosting providers and countries for different abuse types.

To measure the **reputation of each TLD**, the authors used two security metrics: i) occurrence (the number of unique domains extracted from blacklisted URLs) and ii) ratio (the authors normalised the number of occurrences with respect to the size of a TLD). The TLD reputation metrics express the “overall health” of TLD ecosystems consisting of many types of intermediaries such as domain registrars, re-sellers, hosting, content providers, etc.

To measure the **reputation of each registrar**, similarly to TLDs, the authors used the occurrence of registered domain names and rate as security metrics. The registration data of domain names of blacklisted URLs was collected and parsed as soon as they were blacklisted and the authors computed reputation metrics for domain names that they have determined to be malicious. To estimate the size of registrars, registration information for approximately 241 million domain names (96% of all active domains enumerated) was collected. The authors were able to parse the registration information and match the domain names of about 85% of the RDAP/WHOIS records to their respective registrars. The authors calculated rates as the number of maliciously registered domains per 10,000 registrations.

The authors also built **reputation metrics for hosting providers**, more specifically, information society service providers (ISSPs), including access, hosting, and online platform providers. A common way to measure the “size” of hosting providers is the number of IP addresses routed through the corresponding AS (Autonomous System) or the portion of the routed IP address space. The authors used the number of hosted second-level domains as an estimator, which treats shared hosting fairly.

To **distinguish compromised from maliciously registered domain names**, the authors automatically flagged a domain as maliciously registered if it was registered in a batch (i.e., among the blacklisted URLs, there are at least two domain names registered with the same registrar and at precisely the same time). The authors also automatically flagged a domain name as maliciously registered if the time between registration and blacklisting did not

exceed three months. The period was determined based on a sample of manually labeled spam, phishing, malware, and C&C domains and by tuning the parameter. For phishing attacks, the authors built a list of 230 brand names. From the list of enumerated brand names, the authors generated a list of misspelled versions of brand names using standard methods such as omission, insertion, character substitution, and homographs. If a given FQDN contained a brand name or its misspelled version, the registered domain was also considered to be maliciously registered. The authors excluded all free service providers' domains from the classification because they were neither compromised nor maliciously registered, and the domains for which the authors were unable to collect registration information.

Uptimes (or persistence of abuse) are also measured, i.e., how long a malicious URL (or domain name) has been active since it appeared on one of the blacklists. The authors computed uptimes for different intermediaries and abuse types (phishing, malware and botnet C&C). The authors have developed a specific uptime measurement platform for the purpose of this study. Whenever a newly blacklisted URL appeared in one of the blacklist feeds, the authors received the update on their feed server. The authors automatically collected all data for each URL once it got blacklisted, 5 minutes after blacklisting, 30 minutes, 1 hour, 6 hours, 12 hours, 24 hours, 48 hours after blacklisting, and then every week (12 measurements in total). The data includes the content of the malicious URL, the content of the homepage of the registered domain name, and the WHOIS information of the domain name for each malicious URL the authors found in the blacklist feeds.

To evaluate **how effective are notifications of domain abuse or vulnerabilities** to the domain owners, administrators, and webmasters, the authors have developed a scanner to systematically test available direct contacts of domain owners and administrators. The authors first scanned for the DNS MX records of the domain and selected a mail server with the highest priority. Afterwards, the authors established different connections using the Simple Mail Transfer Protocol (SMTP) to the selected mail server. The authors did not send emails, but verified the existence of an email address using the RCPT TO query followed by the destination email address. For each sampled domain name, the authors generated email aliases using the names defined in RFC 2142: for the domain example.com, the authors tested the validity of the following email aliases: hostmaster@example.com, webmaster@example.com (for DNS and HTTP issues), abuse@example.com (for generic abuse and vulnerability notifications), noc@example.com, and security@example.com (for network security). The authors also scanned for DNS SOA records, extracted the host master contact stored in the RNAME field as defined in RFC 1035 and checked whether the syntax of the email address was correct. To measure the reachability rates of the different TLDs, the authors categorised the domains based on their TLD and sampled domains from each group.

The **lack of inbound Source Address Validation (SAV)** can serve as a vector for DNS zone poisoning attacks that may lead to domain hijacking or cache poisoning attacks even if the DNS resolver is correctly configured as a closed resolver. The authors have developed a method for enumerating networks vulnerable to inbound spoofing. A DNS request of type 'A' was sent to each routable IP address (target address) in a packet with a spoofed source IP address: when sending the request to address "a.b.c.n" the authors chose "a.b.c.n+1" as the source IP address. If there was no filtering in either transit networks or at the network edge, the target received the request. If it was a DNS resolver and the authors' spoofed address matched the list of allowed clients, the resolver resolved the request. As the authors controlled the authoritative name server for the queried domains, they could observe queries sent by the resolver under test, either directly or through a chain of forwarding resolvers.

c. Limitations

Due to the absence of a globally accepted definition of DNS abuse and the limitations of the existing reputation blocklists (as discussed below), it is not an easy task to quantify the exact magnitude of the DNS abuse phenomenon and its impact. While third parties often tend to use a narrower definition, the authors adopted a broader definition including misuses of the DNS aimed to propagate cybersecurity threats and to the distribute illegal and harmful content. However, the DNS abuse phenomenon is bigger than measured or reported, and the exact size of the problem is difficult to estimate exactly.

The authors analysed over 2.7 million incidents and 1.68 million abused domain names, using reputed domain and URL blacklists. However, it is challenging to estimate the extent of the problem.

251 million enumerated domain names were used to calculate sizes of domain registrars and hosting providers. Additional information was collected about hosting infrastructure (by resolving the registered domains to their IP addresses and respective autonomous systems) and domain registrars (by collecting the registrar information using the WHOIS or RDAP protocols). However, not having access to the full list of domain names is a limitation of this work: the authors do not have a complete picture of the market share of registrars and hosting providers and, thus, their abuse rates are only computed on available data. More generally, precise data would allow interested parties to conduct research and develop new insights into the security practices of hosting providers or domain registrars, verify their policies or create reliable reputation metrics.

On the other hand, the TLD size information, relevant to the calculation of abuse rates, does not necessarily involve the requirement of having access to the full list of domain names. The authors used available zone files as the most accurate source of sizes. If these were not available, the authors used the sizes of ccTLDs affiliated with the Council of European National Top-Level Domain Registries (CENTR) whose members had explicitly agreed to make this information available for the purpose of this study. For all other TLDs, the approximate sizes reported by DomainTools were used.

Another limitation of this work was that the authors had no information about specific TLD ecosystems, such as for .es, .gr, or .de domain namespaces, for which the WHOIS information was not available, restricted, or provided only via the web-based service. In these cases, domain names (maliciously registered and benign) could not be mapped to relevant registrars in specific TLD ecosystems and abuse rates calculated.

While the authors could identify registrars for about 85% of collected WHOIS records, there were still many non-standard registrar names that they could not reliably labelled (such as personal names or companies accredited by ccTLD registries locally).

The authors' approach to estimate reputation of hosting providers is not without bias. For example, infrastructure providers may lease their IP space to other, smaller providers such as hosting services. There may be a chain of resellers difficult to identify even for autonomous system (AS) operators. For example, Leaseweb provides services to businesses and generally cannot directly control the end users who may host malicious content. However, affected parties typically contact them in case of abuse, and AS operators should directly contact the reseller, which should mitigate hosting abuse.

Even if the presented measurements have some limitations, their extent is remarkable giving much precise view on the phenomenon than previous studies.

To describe the impact of DNS abuse on the European economy and society and the overview of the sectors that are affected the most, the authors of the study collected and

analysed data from different source regarding the estimated the global cost of cybercrime (McAfee Report for the Center for Strategic and International Studies (CSIS), 2018), the sectors involved in DNS abuse with particular reference to cybersecurity threats and the related trends in 2020 (European Union Agency for Cybersecurity (ENISA) Sectoral/thematic threat analysis, 2020), the rates related to the adoption of security measures by Forbes Global 2000 Companies by industry (CSC Global's Domain Security Report, 2020), the amount of EU imports of counterfeit goods in 2019 (Organisation for Economic Co-operation and Development (OECD) and the European Union Intellectual Property Office (EUIPO) Global Trade in Fakes: A Worrying Threat, Illicit Trade, 2021), the estimated lost sales in certain sectors in the EU as a result of counterfeiting (EUIPO 2020 Status Report on IPR Infringement), the estimated total value of counterfeit pharmaceuticals traded worldwide (OECD and EUIPO Trade in Counterfeit Pharmaceutical Products 2020), the brands and names most targeted by phishing (Appendix 1 – Technical Report), the sectors most targeted by cybersquatting (WIPO statistics regarding domain name disputes 2019). However, the in-depth analysis was hampered by the lack of consistent data at EU and international level and, therefore, further studies would be needed to analyse and assess extensively the economic and societal impact of DNS abuse and its various types on EU citizens and businesses and the sectors which are more exposed to the DNS abuse phenomenon.

6. Definition of DNS abuse

The DNS abuse phenomenon is not new and, as mentioned above, no globally accepted definition of DNS abuse exists. Indeed, different terminologies and definitions have often been used to indicate abusive and malicious activities on the Internet: cybercrime, hacking, malicious conduct, (cyber)security threats, illegal and fraudulent activity, etc. These definitions will be analyzed below.

a. Definition of DNS abuse proposed by the authors and assessment of the role of the intermediaries in mitigating DNS abuse

The authors of the study adopt the following **definition**:

Domain Name System (DNS) abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity.

What does the DNS abuse use?

DNS abuse exploits the domain name registration process, the domain name resolution process, or other services associated with the domain name (e.g., shared web hosting service). Notably, we distinguish between:

1. **maliciously registered domain names**: domain names registered with the malicious intent to carry out harmful or illegal activity
2. **compromised domain names**: domain names registered by bona fide third-party for legitimate purpose, compromised by malicious actors in order to carry out harmful and illegal activity.

What is the effect of DNS abuse?

DNS abuse disrupts, damages or otherwise adversely impacts the DNS and the Internet infrastructure, their users or other persons.

Which actors are involved in DNS abuse?

The following three categories of actors are involved in DNS abuse:

1. **the abuser / attacker** – the registrant of the maliciously registered domain name or the actor compromising a legitimately registered domain name (e.g., by exploiting vulnerable websites)
2. **the abused party** – Internet users and/or third parties affected by the abuse causing physical, psychological, or economic harms such as minors in case of child sexual abuse material (CSAM), consumer victims of online scams and frauds, intellectual property rights (IPR) holders, etc.

3. **the intermediaries** – DNS operators (notably TLD registries and registrars) and information society service providers (ISSPs)⁶⁴, including providers of hosting, access, and online platforms operators, as well as regular Internet users of the misused infrastructures that facilitate the distribution of illegal content. They should also be considered as victims (unless they are willingly facilitating malicious activities), because DNS abuse affect their reputation and impose economic costs related to abuse handling. At the same time, this third group of actors plays a key role in effective abuse prevention and mitigation.

How do we categorize DNS abuse?

DNS abuse can be categorized into **three main types that can also appear combined**:

- Type 1** Abuse related to **maliciously registered domain names**
Type 2 Abuse related to the **operation of the DNS** and other infrastructures
Type 3 Abuse related to domain names **distributing malicious content**⁶⁵.

Each abuse incident, regardless of the attack type (e.g., phishing, malware distribution), should be considered separately, as it might require mitigation actions by different intermediaries and at different levels (DNS level and/or hosting level).

Examples of common DNS abuse cases

To illustrate the types of DNS abuse, we give the following examples of common DNS abuse cases along with the appropriate level of mitigation actions (explained in details below):

Example	Abuse Type 1: related to maliciously registered domain name	Abuse Type 2: related to the operation of the DNS	Abuse Type 3: related to domain names distributing malicious content
Maliciously registered domain name serving phishing content	mitigation action at the DNS level		mitigation action at the hosting level
Compromised website serving phishing content			mitigation action at the hosting level
Compromised website used to distribute (deliver) malware			mitigation action at the hosting level
Maliciously registered domain name used to distribute (i.e., to deliver) spam	mitigation action at the DNS level		
Maliciously registered domain name (e.g., algorithmically generated domain name - DGA) used for malicious command-	mitigation action at the DNS level		

⁶⁴ Providers of any information society service defined by the [Directive \(EU\) 2015/1535](#), any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: i) ‘at a distance’ means that the service is provided without the parties being simultaneously present; ii) ‘by electronic means’ means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; iii) ‘at the individual request of a recipient of services’ means that the service is provided through the transmission of data on individual request.

⁶⁵ This type of abuse may take advantage of maliciously registered or compromised domain names.

and-control (C&C) communication (between compromised hosts and a malicious actor)			
File sharing system abused to distribute child sexual abuse material (CSAM)			mitigation action at the hosting level
Maliciously registered domain name used to distribute child sexual abuse material (CSAM)	mitigation action at the DNS level		mitigation action at the hosting level
DDoS attack against a DNS server		mitigation action at the DNS level	
DDoS attack against a web server using DNS open resolvers as amplifiers/reflectors		mitigation action at the DNS level	
Hijacked domain name (e.g., cache or zone poisoning)		mitigation action at the DNS level	

Who should take action to mitigate DNS abuse and why?

The three types of DNS abuse also differ in terms of which relevant entities and levels are responsible and/or best positioned to put in place mitigation measures:

1. Abuse related to **maliciously registered names (Type 1)** is usually best addressed at DNS level by resellers (if any), registrars, and registries with the following proper remediation path:

Domain reseller (if any) → registrar → TLD registry (at DNS level)

2. **Malicious content** can be distributed using a maliciously registered domain name (**Types 1 and 3**) or it can be distributed using a compromised domain name (**Type 3**), where the domain under which the malicious content is made available is registered by an unaware third-party, which uses it legitimately.

2.1 In case of illegal/harmful content distributed using a **maliciously registered domain name (Types 1 and 3)** (e.g., typosquatted domain name serving phishing content), the following remediation path is to be followed in order to effectively mitigate the abuse:

**Hosting reseller (if any) → hosting provider (at hosting level)
AND**

Domain reseller (if any) → registrar → TLD registry (at DNS level)

Mitigating the abuse only at the hosting or DNS level will prevent access to malicious content but will not block *all* elements of the malicious infrastructure. Therefore, both levels have to be involved in the mitigation of the abuse.

2.2 While it is also possible for the reseller (if any) / registrar / TLD registry to take action in case of malicious content hosted on a **compromised domain name (Type 3)**, addressing the abuse at the DNS level can be counterproductive, as it can cause collateral damage to legitimate registrants. In this case, the site operator, the hosting provider (and where it exists, its reseller) are well positioned to take action to curb the abuse. The remediation path is as follows:

Site operator → registrant (if different from site operator) → hosting reseller (if any) → hosting provider (at hosting level)

Mitigating abuse at the hosting level includes removing malicious content from the hacked website and patching the vulnerability. Site operators are best positioned to mitigate abuse in case of so-called unmanaged dedicated servers that they are in complete control and are responsible for their hosting servers and software. Hosting companies are best positioned to mitigate abuse in case of so-called managed shared hosting as they maintain the operating system and application infrastructure.

3. All entities related to the DNS infrastructure (registrars, registries, resellers – if any – operators of authoritative name servers, and DNS resolvers) are concerned with the abuse related to **DNS operations (Type 2)**. This type of abuse is to be addressed **at DNS level**.

Role of the intermediaries in mitigating DNS abuse

The DNS, along with the IP protocol, is the key service of the Internet, mapping applications, hosts, and services from names to IP addresses. Because the DNS encompasses a large ecosystem of different types of intermediaries that maintain the technical DNS infrastructure and hosting, the role of intermediaries in addressing abuse depends on both the type of abuse and the services they provide.

Registry operators are entities that have been delegated a specific TLD or TLDs and are responsible for administering the TLD(s) including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases, and the distribution of TLD zone files across name servers. For example, Donuts is the registry for the .lawyer TLD, providing domain name registration services for the TLD.

Registrars provide domain name registration services for the TLD(s). They are generally accredited by TLD registries and can be accredited by ICANN.

Domain **resellers** are third-party organizations that offer domain name registration services through a registrar but may be not accredited by a TLD registry or ICANN.

Registrants are individuals or organizations that register domain names through domain registrars or resellers.

DNS providers operate authoritative DNS servers that map domain and host names to the corresponding IP addresses. While registrars usually provide such service, registrants may choose to delegate the responsibility to third-party authoritative DNS services (managed DNS service) to their own servers.

Web hosting providers maintain the server infrastructure used to host content for a given domain.

Hosting providers may sell their services to individuals or other web hosting providers—hosting resellers. Some web hosting providers offer so-called managed hosting by which the hosting providers handle the setup, management, and support of a server and/or applications (such as content management systems). Often, multiple (sometimes thousands) of domain names might be hosted on the same physical server sharing the same IP address. Web hosting providers may also offer unmanaged hosting, for example, a dedicated server with, for example, only an operating system installed, so a user (webmaster) needs to install all the necessary software and keep the software up-to-date. Note that the registrant/webmaster may choose to buy a reverse proxy service that can, for

example, hide the existence and characteristics of the origin server, including the IP address of the back-end server.

Finally, **Internet Service Providers (ISPs)** and access providers typically maintain recursive DNS resolvers that resolve domain names on behalf of the end-user's computer willing to access an application, a host, or a service associated with the domains names. We can highlight that different services can be provided by the same provider (e.g., it is common that registrars offer authoritative DNS services and web hosting plans).

It is also worth mentioning the role of the so-called **trusted notifiers** or **trusted flaggers**.

DNS operators have in place several private arrangements, in the forms of memoranda of understanding, codes of practices or other, with trusted notifiers or trusted flaggers to monitor, assess and mitigate some of the categories of abuses, in particular illegal and harmful content, or other sorts of abuse that may fall under an organisation's policies.⁶⁶ According to the DNS Abuse Framework, trusted notifiers should have recognized subject matter expertise, established reputation for accuracy, and a documented relationship with and defined process for notifying DNS operators.⁶⁷ The trusted notifier scheme is also encouraged by the cited EU legislation.

This complex ecosystem requires a bottom-up approach in handling DNS abuse and the collaboration between different intermediaries. Indeed, to effectively address abuse cases, requiring the abuse reporters the exhaust a rigid linear referral path (website operator - registrant - hosting provider - reseller, if any - registrar - registry operator) is not appropriate.

With respect to DNS abuse involving domain names, such as phishing, malware, IPR infringement, CSAM, etc., the DNS intermediary that detects or is notified about abuse must first assess if a given incident is related to DNS infrastructure and/or content abuse, identify and inform an appropriate party that might be in a better position to make such assessment and address abuse.

Let us assume that a DNS operator (e.g., registry or registrar) receives an abuse notification and concludes that the domain name is registered for maliciously registered purposes based on the collected evidence or the evidence provided by the trusted notifier. In this case, the domain name must be blocked by the DNS service operator, i.e., registry, registrar, domain reseller (if any), or authoritative DNS service provider (if different from the registry or registrar) according to applicable policies. Assume that, in addition, the domain name reveals illegal/harmful content, i.e. it is used to distribute malware, to host CSAM material, or it is a phishing website. In this case, the DNS service operator should, in addition to the takedown at the DNS level, identify and contact a hosting provider using, for example, domain registration information (WHOIS data). The domain name must be blocked within the period specified by applicable laws, but also, the hosting is suspended. Otherwise, as mentioned earlier, after the domain name suspension, the attacker may register another domain name and map the newly registered domain name to the operational hosting service. The hosting operator must suspend the hosting or (if not possible) contact the responsible hosting reseller that must suspend the service. Note that if the domain name uses a reverse proxy service (e.g., Cloudflare), the proxy provider must suspend the service

⁶⁶ For example, Verisign collaborates with the Internet Watch Foundation (IWF), National Center with Missing & Exploited Children (NCMEC), FBI, the US National Telecommunications and Information Administration (NTIA) and the US Food and Drug Administration (FDA); Donuts collaborates with Internet Watch Foundation (IWF), National Center with Missing & Exploited Children (NCMEC), Motion Picture Association of America (MPAA), Recording Industry Association of America (RIAA), UK National Crime Agency (NCA); EURid collaborates with Europol, Interpol, Belgian FPS Economy (economic inspection team), Belgian FPS Finance (customs - cybersquad team), Belgian Prosecutor's Office and Belgian police.

⁶⁷ https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf

and contact the hosting provider of the back-end infrastructure, that must suspend the hosting service.

On the other hand, if a DNS operator receives an abuse notification and concludes, based on the collected evidence, or evidence provided by the notifier, that the domain name is legitimate but compromised (hacked), the DNS operator generally should not suspend the domain name. The notified DNS service operator, i.e., registry, registrar, domain reseller (if any), or authoritative DNS service provider (if different from the registry or registrar), should contact the hosting provider. A provider should not suspend the hosting server (especially a shared hosting server) but it should block access to a malicious website used to host or facilitate the distribution of illegal content. The hosting provider must contact the webmaster (possibly the domain owner) and inform about the incident. For unmanaged services, the hosting provider must contact the webmaster directly to mitigate abuse. If the hosting provider is not in a direct relationship with the end user, it must identify the hosting reseller, who must take appropriate steps.

DNS service providers should also establish or improve collaboration with trusted notifiers which have proven expertise in determining the illegality of website content.

b. Overview of the definitions used so far

The following table summarizes the different terminologies and definitions developed so far at international, EU and ICANN level as well as within other fora:

Level	Category	Instrument	Terminology	Definition / types
International	Hard law - public law regulation - multilateral treaty	Council of Europe's Convention on Cybercrime (Budapest Convention) (2001)	Cybercrime	Illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights.
EU	Hard law - public law regulation - legislative	Directive 2013/40/EU on attacks against information systems	Attack against information systems	Illegal access to information systems, illegal system interference, illegal data interference, illegal interception.
	Hard law - public law regulation - legislative	Regulation (EU) 2019/881 on the European Union Agency for Cybersecurity (ENISA) and on information and communications technology cybersecurity certification (Cybersecurity Act)	Cyber threat	Any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.
	Hard law - public law regulation - legislative	Commission Regulation (EC) No 874/2004 (.eu Regulation)	Speculative and abusive registration	A domain name identical or confusingly similar to a name in respect of which a right is recognised or established by national

				and/or Community law, and where it has been registered by its holder without rights or legitimate interest in the name; or has been registered or is being used in bad faith.
	Hard law - public law regulation - legislative	Regulation (EU) 2019/517 (new .eu Regulation)	Abusive registration	A domain name identical or confusingly similar to a name in respect of which a right is established by Union or national law, and where it has been registered by its holder without rights or legitimate interest in the name; or has been registered or is being used in bad faith.
	Hard law - public law regulation - legislative	Directive (EU) 2016/1148 (NIS Directive)	Incident	Any event having an actual adverse effect on the security of network and information systems.
	Hard law - public law regulation - legislative (proposal)	Proposal for a Directive on measures for a high common level of cybersecurity (Proposal for NIS 2) (2020)	Incident	Any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems.
			Cyber threat	Any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.
			DNS abuse	n/a
	Hard law - public law regulation - legislative	Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Proposal for DSA) (2020)	Illegal content	Any information, which, in itself or by its reference to an activity, including the sale of products or provision of services is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law.
ICANN	Hard law - private law regulation - contractual	Uniform Domain Name Dispute Resolution Policy (UDRP) (1999)	Abusive registration	The domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and The registrant has no rights or legitimate interests in respect of the domain name; and

				The domain name has been registered and is being used in bad faith.
n/a	Registration Abuse Policies Working Group (RAPWG) Final Report (2010)	Abuse		An action that causes actual and substantial harm, or a material predicate of such harm, and illegal or illegitimate, or otherwise considered contrary to the intention and design of a stated legitimate purpose, if such purpose was disclosed.
Soft law - ICANN org explanatory notes	New gTLD Program Explanatory Memorandum Mitigating Malicious Conduct (2009)	Malicious conduct		Abusive activities such as trade mark abuse, phishing, willful distribution of malware or other illegal or fraudulent activity.
Hard law - private law regulation - contractual	Registry Agreement (RA) (2013)	Abusive activity		Distributing malware, abusively operating botnets, phishing, piracy, trade mark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to any applicable law.
Hard law - private law regulation - contractual	Registrar Accreditation Agreement (RAA)	Illegal activity		A conduct, involving use of a registered domain name, that is prohibited by applicable law and/or exploitation of registrar's domain name resolution or registration services in furtherance of conduct, involving the use of a domain name, that is prohibited by applicable law.
n/a	Revised Report on DNS Abuse and New gTLD Program Safeguards (2016)	DNS abuse		Intentionally deceptive, conniving, or unsolicited activities that actively made use of the DNS and/or the procedures used to register domain names.
n/a	Competition, Consumer Trust and Consumer Choice (CCT) Review Team Final report (2018)	DNS abuse		Misuse of the universal identifiers for cybercrime infrastructure and directions of users to websites that enable other forms of crime, such as child exploitation, intellectual property infringement, and fraud.
		DNS security abuse or DNS security abuse of DNS infrastructure		Technical forms of malicious activity, such as malware, phishing, and botnets, as well as spam when used as a delivery method for these forms of abuse.

	Hard law - private law regulation - contractual	Domain Abuse Activity Reporting (DAAR) project (2017)	Domain abuse	Domain name registration and security threat.
			Security threat	Phishing, malware, botnet command-and-control and spam.
	Self-regulation	Contracted Party House (CPH)'s Definition of DNS Abuse (2020)	DNS abuse	Malware, botnets, phishing, pharming, and spam when it serves as a delivery mechanism for the other forms of DNS abuse.
	n/a	Second Security, Stability, and Resiliency (SSR2) Review Team Final Report (2021)	DNS abuse	Intentional misuse of the universal identifiers provided by the DNS for cybercrime infrastructure and directed users to websites that enable other forms of crime, such as child exploitation, intellectual property infringement, and fraud
	n/a	ICANN website – Acronyms and terms (2021)	DNS abuse	Any malicious activity aimed at disrupting the DNS infrastructure or causing the DNS to operate in an unintended manner, including corrupting DNS zone data, gaining administrative control of a name server, and flooding the DNS with thousands of messages to degrade name-resolution services.
			DNS misuse	Any activity that uses the DNS protocol or the domain name registration process to carry out malicious or illegal activity, including hijacking domain names, registering domain names to sell counterfeit merchandise, using the DNS to distribute spam, and exploiting the DNS protocol to launch denial-of-service attacks.
Other	n/a	Internet & Jurisdiction Policy Network's Domains & Jurisdiction Program Operational, Approaches, Norms, Criteria, Mechanisms (2019)	Domain name abuse	Technical abuse (spam, malware, phishing, pharming, botnets and fast-flux hosting) and abusive content (child abuse material, controlled substances and regulated goods for sale or trade, violent extremist content, hate speech and intellectual property violations).
	Self-regulation	DNS Abuse Framework (2019)	DNS abuse	Malware, botnets, phishing, pharming, and spam (when it serves as

				a delivery mechanism for the other forms of DNS abuse).
--	--	--	--	---

In the following subsections the authors analyze in details the definitions above, providing also an assessment of those definitions.

c. International level

Multilateral treaties do not expressly provide a definition for DNS abuse while recognising the importance of the DNS itself and combating its misuse.

The **Budapest Convention on Cybercrime (Budapest Convention)** is a multilateral treaty adopted by the Committee of Ministers of the Council of Europe in November 2001. This Convention is the first binding international instrument criminalising acts committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, and violations of network security.⁶⁸ It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

The treaty currently has 66 parties and another 11 countries that have signed it or been invited to accede.⁶⁹ However, according to the Council of Europe, by 30 June 2021, 158 countries have used it as a guideline or source for their domestic legislation.⁷⁰

The Budapest Convention is supplemented by the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (Protocol on Xenophobia and Racism committed through computer systems).⁷¹

The Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence will be adopted by the end of 2021. The finalised text contains provisions (Article 6) on procedures enhancing direct cooperation with providers and entities providing domain name registration services, in particular with reference to requests for domain name registration information.⁷²

Under the Budapest Convention, the following offences are considered **cybercrime**: illegal access (Article 2), illegal interception (Article 3), data interference (Article 4), system interference (Article 5), misuse of devices (Article 6), computer-related forgery (Article 7), computer-related fraud (Article 8), offences related to child pornography (Article 9) and offences related to copyright and neighbouring rights (Article 10). The Convention uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved.⁷³ To facilitate the effective use and implementation of the Budapest Convention, also in the light of legal, policy and technological developments, the Guidance Notes⁷⁴ were issued, which clarify that the

⁶⁸ <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561?module=treaty-detail&treaty-num=185>

⁶⁹ https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=WJqX0M1y

⁷⁰ <https://rm.coe.int/3148-1-3-4-cyberleg-global-state-jun2021-v5-public/1680a302be>

⁷¹ <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f>

⁷² <https://rm.coe.int/0900001680a2aa1c>

⁷³ Paragraph 36 of the Explanatory Report to the Budapest Convention

⁷⁴ <https://www.coe.int/en/web/cybercrime/guidance-notes>

provisions of the Convention apply, among others, to botnets (Guidance Note #2⁷⁵), phishing (Guidance Note #4⁷⁶), DDoS attacks (Guidance Note #5⁷⁷), malware (Guidance Note #7⁷⁸), and spam (Guidance Note #8⁷⁹).

d. EU level

Under the EU legislation no exact definition of DNS abuse exists either.

Directive 2013/40/EU on attacks against information systems⁸⁰ is aligned with the provisions of the Budapest Convention, harmonising Member States' criminal law in the area of **attacks against information systems**. The Directive, just like as the Budapest Convention, uses technology-neutral language and requires Member States to criminalise: illegal access to information systems (Article 3), illegal system interference (Article 4), illegal data interference (Article 5), illegal interception (Article 6). Moreover, the Directive requires the Member States to criminalise the intentional production, sale, procurement for use, import, distribution or otherwise making available, of tools used for committing the aforementioned offences, such as a computer programme, designed or adapted primarily for the purpose of committing any of those offences or a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.

The Regulation (EU) 2019/881 on the European Union Agency for Cybersecurity (ENISA) and on information and communications technology cybersecurity certification (**Cybersecurity Act**) defines as **cyber threat** any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.⁸¹

The Commission Regulation (EC) No 874/2004 (**.eu Regulation**) defines a domain name as **speculative and abusive registration**, which shall be subject of revocation, where that name is identical or confusingly similar to a name in respect of which a right is recognised or established by national and/or Community law, such as the rights mentioned in Article 10(1), and where it has been registered by its holder without rights or legitimate interest in the name; or has been registered or is being used in bad faith.⁸²

The Regulation (EU) 2019/517 (**New .eu Regulation**), amending and repealing the current .eu Regulation, provides that the European Commission should promote cooperation between the Registry of the .eu ccTLD, the European Union Intellectual Property Office (EUIPO) and other Union agencies, with a view to combating the **speculative and abusive registrations** of domain names, including cybersquatting, and providing simple administrative procedures, in particular for small and medium-sized enterprises (SMEs).⁸³

⁷⁵ <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7094>

⁷⁶ <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7096>

⁷⁷ <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e9c49>

⁷⁸ <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e70b4>

⁷⁹ <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7268>

⁸⁰ <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040>

⁸¹ Article 2(8) - <https://eur-lex.europa.eu/eli/reg/2019/881/oj>

⁸² <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32004R0874>

⁸³ Recital 7 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.091.01.0025.01.ENG&toc=OJ:L:2019:091:FULL

It requires the .eu Registry to adopt clear policies aiming to ensure the timely identification of **abusive registrations** of domain names and, where necessary, to cooperate with competent authorities and other public bodies relevant to cybersecurity and information security which are specifically involved in the fight against such registrations, such as national computer emergency response teams (CERTs).⁸⁴ In particular, it requires the .eu Registry to adopt requirements and procedures for registration requests, a policy on the verification of registration criteria, a policy on the verification of registrants' data, a policy on the **speculative registration** of domain names, as well as a policy on **abusive registration** of domain names and a policy on the timely identification of domain names that have been registered and used in bad faith.⁸⁵ The latter is referred to as a domain name identical or confusingly similar to a name in respect of which a right is established by Union or national law, and where it has been registered by its holder without rights or legitimate interest in the name; or has been registered or is being used in bad faith.⁸⁶ The New .eu Regulation will apply from 13 October 2022.

The Directive (EU) 2016/1148 on measures for a high common level of security of network and information systems (**NIS Directive**) currently in force defines as **incident** any event having an actual adverse effect on the security of network and information systems.⁸⁷ The Proposal for a Directive on measures for a high common level of cybersecurity (**Proposal for NIS 2**), with reference to databases of domain names and registration data (WHOIS data), provides that the availability and timely accessibility of these data is essential to prevent and combat **DNS abuse**, in particular to prevent, detect and respond to cybersecurity incidents without providing a definition for DNS abuse.⁸⁸

The Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (**Proposal for DSA**), which once enacted will amend the current Directive 2000/31/EC (the E-Commerce Directive), also contains provisions to achieve the objective of ensuring a safe, predictable and trusted online environment, and proposes to define as **illegal content** any information, which, in itself or by its reference to an activity, including the sale of products or provision of services is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law.⁸⁹ It clarifies that the concept of illegal content should be defined broadly and also covers information relating to illegal content, products, services and activities. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that relates to activities that are illegal, such as the sharing of images depicting child sexual abuse, unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the non-authorised use of copyright protected material or activities involving infringements of consumer protection law.⁹⁰

e. ICANN level

⁸⁴ Recital 20 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.091.01.0025.01.ENG&toc=OJ:L:2019:091:FULL

⁸⁵ Article 11 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.091.01.0025.01.ENG&toc=OJ:L:2019:091:FULL

⁸⁶ Article 4(4) - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.091.01.0025.01.ENG&toc=OJ:L:2019:091:FULL

⁸⁷ Article 4(7) - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148>

⁸⁸ Recital 60 - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823>

⁸⁹ Article 2(g) - <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN>

⁹⁰ Recital 12 - <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN>

The DNS abuse phenomenon and its definition have been subject of active debate for years between the stakeholders of ICANN too.⁹¹

In 1999, ICANN adopted the **Uniform Domain Name Dispute Resolution Policy (UDRP)** applicable to all gTLDs.⁹² It provides for a mandatory administrative proceeding for disputes between the registrant and any third-party (IPR holder) over the registration and use of the domain name (**abusive registrations**). The UDRP is incorporated by reference into the domain name registration agreement between the ICANN-accredited registrars and registrant. It uses a three part test to determine whether a domain name shall be considered abusive registration:

1. The domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
2. The registrant has no rights or legitimate interests in respect of the domain name;
3. The domain name has been registered and is being used in bad faith.

In 2008, ICANN's GNSO set up the **Registration Abuse Policies Working Group (RAPWG)**⁹³ that identified a set of specific issues, but did not deliver policy outcomes, nor provided a discussion of non-binding good practices for registries and registrars.⁹⁴ The final report of the working group defines **abuse** as an action that causes actual and substantial harm, or a material predicate of such harm, and illegal or illegitimate, or otherwise considered contrary to the intention and design of a stated legitimate purpose, if such purpose was disclosed. It also distinguishes between **registration** and **use abuse**.⁹⁵ The former is meant as domain name-related activities performed by the registries and registrars, including but not limited to the allocation of registered names, the maintenance of and access to registration (WHOIS) information, the transfer, deletion, and reallocation of domain names. The latter concerns what a registrant does with his or her domain name after the creation of the domain, the purpose the registrant puts the domain to, and/or the services that the registrant operates on it.

In 2009, in preparation of the launch of the new gTLDs, the **New gTLD Program Explanatory Memorandum Mitigating Malicious Conduct** was adopted and it clearly mentioned the necessity to require the new gTLD registries to mitigate potential **malicious conduct**. In such document, malicious conduct is intended as abusive activities such as trade mark abuse, phishing, wilful distribution of malware, or other illegal or fraudulent activity.⁹⁶

Since the introduction of the so-called public commitments in the **Registry Agreement for new gTLDs (RA)**, extended to **.com Registry Agreement (.COM RA)** in 2020⁹⁷, the registries have been required to include provisions in their registry-registrar agreements to oblige registrars to prohibit, through their registration agreement, a wide range of **abusive activities** of the registrants. Such activities comprise distributing malware, abusively operating botnets, phishing, piracy, trade mark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to any

⁹¹ <https://gac.icann.org/activity/dns-abuse-mitigation>

⁹² <https://www.icann.org/resources/pages/policy-2012-02-25-en>

⁹³ <https://gnso.icann.org/en/group-activities/inactive/2011/rap>

⁹⁴ https://gnso.icann.org/sites/default/files/filefield_26745/discussion-paper-rap-best-practices-28sep11-en.pdf

⁹⁵ ICANN Registration Abuse Policies Working Group Final Report (2010) - https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf

⁹⁶ ICANN New gTLD Program Explanatory Memorandum – Mitigating Malicious Conduct (2009) - <https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf>

⁹⁷ ICANN Third Amendment to the .com Registry Agreement (2020) - <https://itp.cdn.icann.org/en/files/registry-agreements/com/com-proposed-amend-3-03jan20-en.pdf>

applicable law.⁹⁸ Moreover, registries are required to periodically conduct technical analysis to assess whether domains in their TLD are being used to perpetrate **security threats**, such as pharming, phishing, malware, and botnets.⁹⁹

The **Registrar Accreditation Agreement (RAA)** defines as **illegal activity** a conduct, involving the use of a registered domain name, that is prohibited by applicable law and/or exploitation of registrar's domain name resolution or registration services in furtherance of conduct, involving the use of a domain name, that is prohibited by applicable law.¹⁰⁰ Registrars are also required to maintain an abuse contact to receive reports of abuse involving registered domain names, including reports of illegal activity.¹⁰¹

After the launch of the new gTLDs, in 2016, **Revised Report on DNS Abuse and New gTLD Program Safeguards** defined the term **DNS abuse** as intentionally deceptive, conniving, or unsolicited activities that actively made use of the DNS and/or the procedures used to register domain names.¹⁰²

Further to commissioning a study analysing DNS abuse¹⁰³, in 2018, **ICANN's Competition, Consumer Trust and Consumer Choice (CCT) Review Team** in its final report found that *"bad actors have misused these universal identifiers for cybercrime infrastructure and directed users to websites that enable other forms of crime, such as child exploitation, intellectual property infringement, and fraud. Each of these activities may constitute a form of **DNS abuse**. Determinations as to how to characterize these forms of abuse depend largely upon local laws, the roles played by other infrastructure providers, and subjective interpretations. Nonetheless, consensus exists on what constitutes **DNS Security Abuse**, or **DNS Security Abuse of DNS infrastructure** [...]. These forms of abuse include more technical forms of malicious activity, such as malware, phishing, and botnets, as well as spam when used as a delivery method for these forms of abuse."*¹⁰⁴

In 2017, ICANN launched the **Domain Abuse Activity Reporting (DAAR)** project, a system for "studying and reporting on **domain name registration and security threat (domain abuse) behavior**" across top-level domain (TLD) registries.¹⁰⁵ DAAR observes the following **security threats**: phishing, malware, botnet command-and-control and spam. Recently, further to discussions with the community, in particular with registries and registrar, ICANN has recently changed the language used in the DAAR documentation by replacing the term *abuse* with the term **security threat**, as the term *abuse* could include a broader set of threats, including those, according to ICANN, outside of its remit.¹⁰⁶

⁹⁸ ICANN Registry Agreement for new gTLDs Specification 11 (Public Commitments) Section 3(a) (RA) (2013) - <https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm>

⁹⁹ ICANN Registry Agreement for new gTLDs Specification 11 (Public Commitments) Section 3(b) (RA) (2013) - <https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm>

¹⁰⁰ ICANN Registrar Accreditation Agreement Section 1.13 (RAA) (2013) - <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en>

¹⁰¹ ICANN Registrar Accreditation Agreement Section 3.18.1 (RAA) (2013) - <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en>

¹⁰² ICANN Revised Report on DNS Abuse and New gTLD Program Safeguards (2016) - <https://www.icann.org/en/announcements/details/revised-report-on-dns-abuse-and-new-gtld-program-safeguards-now-available-18-7-2016-en>

¹⁰³ Statistical Analysis of DNS Abuse in gTLDs Final Report (SADAG report) (2017) - <https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf>

¹⁰⁴ ICANN Competition, Consumer Trust and Consumer Choice (CCT) Review Final Report (2018) - <https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf>

¹⁰⁵ <https://www.icann.org/octo-ssr/daar>

¹⁰⁶ <https://www.icann.org/en/blogs/details/learn-about-how-the-domain-abuse-activity-reporting-daar-project-is-changing-its-generic-top-level-domain-gtld-monthly-reports-5-5-2021-en>

The gTLD Registries Stakeholder Group (RySG) and the Registrar Stakeholder Group (RrSG) - **Contracted Party House (CPH)'s Definition of DNS Abuse**¹⁰⁷ was published on 16 June 2020. According to such definition **DNS abuse** is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam when it serves as a delivery mechanism for the other forms of DNS abuse, adopting *verbatim* the DNS abuse definition provided by the DNS Abuse Framework – analyzed below), and without mentioning content-related abuses.¹⁰⁸

The **Second Security, Stability, and Resiliency (SSR2) Review Team**, mandated by ICANN Bylaws Section 4.6 (c), has recently defined **DNS abuse** as *“intentional misuse of the universal identifiers provided by the DNS for cybercrime infrastructure and directed users to websites that enable other forms of crime, such as child exploitation, intellectual property infringement, and fraud”*.¹⁰⁹

The Review Team's final report, published on 25 January 2021:

- Notes that ICANN have used inconsistently the terminology DNS abuse.
- Recommends to post a web page that including ICANN's working definition of DNS abuse (i.e., what it uses for projects, documents, and contracts).
- Clarifies that the definition should explicitly note what types of security threats ICANN considers within its remit to address through contractual and compliance mechanisms, as well as those ICANN understands to be outside its remit.
- Also recommends that if ICANN used other similar terminology – e.g., security threat, malicious conduct – ICANN should include both its working definition of those terms and precisely how ICANN as distinguishing those terms from DNS abuse. The page should include links to excerpts of all current abuse related obligations in contracts with contracted parties, including any procedures and protocols for responding to abuse.¹¹⁰

Currently, **ICANN**, on its website, defines **DNS abuse** as:

“any malicious activity aimed at disrupting the DNS infrastructure or causing the DNS to operate in an unintended manner. Abusive activities include corrupting DNS zone data, gaining administrative control of a name server, and flooding the DNS with thousands of messages to degrade name-resolution services”.¹¹¹

Furthermore, ICANN provides an additional definition for **DNS misuse**:

“any activity that uses the DNS protocol or the domain name registration process to carry out malicious or illegal activity. Misuse activities include hijacking domain names, registering domain names to sell counterfeit merchandise, using the DNS to distribute spam, and exploiting the DNS protocol to launch denial-of-service attacks”.¹¹²

Finally, as a related term to DNS misuse, ICANN defines **cybersquatting** as:

¹⁰⁷ https://84e2b371-5c03-4c5c-8c68-63869282fa23.filesusr.com/ugd/ec8e4c_3001326c70194bd4a849413e1f32fc31.pdf

¹⁰⁸ ICANN's gTLD Registries Stakeholder Group and Registrar Stakeholder Group CPH Definition of DNS Abuse (2020) - https://84e2b371-5c03-4c5c-8c68-63869282fa23.filesusr.com/ugd/ec8e4c_3001326c70194bd4a849413e1f32fc31.pdf

¹⁰⁹ Second Security, Stability, and Resiliency (SSR2) Review Team Final Report (2021) : <https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf>

¹¹⁰ ICANN's Second Security, Stability, and Resiliency (SSR2) Review Team Final Report Recommendation 10.1 (2021) - <https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf>

¹¹¹ <https://www.icann.org/en/icann-acronyms-and-terms/domain-name-system-abuse-en>

¹¹² <https://www.icann.org/en/icann-acronyms-and-terms/domain-name-system-misuse-en>

*“a form of misuse in which a party intentionally registers a domain name that coincides with a commercial trade mark or the name of a well-known person”.*¹¹³

Thus, according to ICANN, DDoS, spam, cybersquatting, distribution of illegal content, such as the sale of counterfeit goods, fall all in the same category (DNS misuse), while other activities including but not limited to the corruption of DNS zone data, gaining administrative control of a name server, and flooding the DNS with messages to degrade name-resolution services are to be defined as DNS abuse.

As described above, over the years, the extensive discussion on the definition of DNS abuse within ICANN took the direction to draw up a rigid distinction between **technical** (often called security threats) and **content-related abuses**. While consensus seems to have been reached on the purely technical-related aspects, the content-related ones are under continuous debate. The main reason is that the definition of DNS abuse and abuse mitigation may carry consequences in terms of the scope of activity overseen by ICANN policies and contracts. While governments, law enforcement authorities, and other stakeholders are concerned with the impact of DNS abuse on the public interest, including the safety of consumers and the infringement of intellectual property rights, registries, and registrars are concerned with restrictions on their commercial activities, ability to compete, increased operating costs and liability for consequences registrants may incur when an action is taken on abusive domains. Non-commercial stakeholders on their part are concerned with the infringement of freedom of speech and privacy rights of registrants and Internet users, and share with contracted parties concerns about ICANN overstepping its mission.¹¹⁴

Indeed, the SSR2 Review Team has also recommended to ICANN to establish a cross-community working group (CCWG), involving stakeholders from consumer protection, operational cybersecurity, academic or independent cybersecurity research, law enforcement, and e-commerce to establish a process for evolving the definitions of prohibited DNS abuse.¹¹⁵ On 22 July 2021, the ICANN's Board, in the rationale to its resolution on SSR2 Final Report recommendations, noted that neither ICANN nor the Board could unilaterally establish a CCWG and highlighted that the community continues its discussions over *DNS security threat* mitigation. Discussions include questions around the definitions and scope of DNS security threats that can be considered as coming within ICANN's remit and the extent to which policy or other community work may be required to supplement efforts already underway, such as industry-led initiatives.¹¹⁶

f. Other initiatives

There are also other attempts outside ICANN to define and mitigate DNS abuse. These voluntary initiatives are mostly led by the domain industry.

The **Internet & Jurisdiction Policy Network's** Domains & Jurisdiction Program is A multistakeholder organization fostering legal interoperability in cyberspace.¹¹⁷ It has elaborated a document called **Operational, Approaches, Norms, Criteria,**

¹¹³ <https://www.icann.org/en/icann-acronyms-and-terms/cybersquatting-en>

¹¹⁴ [https://gac.icann.org/briefing-materials/public/icann66-gac-briefing-21-and-29-dns-abuse-mitigation\(v4\).pdf?language_id=1](https://gac.icann.org/briefing-materials/public/icann66-gac-briefing-21-and-29-dns-abuse-mitigation(v4).pdf?language_id=1)

¹¹⁵ ICANN's Second Security, Stability, and Resiliency (SSR2) Review Team Final Report Recommendation 10.1 (2021) - <https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf>

¹¹⁶ <https://www.icann.org/en/system/files/bm/rationale-ssr2-22jul21-en.pdf>

¹¹⁷ <https://www.internetjurisdiction.net/news/domains-jurisdiction-program-contact-group-members>

Mechanisms¹¹⁸ which mentions that **domain name use abuse** covers two dimensions: i) **technical abuse** (spam, malware, phishing, pharming, botnets and fast-flux hosting), which is closely related to the security and stability of the DNS, and ii) **abusive content** (child abuse material, controlled substances and regulated goods for sale or trade, violent extremist content, hate speech and intellectual property violations).

This initiative also highlights that registries and registrars are very diverse in terms of size, activities or governance structures, and the fundamental distinction between ccTLDs and gTLDs in terms of relation with national laws and authorities, which leads to very different approaches and constraints when receiving direct requests or orders for action at the DNS level regarding use abuse, particularly when they originate across borders. It notes that, in the absence of a generally accepted framework regarding how to deal with use abuse, registries' and registrars' practices vary considerably. The document also affirms that, registries and registrars are more inclined to act at the level of the DNS in response to technical abuse than when dealing with abusive content that they usually do not have the competence to properly evaluate given the diversity of applicable national laws, unless a clear threshold of abuse is met. The Internet & Jurisdiction Policy Network has recently launched a **Toolkit on DNS Level Action to Address Abuses**, which again separates domain name abuse into technical abuse and website content abuse.¹¹⁹

In 2019, building on the work of the Internet & Jurisdiction Policy Network's Domains & Jurisdiction Program, 11 registries and registrars voluntarily signed a framework (**DNS Abuse Framework**) to address abuse narrowing the definition of **DNS abuse** to five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for the other forms of DNS abuse).¹²⁰ They have also reiterated that they are not required under their agreements with ICANN to monitor or suspend domains based on **website content abuse** which fall outside the DNS abuse definition. However, registries and registrars have recognised certain forms of website content abuse so egregious that a registry or registrar should act when provided with specific and credible notice. Specifically, even without a court order, signatory registries or registrars should act to disrupt the following forms of website content abuse: child sexual abuse materials, illegal distribution of opioids online, human trafficking and specific and credible incitements to violence. According to the DNS Abuse Framework's signatories, underlying these website content abuses is the physical and often irreversible threat to human life which justifies action. The framework has now grown to over 50 signatories.¹²¹

g. Assessment of the definitions used by others, shortcomings and gaps

The analysis and research conducted by the authors show that the typologies of abuse, the terminologies and the definitions analyzed above have much in common and partly overlap. However, consensus on a global and comprehensive DNS abuse definition is still missing.

The **Budapest Convention**, using technology neutral language, criminalises various conducts carried out via the Internet or information systems and falling under the notion of *cybercrime*, comprising security and content-related threats. The Guidance Notes specify the provisions apply to botnets, phishing, DDoS attacks, malware and spam in addition to

¹¹⁸ Internet & Jurisdiction Policy Network's Domains & Jurisdiction Program Operational, Approaches, Norms, Criteria, Mechanisms (2019) <https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf>

¹¹⁹ <https://www.internetjurisdiction.net/domains/toolkit#toolkit>

¹²⁰ DNS Abuse Framework (2019) - [https://dnsabuseframework.org/media/files/2020-05-](https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf)

[29_DNSAbuseFramework.pdf](https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf)

¹²¹ DNS Abuse Framework signatories - <https://dnsabuseframework.org/>

copyright and neighbouring rights infringement. Neither the Convention, nor the Guidance Notes mention expressly the infringement of other IPR (trademark, etc.).

The multi-layered **EU legislation**, from one hand, harmonises the criminal law aspects of the *attacks against information systems* (corresponding with the notion of cybercrime of the Budapest Convention). The Cybersecurity Act leaves space to a broad interpretation regarding the concept *cyber threat*, while it narrows (at least with reference to the .eu namespace) the meaning of *speculative and abusive registration* to the infringement of prior rights¹²². The recent legislative proposal on cybersecurity measures (Proposal for NIS 2 Directive) would be the first legal instrument within the EU that introduces the term *DNS abuse*. However, the text of the proposal, adopted by the European Commission and under discussion within the European Parliament, does not provide a definition yet, leaving a lack of legal certainty. Another legislative proposal (Proposal for Digital Services Act) intends to cover another aspect of the online harms (*illegal content*), related to the content made available through domain names, without mentioning how this relates to cybersecurity issues.

Within the **ICANN community** and **other initiatives** promoted by the ICANN-contracted parties (i.e., registries and registrars), the discussions around the DNS abuse definition can be summarized in the contraposition of the so-called technical versus content-related threats.

According to the authors, such a rigid distinction cannot be made between the abuse types and there is a great overlap between the two categories (e.g., phishing and malware).

Also, these discussions seem to be driven by legal and liability concerns: on the one hand, the concern related to ICANN's limited remit (i.e. "*ICANN shall not regulate [...] content*"¹²³), and on the other hand, the concern of the ICANN-contracted parties with taking on more contractual obligations. The latter parties also argue on their difficulty to handle content-related abuses due to the differences in legal frameworks regarding what is considered illegal and on the limited availability of tools at their disposal to mitigate abuse (i.e. they cannot remove offending pieces of content from a website, but only disable the entire domain name, often referred to as the "nuclear option") which may not be appropriate and result in collateral damage and liability exposure. Therefore, they tend to narrow the definition of DNS abuse to technical (security) threats, in particular to malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for the other forms of DNS abuse). At the same time, other stakeholders, governments, law enforcement authorities, consumer protection and commercial interests (IPR holders) reiterate the necessity to address the public interest concern and content-related DNS abuses by properly enforcing the already existing contractual obligations (i.e., RAA and RA).

Indeed, a clear-cut distinction between technical (security) and content-related abuses is not possible in many cases and the borderline is blurred due to the great deal of overlap between different types of abuse.

For example, *phishing* is defined as "*domain names that support web pages that masquerade as a trustworthy entity such as a bank, known brand, online merchant or government agency*"¹²⁴ or "*when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g. account numbers, login IDs, passwords), whether*

¹²² Registered national and community trademarks, geographical indications or designations of origin, and, in as far as they are protected under national law in the Member-State where they are held: unregistered trademarks, trade names, business identifiers, company names, family names, and distinctive titles of protected literary and artistic works – Article 10(1) of the Commission Regulation (EC) No 874/2004 - <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32004R0874>

¹²³ <https://www.icann.org/resources/pages/governance/bylaws-en/#article1>

¹²⁴ <https://www.icann.org/octo-ssr/daar-faqs/#security-threats>

through sending fraudulent or 'look-alike' emails, or luring end users to copycat websites. Some phishing campaigns aim to persuade the user to install software, which is in fact malware^{125 126 127} and categorized as security threat or technical abuse. Accordingly, registries and registrars consider that phishing fall inside the DNS abuse definition and on which they *"feel compelled to act upon"*.¹²⁸

However, previous research¹²⁹ shows that, in the sample of manually labelled phishing domains (gathered from blacklisted URLs), while 58% were registered by apparently malicious actors, indicating technical abuse (as intended by the registries and registrars), all of the URLs served abusive content affecting, in the first place, Internet users (by tricking them into revealing sensitive personal or financial information), but also third parties (by incorporating well-known trade marks in the phishing websites), and finally DNS service providers whose infrastructure was misused to host malicious content. The remaining 42% of domains were apparently compromised, meaning that the underlying domains were registered by benign registrants, but vulnerable web hosting was exploited by the abuser.

URLs used to distribute *malware* is another example indicating that the clear-cut distinction between technical and content-related abuse is not appropriate. While the URLs distributing malware serve harmful content (malicious software) to infect end users, as many as 57% of domains were compromised by exploiting, for example, web vulnerabilities.

Finally, as mentioned earlier, the recent voluntary initiatives taken by registries and registrars¹³⁰ categorize domains used to host websites offering counterfeit goods, pirate content, or CSAM material as content-related abuse, thus, considering them falling outside of the DNS abuse. However, similarly to phishing or malware, the abusers may use DNS infrastructure, in particular, maliciously registered domain names to distribute such content in those abuse cases too.

What is also common in all the abuse typologies is that they are affecting online security, cause harm to users and third parties and undermine the trust in the Internet.

Therefore, the authors of the study conclude that, in order to effectively fight the DNS abuse phenomenon, a broader approach ought to be adopted regarding the DNS abuse definition that considers the great deal of overlap between different categories, and can keep up with the development of the technology and adaptable to the everchanging threat landscape.

¹²⁵ <https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf>

¹²⁶ https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf

¹²⁷ https://84e2b371-5c03-4c5c-8c68-63869282fa23.filesusr.com/ugd/ec8e4c_3001326c70194bd4a849413e1f32fc31.pdf

¹²⁸ https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf

¹²⁹ https://mkorczynski.com/COMAR_2020_IEEEEuroSP.pdf

¹³⁰ https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf

7. Magnitude of DNS abuse

To estimate the magnitude of DNS abuse, the authors have conducted primary and secondary research.

a. Measurements carried out by the authors

The authors carried out real-time measurements from **March 2021 to June 2021**. The results are described in details in the **Technical Report**, annexed to the present study as **Appendix 1**.

The measurements concerned the overall health of the TLD ecosystems, as well as different types of intermediaries such as domain registrars, hosting providers and providers of free services, and other services.

Over 2.7 million incidents and 1.68 million abused domain names were analyzed, using reputed domain and URL blacklists.

We recall below the main findings:

1. Overall health of TLDs

- a) In relative terms, new gTLDs with an estimated market share of 6.6%, are the most abused group of TLDs. In the second quarter of 2021, 20.5% of all abused domain names representing phishing, spam, botnet command-and-control (C&C), and malware distribution combined were registered in new gTLDs (Appendix 1 – Technical Report, Section 5, p. 26).
- b) However, not all new gTLDs suffer from DNS abuse to the same extent. The two most abused new gTLDs combined account for 41% of all abused new gTLD names (Appendix 1 – Technical Report, Section 9.2, p. 32).
- c) European Union country code TLDs (EU ccTLDs) are by far the least abused in absolute terms, relative to their overall market share. Only 0.8 percent of all abused (maliciously registered and compromised) domain names were registered under EU ccTLDs (Appendix 1 – Technical Report, Section 5, p. 26).

2. Malicious vs. compromised domains: where does the abuse occur?

- a) The vast majority of spam and botnet C&C domain names are maliciously registered, which is expected given the nature of the abuse (Appendix 1 – Technical Report, Section 10.3, p. 41).
- b) In the analysed data, about 25% of phishing domain names and 41% of malware distribution domain names are presumably registered by legitimate users, but compromised at the hosting level (Appendix 1 – Technical Report, Section 10.3, p. 41).
- c) When looking at compromised domain names, it emerged that for highly used TLDs such as European ccTLDs, there is a higher incidence (42%) of hacked websites. In TLDs with lower usage rates such as new gTLDs, attackers have a much stronger tendency to register directly the domains they intend to use for their malicious activities (Appendix 1 – Technical Report, Section 10.3, p. 42).
- d) TLD registries and registrars can prevent malicious registrations (proactive measures) and mitigate maliciously registered domains (reactive measures) at the DNS level. However, they have no control over the hosting infrastructure (unless they also provide a hosting service). Therefore, the authors have computed reputation metrics for domain names that are found to be maliciously registered and

- exclude domains that are likely compromised at the hosting level (Appendix 1 – Technical Report, Section 11, p. 42).
- e) The top five most abused registrars account for 48% of all maliciously registered domain names (Appendix 1 – Technical Report, Section 11.2, pp. 43-44).
 - f) The study reveals that hosting providers with disproportionate concentrations of spam domains reach 3,000 abused domains per 10,000 registered domain names (Appendix 1 – Technical Report, Section 12.3, pp. 48-49).
 - g) Phishers make heavy use of free subdomain and hosting providers because they incur no cost, which makes them practical for serving malicious content. These services are less suitable for distributing spam and botnet C&C communication (Appendix 1 – Technical Report, Section 13, pp. 53-54).

3. Adoption of DNS security extensions and email protection protocols

- a) The overall level of DNS security extensions (DNSSEC) adoption remains low. In a large sample of 227 million domain names, only 9.4 million domains have all the required DNSSEC resource records (DNSKEY, Resource Record Signature - RRSIG and Delegation Signer - DS). 98.1% of these are correctly signed and have been correctly validated (Appendix 1 – Technical Report, Section 15.3, pp. 62-63).
- b) Based on a large sample of domain names for ccTLDs in the EU, the authors estimated that the .cz (59%), .se (55%), .nl (51%), and .sk (48%) ccTLDs demonstrate the highest percentage of domain names signed with DNSSEC. ccTLD registry operators of these domains provide price incentives and technical support for DNSSEC adoption (Appendix 1 – Technical Report, Section 15.3, pp. 63-65).
- c) The measurements revealed 2.5 million open DNS resolvers worldwide that can be effectively used as amplifiers in distributed denial-of-service (DDoS) attacks (Appendix 1 – Technical Report, Section 16.4, p. 70).
- d) Based on a large sample of 247 million domain names, the measurements revealed more than 60% of domain names without Sender Policy Framework (SPF)¹³¹ and 97% of domains without Domain-based Message Authentication, Reporting and Conformance (DMARC)¹³² records that prevent email spoofing, one of the techniques used in Business Email Compromise (BEC)¹³³ scams (Appendix 1 – Technical Report, Section 17.3, pp. 74-75).

b. Questionnaires conducted by the authors

Furthermore, the authors collected data and inputs from stakeholders through two questionnaires: **1)** the first one surveyed TLD registries, registrars, hosting providers, other DNS operators (total 67 responses received); **2)** the second one surveyed intellectual property rightholders, practitioners, associations, business intelligence and brand protection companies (total 126 responses received).

1) The results of the questionnaire for DNS operators

Types of respondents and services provided

¹³¹ Sender Policy Framework (SPF) is an email authentication protocol designed to detect forging email sender address known as domain or email spoofing.

¹³² Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a protocol that extends SPF and gives the domain name owner the ability to protect their domain from unauthorized use (email spoofing).

¹³³ Business Email Compromise (BEC) is a type of scam involving the hacking, spoofing, or impersonation of a business email address. The victim of a BEC attack receives an email that appears to come from a trusted business. The email looks and feels genuine.

1. Size of respondents: 63,3% of the respondents are small or medium-size enterprises, employing between 11 and 250 employees. 31,7% of the respondents have less than 10 employees (micro enterprise). 15% of the respondents have more than 250 employees.
2. The vast majority of the respondents (90%) provide services in the EU. 15% of the respondents are established in Germany, 13,3% in the United States, 8,3% in France, 6,7% in Switzerland, 5% in Portugal and 5% in the Netherlands.
3. Types of services provided: 55% of the respondents carry out TLD registry activities, 35% are registrars, 33,3% provides DNS hosting and 21,7% web hosting. Other activities include e-mail and file storage, DNS firewall protection and activities, DNS filtering etc. In some cases, intermediaries provided multiple services, such as web hosting and registrar services.

Abuse monitoring and mitigation activities

1. Abuse monitoring and/or mitigation activities are carried out on the following (combined) basis: contractual obligations with ICANN, contractual obligations with TLD registry, local laws, enforcing terms and conditions, voluntary initiatives, court orders, third-party complaints.
2. It has also emerged that 60,3% of the respondents take action only once an incident occurs (reactive actions) and nearly 40% (39,4%) take proactive actions, meaning preventing potential abuse, such as blocking suspicious domain name registrations at the time of registration, vulnerability scans and patching of hosting infrastructure.
3. 65,5% of the respondents involve external expertise in the assessment of abuse and 34,5% carry out the assessment internally.

Abuse types

The most frequent types of abuse in the three-year period 2018-2020 are phishing (71,4%), followed by malware distribution (60,7%), botnet C&C (53,6%), other types of frauds and scams (39,3%), pharming (35,7%), spam (35,7%), maliciously registered domain name (35,7%), DDoS attacks (32,1%), CSAM (28,6%), website selling counterfeit goods (25%), compromised domain name (25%), illicit trade of pharmaceuticals (17,9%), other infringement of IPR (17,9%).¹³⁴

Actions taken

1. The actions taken in case of detected or reported abuse comprise contacting other intermediary to take action, contacting the registrant to take action, taking down or suspending the domain name. A small portion of respondents check the accuracy of the registration data (1,8%).
2. The average turnaround time to mitigate or respond to abuse complaints vary among 1 hour and 1 day.

DNSSEC deployment

42,1% of the respondents replied to facilitate the DNSSEC deployment, while 31,6% do not. 5,3% do not support every algorithm if their nameservers are used, 5,3% supports

¹³⁴ Multiple response was possible when responding to this question of the survey.

the manual deployment, and 5,3% replied that it is up to the reseller to support the DNSSEC deployment.

Content monitoring

1. 56,1% of the respondents do not monitor website content, while 43,9% do monitoring.
2. 33,3% check for specific keywords, brands or services (e.g., banking, luxury) and products (e.g., pharmaceuticals) within the websites.
3. 57,1% of the respondents collect evidence of reported abuse at content level by e.g., making screenshots.
4. 50% of the respondents collect anonymised or aggregated data on domain usage (e.g., parked pages, webshops, industry of registrant, etc.).

Collaborations

1. 46,7% of the respondents have formal processes to collaborate with law enforcement authorities.
2. 44% of the respondents collaborate with trusted notifiers, and 65,4% of these respondents have formal processes in place for their with the trusted notifiers.

One of the issue brought up by the respondents (mostly registrars) was that, in most cases of phishing/BEC frauds, WHOIS data is fake and can, however, be validated on several levels and pass such validations with a 100% score. Crime as a Service operators involved in malware distribution usually never register domain names but hack websites and as such leaving not much of a trail. There is no payment registration or registrant in such cases. Registrars also claimed that disclosing data through the WHOIS not protected by the GDPR would increase DNS abuse, supplying criminals with daily new attack information, and security incidents will rise. The amount of actionable domain names by a registrar is declining. There is a shift within the DNS where the majority of DNS abuse takes place and it is not at the registrar or registry level.

Some of respondents also commented that effective abuse prevention and mitigation can not be done by one simple straightforward procedure at one level. Tackling abuse via the DNS has often only a limited effect. The content will still be available and may soon after the action be reached via a different domain.

2) The results of the questionnaire for intellectual property stakeholders

Abuse types

The most frequent types of abuses reported by the respondents are trademark infringement, sale of counterfeit products, phishing, copyright infringement, spam, other types of frauds and scams, malware, other infringement of IPR, illicit trade of pharmaceuticals, DDoS attacks, pharming, botnet C&C.

Awareness regarding measures of intermediaries

55,7% of the respondents are 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. However, a great portion (44,3%) of the respondents is not aware about those measures.

Contacting intermediaries

91,7% of the respondents contact the registry, the registrar and/or the hosting provider to report abusive and malicious activities.

Responsiveness of intermediaries

The intermediaries' responsiveness was rated by the respondents on a scale of 1-5 where 1 is "not responsive at all" and 5 is "very responsive":

Registries:

1	2	3	4	5
15%	32,7%	34,7%	12,4%	5,3%

Registrars:

1	2	3	4	5
15,5%	36,2%	34,5%	11,2%	2,6%

Hosting providers:

1	2	3	4	5
8,8%	25,7%	42,5%	19,5%	3,5%

Contacting Law Enforcement Authorities (LEA)

75,4% of the respondents contact the law enforcement authorities (police, customs, consumer protection authorities, etc.) to report abusive or malicious activities.

Responsiveness of LEA

The law enforcement authorities' responsiveness was rated by the respondents on a scale of 1-5 where 1 is "not responsive at all" and 5 is "very responsive":

1	2	3	4	5
11,8%	10,8%	39,2%	31,4%	6,9%

Major challenges

The major challenges that the respondents face in combating abusive and malicious activities involving domain names are as follows:

1. Identify and contact the registrant of the domain name

2. Obtain response from the registry operator / registrar / hosting provider to abuse reports
3. Obtain the cancellation / suspension of the domain name in case of inaccurate WHOIS data
4. Cost to be incurred to combat abusive and malicious activities
5. Identify the entity that should take action against the abusive and malicious activity
6. Detect abusive and malicious activities in a timely manner
7. Obtain response from the law enforcement authorities to abuse reports
8. Contact the registry operator / registrar / hosting provider to report abuse.

The respondents of the second questionnaire also highlighted that combatting intellectual property infringement, including by private sector organisations and companies, serves a public interest in upholding the fundamental right to intellectual property as well as in protecting consumers who are regularly exposed to criminal activities when using infringing websites. According to the respondents, this particular form of DNS abuse, the infringement of intellectual property rights online, is also often closely intertwined with other forms of DNS abuse as the operators of infringing websites are often involved with organised crime and money laundering while also commonly using infringing content to attract users to sites used to distribute malware and for phishing attacks. Expedious and effective action by DNS service providers is therefore vital to prevent such DNS abuse. Despite this, a significant obstacle to the creation of a safe online environment is 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. Indeed, respondents encountered significant inconsistencies in the approaches taken by DNS service providers, including domain name registrars and registries. While certain domain name registries are cooperative and assist in the removal of harmful and/or infringing content with simple processes (sometimes relying on sworn evidentiary statements) (e.g., Nominet), others do not respond to requests and/or have very limited abuse reporting procedures (if any). The same can be said for domain name registrars, with the majority being unresponsive to reports of DNS abuse based on IPR infringement. This lack of responsibility is exacerbated when domain name registries offer API services that allow the quick registration and use of domains, which allows the operators of infringing sites the ability to create new domains rapidly in response to action taken by rightholders / registrars or create temporary domains for malicious activity including phishing, pharming and other abuses. Coupled with the non-existent or slow abuse report handling encountered by reporters, this makes enforcement and the prevention of DNS abuse challenging. A related problem is the recent prevention of access to domain registration information for the purpose of legal investigation and enforcement of DNS abuses. Identification of the operators of websites engaging in unlawful activity for the purpose of legal investigation and action is critical to prevent DNS abuse and to making the Internet a more secure place. However, since May 2018, ICANN and domain name registration services have prioritised 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.

The respondents also pointed out that due to the pandemic, they faced an increase of malicious online activities. According to some of them a universal proceeding for the suspension of domain names is needed, e.g., in cases of phishing (criminal activities), they consider unacceptable to wait for months until the dispute resolution proceedings (reactive actions to be initiated by rightholders) end. Others have advocated for the necessity to introduce preventive measures (KYBC procedures, predictive algorithms, delayed delegation).

c. Results of the secondary research on DNS abuse magnitude

In addition to the authors' measurements and the data collected through questionnaires, the authors carried out extensive literary review of relevant industry reports and research, gathered and analysed data and information provided by multiple stakeholders.

Considered that this study does not look at historical data, in addition to the measurements and the questionnaires conducted by the authors and described in the previous sections, the present section contains some, and not all, data released by and collected from third parties related to the magnitude of DNS abuse in the past three years (2019-2021). Of course, this does not mean that DNS abuse is a new phenomenon. As already discussed with reference to the definition of DNS abuse in Section 6, the phenomenon itself and several proposals for mitigation have been subject of active debate for years within and outside the ICANN community. For example, as already mentioned above, subsequent to the launch of the new gTLDs, in 2016, ICANN's Competition, Consumer Choice and Trust (CCT) Review Team commissioned a study to analyse DNS abuse (in particular spam, phishing, and malware distribution) in all gTLDs from 2014 to 2016. The study found the ineffectiveness of the safeguards built in ICANN's New gTLD Program and noted that new gTLDs had been extensively abused.¹³⁵ As reported by several third parties and discussed below, the DNS abuse phenomenon accelerated in the past years harming Internet users all over the world. Additionally, concerns with the ability to effectively mitigate DNS abuse have been heightened by law enforcement, cybersecurity, consumer protection and intellectual property circles as a consequence of the entry into force of the EU General Data Protection Regulation (GDPR) in 2018 and the (still ongoing efforts) to render the WHOIS system, which is essential for crime and abuse investigation and enforcement, compliant with the GDPR. The already existing problems and challenges have been exacerbated by the COVID-19 global health emergency.

The secondary research covered the following threats and malicious activities:

1. **Cyberthreats in general**
2. **Phishing**
3. **Child sexual abuse material (CSAM)**
4. **Intellectual property rights (IPR) infringement**
5. **Online sale of counterfeit pharmaceuticals**
6. **Domain names including COVID-19 related terms**

1. Cybethreats in general

1.1 Interpol's recent **Global Landscape on COVID-19 Cyberthreat**¹³⁶ has found that:

- There has been an increase of malicious domain names registered with the keywords "COVID" or "corona", to take advantage of the growing number of people searching for information about COVID-19. Many of these were considered to be developed with malicious intent – as of the end of March 2020, 2.022 malicious and 40.261 high-risk newly registered domains were discovered.
- Online scams and phishing: cybercriminals have been creating fake websites related to COVID-19 to entice victims into opening malicious attachments or clicking phishing links, resulting in identity impersonation or illegal access to personal accounts. Also, Trend Micro reported that nearly one million spam messages have

¹³⁵ See in particular the Statistical Analysis of DNS Abuse in gTLDs (SADAG) Report for the ICANN's Competition, Consumer Choice and Trust Review Team (CCTRT): <https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf>

¹³⁶ <https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats>

linked to COVID-19 since January 2020. Business Email Compromise (BEC) has become the scheme of choice, involving the spoofing of supplier and client email addresses – or use of nearly identical email addresses – to conduct attacks. The extreme need for key supplies provides an ideal scenario for criminals to harvest details or to divert millions of dollars of procurement funds into criminal accounts.

- Data-harvesting malware: data-harvesting malware such as Remote Access Trojan, info stealers, spyware and banking Trojans infiltrate systems, using COVID-19 related information as a lure to compromise networks, steal data, divert money and build botnets.
- Disruptive malware (ransomware and DDoS): cybercriminals have deployed disruptive malware like ransomware against critical infrastructure and response institutions such as hospitals and medical centres, which are overwhelmed with the health crisis. Such ransomware or DDoS attacks do not typically aim to steal information, but prevent it from accessing critical data or disrupt the system, exacerbating an already dire situation in the physical world.

Indeed, Interpol expected that the cyberthreats facing individuals, businesses and critical infrastructure would continue to evolve causing harm globally, following the rapidly changing social and economic circumstances. Further increases in cybercrime will occur as criminals look for other revenue streams by leveraging the cyber elements of other types of crime.

1.2 Europol's Internet Organized Crime Threat Assessment (IOCTA) Report was published on 5 October 2020.¹³⁷ The data collection for the IOCTA 2020 took place during lockdowns implemented as a result of the COVID-19 pandemic. The report also highlights that cybercriminals have taken advantage of the ongoing pandemic to perpetrate their crimes by the use of the Internet and that:

- Social engineering and phishing remain an effective threat to enable other types of cybercrime. Criminals use innovative methods to increase the volume and sophistication of their attacks, and inexperienced cybercriminals can carry out phishing campaigns more easily through crime as-a-service. Criminals quickly exploited the pandemic to attack vulnerable people; phishing, online scams and the spread of fake news became an ideal strategy for criminals seeking to sell items they claim will prevent or cure COVID-19.
- Encryption continues to be a clear feature of an increasing number of services and tools. One of the principal challenges for law enforcement is how to access and gather relevant data for criminal investigations. The value of being able to access data of criminal communication on an encrypted network is perhaps the most effective illustration of how encrypted data can provide law enforcement with crucial leads beyond the area of cybercrime.
- Malware: ransomware attacks have become more sophisticated, targeting specific organisations in the public and private sector through victim reconnaissance. While the COVID-19 pandemic has triggered an increase in cybercrime, ransomware attacks were targeting the healthcare industry long before the crisis. Moreover, criminals have included another layer to their ransomware attacks by threatening to auction off the comprised data, increasing the pressure on the victims to pay the ransom. Advanced forms of malware are a top threat in the EU: criminals have transformed some traditional banking Trojans into modular malware to cover more personal computer digital fingerprints, which are later sold for different needs.

¹³⁷ Europol Internet Organized Crime Threat 2020: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020>

- Distribution of child sexual abuse material (CSAM): the main threats related to online child abuse exploitation have remained stable in recent years, however detection of online CSAM saw a sharp spike at the peak of the COVID-19 crisis. Offenders keep using a number of ways to hide this type crime, such as P2P networks, social networking platforms, and using encrypted communications applications. Dark web communities and forums are meeting places where participation is structured with affiliation rules to promote individuals based on their contribution to the community, which they do by recording and posting their abuse of children, encouraging others to do the same. Livestream of child abuse continues to increase, becoming even more popular than usual during the COVID-19 crisis when travel restrictions prevented offenders from physically abusing children. In some cases, video chat applications in payment systems are used which becomes one of the key challenges for law enforcement as this material is not recorded.
- Payment fraud: subscriber identity module (SIM) swapping, which allows perpetrators to take over accounts, is one of the new trends in IOCTA 2020. As a type of account takeover, SIM swapping provides criminals access to sensitive user accounts. Criminals fraudulently swap or port victims' SIMs to one in the criminals' possession in order to intercept the one-time password step of the authentication process.
- Criminal abuse of the dark web: in 2019 and early 2020 there was a high level of volatility on the dark web. The lifecycle of dark web market places has shortened and there is no clear dominant market that has risen over the past year. Tor remains the preferred infrastructure, however criminals have started to use other privacy-focused, decentralised marketplace platforms to sell their illegal goods. Although this is not a new phenomenon, these sorts of platforms have started to increase over the last year. OpenBazaar is noteworthy, as certain threats have emerged on the platform over the past year such as COVID-19-related items during the pandemic.

1.3 The rise of cyberthreats has also been reported by the **EU Threat Landscape Report** of the **European Union Agency for Cybersecurity (ENISA)**, released on 20 October 2020.¹³⁸ According to ENISA, cyberattacks are becoming more sophisticated, targeted, widespread and undetected. The report highlights important aspects and trends related to the threat landscape:

- There will be a new norm during and after the COVID-19 pandemic that is even more dependent on a secure and reliable cyberspace.
- The number of fake online shopping websites and fraudulent online merchants reportedly has increased during the COVID-19 pandemic. From copycats of popular brands websites to fraudulent services that never deliver the merchandise, the coronavirus revealed weaknesses in the trust model used in online shopping.
- The number of cyberbullying and sextortion incidents also increased with the COVID-19 pandemic. The adoption of mobile technology and subscription to digital platforms makes younger generations more vulnerable to these types of threats.
- Malicious actors are using social media platforms to increase efficiency in targeted attacks.
- Financial reward is still the main motivation behind most cyberattacks.

¹³⁸ <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends>

- Finely targeted and persistent attacks on high-value data, such as intellectual property and state secrets, are being meticulously planned and executed often by state-sponsored actors.
- Massively distributed attacks with a short duration and wide impact are used with multiple aims such as credential theft.
- The number of phishing victims in the EU continues to grow with malicious actors using the COVID-19 theme to lure them in. COVID-19-themed attacks include messages carrying malicious file attachments and messages containing malicious links that redirect users to phishing sites or malware downloads.
- Business Email Compromise (BEC) and COVID-19-themed attacks are being used in cyber-scams resulting in the loss of millions of euros for EU citizens and corporations. European Small and Medium Enterprises (SMEs) have also fallen victim of these threats in a time when many are going through severe financial difficulties due to the loss of revenue.
- Ransomware remains widespread with costly consequences to many EU organisations.
- Many cybersecurity incidents still go unnoticed or take a long time to be detected.
- The number of potential vulnerabilities in a virtual or physical environment continues to expand as a new phase of digital transformation arises (as technology will keep diversifying).
- With more security automation, organisations will invest more in preparedness using CTI as their main capability.

Malware, web-based attacks, phishing, web application attacks, spam, DDoS, identity theft, data breach, insider threat, botnets, physical manipulation, damage, theft and loss, information leakage, ransomware, cyberespionage, and cryptojacking were considered the 15 top cyber threats in 2020.¹³⁹

The **Sectoral / Thematic Threat Analysis** of ENISA provides an approximate ranking of sectors in terms of observed incidents, together with a trend drawn from the emerging dynamics of the potential exposure of each sector. Moreover, some information on the most popular attack vectors per sector is also given.¹⁴⁰ The threat exposure has been assessed via detailed threat categories that have been developed by ENISA and is used for various sectorial assessments.¹⁴¹

Therefore, the lessons learnt from the COVID-19 pandemic are undoubtedly that, more than ever, it is fundamental to have effective safeguards in place to counteract all forms of DNS abuse and guarantee a safe, stable and resilient cyberspace.

2. Phishing

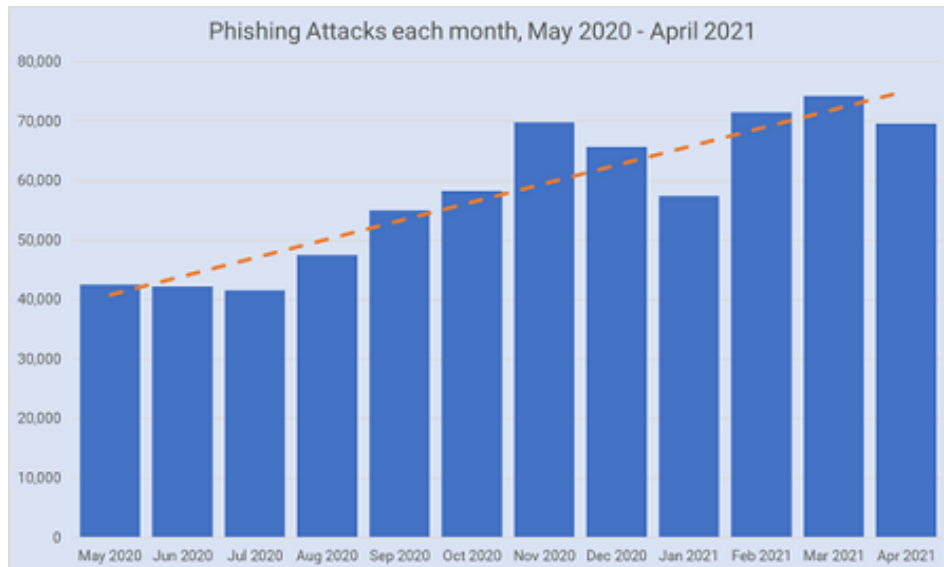
¹³⁹ <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape-2020-top-15-threats>

¹⁴⁰ <https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis>

¹⁴¹ <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view>

2.1 A third-party report also analysed the phishing landscape both in 2020¹⁴² and 2021¹⁴³. The 2021 **Interisle** study analysed nearly 1.5 million phishing reports representing 700,000 phishing attacks, and found that phishing increased by nearly 70% over the period 1 May 2020 through 30 April 2021.

Figure 5: Phishing attacks May 2020 – April 2021 (source Interisle)



The report's major findings and conclusions are:

1. Most phishing is concentrated at small numbers of domain registrars, domain registries, and hosting providers. The study identified 497,949 unique domains used for phishing across the whole year. These domains were registered in 623 TLDs and registered through 997 gTLD registrars. 69% of the domains used for phishing were in 10 TLDs; 69% were registered through 10 registrars.
2. Phishing attacks are disproportionately concentrated in new gTLDs. In June 2020, new TLDs represented 9% of domain names in the world but 18% of domains used for phishing. The new TLDs' market share decreased during our yearly reporting period (to 6% in March 2021), but phishing reported in the new TLDs increased to 21% during our yearly period.
3. Phishing domain registrations in some TLDs are overwhelmingly dominated by a small number of registrars. In some TLDs, 90% or more of the malicious domains were registered through one gTLD registrar.
4. Most phishing occurs on domains purposely (maliciously) registered for phishing attacks. 65% of domains associated with phishing attacks were maliciously registered. In the new TLD space, 70% of phishing domains reported in new TLDs were malicious. Twenty gTLD registrars accounted for 83% of all reported maliciously registered domains. Of these, the top four gTLD registrars (NameCheap, NameSilo, GoDaddy, and Public Domain Registry) account for 53%.
5. Ten hosting networks accounted for 41% of all phishing attacks. The study identified 4,110 hosting networks (ASNs) where phishing web sites were reported; of these,

¹⁴² Interisle Phishing Landscape 2020: A Study of the Scope and Distribution of Phishing: <http://www.interisle.net/PhishingLandscape2020.pdf>

¹⁴³ Interisle Phishing Landscape 2021: An Annual Study of the Scope and Distribution of Phishing: <https://www.interisle.net/PhishingLandscape2021.pdf>

four hosting networks (NameCheap, Cloudflare, Unified Layer, and Google) accounted for 28% of all phishing attacks.

6. 11% of all phishing attacks took place using resources at subdomain service providers. Ten providers accounted for 90% of the phishing attacks hosted at subdomain service providers.
7. Phishers targeted 1,804 businesses or organizations during the 1 May 2020 to 30 April 2021 period. The top 10 brands targeted over the course of our annual period account for 46% of the reported phishing attacks.
8. When phishers register domains, they tend to use them quickly. 57% of domains reported for phishing were used within 14 days following registration and more than half of those were used within 48 hours. 89% of these maliciously registered phishing domain names were reported for phishing within 14 days following registration, and 98% of maliciously registered domain names were reported for phishing within the first year of registration.

This report also shows that phishers can and do register and use large numbers of domains at specific registries and registrars, again and again over time. These levels of phishing activity might be caused by one or more of the following factors:

1. Low pricing, offered as part of a registrar and/or a registry operator's sales strategy. In general, phishers tend to be attracted to low prices.
2. Inattention to abuse problems by the registrar and/or the registry operator. This allows phishers to buy and use domains over time.
3. Features at the registrar that facilitate phishing, such as APIs that allow registrations in bulk, or payment methods that offer anonymity or have weak fraud detection. Cybercriminals take advantage of bulk registration services to "weaponize" large numbers of domain names.

The Iterisle study concludes that:

1. gTLD registrars and TLD operators are in an excellent position to identify and suspend malicious domain name registrations with a high degree of accuracy, often at the time of registration, and often by using the same methods that phishing investigators apply when phishing is first seen in the wild. For example, many domains registered by phishers also have telltale characteristics – name composition, common creation dates, similarities in contact data – that an operator can use to identify malicious registrations quickly and with low false-positive rates.
2. gTLD registrars and TLD operators possess key information – contact data and billing data – that no one else does. This data is highly useful for identifying malicious customers at the time of registration. Access to contact information – the registrant's identity, payment information, IP address, and purchase history – can be essential in a phishing investigation. Traditionally, phishing investigators would use WHOIS contact data to find other domains with similar contact data elements, and thus owned by the same cyber criminals. Only by identifying virtually all of a phisher's domain names can investigators hope to fully mitigate a phishing campaign.
3. gTLD registrars and TLD operators all have terms of service that allow them to suspend domains for malicious and illegal activity. Opportunities exist for registrars and registry operators to monitor for such activity, and to suspend domains for malicious purposes. Many operators have acceptable use policies. Phishing is a

recognized manifestation of fraud in arguably every jurisdiction in which registrars and TLDs operate. Stringently (and uniformly) enforcing a prohibition against phishing should result in a reduction in maliciously registered domains.

4. Maliciously registered phishing domains can be suspended by the registrar or registry operator; this stops the attacks and will not cause any damage or inconvenience to anyone except the phisher. Registries with high numbers of maliciously registered domain names can collaborate with their registrars to adopt phishing identification and prevention measures. When phishing occurs on compromised hosting, hosting providers are best positioned to take appropriate mitigation efforts. While administrators of web sites can remove the phishing pages from the hosting server, phishers are highly unlikely to do so. The responsibility to remove fraudulent phishing content, disable an unauthorized web server, or suspend accounts of subscribers who are perpetrating phishing falls upon hosting operators. Typically, these are violations of the operator's own acceptable use policy. They are also able to deploy measures to detect compromises and to recommend security content management practices that can reduce their customers' web vulnerability attack surfaces.

2.2 The findings of the measurements carried out by the authors and related to phishing confirms the findings of the above-mentioned Interisle study (Appendix 1 – Technical Report).

2.3 Moreover, generally, phishing has also been reported as an increasing threat also by stakeholders (both DNS service providers and rightholders) surveyed by the authors (see Section 7.b above), and domain name dispute resolution service providers (see Section 7.c.4 below).

3. Child Sexual Abuse Material (CSAM)

Over the past 20 years, online child sexual abuse has increased dramatically worldwide.

3.1 The UK-based **Internet Watch Foundation (IWF)** estimates that there are at least 1 million of child sex offenders searching for child sexual abuse material (CSAM) online. As for CSAM, quantifying its precise volume is difficult, as there are numerous ways in which it can be distributed online, and knowledge about its existence – a fraction of what is really out there – is obtained from reports provided by the tech industry, and also by NGOs, users and hotlines on a voluntary basis. Yet, hotlines remain predominantly reactive to reports they receive. A very small number of hotlines engage in proactive search for CSAM online themselves.¹⁴⁴ According to IWF, one of those hotlines that proactively searches CSAM, compared to the 1 million reports of CSAM worldwide in 2010, in 2019 the number increased to 17 million, including nearly 70 million images and videos.¹⁴⁵ Most of these reports are submitted by electronic service providers that find CSAMs with the help of technology, or by their users (who are often the victims of online child abuse themselves).

3.2 In the US, once tech companies have removed such content, they report it to the US-based non-profit **National Center for Missing and Exploited Children (NCMEC)**, as required by US federal law (mandatory reporting). However, they do not have to notify cases and data to the police or prosecutors in the child sex offenders' country of origin. The NCMEC then makes these reports available, on a voluntary basis, to law enforcement authorities around the world to aid with investigations and prosecutions. Thus, the NCMEC

¹⁴⁴ [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/659360/EPRS_BRI\(2020\)659360_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/659360/EPRS_BRI(2020)659360_EN.pdf)

¹⁴⁵ <https://www.iwf.org.uk/report/iwf-2019-annual-report-zero-tolerance>

is a key source in the provision of CSAM reports worldwide, including for EU countries. In the EU, companies are not obliged (until today) to report CSAM by law.

3.3 The International Association of Internet Hotlines (INHOPE), established in 1999 by eight organizations and with support from the European Commission's "Action Plan on promoting safer use of the Internet", is the international umbrella association of Internet hotlines which operate worldwide and accept complaints about CSAM. The network consists of more than 45 hotlines in over 40 countries. Complaints concerning illegal Internet content can thus be forwarded to the relevant responsible partner. In this way, the illegal content is investigated in its respective country of origin, which is also advantageous for criminal prosecution. The INHOPE Annual Report 2019 reported that the number of CSAM related images and videos processed by its hotlines from 2017 to 2019 has almost doubled.¹⁴⁶ In 2019, 183.788 reports were processed, 456.055 images and videos assessed and 320.672 illegal images and videos removed. The Annual Report 2020 is expected to be published in late April / May 2021.

3.4. CSAM during the COVID-19 pandemic

3.4.1 The volume of child abuse materials circulating on the Internet has increased dramatically during the COVID-19 pandemic, as both children and child sex offenders spend more time, and interact more, online. Both **Interpol**¹⁴⁷ and **Europol**¹⁴⁸ confirmed such increase in the number of cases of CSAM, affirming that: *"What the report shows is that we are seeing just the tip of a growing iceberg in terms of online child exploitation material."* The **IWF** has warned that the number of child sexual abuse images being removed globally has fallen by 89% during the pandemic, as, while internet traffic has grown exponentially, many organizations have been working with limited capacity. According to **Europol**, the volume of CSAM in the EU has become simply unmanageable for many of the law enforcement units dealing with it. This ongoing increase reflects the continuous distribution and redistribution of CSAM content.

3.4.2 IWF's Annual Report 2020¹⁴⁹, released on 21 April 2021, reveals that 299.619 reports were assessed by IWF in 2020: 299.531 were reports of URLs (webpages) and 88 were reports of newsgroups. 153.383 URLs were confirmed as containing child sexual abuse imagery or UK-hosted non-photographic child sexual abuse imagery. This is a 16% increase from 2019. IWF also saw an increase in the number of domains being abused to host child sexual abuse material in 2020. The 153.369 URLs which displayed child sexual abuse imagery in 2020 appeared across 5.590 domains, traced to 59 countries. This is a 13% increase from 4.956 domains in 2019. 153.383 reports were confirmed as containing child sexual abuse imagery or UK-hosted non-photographic child sexual abuse imagery. This is a 16% increase from 2019.

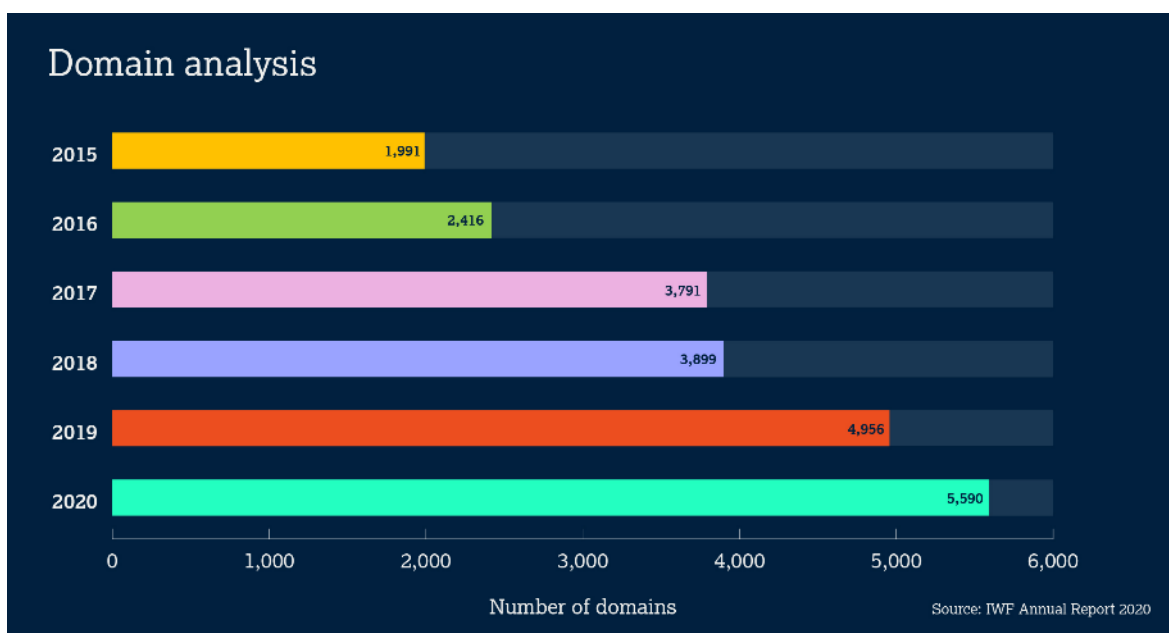
Figure 6: Domain names involved in CSAM (source IWF)

¹⁴⁶ <https://www.inhope.org/EN/articles/inhope-launches-2019-annual-report>

¹⁴⁷ <https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse>

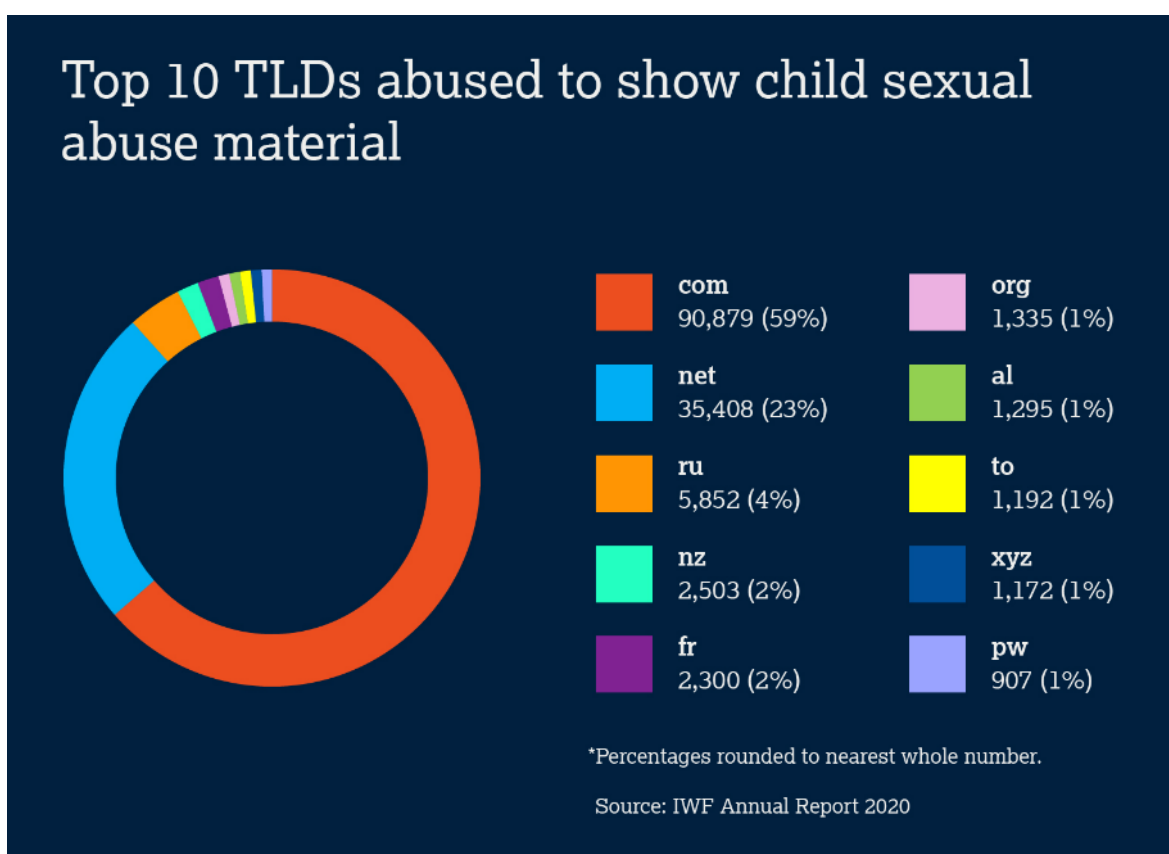
¹⁴⁸ <https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic>

¹⁴⁹ <https://annualreport2020.iwf.org.uk/>



The websites containing child sexual abuse content were registered across 169 top level domains - 81 gTLDs and 88 ccTLDs.

Figure 7: Top 10 TLDs involved in CSAM (source IWF)



New gTLDs being abused for the distribution of child sexual abuse imagery continued to be a trend in 2020. Of the 5,590 domains containing child sexual abuse imagery in 2020, 1,379 (25%) were using one of 71 different new gTLDs. Across these new gTLDs, IWF took action against 4,127 URLs. Of the 5,590 domains containing child sexual abuse imagery in 2020, 3,401 (61%) of these were categorised as dedicated commercial sites. A “dedicated commercial” site is one that IWF believes has been created solely for the purpose of

profiting financially from the distribution of child sexual abuse material online. IWF has also identified a trend of “top-level domain hopping” which offers opportunities for registries and registrars to have a bigger impact in preventing the distribution of online child sexual abuse. “Top-level domain hopping” is when a site (e.g. “badsite.ru”) keeps its second-level domain name (“badsite”) but changes its top-level domain (“.ru”), creating a whole new website with different hosting details but retaining its “name brand”. So from “badsite.ru”, the additional sites “badsite.ga”, “badsite.ml” or “badsite.tk” could be created. This allows instances of a website to persist online after the original has been taken down while keeping the website recognisable and easy to find. From 2015 to 2020, IWF tracked top-level domain hopping among websites created with the primary purpose of sharing child sexual abuse imagery. Over this five-year period, IWF identified 2.293 commercial websites exploiting this technique – that’s websites created to financially gain from distributing child sexual abuse imagery. Of these, 917 were unique second-level domains. That means a further 1.376 websites were created by top-level domain hopping. Forum websites dedicated to sharing child sexual abuse imagery have also relied on top-level domain hopping to remain online. Of the 133 forums IWF took action on, 43 unique second-level domains were used. An additional 90 forum sites were created using top-level domain hopping. That adds up to 1.466 criminal websites that could have been intercepted and kept offline by blocking top-level domain hopping. IWF collaborate with several TLD registries (e.g., Public Interest Registry – PIR and Donuts) providing domain alerts services.¹⁵⁰ As for hosting, Europe has been the top continent with hosting of child sexual abuse webpages since 2016.

Figure 8: Continents hosting CSAM (source IWF)

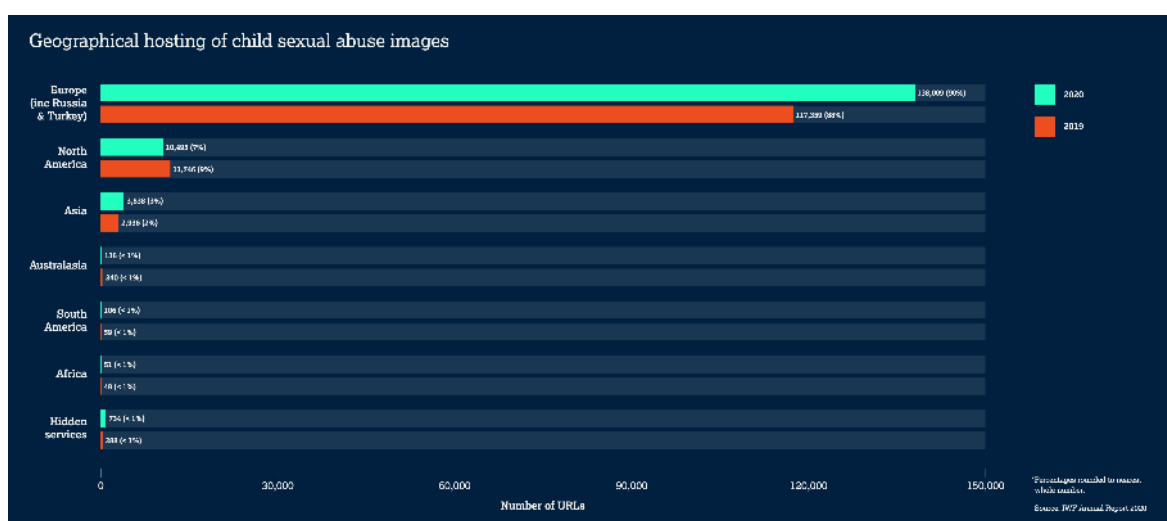
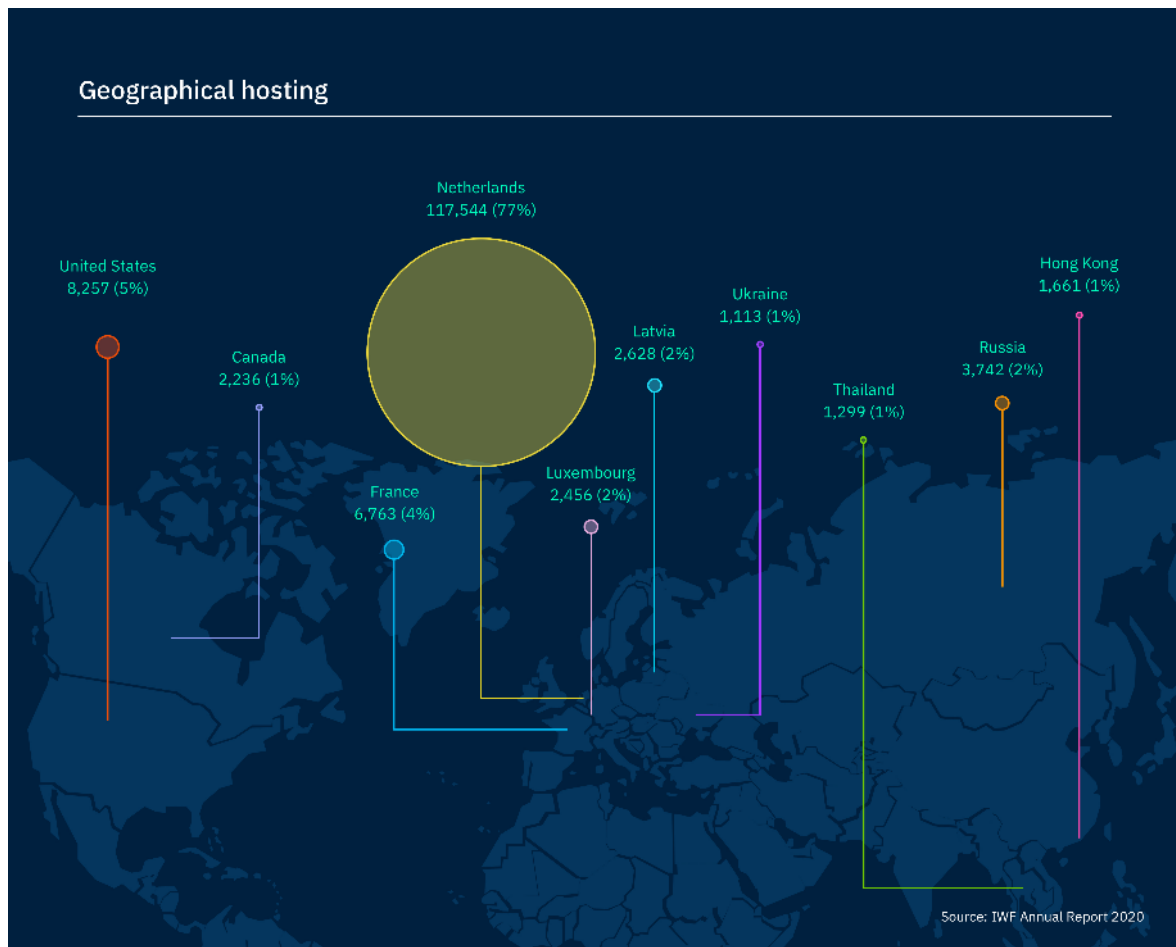


Figure 9 shows the top 10 countries hosting CSAM: the Netherlands, the United States, France, Russia, Latvia, Luxembourg, Canada, Hong Kong, Thailand, Ukraine.

Figure 9: Top 10 countries hosting CSAM (source IWF)

¹⁵⁰ <https://www.iwf.org.uk/our-services/domain-alerts>;
<https://annualreport2020.iwf.org.uk/trends/casestudies/domain>



Regarding the Netherlands, TU Delft released a report on CSAM Hosting Monitor in September 2020 which extensively analyses the phenomenon within the country.¹⁵¹

3.4.3 The Complaints Office of eco – Association of the Internet Industry¹⁵² is the German hotline of INHOPE and handles complaints related to the following illegal Internet content: youth-endangering and development-impairing content; freely accessible adult pornography, pornography depicting violence, animals, children, or juveniles; dissemination of symbols and propaganda material of unconstitutional organizations; incitement of the masses; attempting to cause the commission of offenses; depictions of extreme violence; grooming; dissemination of naked images of minors for profit; public incitement to crime. In addition, the eco Complaints Office handles reports on the unsolicited sending of marketing emails and newsletters.¹⁵³ Contrary to expected increase in reports on illegal Internet content in 2020 due to the pandemic, the eco Complaints Office did not register an increase in reports. In 2020, a total of 14.299 complaints were reported regarding potentially criminal content or content relevant to youth media protection of minors. Nevertheless, the number of justified complaints, with a total of 5.523 cases, is higher than ever before. Compared to 2019 (4.654 cases), the number of justified complaints increased by 18.7%. The principal reason for this is that the proportion of justified complaints has grown in comparison to previous years. In terms of content, child pornography content also – as in previous years – accounted for the largest share of justified complaints.

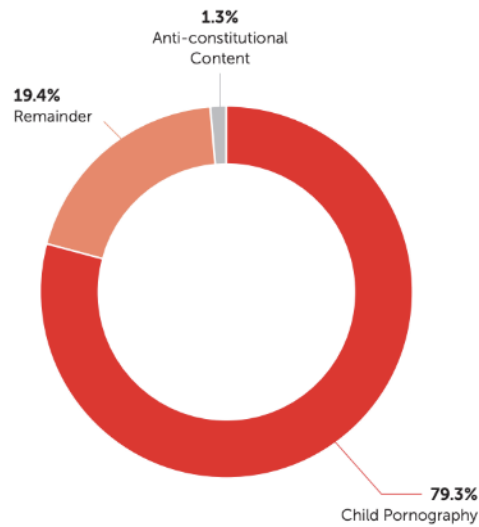
Figure 10: Percentage of justified complaints (source eco Complaints Office)

¹⁵¹ https://mcusercontent.com/9641b809f4358b8638f9a36f1/files/06a5c6a6-6337-40b2-a8c5-071f227bc408/CSAM_Hosting_Monitor_EN_Sept2020.pdf?mc_cid=e6f6727825&mc_eid=cd82eecab8

¹⁵² <https://international.eco.de/>

¹⁵³ <https://international.eco.de/topics/policy-law/eco-complaints-office/>

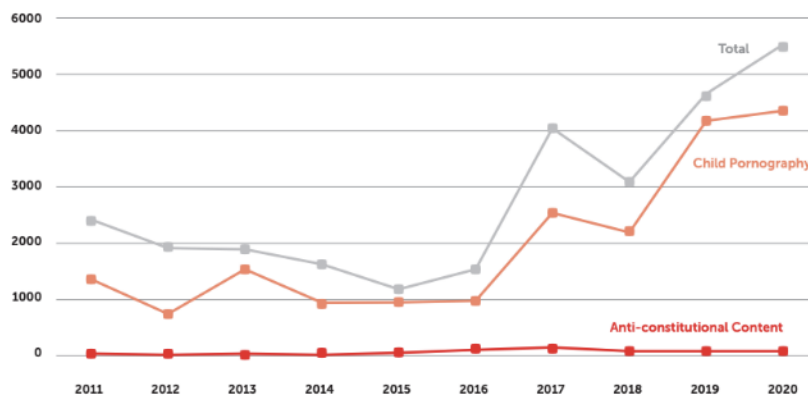
Justified Complaints 2020 (Excluding Spam)



Source: eco Complaints Office, 2021

Figure 11: Growth in number of justified complaints (source eco Complaints Office)

Growth in Number of Justified Complaints



Source: eco Complaints Office, 2021

The breakdown per extensions of the actionable reports received by eco Complaints Office are as follows:

Number and percentage of actionable report broken down per TLD (source eco Complaints Office)

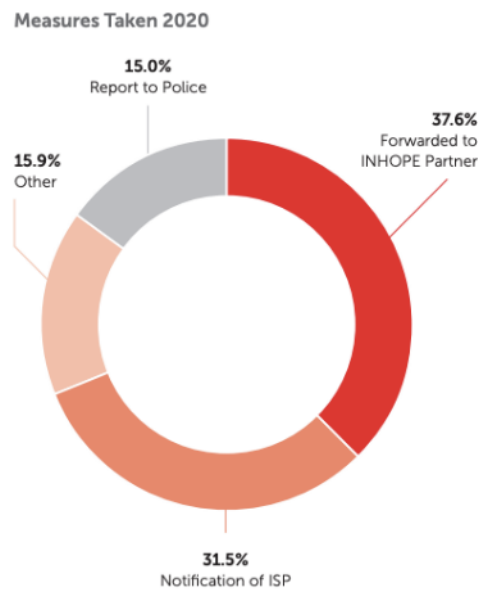
TLD	Amount TLD	Percentage
.com	1909	35%
.club	572	11%
.ml	450	8%
.ru	295	5%
.cf	268	5%

.ga	214	4%
.net	179	3%
.al	174	3%
.org	121	2%
.top	107	2%
.click	99	2%
.gq	86	2%
.xyz	82	2%
.pro	66	1%
.download	47	1%
.ph	47	1%
.pw	47	1%
.buzz	43	1%
.de	43	1%
.to	40	1%
.cc	34	1%
.info	34	1%
.eu	31	1%
.fun	30	1%
.uno	30	1%
.tk	28	1%
.biz	26	0%
.link	20	0%
.men	20	0%
.gg	18	0%
.icu	17	0%
.il	14	0%
.is	13	0%
.jp	12	0%
.ws	11	0%
.gr	10	0%
.cloud	9	0%
.online	9	0%
.pics	9	0%
.io	8	0%
.site	8	0%
.fr	7	0%
.ua	7	0%
.vn	7	0%
.at	6	0%
.best	6	0%
.app	5	0%
.it	5	0%
.space	5	0%

.su	5	0%
.vip	5	0%
.bz	4	0%
.co	4	0%
.me	4	0%
.pink	4	0%
.se	4	0%
.tube	4	0%
.cyou	3	0%
.in	3	0%
.live	3	0%
.monster	3	0%
.uk	3	0%
.wang	3	0%
.cl	2	0%
.dk	2	0%
.li	2	0%
.nl	2	0%
.pet	2	0%
.pk	2	0%
.srl	2	0%
.tv	2	0%
.tw	2	0%
.ac	1	0%
.be	1	0%
.casa	1	0%
.cool	1	0%
.cz	1	0%
.kr	1	0%
.moscow	1	0%
.ms	1	0%
.pm	1	0%
.press	1	0%
.sexy	1	0%
.st	1	0%
.tl	1	0%
.vet	1	0%
.watch	1	0%

In 2020, eco Complaints Office sent a total of 9.080 notifications (in particular to the police, INHOPE partner hotlines, and/or ISPs – not including reminders).

Figure 12: Measure taken in 2020 (source eco Complaints Office)



Source: eco Complaints Office, 2021

The number of justified complaints regarding depictions of the sexual abuse and sexual exploitation of minors increased by around 6% in 2020. Of the total of 4.664 cases from this area of offense, the majority, as in previous years, were regarding content that qualified as child pornography as defined in Section 184b of the German Criminal Code. In comparison to previous years, shorter take-down times were registered in 2020. Websites with child pornography hosted in Germany were offline (“taken down”) within 2.43 days on average, whereas globally it took 6.44 days. For child pornography content overall, a total success rate of 98.79% was recorded (for content hosted in Germany, this came to 100%). From a technical viewpoint, referrer cases and the use of Content Delivery Networks (CDNs) are particularly noteworthy. Depictions of the sexual abuse and sexual exploitation of minors are not infrequently only accessible with a so-called referrer. Here, the user must come from a specific “source” site, which refers across through a link. The “destination” site registers where the user has come from and shows different content depending on the request. Technically, this process can be simulated using particular tools. A more complex, but comparable, method triggers this technical path-setting through the use of cookies. In both cases, different content will be shown depending on the digital path followed or simulated. The involvement of CDNs also makes it more difficult to process cases – for example, in instances where there is a delay in reporting back to the actual host provider, or when the take-down check before a reminder is sent requires a renewed response from the CDN to identify the actual host provider. Occasionally, explanations to the recipient also require a notification that a CDN is involved. Approximately 1.600 reports involved a CDN and 750 URLs required a referrer to see the illegal content.

4. Intellectual Property Rights (IPR) Infringements

IPR infringements in the online environment are diverse and may include:

- Illegal sharing and distribution of copyright protected works;
- Sale and distribution of IPR infringing goods on online marketplaces and social media, using domain names that include a third-party trade mark and the content and design of the website itself resembles that of the brand owner;

- Fraud, extortion and other traditional cybercriminal offences, making use of a domain name that resembles the genuine domain of brand owners;
- Cybersquatting;
- etc.

4.1 According to the **EUIPO – Europol Intellectual Property Crime Threat Assessment Report 2019**, organised crime groups (OCGs) are heavily involved in counterfeiting and piracy, and intellectual property crime is often combined with other types of crime, including money laundering, document fraud, cybercrime, fraud, drug production and trafficking, forced labour and even.¹⁵⁴

4.2 The **EUIPO Status Report on IPR Infringement**¹⁵⁵, published in June 2020, has unsurprisingly found that the business models adopted by counterfeiters make significant use of the Internet to distribute their products and to promote the distribution and consumption of illegal digital content. The supply and consumption of counterfeit goods represents only part of today's IPR infringement picture. The supply and consumption of copyright-infringing digital content across media such as television, films, live sports events, music, games and books via the Internet represents a lucrative market for infringers and consumers alike.

4.3 In order to map the evolving business models used by suppliers of illicit digital content and by sellers of counterfeit goods, the EUIPO carried out a study, resulting in the **Research on Online Business Models Infringing Intellectual Property Rights**¹⁵⁶, published in July 2016. This report identified and examined the techniques used to facilitate online IPR infringements and the associated business models employed. In addition, the analysis examined how the structures and approaches functioned, how they were financed, the revenue streams generated, the content being distributed and the associated customer bases. The analysis found that there were at least 25 online business models that either directly infringed IPR in the sale of counterfeit goods or used the same websites, either on the internet or the darknet, to engage in illegal activity such as phishing, dissemination of malware and the sharing of pirated digital content. In many of these models the infringement of trade marks and copyright was most common, although there were instances of multiple infringements, including cases where IPR was misused in the domain name. One of the key findings of the study is that a number of business models are taking advantage of IPR infringements to carry out traditional cybercriminal activities. Most e-mail phishing scams make use of well-known trade marks in the sender address and in the e-mail itself, thus deceiving the recipients into believing that the e-mail has been sent by the particular brand owner. The phishing e-mail may contain ransomware, which is a malware that is used to infect and “hijack” the recipients computer, whereby the sender demands a “ransom” in order to remove the malware from the computer. Recently, apps for mobile devices have also been infected with ransomware in this way. Phishing e-mails may also include a link to a corresponding website that uses a domain name that includes the third party trade mark and which has a user interface that is a close imitation of the particular brand owner's genuine website (“spoofing”). This type of phishing scam is used to deceive the recipient into disclosing access code or passwords to bank accounts or credit card details –

¹⁵⁴ https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_IP_Crime_Threat_Assessment_Report/2019_IP_Crime_Threat_Assessment_Report.pdf

¹⁵⁵ https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2020_Status_Report_on_IPR_infringement/2020_Status_Report_on_IPR_infringement_en.pdf

¹⁵⁶ https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Research_on_Online_Business_Models_IBM/Research_on_Online_Business_Models_IBM_en.pdf

information that was previously often obtained through illegal hacking. It generally seems that some IPR infringements are carried out in technologically advanced combination with traditional cybercriminal activities with the aim of getting access to illicit revenue, personal data or other valuable information.

4.4 In March 2021, the EUIPO released a discussion paper on **Domain Names: Challenges and good practices from registrars and registries to prevent the misuse of domain for IP infringement activities**.¹⁵⁷ The discussion paper highlights the main challenges in addressing IPR-infringing uses of domain names, such as the use of (i) domain privacy and proxy services that act as intermediaries for domain registrations, (ii) stolen individual or business details to register a domain used for IPR-infringing activities, (iii) subdomains to 'hide' infringing content, and (iv) dispute resolution mechanisms to address infringing use of a trade mark in a domain name. It also identifies good practices from registrars and registries to prevent the misuse of IPR-infringing domain names. Those good practices are classified into the three main phases of the domain name lifecycle and the registry and/or registrar that could take action:

1. Pre-registration

- Registries: Terms and conditions clearly listing IPR infringement as one of the breaches of contract that can lead to suspension of a domain;
- Registries: Prohibiting or limiting the use of proxy services;
- Registries: Alerts and rights protection mechanisms informing trade mark owners of the registration of a domain name identical to their trade mark.

2. Registration

- Registries: Systems to verify the identity of the registrant, using electronic identification solutions, and/or public registries;
- Registries: Systems to automatically detect abusive domain registration applications and suspend them.

3. Post-registration

- Registries: Manual or automated checks to detect fake or incorrect registration information (through a proactive approach or a verification request process);
- Registries: Notice and action mechanisms, to be used for notifying domains with illegal content (e.g. in cooperation with law enforcement authorities);
- Registries and registrars: Cooperation with rightholders to put in place 'trusted notifiers' systems.

4.5 Finally, in May 2021, the EUIPO published a study on **Focus on Cybersquatting: Monitoring and Analysis**.¹⁵⁸ The purpose of this study was to quantify the phenomenon of cybersquatting and to describe the methods and the business models employed by

¹⁵⁷ https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Discussion_Paper_on_Domain_Names/2021_Discussion_Paper_on_Domain_Names_FullR_en.pdf

¹⁵⁸ https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Cybersquatting_Study/2021_Focus_on_Cybersquatting_Monitoring_and_Analysis_Study_FullR_en.pdf

cybersquatters, thus providing a basis for fighting the phenomenon more effectively. For the quantitative analysis, the detection and analysis of domain names was conducted across 560 gTLDs and 250 ccTLDs, covering approximately 239 million registered domain names. The analysis was carried out in the first quarter of 2020. The quantitative analysis focused on a selection of 20 brands protected by trade marks, owned by small, medium and large entities across different categories of goods and services. The study identified suspicious uses of the selected trade marks in registered domain names and analysed the techniques used by cybersquatters to take advantage of the brands built by the trade mark owners. Legacy gTLDs accounted for 679 (68%) of the domain names, 257 (26%) were ccTLDs and 57 (6%) were new gTLDs. Out of those, 338 legacy gTLDs (50%), 116 ccTLDs (45%) and 32 new gTLDs (56%) were considered suspicious. The fact that the new gTLDs accounted for only a small share of suspicious TLDs could simply reflect the low number of such TLDs compared to the legacy TLDs. At that point in time, the new gTLDs were not a significant source of cybersquatting, although the proportion of suspicious domains among new gTLDs was higher than for either ccTLDs or legacy gTLDs. A regular expression (i.e. a domain name containing the trade mark within it) was the most common type of cybersquatting, accounting for 85% of the analysed domains. Many suspicious domain names were recently registered. The study noted that, since many domains were registered for 1-year periods, that may simply reflect that cybersquatters let many domains expire (presumably because they did not generate sufficient traffic and revenue). 40 suspicious domain names were selected for qualitative analysis from the domains that were in active use, thus not parked or otherwise passively held. The key findings were as follows:

- Every domain redirected traffic from the legitimate brand as part of internet traffic features;
- 24 domain names (60%) related to physical or virtual products marketing, while 16 (40%) related to domain name digital misuse;
- 24 (60%) domain names offered infringing products or services, 11 (28%) offered only information and 5 (12%) offered genuine products;
- 22 (55%) domain names attracted visitors by projecting legitimacy and 18 (45%) through both discounts and legitimacy;
- 24 (60%) domain names generated income through customer payments, 13 (33%) through pay-per-click and 3 (7%) through domain name purchase;
- 32 (80%) domain names were unsecured and 8 (20%) were secured.

Information about the cybersquatter was not available for 26 of the 40 suspicious domains, having been marked as 'redacted for privacy', potentially hindering enforcement actions against the registrant. Information concerning the registrant on WHOIS records is the starting point for dealing with suspicious activity. The study concluded that cybersquatting is a genuine problem for legitimate brands. While not all the domains classified as 'suspicious' represented IPR infringement (e.g. fan sites or sites devoted to criticism), a proportion of cybersquatted sites were used to market counterfeit goods or engage in other illicit activity using the legitimate brand to attract visitors and thereby harming the brand in ways that go beyond counterfeiting.

Thus, the quantification of online IPR infringement is in itself not an easy task. The quantification of abusive domain name registrations is even harder. IPR holders seeking to enforce their rights have different mechanisms at their disposal starting from administrative and out-of-court mechanisms to court proceedings. Since the Internet has a global reach and the resolution of cross-border domain disputes through court proceedings is costly and time-consuming, alternative dispute resolution (ADR) mechanisms to resolve such disputes

are internationally recognised as effective enforcement measures for domain name registrations infringing IPR, in particular trade marks, at the level of the string of domain names. The Uniform Domain Name Dispute Resolution Policy (UDRP) was adopted in 1999 by ICANN to provide remedy to the widespread phenomenon of the so-called cybersquatting, i.e. registration of domain names confusingly similar to trade marks for profit. The UDRP is incorporated by reference into all gTLD registration agreements. Therefore, the domain name holder is required to submit to a mandatory administrative procedure in the event that a third party (complainant) states that:

- (i) the domain name is identical or confusingly similar to a trade mark or service mark in which the complainant has rights; and
- (ii) the domain name holder has no rights or legitimate interests in respect of the domain name; and
- (iii) the domain name has been registered and is being used in bad faith.

Circumstances, such as domain names involved in phishing scheme, malware distribution or other scams and fraudulent activities might have relevance in the assessment of the second and third elements mentioned above.

Over the years, the UDRP has proven an efficient way to resolve domain name disputes involving gTLDs and some ccTLDs.¹⁵⁹ Several European ccTLDs adopted domain name dispute resolution policies similar to the UDRP, adapting this latter to their national legal environment.

The following data collected from the UDRP service providers are indicators of the increasing trend on how IPR infringement at the domain name's string level and/or content level intersect with other types of technical abuse. However, it is important to point out that the domain name disputes filed with the domain dispute resolution service providers represent the mere tip of the iceberg and does not reflect the full extent of the phenomenon. In some cases, businesses do not take action due to the lack of awareness on the infringement and/or on the measures available for the enforcement of their IPR or for other reasons (e.g., they consider taking action complex, not affordable or inconvenient). Others reach amicable settlement agreements or simply acquire the abusive domain name from the registrant, one of the main outcomes cybersquatters seek. Some cases are brought before courts, especially when the rightholders aspire to obtain damages. Finally, in cases where the domain names are involved in other types of abuses too (fake registration data, impersonation, scam, malware distribution, phishing, copyright infringement, trade mark infringement within the website content, etc.) the IPR holders might opt for other remedies (e.g., notice and take down actions, court proceedings) or the domain names might be subject to investigation and *ex officio* actions on behalf of the registries, registrars, hosting providers or law enforcement authorities.

4.6 The World Intellectual Property Organization (WIPO) provides alternative dispute resolution services to resolve domain name disputes under the UDRP and for 76 ccTLDs. Since 1999, it has processed over 50.000 UDRP cases, covering almost 91.000 domain names, and involving parties from over 180 countries. According to the WIPO, COVID-19 pandemic has fueled cybersquatting cases, adding to the record WIPO filing seen in 2020. From January through October 2020, the WIPO Center handled 3.405 cases, or an 11% increase over the same period during 2019.

The domain dispute caseload of the WIPO in the period of 2018-2021 is as follows:

2018

588 Terminated
2859 Decided

¹⁵⁹ Currently applicable to: .ag, .ai, .as, .bm, .bs, .bz, .cc, .cd, .co, .cy, .dj, .ec, .fj, .fm, .gd, .gt, .ki, .la, .lc, .md, .me, .mw, .nr, .nu, .pa, .pk, .pn, .pr, .pw, .ro, .sc, .sl, .so, .tj, .tt, .tv, .ug, .ve, .vg, and .ws

2019

654 Terminated
3039 Decided

2020

692 Terminated
24 Pending
10 Suspended
3478 Decided

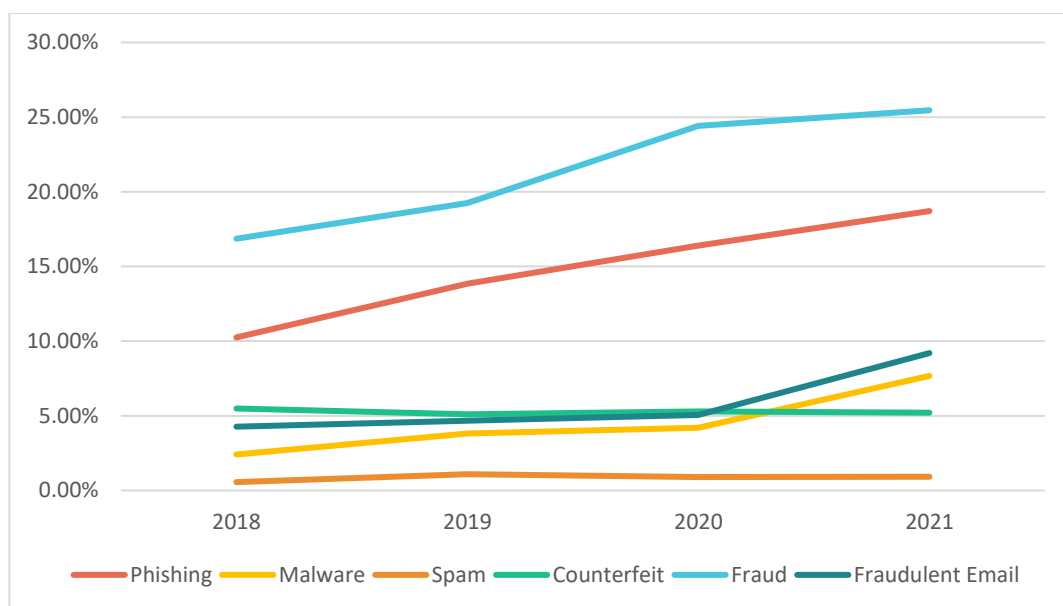
2021

119 Terminated
853 Pending
53 Suspended
326 Decided

According to WIPO statistics, phishing, malware, spam, counterfeiting, fraud or fraudulent e-mail have significantly increased in cybersquatting cases in the period 2018-2021 (data provided on 19 April 2021):

	Phishing	Malware	Spam	Counterfeit	Fraud	Fraudulent Email
2018	10,25%	2,41%	0,56%	5,49%	16,86%	4,27%
2019	13,85%	3,82%	1,09%	5,10%	19,25%	4,67%
2020	16,39%	4,20%	0,89%	5,29%	24,41%	5,06%
2021	18,71%	7,67%	0,92%	5,21%	25,46%	9,20%

Figure 13: Growth in percentage per types of abuse (source WIPO)



4.7 Forum, a US-based domain dispute resolution service provider, has indexed 843 domain name dispute cases (UDRP, usDRP applicable for .us TLDs and CDRP applicable for .ca TLDs) involving technical abuse (in particular phishing) since 2010. Forum's caseload (UDRP/usDRP/CDRP) for the period of 2018-2021 (data provided on 4 May 2021) is as follows:

2018 – 1725/70/19

2019 – 1760/55/12

2020 – 2048/73/8

2021 – 739/32/0

4.8 The Arbitration Center for Internet Disputes of the Czech Arbitration Court (CAC), a provider of UDRP and .eu domain name disputes, reported 260 UDRP decisions and 128 .eu ADR decisions involving technical abuse (in particular phishing) since 2009. The CAC's caseload for the period of 2018-2021 (data provided on 22 April 2021) is as follows:

UDRP:

Year	Total case load	Termination/ suspension	Panel decision	Pending
2018	364	39	335	0
2019	428	50	378	0
2020	564	71	491	2
2021	209	20	117	72

.eu ADR:

Year	Total case load	Panel decision	Pending
2018	39	32	
2019	41	24	
2020	60	54	
2021	17	16	13

4.9 The **Hong Kong International Arbitration Center (HKIAC)** has found DNS misuse (in particular phishing) in 2.8% of its UDRP cases in 2018, 4.9% in 2019 and 3.2% in 2020.

5. Online Sale of Counterfeit Pharmaceuticals

The illegal online sale of pharmaceuticals is an ongoing global problem and as demand grows for more convenient, lower-cost medications and health care delivered virtually, more and more consumers will be put at risk.

There are an estimated 130 million EU citizens buying medicines online. Strong global demand, high profit margins and a low risk of detection make pharmaceuticals especially vulnerable to counterfeiting. It is an undisputed fact that EU citizens are put in harm's way as the sale of counterfeit and substandard medicines is rampant on the Internet. This has already been clearly recognized by the European Commission in its Impact Assessment (2008)¹⁶⁰ for the Falsified Medicines Directive (Directive 2011/62/EU)¹⁶¹.

5.1 According to **Internet Drug Outlet Identification Program** (2016) of the **National Association of Boards of Pharmacy** in 2016 there are between 30,000 to 35,000 online pharmacies operating at any one time¹⁶²; and 20 new illegal online pharmacy sites are launched every day¹⁶³. More than 96% of online pharmacies websites are operating illegally, failing to comply with applicable laws and safety standards.¹⁶⁴

5.2 The **World Health Organization** estimates that 50% of medicines sold online from sites that hide their physical address are counterfeit.¹⁶⁵

5.3 A recent report released by the **OECD** and the **EUIPO** estimates the total value of counterfeit pharmaceuticals traded worldwide to be up to EUR 4.03 billion.¹⁶⁶ Customs seizure data analysed in the study, covering the period 2014-2016, shows that all types of medicines are being falsified. Of particular concern was the fact that antibiotics were being sold and which is believed to be contributing to the rise in antimicrobial resistance.

Undoubtedly, the online and offline sale of counterfeit pharmaceuticals cause economic damage and pose a direct threat to health and life of the EU citizens. Indeed, Forensic tests of suspect samples show that in 90% of cases, counterfeit medicines can harm patients. India and China are identified as the largest producers of counterfeit pharmaceuticals at global level, with Singapore and Hong Kong appearing as the most important transit points in the counterfeit pharmaceutical supply chain. Companies and businesses most affected by counterfeiting and piracy are primarily based in OECD countries such as the United States, the United Kingdom, France, Austria, Germany and Switzerland.

The report has noted the growing role of Internet. The ability of sellers to hide their identity and misrepresent their products is particularly attractive to counterfeiters, providing criminals with a relatively easy point of entry into even the best regulated markets. There are two distinct areas to purchase counterfeit pharmaceuticals online: the dark web and the freely accessible surface web.

5.4 Online Sale of Counterfeit Pharmaceuticals during COVID-19 pandemic

¹⁶⁰ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52008SC2674>

¹⁶¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0062>

¹⁶² Internet Drug Outlet Identification Program, National Association of Boards of Pharmacy, 2016

¹⁶³ The Internet Pharmacy Market in 2016, LegitScript and the Center for Safe Internet Pharmacies, January 2016

¹⁶⁴ Internet Drug Outlet Identification Program, National Association of Boards of Pharmacy, 2016

¹⁶⁵ Substandard, Spurious, Falsely Labelled, Falsified and Counterfeit Medical Products, World Health Organization

¹⁶⁶ <https://www.oecd.org/gov/trade-in-counterfeit-pharmaceutical-products-a7c7e054-en.htm>

The COVID-19 crisis has heightened the dangers posed by the global trade in counterfeit pharmaceutical products. Serious health and safety issues arise when people order fake medicines online; counterfeit medicines are often not properly formulated and may contain dangerous ingredients. During a public health crisis such as the current COVID-19 pandemic, tackling this global scourge becomes even more acute and urgent.

5.4.1 Indeed, a growing volume of fake medicines linked to coronavirus are on sale in developing countries, according to the **World Health Organization**¹⁶⁷, and **Interpol**¹⁶⁸ has also seen an increase in fake medical products related to COVID-19. Seizures of fake COVID-19 tests and personal protective equipment such as facemasks and hand sanitizers have been reported by the **US CBP**¹⁶⁹ and customs of other member countries as well as by the **World Customs Organisation**.¹⁷⁰

5.4.2 The **European Medicines Agency (EMA)** has also urged patients to beware of potential falsified medicines sold by unregistered websites and vendors.¹⁷¹ These vendors have been exploiting fears during the COVID-19 pandemic and claiming that their products can prevent or cure COVID-19. They may also appear to provide easy access to medicines that are otherwise not readily available.

These criminal activities require domain names, which are being used to run phishing, spam, and malware campaigns, and scam sites.

5.4.3 In June 2021 **Interpol** reported that a record number of fake online pharmacies have been shut down under Operation Pangea XIV targeting the sale of counterfeit and illicit medicines and medical products.¹⁷² The operation, coordinated by Interpol, involved police, customs and health regulatory authorities from 92 countries. It resulted in 113,020 web links including websites and online marketplaces being closed down or removed.

6. Domain names including COVID-19 related terms

6.1 In April 2020, **ICANN** revealed that industry actors, such as DNS service providers, registries, and registrars reported that criminals were taking advantage of the pandemic by launching malicious online campaigns.¹⁷³ There have also been numerous reports of spikes in the use of COVID-19-related domain names for DNS Abuse.¹⁷⁴ ¹⁷⁵ In response to that phenomenon, ICANN's Office of the Chief Technology Officer (OCTO) the Security, Stability, and Resiliency team has built the Domain Name Security Threat Information Collection and Reporting (DNSTICR) tool to help to identify abusive domains leveraging the coronavirus pandemic. This system looks for domain names similar to or incorporating terms such as "coronavirus", "covid", "pandemic", "ncov," and others, and once identified, assesses them against multiple high-confidence threat intelligence sources to determine whether or not they are involved in phishing and/or malware distribution. If so, the domain names and the data collected by the system are shared with parties who are in a position

¹⁶⁷ <https://www.bbc.com/news/health-52201077>

¹⁶⁸ <https://www.interpol.int/News-and-Events/News/2020/Global-operation-sees-a-rise-in-fake-medical-products-related-to-COVID-19>

¹⁶⁹ <https://www.cbp.gov/newsroom/national-media-release/cbp-officers-seize-fake-covid-19-test-kits-lax>

¹⁷⁰ http://www.wcoomd.org/en/media/newsroom/2020/march/covid_19-urgent-notice-counterfeit-medical-supplies.aspx

¹⁷¹ <https://www.ema.europa.eu/en/human-regulatory/overview/public-health-threats/falsified-medicines/buying-medicines-online>

¹⁷² <https://www.interpol.int/News-and-Events/News/2021/Thousands-of-fake-online-pharmacies-shut-down-in-INTERPOL-operation>

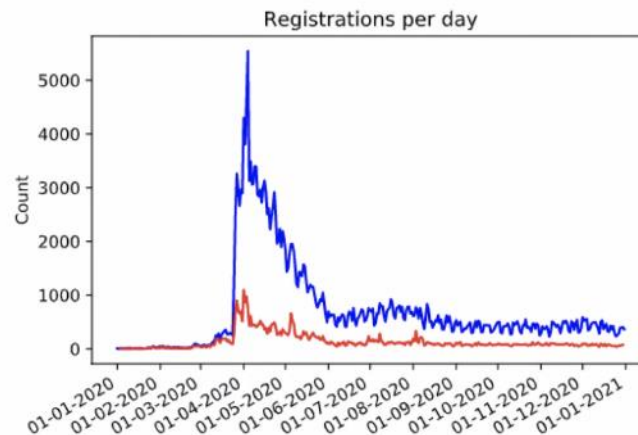
¹⁷³ <https://www.icann.org/en/blogs/details/icann-orgs-multifaceted-response-to-dns-abuse-20-4-2020-en>

¹⁷⁴ <https://www.cyberthreatcoalition.org/> and

¹⁷⁵ Neustar Online Traffic and Cyber Attacks during COVID -19: <https://www.cdn.neustar/resources/whitepapers/security/neustar-covid-19-online-traffic-and-attack-data-report.pdf>

to take action, such as registrars and registries, and in some cases with national and international law enforcement organizations. Between May 2020 and January 2021 175.173 pandemic-related domain names (both legitimate and malicious) were detected. Of those, 10.639 (6,1%) domains had one or more reports in phishing / malware reputation lists and had nameservers or resolved to an IP address.

Figure 14: Pandemic-related domain name registrations (source ICANN)



Registrations per day matching one or more of our filter terms (blue line) plus those which had one or more third-party reports (red line). Dates in DD-MM-YYYY format.

6.2 TLD registries (such as .eu) and registrars have indeed taken steps in order to mitigate malicious activities during the pandemic.^{176 177}

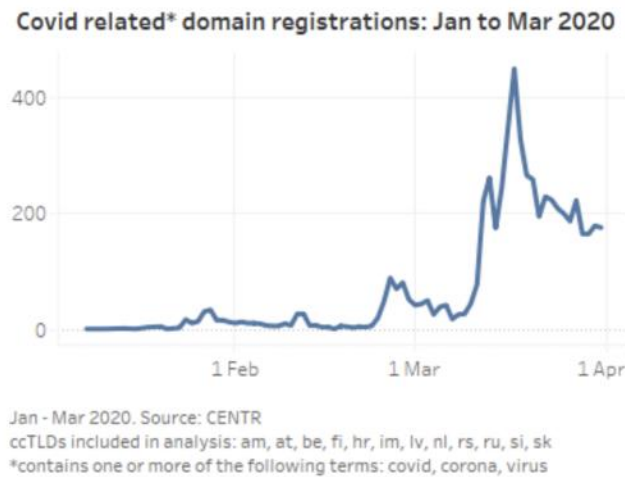
6.3 CENTR has also studied a large sample of domain names across a group of 12 ccTLDs (.am, .at, .be, .fi, .hr, .im, .lv, .nl, .rs, .ru, .si, .sk) to estimate the extent to which the COVID-19 pandemic has had any impact.¹⁷⁸ Domains were analysed for the period of January to March 2020 and restricted to domains which included any of the following terms: “covid”, “corona” or “virus”. A total of 6.164 registrations included these terms, which represented 0.8% of all new registrations in the same group of ccTLDs in this period.

Figure 15: Covid related domain name registrations January-March 2020 (source CENTR)

¹⁷⁶ <https://eurid.eu/en/news/update-covid-dn-checks/>

¹⁷⁷ <https://rrsg.org/wp-content/uploads/2020/03/Registrar-approaches-to-the-COVID-19-Crisis.pdf>

¹⁷⁸ <https://centr.org/news/blog/the-true-effect-of-corona-on-the-dns.html>



CENTR has found that when it comes to actual abuse associated with newly-registered COVID-19 related domain names, the number of reported cases has remained marginally low across European ccTLDs. This is also thanks to actively scanning the newly-registered domains for terms such as “covid”, “corona” or “virus”. Indeed, a survey launched among the ccTLDs showed that 80% of the respondents were performing such active scanning. Roughly half of this 80% verified the registration data of COVID-19 related domains more closely than with other newly-registered domains as a response to the pandemic, and filtered out the ones registered in bad faith. Additionally, about half of the respondents shared lists of newly-registered domain names with national authorities or national CERTs.

The efforts made and actions taken by different stakeholders to combat malicious COVID-19-related domain names and collaborate with authorities clearly show that when public interest (health of citizens) is considered as top priority, DNS abuse cases decrease.

d. Impact of DNS abuse and the sectors involved

Undoubtedly, the DNS abuse phenomenon is detrimental to the users’ trust in Internet. Moreover, it causes economic and societal harms to its victims and more broadly, to the society.

In 2018, McAfee for the **Center for Strategic and International Studies** (CSIS) estimated the global cost of cybercrime to reach \$600 billion, nearly one percent of global GDP.¹⁷⁹

The **World Economic Forum**’s Global Risks Report 2021 ranked cybersecurity failure as a significant global risk.¹⁸⁰ The COVID-19 pandemic has accelerated technological adoption, yet exposed cyber vulnerabilities and unpreparedness, while at the same time exacerbated the tech inequalities within and between societies.








According to **ENISA**, the sectors involved in DNS abuse with particular reference to cybersecurity threats and the related trends in 2020 were as follows¹⁸¹:

Figure 16: Trends in incidents (source ENISA)

¹⁷⁹ <https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf>

¹⁸⁰ <https://www.weforum.org/reports/the-global-risks-report-2021>

¹⁸¹ <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-sectoral-thematic-analysis-of-threats>

SECTOR	MOST POPULAR THREATS/ATTACKS	INCIDENTS TRENDS
Individual	<ul style="list-style-type: none"> Phishing² Malware² Information leakage² Data theft² 	 Stable
Multiple industries	<ul style="list-style-type: none"> Web application attacks² Phishing² Malware² 	 Increasing
Public Administration, Defence, Social Services	<ul style="list-style-type: none"> Malware² Phishing² Web based attack² 	 Stable slightly decreasing
Financial/Banking/ Insurance	<ul style="list-style-type: none"> Web application attacks² Insider threat (unintentional abuse)² Malware² Data theft² 	 Stable
Health/Medical	<ul style="list-style-type: none"> Malware² Insider threat (unintentional abuse/error)² Web application attacks² 	 Increasing
Education	<ul style="list-style-type: none"> Malware² Ransomware² Web based attacks² 	 Stable slightly decreasing
Information and Communication	<ul style="list-style-type: none"> Web application attacks² Insider threat (unintentional abuse/error)² Malware² 	 Stable
Professional/Digital Services	<ul style="list-style-type: none"> Web application attack² Insider threat (unintentional abuse/error)² Malware² 	 Stable
Arts, Entertainment and gaming³	<ul style="list-style-type: none"> Web application attacks² Malware² Phishing² 	 Stable
Manufacturing	<ul style="list-style-type: none"> Malware² Web application attacks² Insider threat (unintentional abuse/error)² 	 Stable

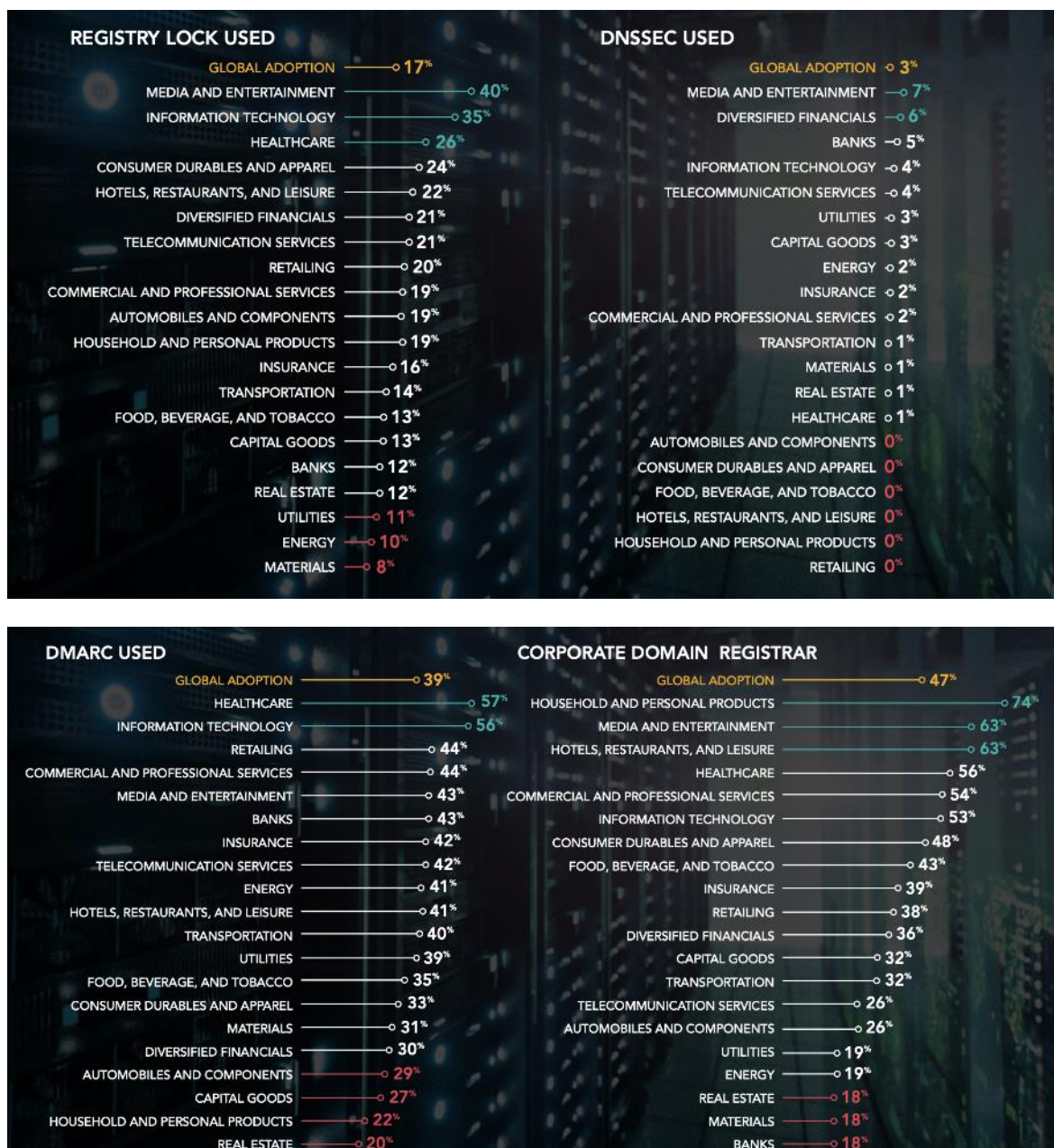
CSC Global's Domain Security Report: Forbes Global 2000 Companies (June 2020)¹⁸² found that 83% of Global 2000 organizations were at greater risk of domain name hijacking, because they had not adopted basic domain security measures like the registry lock protocol. It has also found that:

- Adoption rates for DNSSEC are very low at only 3%. This means 97% of all Global 2000 companies are prone to a cache poisoning attack.
- Only 4% of Global 2000 companies have Certificate authority authorization (CAA) records.
- 15% of Global 2000 companies are still just using domain validation (DV) certificates.
- DMARC use is only at 39% for the Global 2000 companies.

The domain name security controls adoption by industry groups is as follows:

¹⁸² https://www.cscdb.com/assets/pdfs/Domain-Security-Report-2020-June_EN.pdf

Figures 17-18: Domain name security controls adoption: by industry groups (source CSC Global)



With reference to child sexual abuse material (CSAM), of course, its impact on victims, and more broadly on the society, is inestimable in terms of harm

In 2019, the **European Union Intellectual Property Office (EUIPO)**, together with the **European Patent Office (EPO)**, estimated that in 2014-2016 IPR-intensive industries accounted for 45% of the EU's economic output (Euro 6.6 trillion annually) and 29% of employment (with another 10 % generated in sectors that supply goods and services to the IPR-intensive industries). Those sectors account for the bulk of the EU's trade with the rest of the world, generating 96% of goods exports from the EU.¹⁸³ Because of the high value

¹⁸³ EPO/EUIPO, IPR-intensive industries and economic performance in the European Union, third edition, September 2019. Available at: <https://euiipo.europa.eu/ohimportal/en/web/observatory/ip-contribution>.

associated with IPR, infringement of those rights is a lucrative criminal activity with a relatively low level of risk in terms of likelihood of detection and punishment if detected.

According to a study carried out by the **Organisation for Economic Co-operation and Development (OECD) and the EUIPO (2021)**, imports of counterfeit goods in 2019 amounted to EUR 119 billion, which represents up to 5.8% of EU imports.¹⁸⁴ In a series of sectorial studies, the EUIPO has estimated lost sales in 11 sectors in the EU (directly in the industries being analysed and across their associated supply chain), as a result of counterfeiting. These losses totalled more than EUR 83 billion per year during the period 2013-2017. In addition, more than 671 000 jobs in legitimate businesses were lost, and the Member States lost EUR 15 billion per year in tax revenue. As serious as these economic damages are, the harm caused to public health, consumer safety and the environment as a result of counterfeit goods is arguably an even more serious consequence.¹⁸⁵

As **OECD** and **EUIPO** report on Trade in Counterfeit Pharmaceutical Products has highlighted the total value of counterfeit pharmaceuticals traded worldwide is estimated to be up to EUR 4.03 billion (USD 4.4 billion).¹⁸⁶ Between 2014 and 2016, the largest exporters of pharmaceuticals were EU countries, as well as Switzerland, the United States, India, China, Singapore, Israel and Japan. Together, these economies represented more than 92% of the total value of global exports of pharmaceuticals. In many countries the industry represents a significant share of total employment (between and 0.8 to about 1% in countries such as Switzerland, Slovenia and Denmark). Many of these jobs are in research and development activities. Companies registered in the United States are hit the hardest by this trade in counterfeits; those in other OECD countries are also strongly affected (Switzerland, Germany and France). The impact of counterfeits on legitimate producers are multiple and include: lost sales and profits, costs of protecting brands, loss of reputation, the potential cost of managing the disposal of counterfeits and litigation costs, and possibly people who were unknowingly victimised by counterfeits. Counterfeit medicines affect economies in a number of areas:

- Individuals who fall victim to low quality counterfeit products that may not adequately treat their medical needs.
- Legitimate producers, who can lose sales to counterfeiters, and need to take steps to ensure that counterfeiters do not infiltrate their supply chains, and to mount efforts to combat counterfeiters.

Governments, which are actively involved in managing health care in countries. Entire economies, in the form of the impact on crime levels, the environment and the possible effects on jobs and foreign investment.

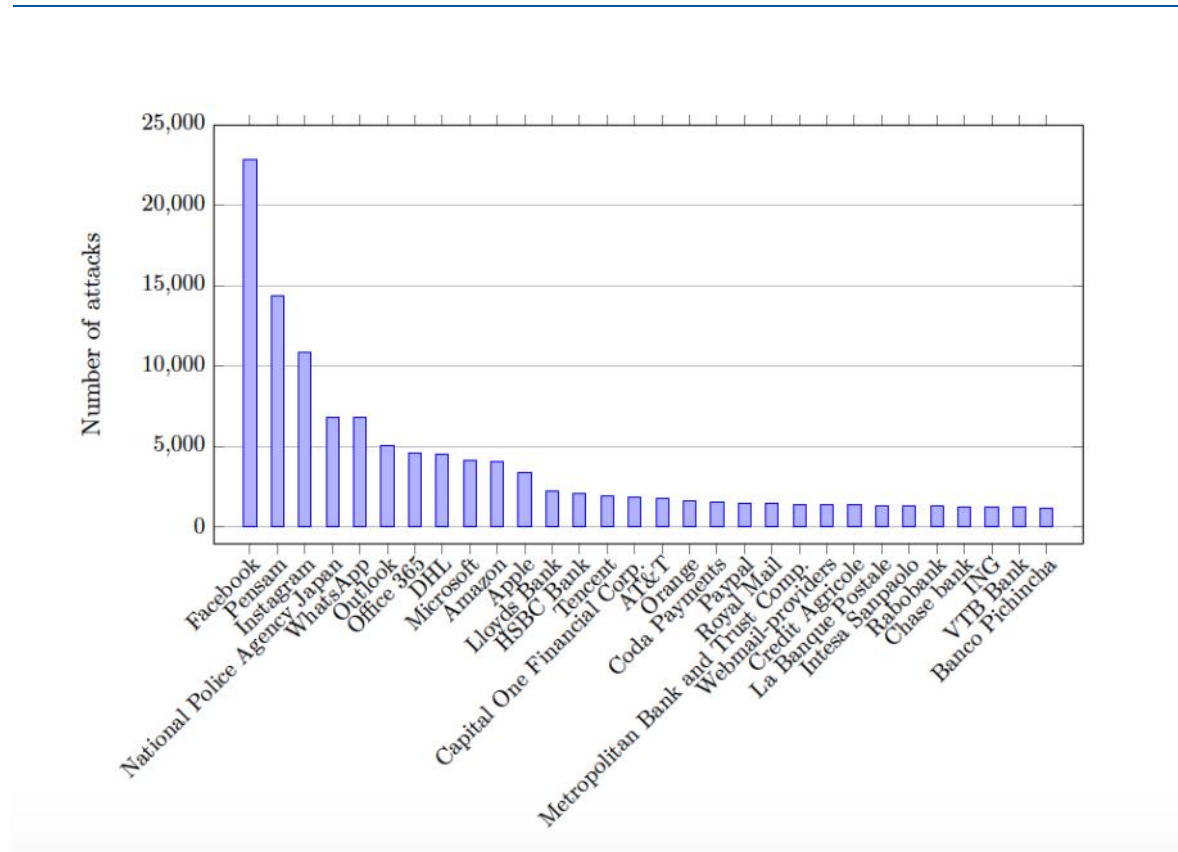
The real-time measurements conducted between March/April and June 2021 by the authors, especially the results with reference to phishing, also show that the most targeted brands and names are from the IT, social media, telecom, and financial and banking sectors (**Appendix 1 – Technical Report**):

Figure 19: Phishing – Top 30 most targeted brands and names

¹⁸⁴ OECD and EUIPO, Global Trade in Fakes: A Worrying Threat, Illicit Trade, 2021. These amounts do not include domestically produced and consumed counterfeit and pirated goods, and pirated digital goods distributed online. <https://www.oecd.org/publications/global-trade-in-fakes-74c81154-en.htm>

¹⁸⁵ https://euiipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2020_Status_Report_on_IPR_infringement/2020_Status_Report_on_IPR_infringement_en.pdf

¹⁸⁶ <https://www.oecd.org/gov/trade-in-counterfeit-pharmaceutical-products-a7c7e054-en.htm>



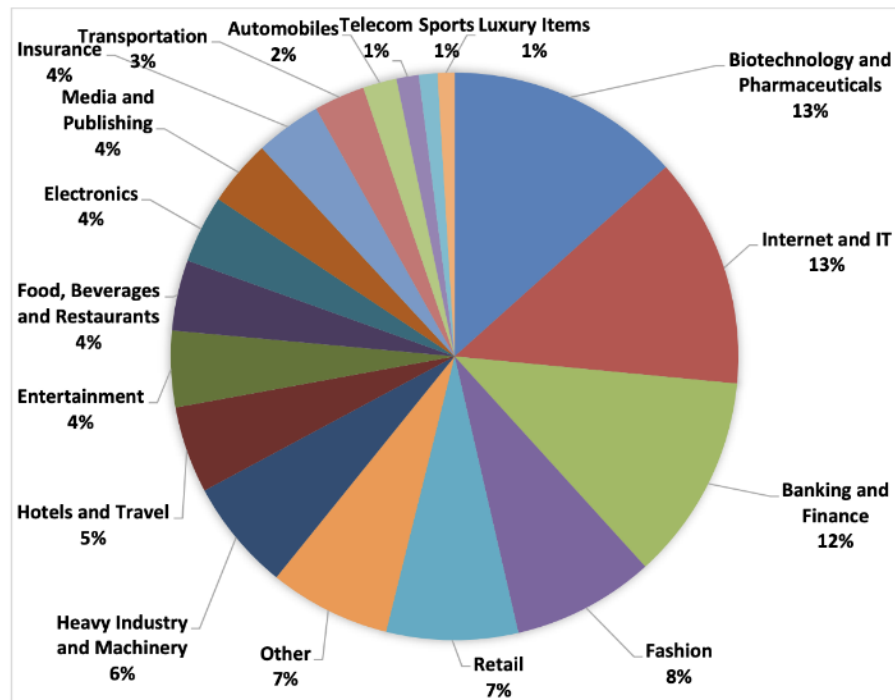
As for WIPO statistics regarding domain name disputes in 2019¹⁸⁷ ¹⁸⁸, the following sectors were enlisted as the most targeted by cybersquatting:

Figure 20: Cybersquatting – Industry of Complainants’ (source WIPO)

¹⁸⁷ <https://www.wipo.int/amc/en/new/2019review.html>

¹⁸⁸ <https://www.wipo.int/export/sites/www/amc/en/docs/pr2020annex4.pdf>

Areas of WIPO Domain Name Complainant Activity (2019)



Due to the lack of consistent dataset in-depth analysis was not possible by the authors. Further studies would be needed to analyse and assess extensively the economic and societal impact of DNS abuse and its various types on EU citizens and businesses and the sectors which are more exposed to such phenomenon.

8. Internet of Things (IoT) and 5G: impact on the magnitude and risks associated to DNS abuse

a. Internet of Things (IoT)

The Internet of Things (IoT) corresponds to a vision of a world in which billions of constrained devices with embedded intelligence, communication means, and sensing and actuation capabilities will connect over IP networks. Most of low-end IoT devices are highly constrained: they have little memory, limited processing capacity, and limited power. IETF distinguishes three classes of devices: Class 0 devices are very constrained sensor-like motes with a RAM size much less than 10 KB and flash memory much less than 100 KB. For Class 1, they are around 10 KB and 100 KB, respectively. Finally, Class 2 is the least constrained with around 50 KB of RAM and 250 KB flash memory.¹⁸⁹ Ultra-low energy consumption is critical for IoT devices since they mostly operate on batteries and they need to reach lifetimes of the order of several years without battery replacement.

Recent IoT networks include Low Power Wide Area Networks (LPWAN) such as SIGFOX and LoRa operating in the unlicensed bands of spectrum and cellular mobile networks with LTE Category M1 (LTE Cat-M1, also referred to as LTE-M), NB-IoT (Narrow Band IoT), and Machine-Type Communication (MTC) in 5G.

5G aims at supporting the IoT by enabling a massive growth in the number of connected devices. The standardization process of 5G set up several requirements for supporting IoT connected devices: devices need to be i) cheap (< 10\$), ii) low power, energy efficient (battery operation of 10 years or more on energy harvesting), iii) low latency (below 1ms), and iv) scalability to billions of devices network wide (>100K per cell). IoT devices share some general requirements such as unmanaged operation, large coverage, and IP connectivity, but may have different specific needs in terms of QoS (Quality of Service), reliability, security, and privacy.

To support IoT devices, 5G aims at taking into account Machine Type Communications (MTC). MTC are different from the data traffic generated by humans in traditional mobile cellular networks: MTC is mainly uplink, the amount of data is small, and the number of connected devices may be very large. Furthermore, Massive MTC and Ultra Reliable MTC can be distinguished. Massive MTC can live with longer delays and intermittent connectivity, but require minimal energy consumption. Ultra Reliable MTC targets industrial applications that need to satisfy stringent latency, throughput, and reliability requirements. The major challenges are thus related to the constraints on IoT devices (low memory, low computational power, and limited energy), scalability, and support for a suitable level of QoS and reliability.

The performance of IoT networks varies from very low rate of 100 b/s provided by SIGFOX for 12-byte payloads and 293 b/s – 5.47 kb/s for LoRa with 59 – 230 bytes of payload. Nevertheless, SIGFOX and LoRa can cover long distance of the order of 10 km. When devices only send sporadic messages, the low rates are compensated by long lifetimes. The new variant of LoRa operates in the 2.4 GHz ISM band and brings important improvements to the data rates and payload sizes – the rate increases to 253 kb/s with the payload sizes up to 255 B. The 2.4 GHz band makes the coverage range smaller, which becomes around 3 km compared to around 10 km of the 868 MHz LoRa variant.

LTE Cat-M1 devices achieve a maximum throughput of up to 1 Mb/s in both uplink and downlink operations with much shorter lifetimes than SIGFOX or LoRa. NB-IoT is expected

¹⁸⁹ RFC 7228, Terminology for Constrained-Node Networks - <https://tools.ietf.org/html/rfc7228>

to obtain a maximum throughput of 50 kb/s with a large coverage and longer lifetimes than LTE Cat-M1.

IoT devices are different from human-controlled computers in many aspects. Usually, they are constrained with limited computing/memory resources and power. Their interface may be very simple or just not existent even though they start to control traditionally human-directed activities at much larger scales than observed previously. There is no user to detect or respond to malfunction so that a device may break and go undetected until a security event. An important characteristic is a large scale of tens of billions of widely heterogeneous deployments and autonomous operation of IoT devices. Moreover, commodity devices are not routinely upgraded or patched, and they are not always managed according to good practices.

IoT presents a number of security risks to both consumers and businesses. IoT devices generally lack sufficient built-in security to protect themselves from causing or becoming a source of harm. Security risks include compromising the end-device hardware, cloning or substitution of devices, tampering with the software in the end-device, compromising the communication in IoT networks like eavesdropping, and Man-in-the-Middle (MitM) attacks. Poorly secured IoT devices and services can become entry points for cyberattacks, compromising sensitive data, weaponization, and threatening the safety of individual users.

Current security mechanisms in IoT are usually based on proprietary closed solutions, which translates to an increased cost for end users and businesses. Weak IoT security has its roots in economic factors because of the tension between costs and security objectives. Including effective security and privacy in IoT costs money and slows down the product development process.

Compared to traditional computers, many IoT applications have physical world safety implications that may result in human harm or in disruption of critical infrastructure services. Many attacks against IoT showed that commodity devices are easily hacked—reported examples include: prison security control systems, heart monitors, insulin pumps, nuclear power plants, oil pipelines, or airline control systems.

IoT devices communicate with services hosted in the Internet and rely on DNS for name resolution as for any other Internet application. However, the difference is that IoT services support IoT devices with sensing and acting upon the physical world whereas traditional Internet applications help users interact with content or services.¹⁹⁰ ¹⁹¹ Moreover, IoT services are usually hidden from users as their configuration is done by the manufacturer.

DNS security extensions (DNSSEC) are important for IoT devices because the validation of DNS responses may avoid MitM or hijacking attacks. Without DNSSEC, devices may miss such attacks and communicate with malicious destinations implying possible malfunction and damage.

Various measurement studies suggest that IoT devices could stress DNS in three main ways with: i) the increased size and complexity of DDoS attacks powered by IoT botnets, ii)

¹⁹⁰ ICANN Security and Stability Advisory Committee (SSAC). SAC 105 The DNS and the Internet of Things: Opportunities, Risks, and Challenges. 2019. Accessible at: <https://www.icann.org/en/system/files/files/sac-105-en.pdf>

¹⁹¹ Cristian Hesselman et al. The DNS in IoT: Opportunities, Risks, and Challenges. IEEE Internet Computing, 24(4):23–32, 2020.

improper redundant DNS query generation at the IoT scale, and iii) an increased number of open DNS resolvers resulting in possible DDoS amplification.^{192 193 194 195 196}

IoT botnets can launch large-scale DDoS attacks, which are one of the largest risks to many service providers on the Internet. For instance, the Mirai¹⁹⁷ botnet exploited weak or non-existent passwords to gain control of hundreds of thousands IoT devices to launch DDoS attacks on important Internet services. Three waves of Mirai attacks disrupted high-profile websites including Amazon, GitHub, Slack, Visa, and HBO. The Mirai example shows that other commodity devices may follow a similar path.

In a similar way, most routers and switches operate continuously, they are always connected to the Internet, and use firmware with hardcoded default user names and passwords. Moreover, the Universal Plug-in-Play (UPnP) protocol used by many devices automatically open ports for data transfer. Such security vulnerabilities provide easy access for taking control, installing malware, and launching a DDoS attack.¹⁹⁸

As IoT expands, the number of botnets may grow to millions of devices and become a platform for increasingly large-scale DDoS attacks.¹⁹⁹ Recent IoT botnets used 400–600K infected devices (Mirai²⁰⁰, Hajime²⁰¹). The attacks can achieve high impact with exploitation of around 3 million open DNS resolvers that enable amplification of DDoS attacks by factors between 29 and 64.

Another aspect is the increased complexity of DDoS attacks and the difficulty to mitigate them. As the behaviour of IoT botnets becomes highly dynamic with important churn (the change in the number of new compromised devices and leaving the botnet),²⁰² it is increasingly difficult to filter out DDoS traffic based on IP addresses²⁰³. Furthermore, the propagation rate of botnets constantly increases. For example, the Hajime botnet started to

¹⁹² ICANN Security and Stability Advisory Committee (SSAC). SAC 105 The DNS and the Internet of Things: Opportunities, Risks, and Challenges. 2019. Accessible at: <https://www.icann.org/en/system/files/files/sac-105-en.pdf>

¹⁹³ Cristian Hesselman et al. The DNS in IoT: Opportunities, Risks, and Challenges. IEEE Internet Computing, 24(4):23–32, 2020.

¹⁹⁴ Manos Antonakakis et al. Understanding the Mirai Botnet. In 26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16–18, 2017, pages 1093–1110. USENIX Association, 2017.

¹⁹⁵ Open Resolver Scanning Project. [Online]. Available at: <https://dnsscan.shadowserver.org/>

¹⁹⁶ C. Hesselman, “Collaboratively increasing the resilience of critical services in the Netherlands through a national DDoS clearing house,” [Online]. Available at: https://www.sidnlabs.nl/downloads/BMU5MdebRqa7511wfxTakg/7621baeadf89ddc791802c58087066d1/Collaborative_DDoS_Mitigation.pdf

¹⁹⁷ Manos Antonakakis et al. Understanding the Mirai Botnet. In 26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16–18, 2017, pages 1093–1110. USENIX Association, 2017.

¹⁹⁸ Gregory Falco et al. NeuroMesh: IoT Security Enabled by a Blockchain Powered Botnet Vaccine. In Proceedings of the International Conference on Omni-Layer Intelligent Systems, COINS 2019, Crete, Greece, May 5–7, 2019, pages 1–6. ACM, 2019.

¹⁹⁹ Cristian Hesselman et al. The DNS in IoT: Opportunities, Risks, and Challenges. IEEE Internet Computing, 24(4):23–32, 2020.

²⁰⁰ Manos Antonakakis et al. Understanding the Mirai Botnet. In 26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16–18, 2017, pages 1093–1110. USENIX Association, 2017.

²⁰¹ Stephen Herwig et al. Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet. In 26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24–27, 2019. The Internet Society, 2019.

²⁰² Stephen Herwig et al. Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet. In 26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24–27, 2019. The Internet Society, 2019.

²⁰³ Cristian Hesselman et al. The DNS in IoT: Opportunities, Risks, and Challenges. IEEE Internet Computing, 24(4):23–32, 2020.

exploit and infect gigabyte passive optical network routers, which significantly increased the size of the botnet.²⁰⁴

One possibility for the protection from possible DDoS attacks from IoT devices is through a Manufacturer Usage Description (MUD)²⁰⁵ —an IETF standard for describing the expected network behaviour of the device in terms of what domain names and protocols it will use. Security systems in edge networks can whitelist the regular behaviour based on MUD and block all other traffic such as outbound DDoS.

IoT devices could also stress DNS with improper redundant DNS query generation at the IoT scale.²⁰⁶ An example was the generation of a large number of DNS queries by a music application for checking network connectivity, which filled up the DNS resolver cache and started to look like a DDoS attack.

Data and meta-data generated by IoT devices can reveal personal information on individuals. A combination of data from different IoT sources might create new knowledge on individuals that might not be revealed by separately examining the underlying data sets. As all DNS traffic is currently sent in clear (unencrypted) form, privacy becomes an important issue touching all Internet users.²⁰⁷ Recent DNS extensions allow IoT devices to authenticate resolvers and encrypt DNS traffic: DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT) encrypt DNS messages between a DNS client and its resolver, thus hiding DNS queries and responses from an eventual intruder. At the same time, it creates the problem of possible profiling of users by an open resolver: it knows the IP source address of the device and the DNS query, so it may track or create user profiles. Oblivious DNS²⁰⁸ decouples the knowledge of the client source IP address and the DNS query, but its scalability is limited by the use of the single authoritative name server for the specific .odns domain. The Cloudflare onion service also proposed solution to the problem. However, it requires TOR configuration of the client, which is not suitable for IoT devices.

DNS may become a means for overcoming many security issues related to IoT. A recent NIST Report recommends to address cybersecurity and privacy risks for IoT devices with three high-level mitigation goals: i) protect device security (prevent a device from conducting attacks), ii) protect data security (guarantee confidentiality, integrity, and/or availability of data), and iii) protect privacy (prevent disclosure of personally identifiable information). Advanced DNS functionalities such as DNSSEC and DANE (DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA) can be used in a framework for trust, security, accountability, and privacy.²⁰⁹ The main idea is to replace the trust and security schemes based on the conventional PKI with a novel approach that relies on the DNS infrastructure and builds all the required functionalities upon DNS. DNS brings the advantage of a single trust anchor with lightweight authentication schemes suitable for constrained IoT devices and easily automated for large-scale IoT deployments.

The EU IoT Expert Group on the Internet of Things (IoT-EG) identified the requirements for a suitable IoT identification, addressing, and naming scheme: it should be transparent and

²⁰⁴ Stephen Herwig et al. Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet. In 26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019. The Internet Society, 2019.

²⁰⁵ Ayyoob Hamza, Hassan Habibi Gharakheili, and Vijay Sivaraman. Combining MUD Policies with SDN for IoT Intrusion Detection. In Proceedings of the 2018 Workshop on IoT Security and Privacy, pages 1–7, NY, USA, 2018. ACM.

²⁰⁶ Cristian Hesselman et al. The DNS in IoT: Opportunities, Risks, and Challenges. IEEE Internet Computing, 24(4):23–32, 2020.

²⁰⁷ S. Bortzmeyer. DNS Privacy Considerations. RFC 7626, 2015.

²⁰⁸ Paul Schmitt, Anne Edmundson, Allison Mankin, and Nick Feamster. Oblivious DNS: Practical Privacy for DNS Queries. Proceedings on Privacy Enhancing Technologies, 2019(2):228–244, 2019.

²⁰⁹ NIST. Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. NISTIR 8228.

network independent, scalable to a large number of devices, efficient for constrained devices, preserving privacy, allowing for flexible authentication and interoperability. It can be noted that a naming scheme based on DNS and adapted to constrained IoT devices corresponds to the requirements.

Current IoT devices that require strong security rely on the conventional PKI, which means storing trust anchors similar to what most Internet browsers provide with the root certificates trusted by default. The conventional PKI does not fit constrained IoT devices: the required computing power, storage for the chain of trust, bandwidth for sending and receiving certificates, encrypted data using large block ciphers and signatures, as well as obtaining revocation lists, is technically and economically infeasible for this class of devices. The DNS infrastructure brings many desirable features: scalability, resilience, a single trust anchor, and capacity to evolve.

Another aspect related to IoT is the management of digital identities that needs to be lightweight and automated. Several initiatives proposed to build a digital identity framework on top of an immutable permissioned blockchain.²¹⁰ However, such a solution raises several issues: i) credentials such as certificates are becoming increasingly short lived, (e.g., Let's Encrypt certificates have the lifetime of three months) so they need to be renewed frequently, ii) managing multiple different identities for various usage and services means frequent updates of credentials-add new ones, renew old ones, which requires revocation of the information stored in a blockchain, iii) right to forget-all information related to ephemeral identifiers needs to disappear when no longer used, which is impossible with a ledger, and iv) storing public information in a blockchain requires trust in the blockchain verification entities, which may hinder its adoption.

It can be observed that DNS has all required characteristics to become a public directory of identities for IoT devices:

- DNS is a highly distributed, large-scale system offering high availability via redundancy;
- It is fast and efficient thanks to delegation;
- There are multiple providers that offer registering services;
- DNSSEC guarantees integrity of the information obtained from DNS;
- It is mutable thanks to dynamic updates, so no revocation is needed;
- Already provides support for storing keys, their fingerprints, and certificates (DANE).

DNS as a directory for IoT identities brings the advantage of a single trust anchor with operation easily automated for large-scale deployments and guarantee privacy by user-controlled minimal disclosure of sensitive data.

IoT devices represent a real game-changer because of the scale and the difficulty of improving their security due to the tension between costs and security objectives. Another important aspect is the difficulty of updating software or applications when vulnerabilities are detected so most of the IoT and commodity devices run the factory installed software that is never changed. The required security measures include the detection of

²¹⁰ Mariusz Kamola. Internet of Things with Lightweight Identities Implemented Using DNS DANE - Architecture Proposal. Sensors, 18(8):2517, 2018.

compromised devices and prevention of botnet proliferation as well as protection against DDoS attacks spawned from IoT devices.

b. 5G

5G aims at providing very high data rates and larger coverage through dense base station deployment with increased capacity, significantly better Quality of Service (QoS), and extremely low latency.²¹¹ Its main characteristic is the adoption of the concepts of Cloud Computing in the 5G eco-systems and extensive use of Software Defined Networking (SDN) and Network Function Virtualization (NFV). The core network will become “IP native” and will extensively use the Internet-type of Cloud and Edge computing resources. It will also interconnect IoT devices with massive Machine-Type Communications (MTC) over mobile broadband.

The 5G system architecture includes two main parts: the Radio Access Network (RAN) and the Core Network (CN). RAN is composed of next generation base stations gNB connecting UE mobiles with the Core Network. gNB manages user communications and supports network slices, logical instances providing different quality of service. To lower latency, Multi-access Edge Computing (MEC) brings cloud-computing capabilities and an IT service environment closer to the edge of the network.

5G adopted a Service Based Architecture (SBA) enabling disaggregation and virtualization of self-contained functions, communicating in a micro-services environment with all elements working together to deliver services and applications. NFV allows the separation of the hardware from the network software so that specific functions and services do not require dedicated hardware, which significantly reduce costs. In SBA, all Network Functions (NF) are interconnected via a logical bus, i.e., every NF can communicate with every other NF. Network functions can only use service-based interfaces for their interactions based on either a request-response or a subscribe-notify over HTTP/2 transferring elements in JavaScript Object Notation (JSON). HTTP/2 uses URIs (Universal Resource Identifier) containing DNS names, which implies name resolution.

When the User Equipment (UE) mobile registers in the network, several network functions are involved: the Access and Mobility Management Function (AMF) holds the session establishment request and chooses AUSF (Authentication Server Function) to authenticate the mobile to the core. The selection of the AUSF function relies on the Network Repository Function (NRF) that allows every NF to discover the services offered by other NFs. NRF acts as a service directory and uses DNS for lookups. Each NF function registers, provides an URI and an IPv4, or an IPv6 address, and a port as a contact point. To process mobile registration, AUSF uses EAP (Extensible Authentication Protocol) for authentication, chooses SMF (Session Management Function), which in turn selects PCF (Policy Control Function) and UCF (User Plane Function), and allocates an IP address. PCF provides policy rules for control plane functions including slicing, roaming, and mobility management. UCF performs all the user plane functions – it identifies the user plane traffic flow based on information received from SMF over the Packet Forwarding Control Protocol (PFCP). PFCP sessions define how packets are identified, forwarded, processed, marked, and reported. Finally, AMF reserves resources with help of the NSSF (Network Slice Selection Function) assisting in the selection of logical network instances for a defined network slice.

²¹¹ M. Agiwal, A. Roy, and N. Saxena, “Next Generation 5G Wireless Networks: A Comprehensive Survey,” IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 1617–1655, 2016.

These characteristics mean that 5G inherit the vulnerabilities of 4G LTE networks (e.g., attacks that impair the confidentiality and privacy of LTE communication^{212 213 214}) and will be subject to new threats related to the use of Internet protocols.²¹⁵ In particular, it can be observed that the SBA architecture of the 5G Core is based on HTTP/2, the common protocol widely used on the Internet with many known vulnerabilities. The positive aspect of this design is that vulnerabilities will be rapidly identified and fixed by the developer community, however, the drawback is that attackers are also familiar with HTTP/2. In theory, operators should use HTTP/2 over TLS but its use is not mandatory and in practice, 5G core networks do HTTP/2 without authentication and encryption (mainly for debugging reasons). The use of TLS needs to leverage a common PKI for identity and require the full lifecycle management of the identity certificates.

Communication between NFs and the NRF service discovery heavily depend on DNS for domain name to IP address resolution. Moreover, one of the key evolutions in 5G internal requirements relates to finding resources using DNS. It enables complex network topologies and scale-out principles for all the internal components of the network. This support is enabled by a strict implementation of required features using S-NAPTR, SRV and A/AAAA DNS records as stated in the 3GPP normalization and also in the Internet standard like IETF RFC 3958 (Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)). Intercepting or poisoning DNS entries may lead to a lot of security issues. Changing legitimate DNS requests to return malicious IP addresses can allow the attacker to perform MITM attacks, steal credentials, or deploy remote malware.

Although the 5G core can be considered and operated as a private network, some functions are exposed to external access via Network Exposure Function (NEF) that provides a direct access to 5G Core functions for third party applications. NEF may become a security threat, if an exchanged message is spoofed or tampered with. It may become an entrance point to the private network of an operator.

The important role of the Internet protocols and the critical role of DNS in NFV virtualization calls for strengthened resiliency and high availability of the DNS service infrastructure. It needs to be scalable to accommodate for traffic variation and it should never fail to provide a good resolution service whenever the underlying network is still functioning. DNS security must therefore be inherent in the architecture of a DNS platform. To protect end users, DNS servers need to support integrity of any answer with DNSSEC, which will be critical for IoT devices (to avoid Distributed Denial of Service (DDoS) attacks), for connected vehicles (to avoid hijacking), and for healthcare devices (to avoid confidential data breaches). DNS servers can also avoid eavesdropping, data traffic between the connected device and its first resolver will need to use DoT (DNS over TLS) or DoH (DNS over HTTPS).

The DNS service infrastructure also should be protected against a DDoS attack with scaling mechanisms and selective dropping/throttling of traffic surges. As a primary DDoS mechanism is the reflection or amplification attack on DNS servers, the internal operator networks should be protected against outbound and inbound spoofing. The inclusion of IoT devices in 5G networks will make this type of attacks much more critical and potentially easier to perform. A huge number of infected IoT devices can overload the signalling plane (e.g., DDoS flood from IoT devices over N3 interface between RAN and UPF) as an attempt to gain access or perform a DoS attack. Similar problems may arise in Internet facing

²¹² David Rupprecht, Katharina Kohls, Thorsten Holz, Christina Pöpper: Breaking LTE on Layer Two. IEEE Symposium on Security and Privacy 2019: 1121-1136.

²¹³ David Rupprecht, Katharina Kohls, Thorsten Holz, Christina Pöpper: IMP4GT: IMPersonation Attacks in 4G NeTworks. NDSS 2020.

²¹⁴ David Rupprecht, Katharina Kohls, Thorsten Holz, Christina Pöpper: Call Me Maybe: Eavesdropping Encrypted LTE Calls with ReVoLTE. USENIX Security Symposium 2020: 73-88.

²¹⁵ Positive Technologies, "5G Security", 2019.

functions (e.g., N6 interface connecting UPF to an external data network) and possible attack scenarios on the N4 interface between user and control plane that may result in denial of service or redirection of data.

Unlike 4G, 5G introduces Packet Data Convergence Protocol (PDCP) protection policies enabling user plane integrity protection. However, they may not be supported by all 5G user mobiles thus opening an attack vector for active manipulation of the ciphertext. Such an attack in 4G exploited this vulnerability by deploying a malicious MitM (Man in the Middle) relay between the use mobile and the base station to manipulate the (encrypted) payload of user data transmissions and perform a DNS redirection attack.²¹⁶

The Multi-access Edge Computing (MEC) part of 5G networks introduces some security issues. For the MEC interfaces, transport security should provide confidentiality, integrity, and replay protection to prevent any attacker from eavesdropping, information manipulation, or replay. In particular, if the access to EES (Edge Enabler Server) is not authenticated and authorized, attackers may request service from EES to obtain unauthorized information or launch a DDoS attack. With respect to DNS, an enhanced DNS forwarder referred to as LDNSR enables EAS (Edge Application Server) discovery using DNS and the knowledge of the UE connectivity. The lack of the DNS message protection may allow attackers to eavesdrop or manipulate DNS messages to redirect to a compromised Edge server. A possible mitigation is to reuse SBI based security for message protection between Session Management Function and LDNSR to ensure confidentiality, integrity, and replay protection. To enable DNS security, DoT or DoH can be used for secure discovery of edge services.

Roaming between different networks involves interaction of several 5G networks. Interconnection signalling has long been a source of security and fraud risks for network operators. 5G defines a Security Edge Protection Proxy (SEPP) that enables secure interconnection between 5G networks. SEPP ensures end-to-end confidentiality and/or integrity between source and destination network for all 5G interconnect roaming messages. It provides: i) a separate security negotiation interface and an end-to-end encrypted application interface, ii) encapsulation of HTTP/2 core signalling messages using the JOSE protection, iii) trusted intermediary IPX (IP eXchange) nodes can read and possibly modify specific information in the HTTP message, while completely protecting all sensitive information end-to-end. SEPP adds end-to-end application level security to improve security in interconnection scenarios between networks and makes it impossible to read, alter, or manipulate message content without prior agreement with the traversing operator. The traversing operators control what JSON information elements are readable or non-readable (encrypted) and which elements can be manipulated in the intermediate IPX crossings. This control is provided using JSON Web Encryption (JWE), JSON Web Security (JWS) and the ability to specify which information elements can be modified by IPXs. A network operator agrees with its IPX providers and every roaming partner which Information Elements can be changed by the IPX provider. When the IPX Provider makes a change, it signs off that change with a certificate, and the receiving operator can verify who made the change and whether it was allowed.

The roaming architecture includes a visited network and home network version of SEPP: cSEPP and pSEPP (designated with prefixes c - consumer, p - producer). It involves both the SEPP entities and up to two IPX providers. If both SEPP proxies are directly connected, security is assured by TLS and in the case of intermediate IPX crossings, SEPP performs application layer security with PRINS (PRotocol for N32 Interconnect Security) on all HTTP messages before they are sent externally over the roaming interface.

²¹⁶ David Rupprecht, Katharina Kohls, Thorsten Holz, Christina Pöpper: Call Me Maybe: Eavesdropping Encrypted LTE Calls with ReVoLTE. USENIX Security Symposium 2020: 73-88.

Roaming involves the current SMF for which a SEPP are looked for based a DNS resolution of a domain like 3gppnetwork.org. For topology hiding, SEPP supports TLS wildcard certificate for its domain name. SEPP rewrites the domain name from the received HTTP/2 message with a telescopic domain name (i.e., a name with a single label as the first element and the SEPP domain as the trailer component) and forwards the modified HTTP/2 message to the target NF inside the visited network. The name rewriting may imply the use of DNS services. For the HTTP/2 message protection, SEPP reformats the HTTP/2 message to produce the input to JSON Web Encryption (JWE), applies JWE to protect the reformatted message, and encapsulates the resulting JWE object into a HTTP/2 message (as the body of the message). The N32-interface is fairly complex and many options makes it hard to say exactly what kind of security is actually achieved. The roaming interface of SEPP is highly exposed and may be subject to external attacks.

The SEPP shall implement anti-spoofing mechanisms that enable cross-layer validation of source and destination address and identifiers (e.g., domain names or networks IDs). For instance: if there is a mismatch between different layers of the message or the destination address does not belong to the SEPP own network, the message is discarded.

Following on the Commission's Recommendation on the cybersecurity of 5G networks²¹⁷, ENISA developed the Threat Landscape for 5G networks that provides a detailed technical view on the 5G architecture, sensitive assets, cyberthreats affecting the assets and threat agents.²¹⁸ In relation to DNS abuse, it points out the possibility of *"Manipulation of network configuration data: Inadequate policies in the management and protection of critical configuration data may lead to unpredictable system behaviour and unauthorised access to critical platforms, with impact on the confidentiality and integrity of the network. This threat involves compromising a core network element (e.g. SDN controller, network function, management and orchestration function) by forging configuration data to launch other attacks (e.g., DoS). While configuration data forging may, in principle, relate to data held by any component of the network, this threat refers specifically to configuration and/or control plane data."* Examples of configuration data manipulation are routing tables manipulation, falsification of configuration data, and DNS manipulation.

The report also brings attention to the danger of malicious flooding of the core network components, which may come in the flavour of distributed DoS attacks with a large number of sources that may be orchestrated to generate the message floods. These sources could, for example, be the members of a botnet, a collection of devices infected with malware to the point that they can all be controlled by an attacker to execute the attack. One approach to mitigate threats is Customer Edge Switching (CES) that serves as an extension of the classical firewall functionality able to communicate with other security devices to establish whether network traffic should be considered as benign or malicious.²¹⁹ CES may benefit from DNSCrypt and DNSSEC for encrypting and authenticating DNS packets thus improving the overall CES security.

Another recent ENISA report gives a large picture of the standardisation environment pertaining to 5G security to improve understanding of 3GPP security specifications and its main elements and security controls.²²⁰ It points out that *"lack of integrity and reply protection of signalling data traffic between UE (User Equipment) and the gNB (Base Station) or AMF (Access and Mobility Management Function) could lead to compromise and alteration of data and may facilitate various MitM attacks. Moreover, possibility to also have*

²¹⁷ Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks C/2019/2335 - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0534>

²¹⁸ ENISA, "Threat Landscape For 5G Networks", November 2019.

²¹⁹ Slawomir Nowaczewski, Wojciech Mazurczyk: Securing Future Internet and 5G using Customer Edge Switching using DNSCrypt and DNSSEC. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl. 11(3): 87-106 (2020).

²²⁰ ENISA, "Security In 5G Specifications", February 2021.

user plane integrity protection, as a new feature added to 5G specification, is important to prevent malicious alteration of user data. Such alteration, as researches have shown²²¹, may have a major impact, such as redirecting of DNS request from UE to a malicious server.” As some interfaces rely on TLS (Transport Layer Security), the report observes the need for correct support of client and server certificates, the problem also related to the management of domain names.

One of the recommendations of the report is *“Network design, configuration and deployment shall follow security best practices. This may include having defined processes for activation of security features, for secure provisioning, for establishment of PKI infrastructure and certificate management, for hardening of the virtualization and/or cloud environment and for secure admin infrastructures and would typically also include ensuring adequate network segmentation and protection of internal interfaces from external access.”* This aspect is also related to the resilient DNS infrastructure.

Finally, all issues raised by IoT devices will also become aggravated with future 5G MTC. As IoT connectivity will increasingly rely on 5G, millions of connected IoT devices offer an increased opportunity for botnets, which refers to the same types of problems as discussed above. In 2017, a Mirai attack took down nearly 1 million Deutsche Telekom DSL routers and caused mass disruption of communications in Europe. In 2018, Positive Technologies experts found vulnerabilities in ZTE CPE terminals allowing to remotely execute arbitrary code. At that time, on the Shodan search engine one could find over a million devices vulnerable to including in a new botnet potentially even larger than Mirai.

The advent of IoT with a large number of constrained devices with embedded intelligence contributes to the increase of security risks related to the DNS abuse that include compromising the end-device hardware, cloning or substitution of devices, tampering with the software in the end-device, compromising the communication in IoT networks like eavesdropping, and Man-in-the-Middle (MitM) attacks. Poorly secured IoT devices and services can become entry points for cyberattacks, compromising sensitive data, weaponization, and threatening the safety of individual users. Many attacks against IoT showed that commodity devices are easily hacked and installed botnets can launch large-scale DDoS attacks, Mirai being one of the recent significant attacks that disrupted high-profile websites and DNS services. High churn of compromised devices makes increasingly difficult to filter out DDoS traffic based on IP addresses. The existence of open DNS resolvers and other amplification servers also contributes to the large scale of DDoS attacks.

With respect to 5G networks, the important change is the adoption of the Service Based Architecture with Network Functions interconnected via a logical bus and the exposure of some functions to direct access by 3rd party applications. As the Service Based Architecture is based on HTTP/2 commonly used in the Internet, the 5G core will be subject to the existent and new threats related to the use of such Internet protocols. Moreover, communication between Network Functions and service discovery will heavily depend on DNS for domain name to IP address resolution, which requires strengthened resiliency and high availability of the DNS service infrastructure handled by operators.

The fact that the future mobile networks will use Internet protocols in cloud environments is an important change of the paradigm with respect to the previous variants when mobile networks were closed and internally managed by operators. All issues raised by IoT devices will also become aggravated with future 5G Machine Type Communications oriented towards IoT devices. As IoT connectivity will increasingly rely on 5G, millions of connected

²²¹ David Rupprecht, Katharina Kohls, Thorsten Holz, Christina Pöpper: Breaking LTE on Layer Two. IEEE Symposium on Security and Privacy 2019: 1121-1136.

IoT devices offer an increased opportunity for botnets that may attack either some victims on the Internet or servers in the 5G core.

The DNS service infrastructure of 5G should be protected against DDoS attacks as well as against outbound and inbound spoofing. Strengthening DNS protection and other measures against its abuse will also contribute to enhanced security of future mobile networks.

9. Regulatory framework of DNS abuse

a. Introduction

At the outset, the DNS is not governed by any international treaty, nor are the ccTLDs that are specific for each EU Member State subject to harmonisation at the EU level. However, international, EU and national laws have significant impact on DNS operators.

As mentioned in the above, Internet is a globally distributed network comprising many interconnected autonomous networks. It operates without a central governing body with each constituent network setting and enforcing its own policies. Its governance is conducted by a decentralised and international multistakeholder network of entities drawing from civil society, the private sector, the academic and research communities, governments and international organizations. They work cooperatively to create shared policies and technical standards to maintain the Internet's global interoperability for a public good.²²²

To ensure interoperability, ICANN, a non-profit public benefit corporation set up in 1998 under California law, manages and oversees some of the critical underpinnings of the Internet, such as the DNS and IP addressing (IANA function). In order to perform the IANA function (to assign and register IPs and parameters), ICANN needs to follow the criteria and procedures of the documents drawn up and specified by IETF (Request for Comments – RFCs, Proposed and Internet Standards, etc.). The initial general framework of the DNS system structure and delegation was documented in RFC 1591. Since May 1999, ICANN follows ICP-1: Internet DNS Structure and Delegation.

ICANN makes its policy decisions using a multistakeholder model of governance, in which a “bottom-up” collaborative process is open to all constituencies of the Internet stakeholders.²²³

ICANN is not an international organisation set up under public international law. It is international in the sense that its Articles of Incorporation and Bylaws mandate cooperation with individuals and organisations in numerous countries, as well as governments (through the Governmental Advisory Committee - GAC, where the EU is also represented).

A network of formal and informal arrangements with various public law actors has been gradually built over the years. Furthermore, as part of its DNS managing duties, ICANN contracts with gTLD registries (Registry Agreement – RA) and accredits registrars (Registry-Registrar Agreement – RRA) with whom the registries deal. Together they are often referred to as the ICANN-contracted parties. These contracts constitute the lower levels of the DNS administrative hierarchy. Domain name registries are in charge of maintaining and coordinating the database of all domain names registered within a TLD. Registrars offer domain name registration services to the general public (registrants) and collect customers' information and payment in order to make a unique domain name entry into the registry. The registrar service is, thus, governed by contract. A standard template contract between ICANN and the registrars sets out some basic requirements and policies (Registrar Accreditation Agreement – RAA), and within that framework, each registrar has its own terms of service that bind their registrants. This is basically true for the governance of the gTLD namespace.

As mentioned above, the management of ccTLD namespace varies with some countries having formal contractual arrangements with ICANN (e.g., sponsorship agreements with .au, .jp, .ke), while others having only informal arrangements with ICANN (exchange of

²²² https://en.m.wikipedia.org/wiki/Internet_governance

²²³ <https://www.everycrsreport.com/reports/R42351.html>

letters with .no, .uk, .at, .br). Some countries and territories have also statutory regulation of their ccTLD (e.g., .no, .eu). Indeed, according to the principle of subsidiarity expressed in the Principles and guidelines for the delegation and administration of country code top level domains adopted by the GAC, “ccTLD policy should be set locally, unless it can be shown that the issue has global impact and needs to be resolved in an international framework. Most of the ccTLD policy issues are local in nature and should therefore be addressed by the local Internet Community, according to national law”.²²⁴ Registrations under ccTLDs are managed similarly to those of gTLDs, that is, through agreements between the ccTLD registry and registrars, the latter assisting registrants in the registration of domain names. However, in the case of ccTLDs, there is no system of ICANN accreditation of registrars. It is usually the respective ccTLD registry that accredits its registrars.

Thus, there are several regulatory types in regulating the Internet and in particular the DNS, including:

1. Private law regulation
2. Public law regulation
3. Private-public arrangements
4. Self-regulation
5. Technical code or *lex informatica*.

Private law regulation is predominant in the gTLD namespace where a complex web of contracts is used between ICANN, registries, and registrars. Contracts and more informal private law instruments are also used, although in a lesser degree, in the regulation of the ccTLD namespace between registries and registrars where private-public arrangements are frequent (governments setting up private entities to govern their namespace). Public law plays a significant weight when it comes to the role of national governments in the governance of the DNS. Computer code is used as the technical backbone of cyberspace (*lex informatica*). The technical rules underlying the technical structure and function of the Internet include technical standards, good practices, and other self-regulatory instruments (soft law).

In the EU, operators of digital infrastructure (internet exchange points, domain name system service providers, top level domain name registries) are considered essential entities regulated by hard law at national and EU level (Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union – NIS Directive).²²⁵ These operators have to take appropriate cybersecurity measures and to notify serious incidents to the relevant national authority. Due to the inconsistent transposition of the NIS Directive in Member States’ laws, further harmonisation has become necessary. The proposed legislation (NIS 2 Directive)²²⁶, which will be analysed below, requires to include all providers of DNS services along the DNS resolution chain, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolver, imposing further obligations on such providers. Further EU law (both horizontal and vertical rules, and soft-law), analysed below, also refers to and have impact on DNS service providers and their activities.

b. Domain registration information (WHOIS data)

²²⁴ Article 1.2 GAC Principles and guidelines for the delegation and administration of country code top level domains - https://gac.icann.org/principles-and-guidelines/public/principles-cctlds.pdf?language_id=1

²²⁵ <https://eur-lex.europa.eu/eli/dir/2016/1148/oj>

²²⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN>

Prior to proceeding with the overview and assessment of the regulatory framework, the authors of the study hereby point out the importance of the domain registration information (WHOIS data) and its accessibility and accuracy, since it is strictly connected to the issue of DNS abuse.

For all domain name registrations, registrants must provide information about themselves and about contacts associated with their domain name, including name, email address, postal address and phone number as part of the domain name registration process. Thus, the domain name registration data enables to identify who registered and controls a domain name. This information has long been available in a public lookup system called WHOIS. The WHOIS is not a single, centrally-operated database. Instead, domain registration data is managed by registrars and registries.

For more than 20 years, ICANN has administered the collection and availability of WHOIS data for gTLDs. Based upon existing consensus policies and contracts (RRA Section 1(e) of the Whois Accuracy Program Specification²²⁷), ICANN has stated that it is committed to implementing measures to maintain timely access to accurate registration (WHOIS) data for generic top-level domain names (gTLDs), subject to applicable laws.

Until May 2018, publicly accessible WHOIS data was used for a variety of purposes by both public and private sector organisations, including law enforcement authorities, cybersecurity investigators, network technology professionals, child protection organisations, patient safety organisations, consumer welfare organisations, and anti-counterfeiting and anti-piracy organisations. Government agencies and private sector organisations routinely used WHOIS data as the first step in their work of investigating websites engaged in potential illegal or abusive activity. Consumers concerned about the legitimacy of a website could easily (and routinely did) consult WHOIS data via a WHOIS portal hosted by the registry or registrar, or a centralised look-up operated by ICANN to find out who had registered the domain name of the website and determine whether that information matched or supported what the website was purporting to be.

On 17 May 2018, the ICANN Board adopted the **Temporary Specification for generic top-level domain (gTLD) Registration Data (Temporary Specification)**²²⁸ intended to comply with EU's **General Data Protection Regulation (GDPR)**, adopted in May 2018. The Temporary Specification provides modifications to existing requirements in the Registrar Accreditation (RRA) and Registry Agreements (RA) allowing registrars and gTLD registry operators to redact (withhold) personally identifiable data (and also those of legal persons) from publication in WHOIS.

Further to the entry into force of the Temporary Specification, registries and registrars have consistently refused reasonable access to the redacted WHOIS data to third parties on request, such as law enforcement authorities or anti-counterfeiting organisation, and ICANN has stated that it is unwilling to enforce the Temporary Specification to require access in any case where a registry or registrar has refused it.

On 19 July 2018, the GNSO Council initiated an **Expedited Policy Development Process (EPDP)** and chartered the EPDP on the Temporary Specification team. During phase 1 of its work, the EPDP team was tasked to determine if the Temporary Specification should become an ICANN consensus policy as is, or with modifications.²²⁹ The Final Report of phase 2, covering among others the establishment of a system for standardized

²²⁷ <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy>

²²⁸ <https://www.icann.org/resources/pages/gtld-registration-data-specs-en/#temp-spec>

²²⁹ <https://www.icann.org/resources/pages/interim-registration-data-policy-en>

access/disclosure to nonpublic registration data (SSAD), was published on 31 July 2020.²³⁰ However, minority statements (Annex F of the Final Report) found that the report recommendations did not appropriately balance the rights of those providing data to registries and registrars with the public interest to prevent harms associated with malicious activities that leverage the DNS. Moreover, SSAD leaves WHOIS data disclosure decisions almost entirely to the subjective judgment of domain registries and registrars. Furthermore, the policy recommendations set service level guidelines allowing several days for registrars and registries to respond to requests for disclosure of WHOIS data. Yet for investigations of cybersecurity threats and other criminal activity, including child sexual abuse, responses are needed in minutes or hours, not days or weeks.

With reference to questions left open by the EPDP phase 2, the governments represented in GAC noted that *“failing to provide recommendations aimed at ensuring the accuracy of gTLD registration data, including for the purpose for which it is processed in an SSAD, in light of the systemic inaccuracies highlighted by the RDS-WHOIS2 Review, risks fundamentally undermining the compliance of the system with data protection law”*.²³¹

Indeed, in September 2019, the final report of ICANN's Registration Directory Service (RDS)-WHOIS2 Review Team²³² found that ICANN Contractual Compliance had not monitored and enforced the registrars' obligation regarding data accuracy (neither in front of the inaccuracy complaints received) and recommended, among others, that *“The ICANN Board should initiate action to ensure ICANN Contractual Compliance is directed to proactively monitor and enforce registrar obligations with regard to RDS (WHOIS) data accuracy using data from incoming inaccuracy complaints and RDS accuracy studies or reviews to look for and address systemic issues. A risk-based approach should be executed to assess and understand inaccuracy issues and then take the appropriate actions to mitigate them”*.

In 2019, **Interisle's** study on Criminal Abuse of Domain Names Bulk Registration and Contact Information Access²³³ highlighted that cybercriminals took advantage of bulk registration services, using a large number of domain names to launch their attacks and poited out the detrimental effect of ICANN's interim policy (Temporary Specification) redacting WHOIS point of contact information to comply with the EU GDPR on cybercrime investigations. A further study on Domain Name Registration Data at the Crossroads: The State of Data Protection, Compliance, and Contactability at ICANN (2020)²³⁴ found widespread problems, most notably:

- Registrars fail to meet their contractual obligations. A significant portion of the registrar industry is still not running reliable and compliant WHOIS services.
- After one-and-a-half years, a significant percentage of registrars do not fully comply with ICANN's Temporary Specification.
- A number of registrars mis-handle their obligations under GDPR.
- Some registrars prevent people from reaching out to domain owners for any purpose. Some registrars do not make the required contactability information available as required. Others have deployed procedures that make it unnecessarily

²³⁰ <https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf>

²³¹ <https://gac.icann.org/contentMigrated/next-steps-on-key-policy-issues-not-addressed-in-epdp-phase-2>

²³² <https://www.icann.org/en/system/files/files/rds-whois2-review-03sep19-en.pdf>

²³³ <http://interisle.net/sub/CriminalDomainAbuse.pdf>

²³⁴ <http://interisle.net/sub/DomainRegistrationData.pdf>

difficult for people to contact their registrants. In some cases, the contactability mechanisms provided by registrars literally fail to deliver.

- Some registrars even constrain access to non-sensitive domain registration data (the “public data set”). This set contains no personally identifiable information, so there is no need to protect it, and restricting access to it prevents its use for important and legal purposes, such as cybersecurity.
- Registration Data Access Protocol (RDAP)²³⁵ services are not yet technically reliable enough for use. RDAP became mandatory for registrars and registry operators to provide in August 2019, but as of March 2020 the rollout is moving very slowly, and there are notable operational and noncompliance problems.

Finally, the report on WHOIS Contact Data Availability and Registrant Classification Study²³⁶, released on in January 2021, finds that ICANN's GDPR-driven policy has resulted in the redaction of contact data for 57% of all generic Top-level Domain (gTLD) names. ICANN's policy has allowed registrars and registry operators to hide much more contact data than is required by the GDPR—perhaps five times as much. Including ‘proxy-protected’ domains, for which the identity of the domain owner is deliberately concealed, 86.5% of registrants can no longer be identified via WHOIS—up from 24% before the ICANN policy went into effect. The implications of this ICANN policy change are profound: consumers can no longer use WHOIS to confirm the identities of parties they may want to transact with on the Internet, it is harder for law enforcement personnel and security professionals to identify criminals and cybercrime victims, and brand owners face greater challenges defending misuse of their intellectual property.

In June 2021, the **Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG)** and the **Anti-Phishing Working Group (APWG)** also published a report²³⁷ on the results of a follow up survey of cyber investigators and anti-abuse service providers to determine the ongoing impacts of ICANN's implementation of the EU GDPR and the Temporary Specification, adopted in May 2018. From the analysis of over 270 survey responses, M3AAWG and APWG have found that respondents report that changes to WHOIS access following to the adoption of the Temporary Specification, continue to significantly impede cyber applications and forensic investigations and thus cause harm or loss to victims of phishing, malware or other cyber attacks. Specifically, the survey responses indicate that the Temporary Specification has reduced the utility of public WHOIS data due to wide-ranging redactions, beyond what is legally required. It also introduces considerable delays, as investigators have to request access to redacted data on a case-by-case basis; often with unactionable results. Furthermore, with limited or no access to the data that had previously been obtained or derived from WHOIS data, some investigators struggle to identify perpetrators and put an end to criminal campaigns. The resulting delays and roadblocks are a boon to attackers and criminals, prolonging their windows of opportunity to cause harm during cybercrime activities such as phishing and ransomware distribution, or the dissemination of fake news and subversive political influence campaigns. M3AAWG and APWG have observed that there are four issues that ICANN needs to address:

1. Access to some relevant data like contact data of legal persons needs to be readily available while protecting natural persons' privacy.
2. Both sporadic WHOIS users who make relatively few requests, as well as bulk users who use data-driven approaches for blocklisting should be accommodated by ICANN.

²³⁵ <https://www.icann.org/rdap>

²³⁶ <http://interisle.net/ContactStudy2021.pdf>

²³⁷ https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

3. ICANN should establish a functional system of registrant data access for accredited parties; such a system needs to be workable for cybersecurity professionals and law enforcement in terms of time delays and administrative burden, and should include strict privacy and security controls.

4. The survey responses indicate that the solutions currently discussed at ICANN would not meet the needs of law enforcement and cybersecurity actors in terms of timelines.

The respondents of the **questionnaire conducted by the authors of the present study** also noted that the inability to quickly access full registration data has hampered brand owners' ability to enforce on their trade mark and other IPR, and has added time and cost to such enforcement efforts. Requests for data disclosures have proven ineffective under current rules – there is no incentive for registrars or registry operators to voluntarily disclose registrant contact data even in response to well-founded disclosure requests based on legitimate purposes including IPR enforcement, anti-phishing and anti-fraud enforcement efforts, and cybersquatting investigations. The inability to perform “reverse WHOIS” searching based on a public registrant email address necessitates more one-off enforcement actions and prevents brand owners from identifying networks of infringing or abusive domains associated with the same registrant for more comprehensive mitigation measures. ICANN's proposed System for Standardized Access/Disclosure (SSAD) may bring some efficiency to the disclosure request process, but still affords discretion to contracted parties to make disclosure decisions, which they will still have no incentive to make; regardless, any SSAD will likely not be available for years to come, and the status quo will remain in the meantime. This has had impacts also on the costs and pendency times for Uniform Rapid Suspension (URS) and Uniform Domain Name Dispute resolution Policy (UDRP) proceedings, given the need now in almost all cases to prepare an initial and subsequent amended complaint following disclosure to the dispute resolution provider and subsequently the complainant. With ICANN and its contracted parties demonstrating an unwillingness to take meaningful steps to facilitate reasonable publication and disclosure of domain registration data, and facilitate cross-domain correlation based on registrant email address or other consistently-published registrant data elements, enforcement has become more challenging since 2018. Furthermore, ICANN itself no longer has the ability under current rules to receive and verify that appropriate data accuracy verification is being performed by registrars; with no ability of third parties to independently check registrant data accuracy, there is no guarantee of actionable registrant data even in the event of disclosure (whether voluntary or through mandatory means like in the context of dispute resolution proceedings). It is clear that further regulatory guidance is needed to address these matters, which themselves were precipitated in part due to changes in the regulatory landscape (primarily due to the GDPR).

Regarding the privacy and proxy registration services that prevent registrant information from being published, until the adoption of the 2013 Registrar Accreditation Agreement (RAA), there were few ICANN rules or policies applicable to these services. The 2013 RAA includes an Interim Specification that describes a minimum set of requirements for privacy and proxy services offered by a registrar or its affiliates. These requirements were adopted on a temporary basis (expiring on 31 January 2021). The GNSO Council unanimously supported an accreditation policy for privacy and proxy service providers prescribing requirements on responses to law enforcement and intellectual property holders.²³⁸ While the policy was approved by the ICANN Board in August 2016, it has not been implemented yet. GAC's Public Safety Working Group has found during the COVID-19 pandemic that the majority of domains involved in pandemic-related fraud, phishing, or malware have employed privacy/proxy services to hide the identity of the registrant.²³⁹ .us is one of the few

²³⁸ https://gnso.icann.org/sites/default/files/filefield_48305/ppsai-final-07dec15-en.pdf

²³⁹ <https://gac.icann.org/presentations/icann68-session-8-dns-abuse-slides.pdf>

ccTLDs that prohibits the use of privacy / proxy registration to maintain a complete and accurate WHOIS database for .us registrants.²⁴⁰

As for ccTLDs, at least as regards the European ones, complying with the GDPR was a smoother process than for the gTLDs. Some ccTLD registries also adopt regular WHOIS accuracy checks to guarantee accurate data in their databases and, thus, reduce malicious and abusive registrations (analyzed in detail under Section 10.b).

c. Overview of the regulatory framework

The following table summarizes the regulatory framework concerning DNS abuse at international, EU and ICANN level as well as within other fora:

Level	Category	Instrument	Provisions and direct obligations on TLD registries, registrars and other DNS service providers
International	Hard law - public law regulation - multilateral treaty (to be adopted in Nov 2021)	Second Additional Protocol to the Convention on Cybercrime enhanced cooperation and disclosure of electronic evidence (2021)	Article 6: direct cooperation mechanism between law enforcement authorities of a requesting country with service providers and entities providing domain name registration services in other countries for the disclosure of information to identify suspects of cybercrime.
EU	Hard law - public law regulation - legislative (proposal)	Proposal for Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for Directive on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (2018)	Cooperation obligations of the providers of internet domain name and numbering services (domain name registrars and registries and privacy and proxy service providers, or regional internet registries for internet protocol addresses) with the law enforcement and judicial authorities to provide the electronic evidence (data) needed for investigation and potential prosecution of criminals and terrorists.
	Hard law - public law regulation - legislative	Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC (2021)	Temporary derogation from e-Privacy Directive for service providers to process personal and other data to combat CSAM.
	Hard law - public law regulation - legislative	Directive (EU) 2016/1148 on security of network and information systems (NIS Directive)	DNS service providers are operators of essential services and shall take appropriate cybersecurity measures and notify serious incidents to the relevant national authority.

²⁴⁰ <https://www.about.us/policies/us-privacy-services-policy>

	Hard law - public law regulation - legislative (proposal)	Proposal for a Directive on measures for a high common level of cybersecurity (Proposal for NIS 2) (2020)	All providers of DNS services along the DNS resolution chain, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers are to be considered essential entities. Essential entities shall fulfill with cybersecurity risk management and reporting obligations as well as with obligations on cybersecurity information sharing. Article 23: TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data, publish without undue delay after the registration of a domain name, domain registration data which are not personal data, provide access to domain name registration data upon lawful and duly justified requests of legitimate access seekers, and reply without undue delay to all requests for access.
	Hard law - public law regulation - legislative (proposal)	Proposal for Directive on Critical Entities Resilience (CER Directive) (2020)	Providers of the digital infrastructure sector (critical entities) shall protect physical assets, networks, and grids from getting tampered with.
	Hard law - public law regulation - legislative (proposal)	Regulation (EU) 2017/2394 on cooperation between national authorities responsible for the enforcement of consumer protection laws	Article 9, paragraph 4, letter g): the competent authorities shall have the powers to order hosting providers to remove, disable or restrict access to an online interface, or order domain registries or registrars to delete a domain name and to allow the competent authority concerned to register it.
	Hard law - public law regulation - legislative (proposal)	Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Proposal for DSA) (2020)	Providers of services establishing and facilitating the underlying logical architecture and proper functioning of the internet, including technical auxiliary functions, can benefit from the exemptions from liability (Articles 3-5), to the extent that their services qualify as “mere conduit”, “caching” or “hosting”. All providers shall fulfill with due diligence obligations: points of contact (Article 10), legal representative (Article 11), terms and conditions (Article 12), transparency reporting obligations on content moderation (Article 13). Hosting providers shall also put in place notice and action mechanisms (Article 14) and provide statement of reasons of the removal or disabling access to the content (Article 15). Online platforms shall also establish internal complaint-handling system (Article 17), Know Your Business Customer (KYBC) procedures (Article 22), and collaborate with trusted notifiers (trusted flaggers) (Article 18).
ICANN	Hard law - private law regulation - contractual	Registry Agreement (RA) (2013)	Specification 11 (Public Commitments) Section 3 (a): (new)gTLD registries shall include a provision in the Registry-Registrar

			<p>Agreement that requires registrars to include in their Registration Agreements a provision prohibiting registrants from distributing malware, abusively operating botnets, phishing, piracy, trade mark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to any applicable law.</p> <p>Specification 11 (Public Commitments) Section 3 (b): (new)gTLD registries shall periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets, maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks, provide these to ICANN upon request.</p>
	Hard law - private law regulation - contractual	Registrar Accreditation Agreement (RAA)	<p>Section 3.18.1: registrars shall maintain an abuse contact to receive reports of abuse (including reports of illegal activity), shall publish an email address to receive such reports on the home page of registrar's website, take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse.</p> <p>Section 3.18.2: registrars shall establish and maintain a dedicated abuse point of contact, including a dedicated email address and telephone number that is monitored 24 hours a day, seven days a week, to receive reports of illegal activity by law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the registrar is established or maintains a physical office. Well-founded reports of illegal activity submitted to these contacts must be reviewed within 24 hours by an individual who is empowered by the registrar to take necessary and appropriate actions in response to the report.</p> <p>Section 3.18.3: registrars shall publish on its website a description of its procedures for the receipt, handling, and tracking of abuse reports, shall document receipt of and response to all such reports, maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and provide such records to ICANN upon reasonable notice.</p> <p>Section 3.7.8: registrars shall comply with the obligations specified in the Whois Accuracy Program Specification, abide by any consensus policy requiring reasonable and commercially practicable (a) verification, at the time of registration, of contact information associated with a domain name or (b) periodic re-verification of such information. Registrars shall, upon notification by any person of an inaccuracy in the contact information associated with a domain name, take reasonable steps to investigate that claimed inaccuracy. In the event Registrars learn of inaccurate contact</p>

			information associated with a domain name, take reasonable steps to correct that inaccuracy.
Other	n/a	Internet & Jurisdiction Policy Network's Domains & Jurisdiction Program	Operational, Approaches, Norms, Criteria, Mechanisms (2019): Thresholds in determining when taking action at the DNS level; Identifying the components to be contained in a "good" complaint notice; Encouraging registries and registrars to develop metrics for collecting and reporting (in exportable and accessible formats) coherent statistics pertaining to abuse notifications and implemented actions; Encouraging registries and registrars to make available to the public the criteria determining when action at the DNS level is appropriate, the types of abusive content they are willing to take action on, their abuse point(s) of contact, their internal criteria for decision-making and the channels for appeals/recourse; Encouraging the setting up of an easy to use abuse reporting interface. Toolkit on DNS Level Action to Address Abuses for registries and registrars (2021).
	Self-regulation voluntary	– DNS Abuse Framework (2019)	Defining DNS abuse as technical (security abuse) and identifying other forms of abuse falling outside this DNS abuse definition, but that a registry or registrar should nonetheless take steps to address.

In the following subsections we analyze in details the regulatory framework mentioned above, providing also an assessment of such framework.

d. International level

The Council of Europe's **Budapest Convention on Cybercrime (Budapest Convention)**²⁴¹ (European Treaty Series No. 185) was adopted by the Committee of Ministers of the Council of Europe on 8 November 2001 and opened for signature in Budapest on 23 November 2001. By 30 June 2021, 66 countries, members of the Council of Europe, had become parties and further 11 countries had signed it or been invited to accede to the Convention.

The Convention aims principally at harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime; providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form; setting up a fast and effective regime of international co-operation.

The following offences are defined by the Convention as cybercrime: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights. The provisions of the Budapest Convention are applicable to botnets, phishing, DDoS attacks, malware and spam, as clarified by the Guidance Notes²⁴².

²⁴¹ https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=WJqX0M1y

²⁴² <https://www.coe.int/en/web/cybercrime/guidance-notes>

The Budapest Convention also sets out the following procedural powers: expedited preservation of stored data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of computer data; real-time collection of traffic data; interception of content data.

Finally, it also contains provisions concerning traditional and computer crime-related mutual assistance as well as extradition rules.

The Budapest Convention is supplemented by a **Protocol on Xenophobia and Racism committed through computer systems** (European Treaty Series No. 189).²⁴³ The Protocol was opened for signature in Strasbourg on 28 January 2003 by the States which have signed the Convention on Cybercrime. It entered into force on 1 March 2006 and, up to date, it has been ratified or accessed to by 33 countries. The Protocol entails an extension of the Cybercrime Convention's scope, including its substantive, procedural and international cooperation provisions, so as to cover also offences of racist or xenophobic propaganda. Thus, apart from harmonising the substantive law elements of such behaviour, the Protocol aims at improving the ability of the State Parties to make use of the means and avenues of international cooperation set out in the Convention on Cybercrime in this area.

The State Parties to the Budapest Convention searched for further solutions for some time, that is, from 2012 to 2014, through a working group on transborder access²⁴⁴ to data and from 2015 to 2017 through the Cloud Evidence Group²⁴⁵. In 2014, they also adopted a set of Recommendations²⁴⁶ to enhance the effectiveness of mutual assistance, and in 2017 a Guidance Note²⁴⁷ on Article 18 Budapest Convention on production orders with respect to subscriber information. This note explains how domestic production orders for subscriber information can be issued to a domestic provider irrespective of data location (Article 18.1.a) and to providers offering a service on the territory of a Party (Article 18.1.b).

The preparation of an additional protocol to the Budapest Convention was initiated in 2017. The finalised text of the **Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence** provides for:

- Direct cooperation with service providers and entities providing domain name registration services in other countries for the disclosure of information to identify suspects of cybercrime (Article 6);
- Expedited forms of cooperation between countries for the disclosure of subscriber information and traffic data;
- Expedited cooperation and disclosure in emergency situations;
- Additional tools for mutual assistance;
- Data protection and other rule of law safeguards.²⁴⁸

In particular, **Article 6** of the Second Additional Protocol to the Convention on Cybercrime provides for a mechanism for law enforcement in a requesting country to obtain domain name registration information directly from an entity in another country – without going through the mutual legal assistance process. In response to a valid request, the entity providing domain name registration services is expected to provide the relevant information in the entity's possession or control. The term "domain name registration information" is intended to provide information for "identifying and contacting the registrant of a domain name", i.e. name, physical address, email address and telephone number of a registrant.

²⁴³ Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) - <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f>

²⁴⁴ <https://www.coe.int/en/web/cybercrime/tb>

²⁴⁵ <https://www.coe.int/en/web/cybercrime/ceg>

²⁴⁶ <https://rm.coe.int/16802e726c>

²⁴⁷ <https://rm.coe.int/16806f943e>

²⁴⁸ <https://rm.coe.int/2nd-additional-protocol-budapest-convention-en/1680a2219c>

- “1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, for purposes of specific criminal investigations or proceedings, to issue a request to an entity providing domain name services in the territory of another Party for information in the entity’s possession or control, for identifying or contacting the registrant of a domain name.*
- 2. Each Party shall adopt such legislative and other measures as may be necessary to permit an entity in its territory to disclose such information in response to a request under paragraph 1, subject to reasonable conditions provided by domestic law.*
- 3. The request under paragraph 1 shall include:*
- a. the date issued and the identity and contact details of the competent authority issuing the request;*
 - b. the domain name about which information is sought and a detailed list of the information sought, including the particular data elements;*
 - c. a statement that the request is issued pursuant to this Protocol, that the need for the information arises because of its relevance to a specific criminal investigation or proceeding and that the information will only be used for that specific criminal investigation or proceeding; and*
 - d. the time and the manner in which to disclose the information and any other special procedural instructions.*
- 4. If acceptable to the entity, a Party may submit a request under paragraph 1 in electronic form. Appropriate levels of security and authentication may be required.*
- 5. In the event of non-cooperation by an entity described in paragraph 1, a requesting Party may request that the entity give a reason why it is not disclosing the information sought. The requesting Party may seek consultation with the Party in which the entity is located, with a view to determining available measures to obtain the information.*
- 6. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance or approval, or at any other time, communicate to the Secretary General of the Council of Europe the authority designated for the purpose of consultation under paragraph 5.*
- 7. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities designated by the Parties under paragraph 6. Each Party shall ensure that the details that it has provided for the register are correct at all times.”*

The Second Additional Protocol to the Convention on Cybercrime is expected to be finalized and adopted in the course of 2021.

e. EU level

There exist a variety of and multi-layered legal instruments relevant to DNS service providers. We review below some of these legal instruments.

Cybercrime

EU laws on cybercrime correspond to and build on different provisions of the Council of Europe Convention on Cybercrime (Budapest Convention):

1. **Directive 2013/40/EU on attacks against information systems**²⁴⁹ harmonises criminal law of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities, including the police and other specialised law enforcement services of the Member States, as well as the competent specialised Union agencies and bodies, such as

²⁴⁹ <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040>

Eurojust, Europol and its European Cyber Crime Centre, and the European Network and Information Security Agency (ENISA).

2. **Proposals for Regulation²⁵⁰ and Directive²⁵¹ facilitating cross-border access to electronic evidence for criminal investigation** (2018). The new rules make it easier and faster for law enforcement and judicial authorities to obtain the electronic evidence needed for investigation and potential prosecution of criminals and terrorists. They also ensure that all providers that offer services in the EU are subject to the same obligations in providing evidence. The following types of service providers fall under the scope of the Regulation: providers of electronic communications services, providers of information society services for which the storage of data is a defining component of the service provided to the user, including social networks to the extent they do not qualify as electronic communications services, online marketplaces facilitating transactions between their users (such as consumers or businesses) and **other hosting service providers**, and **providers of internet domain name and numbering services**. Indeed, the Regulation considers that **data held by providers of internet infrastructure services, such as domain name registrars and registries and privacy and proxy service providers, or regional internet registries for internet protocol addresses, may be of relevance for criminal proceedings as they can provide traces allowing for identification of an individual or entity involved in criminal activity**. The new rules also foresee the creation of a European Production Order and Preservation Order.
3. **Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment²⁵²** updates the legal framework, removing obstacles to operational cooperation and enhancing prevention and victims' assistance, to make law enforcement action against fraud and counterfeiting of non-cash means of payment more effective.
4. **Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC** (e-Privacy Directive) as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting online child sexual abuse.²⁵³

Cybersecurity initiatives

The EU has a range of instruments to protect electronic communications networks relevant for the purpose of this study.

Under the **Directive (EU) 2016/1148 on security of network and information systems (NIS Directive)²⁵⁴**, currently in force, considered the importance of the DNS, **DNS service providers are included in the list of entities for which operators of essential services** should be identified by the Member States. These providers have to take appropriate cybersecurity measures and to notify serious incidents to the relevant national authority. The security measures include: preventing risks (technical and organisational measures that are appropriate and proportionate to the risk); ensuring security of network and information systems (the measures should ensure a level of security of network and information systems appropriate to the risks); handling incidents: the measures should prevent and minimize the impact of incidents on the IT systems used to provide the services.

²⁵⁰ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:225:FIN>

²⁵¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:226:FIN>

²⁵² https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.123.01.0018.01.ENG

²⁵³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1232>

²⁵⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148>

However, the NIS Directive has been transposed by the Member States inconsistently. Some Member States have identified operators of essential services within the DNS while others have not. Indeed, thresholds chosen by Member States in the Digital Infrastructure sector do not only vary quantitatively (for example, in Germany DNS providers are identified as OES if they manage at least 250 000 domains, while Poland has set a threshold of only 100 000 domains) but also qualitatively (for example “number of connected autonomous systems” vs. “market share”).²⁵⁵

To overcome several weaknesses that prevented the NIS Directive from unlocking its full potential, on 15 December 2020, the European Commission adopted the **Proposal for a Directive on the measures for a high common level of cybersecurity (Proposal for NIS 2 Directive)**²⁵⁶, repealing Directive (EU) 2016/1148.

The Proposal for NIS2 Directive is part of a package of measures aimed to improve further the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole in the field of cybersecurity and critical infrastructure protection. Its scope, therefore, is to modernise the existing legal framework taking into account the increased digitisation of the internal market in recent years and an evolving cybersecurity threat landscape, both amplified since the onset of the COVID-19 crisis.

The proposal lays down:

- Obligations on Member States to adopt a national cybersecurity strategy, designate competent national authorities, single points of contact and computer security incident response teams (CSIRTs) (Articles 5-16);
- Cybersecurity risk management and reporting obligations for entities referred to as essential entities in Annex I and important entities in Annex II (Articles 17-25);
- Obligations on cybersecurity information sharing (Articles 26-34).

Annex I of the Proposal for NIS2 Directive enlists the following providers of the digital infrastructure as **essential entities**:

- Internet Exchange Point providers
- DNS service providers
- TLD name registries
- Cloud computing service providers
- Data centre service providers
- Content delivery network providers
- Trust service providers referred to in point (19) of Article 3 of Regulation (EU) No 910/2014
- Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972 or providers of electronic communications services referred to in point (4) of Article 2 of Directive (EU) 2018/1972 where their services are publicly available.

With reference to providers of DNS services, the proposal states that “[u]pholding and preserving a reliable, resilient, and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, **this Directive should apply to all providers of DNS services along the DNS resolution chain, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers**” (Recital 15). DNS service providers, thus, would be automatically under the scope of NIS2 Directive

²⁵⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0546>

²⁵⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN>

without the need for EU Member States to identify operators of essential services within the DNS.

All essential entities should fall under the jurisdiction of the Member State where they provide their services. If the entity provides services in more than one Member State, it should fall under the separate and concurrent jurisdiction of each of these Member States. To take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, content delivery network providers, cloud computing service providers, data centre service providers and digital providers, only one Member State should have jurisdiction over these entities. Jurisdiction should be attributed to the Member State in which the respective entity has its main establishment in the EU. DNS service providers not established in the EU but offering services within the EU, shall designate a representative established in one of the Member States and shall be deemed to be under the jurisdiction of the Member State where the representative is established (**Article 24**). ENISA shall create and maintain a registry for essential (and important) entities.

The Proposal for NIS2 Directive requires Member States to provide that management bodies of all entities under the scope to approve the cybersecurity risk management measures taken by the respective entities and to follow specific cybersecurity-related training. Member States are required to ensure that entities under the scope take appropriate and proportionate technical and organisational measures to manage the cybersecurity risks posed to the security of network and information systems. They are also required to ensure that entities notify the national competent authorities or the CSIRTs of any cybersecurity incident having a significant impact on the provision of the service they provide.

Moreover, maintaining accurate and complete databases of domain names and registration data (WHOIS data) and providing lawful access to such data is essential to ensure the security, stability, and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the EU (Recital 59). This reflects the Cybersecurity Strategy which reiterated that the access to WHOIS data serves public interest since it is important for criminal investigations, cybersecurity and consumer protection.²⁵⁷

Article 23 (Databases of domain names and registration data) of the **Proposal for NIS2 Directive** requires that:

- “1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data.*
- 2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain relevant information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs.*
- 3. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD have policies and procedures in place to ensure that the databases include accurate and complete information. Member States shall ensure that such policies and procedures are made publicly available.*
- 4. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD publish, without undue delay after the registration of a domain name, domain registration data which are not personal data.*
- 5. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance*

²⁵⁷ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605&from=EN>

with Union data protection law. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD reply without undue delay to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.”

In addition, the European Commission’s **Proposal for Critical Entities Resilience (CER)²⁵⁸ Directive**, adopted on 16 December 2020, intends to cover, among others, the providers of the digital infrastructure sector as critical entities to address their physical resilience too, imposing rules to protect physical assets, networks, and grids from getting tampered with.

Consumer protection

The Regulation (EU) 2017/2394 on cooperation between national authorities responsible for the enforcement of consumer protection laws²⁵⁹ lays down the conditions under which competent authorities, having been designated by their Member States as responsible for the enforcement of Union laws that protect consumers’ interests, cooperate and coordinate actions with each other and with the Commission, to enforce compliance with those laws and to ensure the smooth functioning of the internal market, and in order to enhance the protection of consumers’ economic interests.

Under Article 9 (Minimum powers of competent authorities), paragraph 4, letter g), the competent authorities shall have at least the following enforcement powers where no other effective means are available to bring about the cessation or the prohibition of the infringement covered by the Regulation and in order to avoid the risk of serious harm to the collective interests of consumers:

- i. the power to remove content or to restrict access to an online interface or to order the explicit display of a warning to consumers when they access an online interface;
- ii. the power to order a hosting service provider to remove, disable or restrict access to an online interface; or
- iii. where appropriate, the power to order domain registries or registrars to delete a fully qualified domain name and to allow the competent authority concerned to register it;

including by requesting a third party or other public authority to implement such measures.

Illegal content online

Currently, the **Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce (E-Commerce Directive)²⁶⁰** of 2000 contains the baseline regime applicable to all service providers providing information society services and to all types of online content. Information society services refer to those services which are “provided for remuneration at a distance, via electronic means, through devices of data elaboration and memorization and at the individual request of a recipient of services”.²⁶¹

The E-Commerce Directive provides the following rules: (i) the country of origin principle, which is the cornerstone of the Digital Single Market; (ii) an exemption of liability regime for “mere conduit”, “caching” and “hosting” (Articles 12-14); (iii) the prohibition of general

²⁵⁸ [https://ec.europa.eu/home-](https://ec.europa.eu/home-affairs/sites/default/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf)

[affairs/sites/default/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf](https://ec.europa.eu/home-affairs/sites/default/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf)

²⁵⁹ <https://eur-lex.europa.eu/eli/reg/2017/2394/oj>

²⁶⁰ <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031>

²⁶¹ Article (1)(1)(b) of Directive (EU) 2015/1535 - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L1535&qid=1610388032306>

automatic and passive nature. Interpersonal communication services, such as emails or private messaging services as well as services providing cloud infrastructures do, in principle, not fall under the Regulation.

4. **Content infringing Intellectual Property Rights (IPR)** – including **Directive 2001/29/EC on the harmonisation of certain aspects of copyrights and related rights in the information society**²⁶⁹, **Directive 2004/48 on enforcement of IPR (IPRED)**²⁷⁰, and **Directive (EU) 2019/790 on Copyright in the Digital Single Market**²⁷¹. The Copyright Directive (EU) 2019/790 establishes a new liability regime for online content-sharing platforms; they must conclude an agreement with the rights-holders for the exploitation of the works and, if they fail to do so, they are liable for the content violating copyright on their platforms unless they make their best effort to alleviate such violations. The IPRED concerns the measures, procedures and remedies necessary to ensure the enforcement of IPR within the Internal Market.

EU hard law, in particular the baseline E-Commerce Directive, is complemented by soft law, such as the Communication on Tackling Illegal Content Online²⁷² (2017) and the Commission Recommendation 2018/334 on measures to effectively tackle illegal content online²⁷³, and self-regulatory initiatives, such the EU Internet Forum²⁷⁴ (2015) with reference to terrorist content, the Alliance to Better Protect Minors Online²⁷⁵ (2017) with reference to CSAM, the Code of Conduct on illegal hate speech online²⁷⁶ (2016) and the Memorandum of Understanding on counterfeit goods online²⁷⁷ (2011, rev. 2016). The self-regulatory initiatives contain commitments, practices and other provisions supporting such practices, but the evaluation of such initiatives shows difficulties in measuring the commitments taken and in reporting their effectiveness.

DNS service providers have not directly been addressed neither within the intermediaries' liability regime of the E-Commerce Directive²⁷⁸, nor by the additional vertical rules, and only limited case law have addressed their role in this context.^{279 280}

To overcome such legal uncertainty, the European Commission's **Proposal for a Regulation on a Single Market for Digital Services (Proposal for DSA)**²⁸¹, amending partially the E-Commerce Directive, clarifies that providers of services establishing and facilitating the underlying logical architecture and proper functioning of the internet, including technical auxiliary functions, can also benefit from the exemptions from liability set

²⁶⁹ <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32001L0029>

²⁷⁰ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32004L0048>

²⁷¹ <https://eur-lex.europa.eu/eli/dir/2019/790/oj>

²⁷² <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0555>

²⁷³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018H0334>

²⁷⁴ https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6243

²⁷⁵ <https://digital-strategy.ec.europa.eu/en/policies/protect-minors-online>

²⁷⁶ https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-counteracting-illegal-hate-speech-online_en

²⁷⁷ https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en

²⁷⁸ Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("E-Commerce Directive") - <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031>

²⁷⁹ Schwemer S.F., (2020). The regulation of abusive activity and content: a study of registries' terms of service - <https://policyreview.info/articles/analysis/regulation-abusive-activity-content-study-registries-terms-service>

²⁸⁰ Schwemer, S., Mahler, T. & Styri, H. (2020). Legal analysis of the intermediary service providers of non-hosting nature - <https://op.europa.eu/en/publication-detail/-/publication/3931eed8-3e88-11eb-b27b-01aa75ed71a1/language-en/format-PDF/source-179885922>

²⁸¹ <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN>

out in the Proposal for DSA (Articles 3-5), to the extent that their services qualify as “*mere conduit*”, “*caching*” or “*hosting*”.

- Mere conduit service consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network.
- Caching service consists of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request.
- Hosting service consists of the storage of information provided by, and at the request of, a recipient of the service. Within the broader category of providers of hosting services, the DSA distinguishes the subcategory of online platforms.

Such services include, as the case may be, wireless local area networks, DNS services, TLD registries, certificate authorities that issue digital certificates, or content delivery networks, that enable or improve the functions of other providers of intermediary services.²⁸²

The Proposal for DSA, adopted on 15 December 2020, would apply to intermediary services provided to recipients of the service that have their place of establishment or residence in the EU, irrespective of the place of establishment of the providers of those services. The general scope is to update the horizontal rules (E-Commerce Directive), focusing on issues such as liability of intermediaries for third party illegal content, safety of users online, and asymmetric due diligence obligations for different providers of information society services depending on the nature of the societal risks such services represent.

Illegal content is any information, which, in itself or by its reference to an activity, including the sale of products or provision of services is not in compliance with EU law or the law of a Member State, irrespective of the precise subject matter or nature of that law. For the purpose of the Proposal for DSA, the concept of illegal content should be defined broadly and also covers information relating to illegal content, products, services and activities. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that relates to activities that are illegal, such as the sharing of images depicting child sexual abuse, unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the non-authorised use of copyright protected material or activities involving infringements of consumer protection law. Harmful (yet not, or at least not necessarily, illegal) content is not defined in the Proposal for DSA and should not be subject to removal obligations, as this is a delicate area with several implications for the protection of freedom of expression.

For providers of DNS services, the Proposal for DSA could bring certainty (Recital 27) and proportionality when tackling illegal content online (Recital 26).

The due diligence obligations of **all providers of intermediary services**, thus are as follows:

- Points of contact: establishing a single point of contact allowing for direct communication by electronic means (Article 10);
- Legal representatives: designating a legal or natural person as legal representative in one of the Member States where the provider, not established in the EU offers its services (Article 11);

²⁸² Recital 27 of proposal for Digital Services Act - <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN>

- Terms and conditions: including information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions (Article 12);
- Transparency reporting obligations: shall publish, at least once a year, clear, easily comprehensible and detailed reports on any content moderation they engaged in during the relevant period (Article 13).

Hosting services shall also put in place notice and action mechanisms (Article 14) and provide statement of reasons of the removal or disabling access to the content (Article 15). **Online platforms** have additional obligations, among which establishing internal complaint-handling system (Article 17), Know Your Business Customer (KYBC) procedures (Article 22), collaboration with trusted notifiers (called trusted flaggers) (Article 18) etc.

A trusted notifier-system refers according to the European Commission to a mechanism, where a privileged notification channel is provided by an intermediary to specialised entities with specific expertise in identifying illegal content, and dedicated structures for detecting and identifying such content online.²⁸³ The Commission has, indeed, encouraged the close collaboration of intermediaries and trusted flaggers because, compared to ordinary users, trusted flaggers can be expected to bring their expertise and work with high quality standards, which should result in higher quality notices and faster takedowns. In the Commission's subsequent Recommendation on measures to effectively tackle illegal content online has reiterated such encouragement.²⁸⁴ Moreover, according to the Proposal for DSA, action against illegal content should be taken more quickly and reliably where intermediaries take the necessary measures to ensure that notices submitted by trusted flaggers through notice and action mechanisms are treated with priority, without prejudice to the requirement to process and decide upon all notices submitted under those mechanisms in a timely, diligent, and objective manner., the trusted flagger status should only be awarded to entities, and not individuals, that have demonstrated, among other things, that they have particular expertise and competence in tackling illegal content, that they represent collective interests, and that they work in a diligent and objective manner. Such entities can be public in nature, such as, for terrorist content, internet referral units of national law enforcement authorities or of the Europol or they can be non-governmental organisations and semi-public bodies, such as the organisations part of the INHOPE network of hotlines for reporting child sexual abuse material and organisations committed to notifying illegal racist and xenophobic expressions online. For intellectual property rights, organisations of industry and of right-holders could be awarded trusted flagger status, where they have demonstrated that they meet the applicable conditions.

While all providers of intermediary services are encouraged to carry out voluntary own-initiative investigations or other activities aimed at detecting, identifying and removing, or disabling of access to, illegal content, or take the necessary measures to comply with the requirements of EU law, there is no obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on the providers of intermediary services.

Several stakeholders interviewed for the purpose of this study advocated for stricter obligations to be imposed on the DNS service providers by the forthcoming DSA.

f. ICANN level

As mentioned above in the Section 6, malicious activities on the Internet are not a new phenomenon and DNS abuse existed also before ICANN was set up. While no express and consensus definition for DNS abuse has been developed, upon the call of law enforcement,

²⁸³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0555>

²⁸⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018H0334>

governments, security communities, commercial and user interest groups to prevent that malicious actors exploit the launch of the new gTLDs, ICANN adopted certain requirements in the **Memorandum on Mitigating Malicious Conduct**²⁸⁵ to address the following issues:

1. *How do we ensure that bad actors do not run registries?*
2. *How do we ensure integrity and utility of registry information?*
3. *How do we ensure more focused efforts on combating identified abuse?*
4. *How do we provide an enhanced control framework for TLDs with intrinsic potential for malicious conduct?*

Those requirements included:

1. **Vetting registry operators** through background checks to reduce the risk that a potential registry operator has been party to criminal, malicious, and/or bad faith behaviour;
2. **Requiring Domain Name System Security Extension (DNSSEC) deployment** on the part of all new registries to minimize the potential for spoofed DNS records;
3. **Prohibiting “wildcarding”** to prevent DNS redirection and synthesized DNS responses that may result in arrival at malicious sites;
4. **Encouraging removal of “orphan glue” records** to minimize use of these remnants of domains previously removed from registry records as “safe haven” name server entries in the TLD’s zone file that malicious actors can exploit;
5. **Requiring “Thick” WHOIS records** to encourage availability and completeness of WHOIS data²⁸⁶;
6. **Centralizing Zone File access** to create a more efficient means of obtaining updates on new domains as they are created within each TLD zone;
7. **Documenting registry and registrar level abuse contacts and policies** to provide a single point of contact to address abuse complaints;
8. **Providing an expedited registry security request process** to address security threats that require immediate action by the registry and an expedited response from ICANN;
9. **Creating a draft framework for a high security zone verification program** to establish a set of criteria to assure trust in TLDs with higher risk of targeting by malicious actors —e.g. banking and pharmaceutical TLDs— through enhanced operational and security controls.

²⁸⁵ <https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf>

²⁸⁶ A thin WHOIS only includes technical data sufficient to identify the sponsoring registrar, status of the registration, and creation and expiration dates for each registration. Thick WHOIS maintain the registrant’s contact information and designated administrative and technical contact information, in addition to the sponsoring registrar and registration status information supplied by a thin WHOIS – <https://whois.icann.org/en/what-are-thick-and-thin-entries>

Furthermore, the so-called public commitments were included in the contracts with new gTLD registries and registrars, imposing thus express obligations (and prohibitions) regarding malicious activities.

As for registries, the New gTLD **Registry Agreement (RA)** was approved by the ICANN Board on 2 July 2013, including **Specification 11 (Public Commitments) Section 3 (a)** which provides as follows:

*“Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision **prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing** (consistent with applicable law and any related procedures) **consequences for such activities including suspension of the domain name.**”*

The subsequent **Section 3 (b)** provides that:

*“Registry Operator will periodically conduct a technical analysis to **assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets.** Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.”*

In response to some questions raised by some registries, in June 2017, ICANN published an **Advisory, New gTLD Registry Agreement Specification 11 (3)(b)**, providing a voluntary approach to perform technical analyses to assess security threats and produce statistical reports.²⁸⁷

In October 2017, the **Framework for Registry Operator to Respond to Security Threats** was developed and published.²⁸⁸ It is a voluntary and non-binding document designed to articulate the ways registries may respond to identified security threats. It is not clear if and how many registries adopted such Framework.

On 27 March 2020, the contractual provisions (including Specification 11 (3)(a)-(b)) were included in the amended **.COM RA**, extending, therefore, their applicability to two-third of the gTLD namespace.

The gTLD Registries Stakeholder Group (RySG) elaborated the **Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets**²⁸⁹, and the document **Combatting DNS Abuse - Registry Operator Available Actions**²⁹⁰ (March 2021), recalling basically the 2017 Framework and the Internet and Jurisdiction Policy Network’s document **DNS Technical Abuse: Choice of Action**²⁹¹ (2020).

²⁸⁷ <https://www.icann.org/resources/pages/advisory-registry-agreement-spec-11-3b-2017-06-08-en>

²⁸⁸ <https://www.icann.org/resources/pages/framework-registry-operator-respond-security-threats-2017-10-20-en>

²⁸⁹ <https://www.rysg.info/wp-content/uploads/assets/Framework-on-Domain-Generating-Algorithms-DGAs-Associated-with-Malware-and-Botnets.pdf>

²⁹⁰ <https://www.rysg.info/wp-content/uploads/archive/DNS-Abuse-RY-Choice-of-Action-22-March-2021.pdf>

²⁹¹ <https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-20-114-Choice-of-Action.pdf>

With reference to registrars, **Section 3.18 of the Registrar Accreditation Agreement (RAA)** approved by the ICANN Board on 27 June 2013 provides that:

*“3.18.1 Registrar shall maintain an abuse contact to receive reports of **abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity**. Registrar shall publish an email address to receive such reports on the home page of Registrar's website (or in another standardized place that may be designated by ICANN from time to time). Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse.*

*3.18.2 Registrar shall establish and maintain a **dedicated abuse point of contact**, including a dedicated email address and telephone number that is monitored 24 hours a day, seven days a week, to receive reports of Illegal Activity by law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the Registrar is established or maintains a physical office. Well-founded reports of Illegal Activity submitted to these contacts **must be reviewed within 24 hours** by an individual who is empowered by Registrar to take necessary and appropriate actions in response to the report. In responding to any such reports, Registrar will not be required to take any action in contravention of applicable law.*

*3.18.3 Registrar shall publish on its website a **description of its procedures for the receipt, handling, and tracking of abuse reports**. Registrar shall document its receipt of and response to all such reports. Registrar shall maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and during such period, shall provide such records to ICANN upon reasonable notice.”*

Illegal activity is defined in Section 1.13: *“Illegal Activity means conduct involving use of a Registered Name sponsored by Registrar that is prohibited by applicable law and/or exploitation of Registrar's domain name resolution or registration services in furtherance of conduct involving the use of a Registered Name sponsored by Registrar that is prohibited by applicable law”.*

Moreover, with reference to registration data accuracy, **Section 3.7.8 of the RRA** provides that:

*“Registrar shall comply with the obligations specified in the Whois Accuracy Program Specification. In addition, notwithstanding anything in the Whois Accuracy Program Specification to the contrary, Registrar shall abide by any Consensus Policy requiring reasonable and commercially practicable (a) **verification, at the time of registration, of contact information associated with a Registered Name sponsored by Registrar** or (b) **periodic re-verification of such information**. Registrar shall, upon notification by any person of an inaccuracy in the contact information associated with a Registered Name sponsored by Registrar, take reasonable steps to investigate that claimed inaccuracy. In the event Registrar learns of inaccurate contact information associated with a Registered Name it sponsors, it shall take reasonable steps to correct that inaccuracy.”*

In March 2020, the Registrar Stakeholder Group (RrSG) published the **Guide to Registrar Abuse Reporting Practices**²⁹² on the abuse reporting requirements. It is unclear which registrars follow such guide. The Contracted Party House (RySG and RrSG) also published the **Minimum Required Information for Whois Data Requests**²⁹³. However, as third-party studies²⁹⁴ found, and as respondents to the second questionnaire of this study reported,

²⁹² <https://rrsg.org/wp-content/uploads/2020/03/Guide-to-Registrar-Abuse-Reporting-v1.8.pdf>

²⁹³ <https://rrsg.org/wp-content/uploads/2020/10/CPH-Minimum-Required-Information-for-a-Whois-Data-Requests.docx.pdf>

²⁹⁴ https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

there is inconsistent behavior among registrars after requesting registration data disclosure and the overwhelming majority of requests are not acknowledged, denied without explanation or answered with fake or otherwise non-actionable data.

Domain name resellers are not ICANN-contracted parties and hence not directly subject to ICANN's enforcement authority over standard contract requirements. Reseller is a person or entity that participates in the registrar's distribution channel for domain name registrations (a) pursuant to an agreement, arrangement, or understanding with registrar or (b) with Registrar's actual knowledge, provides some or all registrar services, including collecting registration data about registrants, submitting that data to registrar, or facilitating the entry of the registration agreement between the registrar and the registrant (Section 1.24 RRA). However, in accordance with **Section 3.12 of the RRA**: the *"Registrar is responsible for the provision of Registrar Services for all Registered Names that Registrar sponsors being performed in compliance with this Agreement, regardless of whether the Registrar Services are provided by Registrar or a third party, including a Reseller. Registrar must enter into written agreements with all of its Resellers that enable Registrar to comply with and perform all of its obligations under this Agreement"*.

The above-mentioned safeguards built in the New gTLD Program, the contractual obligations, in force since 2013 and extended to .com since 2020, have, however, been found by periodic reviews, mandated by ICANN Bylaws to assess whether the ICANN fulfills its mission, to be unachieved, ineffective, and/or unenforced.

Indeed, the **Competition, Consumer Trust and Consumer Choice (CCT) Review Team** commissioned the independent study on **Statistical Analysis of DNS Abuse in gTLDs (SADAG report)** to analyse rates of spam, phishing, and malware distribution in the global gTLD DNS, distinguishing between legacy and new gTLDs. The study provided measures and analysis of:

- Absolute counts of abusive domains per gTLD and registrar from 1 January 2014 until 31 December 2016;
- Abuse rates, based on an "abused domains per 10,000" ratio (as a normalization factor to account for different TLD sizes), per gTLD and registrar from 1 January 2014 until 31 December 2016;
- Abuse associated with privacy and proxy services;
- Geographic locations associated with abusive activities;
- Abuse levels distinguished by "maliciously registered" versus "compromised" domains;
- Effects of DNSSEC, domain parking, and registration restrictions on abuse levels

The SADAG report, published in August 2017, found that there were significant abuse issues in the DNS²⁹⁵:

- In certain new gTLDs, over 50% of the registrations were abusive
- Five new gTLD extensions accounted for 58.7% of all of the blacklisted domains involved in phishing.

²⁹⁵ <https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf>

- Domain names registered for malicious purposes often contained strings related to trademarked terms.

It also found correlation between domain name retail pricing and abuse rates. Consequently, in September 2018, the CCT Review Team's Final Report formulated 35 full consensus recommendations to ICANN.²⁹⁶

In particular, the report recommended the inclusion of provisions in the RA to incentivise the adoption of anti-abuse measures (Recommendation 14), to prevent systematic use of specific registrars of registries for DNS abuse, including thresholds of abuse at which compliance inquiries are automatically triggered and consider a possible DNS Abuse Dispute Resolution Policy (Recommendation 15), the improvement of research on DNS abuse (Recommendation 16), the improvement of WHOIS accuracy (Recommendation 18), and effectiveness of contractual compliance complaints handling.

In March 2019 ICANN Board accepted 6 of the 35 recommendations.²⁹⁷ 17 recommendations were placed in pending status. 14 recommendations were passed through to community groups for consideration. An implementation plan²⁹⁸ was adopted on 26 January 2020 of 6 recommendations accepted and a resolution²⁹⁹, including action³⁰⁰ on 11 of 17 recommendations placed in pending status. In November 2019 the GAC advised the ICANN Board not to proceed with a new round of gTLDs until the complete implementation of the recommendations of the CCT Review Team Final Report considered as prerequisites or as high priority.³⁰¹ The ICANN Board has neither accepted nor rejected the GAC advice. The GNSO Policy Development Process Working Group on New gTLD Subsequent Procedures in its Final Report determined "*not making any recommendations with respect to mitigating domain name abuse other than stating that any such future effort must apply to both existing and new gTLDs (and potentially ccTLDs)*".³⁰² Thus, the progress on the implementation of accepted recommendations and consideration of pending recommendations remains unclear and continues to be postponed.

Domain Abuse Activity Reporting (DAAR). The DAAR project began in 2017 is a "*system for studying and reporting on domain name registration and security threat (domain abuse) behavior across top-level domain (TLD) registries*".³⁰³ Its declared overarching purpose is "*to report security threat activity to the ICANN community, which can use the data to make informed decisions*".³⁰⁴ The system collects TLD zone data and complements these data sets with reputation (security threat) data feeds. In particular, the system has two major components:

- Collection system, which gathers zone files of every TLD for which ICANN is able to obtain data, compiles domain abuse data from independent security threat-reporting sources and associates security threat activity to individual TLDs.
- Graphical user interface (GUI) administration system, which provides tabular and graphical visualizations of domain registration and abuse activities, including the

²⁹⁶ <https://www.icann.org/en/system/files/files/cct-final-08sep18-en.pdf>

²⁹⁷ <https://www.icann.org/en/system/files/files/resolutions-final-cct-recs-scorecard-01mar19-en.pdf>

²⁹⁸ <https://www.icann.org/public-comments/cct-rt-implementation-plan-2019-09-11-en>

²⁹⁹ <https://www.icann.org/resources/board-material/resolutions-2020-10-22-en#2.a>

³⁰⁰ <https://www.icann.org/en/system/files/files/cct-pending-recs-board-action-22oct20-en.pdf>

³⁰¹ <https://gac.icann.org/contentMigrated/icann66-montreal-communicue>

³⁰² <https://gnso.icann.org/sites/default/files/file/field-file-attach/final-report-newgtld-subsequent-procedures-pdp-02feb21-en.pdf>

³⁰³ <https://www.icann.org/octo-ssr/daar>

³⁰⁴ <https://www.icann.org/octo-ssr/daar-faqs/#purpose>

display of historical data. The GUI allows ICANN to study security threat activities and to export data for report generation.

According to ICANN, the aggregated and anonymized data collected by the DAAR system can serve as a platform for studying or reporting daily or historical registration or abuse activity by each registry. The data collected out of the DAAR system is being used to generate the DAAR monthly reports which are published on ICANN's website since January 2018.³⁰⁵ The reports are point-in-time analysis of all TLDs for which data is available. The report provides aggregated statistics and time-series analysis about security threats of interest to DAAR, namely phishing, malware, botnet command-and-control and spam. The DAAR system collects security threat data from multiple reputation service providers.³⁰⁶

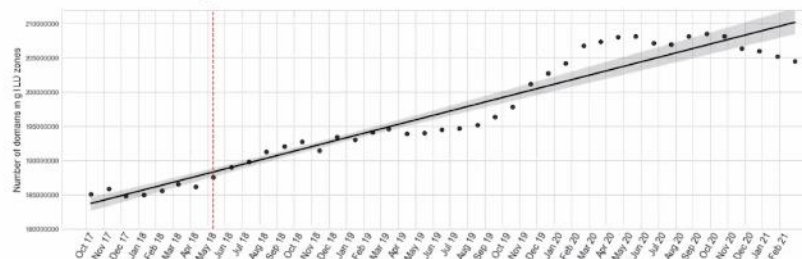
However, ICANN highlights that the reputation service providers do not list all threat activities happening on the Internet. Therefore, DAAR provides a baseline measurement and the amount of security threats associated with domain names is larger than what this system catalogues.

The following ccTLDs also voluntarily participated in DAAR³⁰⁷: .au, .se, .tw, .cl, .nu, .ee, .tz, .gt, .sv, .mw, .gg, .je, .ch, .ke, .in, .ca, .li.

In March 2021, ICANN showcased the following decreasing trends in security threats resulting from the DAAR project:

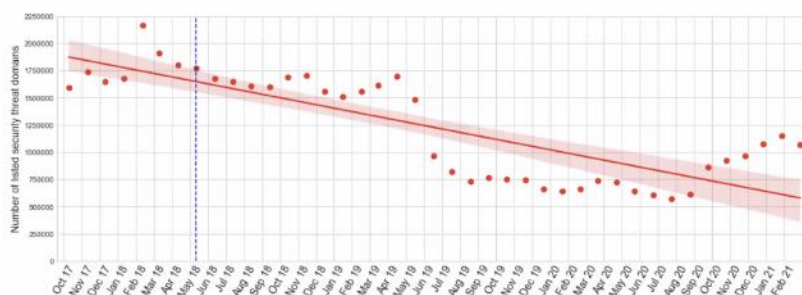
Figures 21-23: DAAR data (source ICANN)

General trends in gTLDs



Domains in gTLD zones

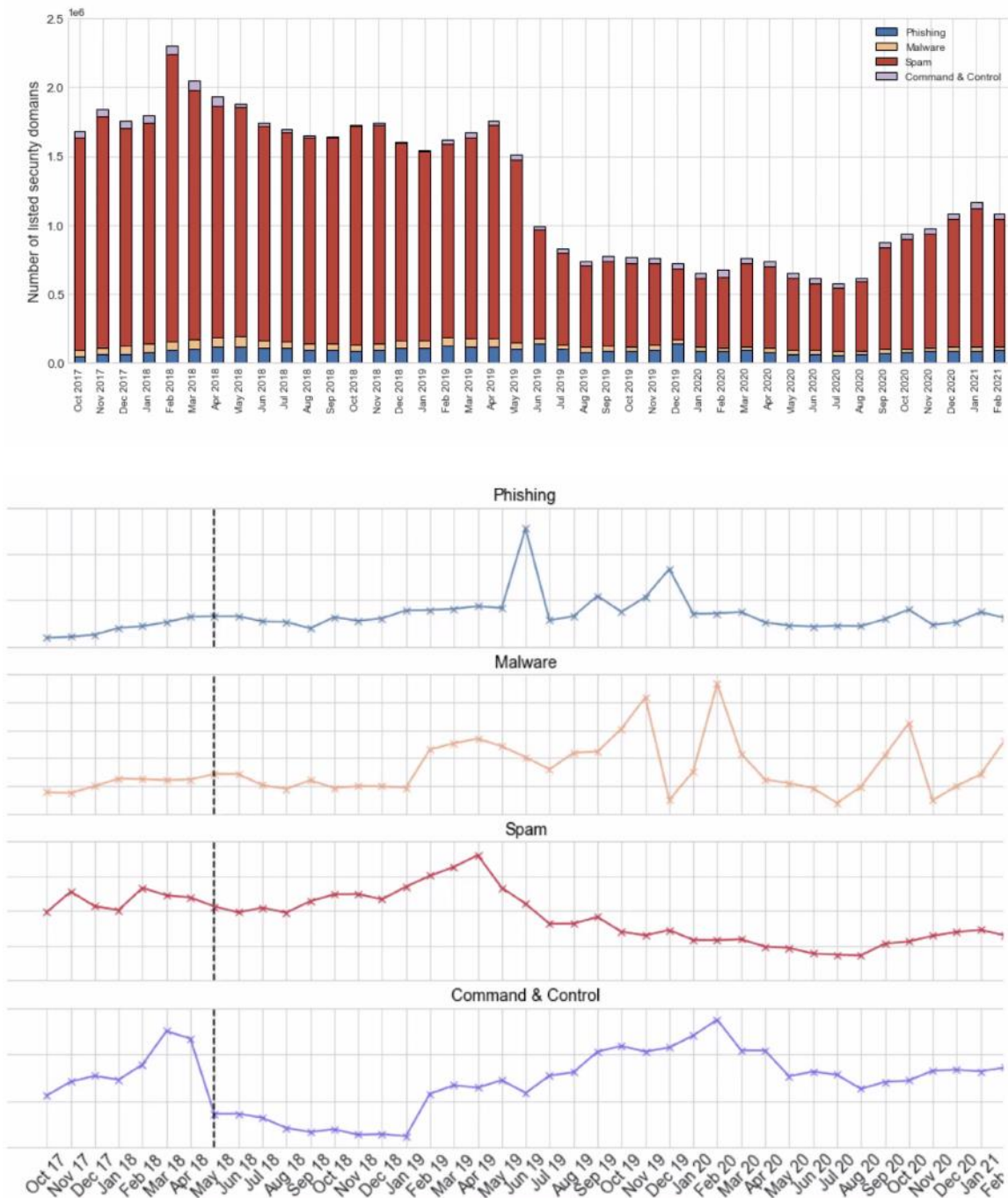
Security threat domains in gTLDs



³⁰⁵ <https://www.icann.org/octo-ssr/daar>

³⁰⁶ Currently, DAAR collects data from Spamhaus Domain Blocklist, SURBL, Anti-Phishing Working Group, Phishtank, Malware Patrol, Ransomware Tracker, Feodotracker

³⁰⁷ <https://www.icann.org/en/blogs/details/country-code-top-level-domain-participation-in-icanns-daar-system-29-7-2021-en>



However, several stakeholders and initiatives within the ICANN community have commented on the limitation of DAAR.^{308 309} The SSR2 Review Team's Final Report³¹⁰ has pointed out that the granularity of the DAAR monthly reports does not allow conclusions about which registrars/registries are harbouring significant abuse and ICANN does not share complete (raw) data with researchers who could help improve the methodology or confirm findings. According to the SSR2 Review Team:

³⁰⁸ <https://www.icann.org/en/system/files/correspondence/upton-to-marby-et-al-05apr19-en.pdf>

³⁰⁹ <https://www.icann.org/en/system/files/correspondence/austin-to-conrad-09sep20-en.pdf>

³¹⁰ <https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf>

- Identifying registries and registrars harbouring disproportionate levels of abuse would facilitate informed policymaking and add a measure of transparency and accountability to the domain name registration system that does not exist today;
- ICANN is apparently structuring agreements with data providers to be a significant inhibitor of these goals and proposes an overhaul of its DNS Abuse Analysis program with transparency, reproducibility, and actionable data products as its primary objectives;
- Discontinuing the DAAR program would be appropriate if the community and ICANN were unable to overhaul DAAR to achieve these objectives.

Contractual Compliance. Between March and September 2018 ICANN Contractual Department conducted audits in 20 gTLDs and found incompleting analyses and security reports for 13 gTLDs and lack of standardized or documented abuse handling procedures and lack of action on identified threats.³¹¹ The final report of a subsequent audit, initiated in November 2018, among all gTLDs concluded that:

- The vast majority of registry operators were committed to addressing DNS security threats;
- The prevalence of such threats is concentrated in a relatively small number of registries;
- Some registries interpreted the contractual obligation under Specification 11 3(b) in a way that it made difficult to assess whether their actions to mitigate security threats were compliant and effective.³¹²

The **Second Security, Stability, and Resiliency (SSR2) Review Team**, mandated by the ICANN Bylaws to review how effectively ICANN is meeting its commitment to enhance the operational stability, reliability, resiliency, security and global interoperability of the systems/processes (internal/external) that affect the Internet's unique identifiers, initiated its review in March 2017, suspended by ICANN Board from October 2018 to the beginning of June 2018. On 24 January 2020, the SSR2 Review Team released its draft report. On 25 January 2021, the SSR2 Review Team submitted a final report containing 63 full consensus recommendations to the ICANN Board for consideration. The final report concluded that *"the current ICANN-coordinated system does not sufficiently address DNS abuse and its associated harms"*.³¹³

According to the SSR2 Review Team none of the 28 SSR1 recommendations³¹⁴ were deemed to have been fully implemented since 2012. The SSR2 Final Report noted that governments (via the GAC) had asserted for over a decade that they did not find ICANN processes and procedures sufficient to address public safety interests.³¹⁵ With reference to the contractual obligations imposed by the RA and the RRA, the Final Report observed that later attempts to improve security practices through contractual amendments received criticism for lack of transparency and community engagement in the process.³¹⁶ CCT Final

³¹¹ <https://www.icann.org/en/blogs/details/contractual-compliance-addressing-domain-name-system-dns-infrastructure-abuse-8-11-2018-en>

³¹² <https://www.icann.org/en/system/files/files/contractual-compliance-registry-operator-audit-report-17sep19-en.pdf>

³¹³ <https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf>

³¹⁴ <https://www.icann.org/en/system/files/files/final-report-20jun12-en.pdf>

³¹⁵ ICANN Governmental Advisory Committee, "GAC Statement on DNS Abuse," 18 September 2019 - <https://gac.icann.org/file-asset/public/gac-statement-dns-abuse-final-18sep19.pdf>

³¹⁶ ICANN GNSO Business Constituency, "Comment on Proposed Amendments to Base New gTLD Registry

Report together with the SADAG report, as well as other third-party reports, also found that after the launch of the New gTLD Program, some registries and registrars promptly established practices to quickly and substantially increase domain registrations, e.g., bulk registrations, many of which are used for abuse and criminal activities.³¹⁷

The SSR2 Final Report has also noted that ICANN Contractual Compliance did not sufficiently address this ongoing, systemic abuse even after many organizations repeatedly called their attention to it.³¹⁸ Considered the evident lack of representation of public safety and consumers interests in the contract negotiations between ICANN and contracted parties (registries and registrars), the SSR2 Final Report has recommended to include independent abuse and security specialists in these negotiations with the objective of improving the security, stability and resilience of the DNS for end-users, businesses, and governments (Recommendation 8.1).

As for monitoring and enforcing contractual obligation, the SSR2 Final Report has recommended as follows:

- Recommendation 9.1: The ICANN Board should direct the compliance team to monitor and strictly enforce the compliance of contracted parties to current and future SSR and abuse-related obligations in contracts, baseline agreements, temporary specifications, and community policies.
- Recommendation 9.2: ICANN should proactively monitor and enforce registry and registrar contractual obligations to improve the accuracy of registration data. This monitoring and enforcement should include the validation of address fields and conducting periodic audits of the accuracy of registration data. ICANN should focus their enforcement efforts on those registrars and registries that have been the subject of over 50 complaints or reports per year regarding their inclusion of inaccurate data to ICANN.
- Recommendation 9.3: ICANN should have compliance activities audited externally at least annually and publish the audit reports and ICANN response to audit recommendations, including implementation plans.
- Recommendation 9.4: ICANN should task the compliance function with publishing regular reports that enumerate tools they are missing that would help them support ICANN as a whole to effectively use contractual levers to address security threats in the DNS, including measures that would require changes to the contracts.

The SSR2 Review Team found two classes of persistent challenges to progress: one related to definitions and scope of abuse that ICANN contractual obligations can manage, and the other related to access to data that can inform detection, mitigation, prevention, and response to abuse. SSR2 Final Report's Recommendations 11 through 14 target improved transparency and accountability in both areas. The report has also mentioned that ICANN Contractual Compliance asserted that the current contracts with registries and registrars

Agreement,” Business Constituency Submission, version 3, 20 July 2016 - https://www.bizconst.org/assets/docs/positions-statements/2016/2016_07july_20%20bc%20comment%20on%20proposed%20gTLD%20base%20registry%20agreement%20final.pdf

³¹⁷ Piscatello, Dave, “Weaponizing Domain Names: how bulk registration aids global spam campaigns,” Spamhaus, 21 March 2020 - <https://www.spamhaus.org/news/article/795/weaponizing-domainnames-how-bulk-registration-aids-global-spam-campaigns>

³¹⁸ Letter from Adobe Systems, DomainTools, eBay, Facebook, Microsoft, and Time Warner (aka, Independent Compliance Working Party) to Jamie Hedlund, SVP, ICANN Contractual Compliance & Consumer Safeguards and Managing Director, Washington D.C. Office, 27 February 2018 - <https://www.icann.org/en/system/files/correspondence/vayra-to-hedlund-27feb18-en.pdf>

did not authorize ICANN to require registries to suspend or delete potentially abusive domain names and were thus ineffective in allowing ICANN to pursue those engaged in systemic DNS abuse and that lack of a contractual prohibition on “systematic DNS abuse” prevents ICANN Contractual Compliance from effectively addressing it until there is a community consensus policy defining and prohibiting it. ICANN also announced that it would delay moving forward with CCT Review recommendations 14 and 15, which recommended amendments to existing agreements to help prevent DNS abuse. The ICANN Board underlined that this delay is because *“there are still ongoing community discussions to reach a common community understanding of DNS abuse and related terms”*.³¹⁹ The SSR2 Review Team has observed that *“the unstructured and unbounded nature of these discussions complicates finding a resolution and that ICANN org and contracted parties have an incentive to postpone resolution of this problem indefinitely”*. Back in 2010, the Registration Abuse Policies Working Group (RAPWG) recommended a community process, supported by ICANN resources, to create non-binding good practices to help registrars and registries address the illicit use of domain names.³²⁰ However, ten years later, ICANN has still not made substantive progress on these issues.

The SSR2 Review Team noted that the access to the following types of data is problematic and being unresolved for years:

- Registration data, which facilitates tracking abusive activity to the owner and operator of the associated domain
- TLD zone file data (via the Centralized Zone Data Service - CZDS), which supports security research
- Reported abuse data used to inform ICANN's analysis of DNS abuse
- Contractual compliance data to support trend analysis and evaluation of operational approaches to mitigate abuse.

Therefore, the SSR2 Final Report recommended to ICANN to:

- Provide clarity on definitions of abuse-related terms (Recommendation 10)
- Resolve CZDS data access problems (Recommendation 11)
- Overhaul DNS abuse analysis and reporting efforts to enable transparency and independent review (Recommendation 12)
- Increase transparency and accountability of abuse complaint reporting and establish maintain a central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties (Recommendation 13).

To move forward with the implementation of the recommendations, the SSR2 Review Team has suggested to ICANN different ways: conducting contract negotiations, issue advisories to contracted parties, use a timelimited and expert-supported cross-community working group, or even issue a Temporary Specification based on the conviction that DNS abuse is an acute public safety concern that needs urgent attention.

³¹⁹ ICANN Board, “Approved Resolutions | Regular Meeting of the ICANN Board,” Main Agenda, Competition, Consumer Trust, Consumer Choice Review Team (CCT-RT) Pending Recommendations, 22 October 2020 - <https://www.icann.org/resources/board-material/resolutions-2020-10-22-en#2.a>

³²⁰ RAPWG Final Report - https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf

The public comment period of the SSR2 Final Report took place between 28 January and 8 April 2021.³²¹ The comments represented a significant diversity of views. ICANN Board had to consider the final report and its recommendations, as well as the public comments within six months of receipt, i.e., by 25 July 2021, in accordance with Bylaw requirements.³²²

On 22 July 2021, the Board deliberated on the report, posted at ICANN's website on the 26 July.^{323 324 325} ICANN Board noted that the SSR2 recommendations are considerable in number, complex, and have interdependencies with other significant areas of work underway. It also noted that several recommendations repeat, duplicate or significantly overlap with existing ICANN operations, or recommendations issued by other Specific Review teams.

13 recommendations of the SSR2 Final Report were approved (1.1, 4.1, 5.1, 5.2, 9.1, 10.1, 16.1, 21.1, 22.1, 22.2, 23.1, 23.2 and 24.2), of which, according to ICANN Board, two recommendations were already fully implemented. With reference to Recommendation 9.1 (calling for the ICANN Board to *“direct the compliance team to monitor and strictly enforce the compliance of contracted parties to current and future SSR and abuse related obligations in contracts, baseline agreements, temporary specifications, and community policies.”*) the ICANN Board noted that *“ICANN org’s Contractual Compliance team’s work already monitors and supports that registries and registrars fulfill the requirements in in their agreements with ICANN org. Reporting and performance measurement metrics are published to icann.org. In addition, details regarding Registrar- and Registry-related Abuse complaints can be found in the monthly metrics published by ICANN org Contractual Compliance. This includes the number of Registrar Abuse Complaints related to pharming/phishing, malware/botnets, spam, counterfeiting, fraud, pharmaceuticals and trademark etc. as well as number of complaints related to GAC Category 1 Safeguards. As such, the Board accepts ICANN org’s representation that the Contractual Compliance operations that ICANN org has in place already meet the SSR2 Review Team’s defined measures of success for Recommendation 9.1. Therefore, the Board approves this recommendation, with the understanding that this recommendation is already fully implemented, and no further action is required”*.

The ICANN Board rejected 6 recommendations of the SSR2 Final Report because the recommendations could not be approved in full: 4.2, 8.1, 9.4, 10.2, 10.3 and 17.2. With reference to Recommendation 8.1 (calling for ICANN to *“commission a negotiating team that includes abuse and security experts not affiliated with or paid by contracted parties to represent the interests of non-contracted entities and work with ICANN org to renegotiate contracted party contracts in good faith, with public transparency, and with the objective of improving the SSR of the domain name system for end-users, businesses, and governments”*), the ICANN Board noted that the aspect of the recommendation that calls for the introduction of a third party into the bilateral negotiation process is not proper or feasible. The RA and RAA do not allow for third-party beneficiaries.

The ICANN Board rejected 10 recommendations: 2.1, 2.2, 2.3, 2.4, 14.1, 14.3, 14.4, 14.5, 15.1, and 15.2. With reference to Recommendations 14.1, 14.3, 14.4, 14.5, 15.1 and 15.2, related to creating a Temporary Specification and launching an Expedited Policy Development Process (EPDP) for evidence-based security improvements, the Board noted that *“Temporary Policies can only be established by the Board upon specific requirements, such as when the Board <reasonably determines that such modifications or amendments are justified and that immediate temporary establishment of a specification or policy on the subject is necessary to maintain the stability or security of Registrar Services, Registry*

³²¹ <https://www.icann.org/public-comments/ssr2-final-report-2021-01-28-en>

³²² Bylaws Section 4.6(a)(vii)(C), <https://www.icann.org/resources/pages/governance/bylaws-en/#article4.6>

³²³ <https://www.icann.org/en/blogs/details/board-action-and-next-steps-on-the-ssr2-review-26-7-2021-en>

³²⁴ <https://www.icann.org/resources/board-material/resolutions-2021-07-22-en#2.a>

³²⁵ <https://www.icann.org/en/system/files/bm/rationale-ssr2-22jul21-en.pdf>

Services, the DNS or the Internet>. The Board notes that Recommendation 14.1 does not provide such emergency grounds” and “[t]he Board [...] will not take the place of the community within the multistakeholder model and initiate a PDP upon a Specific Review team’s recommendation”.

4 recommendations (5.4, 19.1, 19.2 and 20.2) were placed into “pending, likely to be approved once further information is gathered to enable approval”, 24 recommendations into “pending, holding to seek clarity or further information”: 3.1, 3.2, 3.3, 4.3, 5.3, 7.1, 7.2, 7.3, 7.5, 9.3, 11.1, 12.1, 12.2, 12.3, 12.4, 13.1, 13.2, 14.2, 17.1, 18.1, 18.2, 18.3, 20.1 and 24.1, and 6 recommendations into “pending, likely to be rejected unless additional information shows implementation is feasible”: 6.1, 6.2, 7.4, 9.2, 16.2 and 16.3. With reference to Recommendation 9.2 (recommending ICANN to “proactively monitor and enforce registry and registrar contractual obligations to improve the accuracy of registration data”) the ICANN Board noted that “ICANN org does not have authority to require validation beyond what is in the Registry Agreement and Registrar Accreditation Agreement”.

g. Other voluntary initiatives

Internet and Jurisdiction Policy Network’s (I&JPN)

The Internet and Jurisdiction Policy Network’s³²⁶ (I&JPN) **Operational Approaches, Norms, Criteria, Mechanisms**³²⁷ document was published in April 2019 by the Domains & Jurisdiction Program’s Contact Group. Such document refers to the distinction between registration abuse and use abuse mentioned in ICANN’s Registration Abuse Policies Working Group Final Report (2010).³²⁸ The I&JPN’s document also points out that use abuse covers two dimensions: technical abuse (e.g., phishing, malware distribution, etc.), which is closely related to the security and stability of the DNS, and abusive content (e.g., child abuse material, intellectual property violations, etc.). It also highlights that: i) registries and registrars are very diverse in terms of size, activities, or governance structures; and ii) the fundamental distinction between country code and generic TLDs in terms of relation with national laws and authorities, leads to very different approaches and constraints when receiving direct requests or orders for action at the DNS level regarding use abuse, particularly when they originate across borders.

In the absence of a generally accepted framework regarding how to deal with use abuse, registries’ and registrars’ practices vary considerably. In light of such circumstances, registries and registrars are more inclined to take action at the level of the DNS in response to technical abuse than when dealing with abusive content that they usually do not have the competence to properly evaluate given the diversity of applicable national laws, unless a clear threshold of abuse is met. Indeed, registries and registrars prefer to simply have to comply with authoritative decisions (i.e., court orders), which provide procedural guarantees and clarity of applicable law.

Regarding the role of “notifiers”, the I&JPN’s document highlights that there is no external accreditation mechanism to certify their credibility. Registries and registrars “can use various factors to decide whether to enter into an agreement with a notifier or accept its requests, including its structure and governance framework, the explicit criteria and legal basis (national or more general) upon which its evaluations are based, its neutrality and potential conflicts of interest, and the procedural guarantees it provides. The overarching criterion however is reputation over time: how long the notifier has been active, its track

³²⁶ <https://www.internetjurisdiction.net/about/mission>

³²⁷ <https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf>

³²⁸ https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf

record on the market and, more importantly, whether it is willing to defend its notices and stand by the operator in case of litigation”.

Technical abuses:

Technical abuse occurs when the domain name is misused to propagate different types of technical abuse, including but not limited to the following: spam, malware, phishing, pharming, botnets, fast-flux hosting.

Website content abuses:

As mentioned above, the registries and registrars treat requests to deal with problematic website content differently from technical abuses. Registries and registrars cannot remove offending pieces of content from a website and the suspension of the domain name implies that all related service (e-mail, website, etc.) will be unavailable and have a geographically global impact. Therefore, registries and registrars reiterate that the proper content complaint referral path should be: website operator - registrant - hosting provider - registry.

The following content-related abuses are enlisted in the document:

- Child abuse material consists of photos or videos taken by an offender, documenting the sexual abuse of a child.
- Controlled substances and Regulated goods for sale or trade include illegal drugs, the illegal sale of legal drugs, illegal services, stolen goods, and illegal firearms or other weapons. The legality of a given substance or good will vary across jurisdictions.
- Violent extremist content includes content that depicts graphic violence, encourages violent action, endorses a terrorist organization or its acts, or encourages people to join such groups.
- Hate speech includes advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.
- Intellectual property related domain name suspension requests in response to website content (not relating to the domain name itself) have been issued on the basis of alleged trademark (e.g. sale of counterfeit goods), patent or trade secret infringement, or piracy of copyrighted works. As with all categories above, laws regarding intellectual property differ across jurisdictions.

The I&JPN's document also emphasizes that thresholds determining when taking action at the DNS level to address abuse is at the basis of any voluntary approach regarding requests for action. While acting at the DNS level would generally be justified in situations of technical abuse to protect the stability and security of the global infrastructure of the internet, given the geographically global impact of an action at the DNS level, doing so regarding abusive content could only be justified if a particularly high threshold of abuse/harm is met, regarding inter alia:

- a. The degree of global normative consistency regarding the alleged abuse: i.e. whether the content at issue is considered illegal across a sufficient number of jurisdictions;
- b. The proportion of the site effectively dedicated to the infringing content;
- c. The manifest intended purpose or bad faith of the registrant, and
- d. The lack of available alternative measures to remediate the situation.

Since badly formulated and incomplete complaint notices, lacking sufficient justification, sent to the wrong recipient, are burdensome for registries and registrars to handle and create inefficiencies, the I&JPN document identifies the components to be contained in a “good” complaint notice to facilitate interactions between issuers and the registries and registrars.

Furthermore, the I&JPN document encourages registries and registrars to develop metrics for collecting and reporting (in exportable and accessible formats) coherent statistics

pertaining to abuse notifications and implemented actions and make available to the public the criteria determining when action at the DNS level is appropriate, the types of abusive content they are willing to take action on, their abuse point(s) of contact, their internal criteria for decision-making and the channels for appeals/recourse.

Finally, the I&JPN's document launches the idea of an easy to use "abuse reporting interface", which would enable sending properly documented notices to the right recipient through: a targeted WHOIS query (to obtain the abuse point of contact email field), and a detailed form for entering technical details and justification for the notice of abuse.

The I&JPN has recently launched a Toolkit on DNS Level Action to Address Abuses.³²⁹

Framework to Address Abuse (DNS Abuse Framework)

The DNS Abuse Framework³³⁰ was launched in October 2019. Currently, it has 48 signatories, gTLDs registries (e.g. Donuts, PIR, Centralnic, Xyz) and registrars (GoDaddy, Namecheap, etc.).

The DNS Abuse Framework refers to the I&JPN's work (Operational Approaches, Norms, Criteria, Mechanisms) and provides the definition of DNS abuse, which TLD registries and registrars should feel compelled to act upon. Furthermore, it identifies other forms of abuse that (according to the registries and registrars) fall outside this DNS abuse definition, but that a registry or registrar should nonetheless take steps to address.

According to such definition, DNS abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for the other forms of DNS Abuse). The signatories of the DNS Abuse Framework believe that registries and registrars must act upon the afore-mentioned categories of abuse.

On the other hand, registries and registrars reiterate that they are not required under their agreements with ICANN to monitor or suspend domains based on website content abuse. Such DNS operators retain that this distinction is critical for the Internet to remain open for free expression. The determination as to whether a content is illegal (i.e. violates any law) varies across jurisdictions. Universally accepted global standard for evaluating content is not possible, nor is it (according to the signatories) ICANN's remit to create international online-content regulations. However, certain forms of website content abuse are so egregious that a registry or registrar should act when provided with specific and credible notice. Specifically, even without a court order, a registry or registrar should act to disrupt the following forms of website content abuse:

- 1. Child sexual abuse materials ("CSAM");**
- 2. Illegal distribution of opioids online;**
- 3. Human trafficking;**
- 4. Specific and credible incitements to violence.**

According to the signatories, underlying these website content abuses is the physical and often irreversible threat to human life.

Regarding website content abuse, registries and registrars encourage to contact first those who can remove or alter website content and, thus, follow the proper complaint referral path: website operator - registrant - hosting provider - reseller (if any) - registrar - registry operator.

The signatories call for cooperation between registries and registrars in case of receipt of abuse complaints. When a registry identifies abuse, it should always provide notice to the registrar, given the registrar's closer business or contractual relationship with the registrant.

³²⁹ <https://www.internetjurisdiction.net/domains/toolkit>

³³⁰ https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf

This relationship allows the registrar to work with its customer to address the abuse, provide mitigating information, or, in the case of a compromised domain (where a registrant's credentials are compromised and the domain is put to abusive purposes without the registrant's consent or knowledge) to reinstate the domain to its prior, unabused state.

The DNS Abuse Framework also mentions the important role of trusted notifiers to monitor and help address some of the categories of website content abuse identified above, or other sorts of abuse that may fall under an organization's policies. Trusted notifiers earn the registries' and registrars' trust with a recognized subject matter expertise, an established reputation for accuracy, and a documented relationship with and defined process for notifying the registries and registrars of alleged abuse.

h. Assessment of the regulatory framework, shortcomings and gaps

Regulation regarding DNS abuse brings enormous challenges in how it takes place and what can realistically be achieved. Most is only feasible on a transnational level, and the active involvement of private actors is often essential.

Due to the high rate of technological development, it is increasingly difficult to create top-down public regulation that is sufficiently effective and future-proof. The limited viability of such regulation quickly becomes apparent with the emergence of new technological developments and new service providers in the value chain whose activities will fall outside its scope or, at best, under a different set of rules. For long-term benefits for stakeholders, consumers and society as a whole, the system should be flexible and future-proof.

Consequently, all regulatory types regulating the DNS (public law regulation, private law regulation, private-public arrangements, self-regulation, and technical standards) ought to converge and set as a common goal the fight against DNS abuse to reduce significantly the phenomenon.

The latest legislative initiatives, both at *international* (Second Additional Protocol to the Convention on Cybercrime – 2021) and *EU* levels (Proposal for Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for Directive on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings – 2018, Proposal for NIS2 Directive – 2020, Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC – 2021), targeted the above-described issue related to the unavailability, unaccessibility, and inaccuracy of the WHOIS data which exacerbates the DNS abuse phenomenon by hindering the investigation of malicious and abusive activities and the enforcement efforts against these activities.

Other (EU) legislative initiatives provide or going to provide for enhanced security measures, accountability issues and promote public-private arrangements (collaborations) and self-regulatory initiatives.

As mentioned above, **international law** criminalises malicious activities related both to the DNS infrastructure and to content (e.g., CSAM and copyright infringement). The **Budapest Convention** uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved. Guidance Notes clarify which provisions of the Convention apply, among others, to botnets, phishing, DDoS attacks, malware, and spam. The **Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence** is expected to be finalized and adopted in the course of 2021. By including provisions on direct cooperation between law enforcement authorities (LEA) and entities providing domain

name registration services, requiring these latter to disclose domain registration (WHOIS) data to LEA, is a clear sign of action being taken at international level to prevent and fight DNS abuse.

Provisions of the **current EU legislative instruments** already impose on DNS service providers measures to guarantee the security of network and information systems against cybersecurity threats (NIS Directive). However, such Directive has been implemented by the Member States inconsistently. On the other hand, regarding content-related issues, the DNS service providers have not directly been addressed by the E-Commerce Directive, nor by the additional vertical rules. The current legislative proposals intend to address the above-identified lack of legal certainty regarding the liability issues, consistent security measures, accuracy of registration data and international cooperation.

Taken into account the importance of the DNS for the functioning of the internal market and the need of further harmonisation, the authors consider appropriate and proportionate recognising all DNS service providers offering services in the EU as essential entities (**Proposal for NIS2**). Threshold criteria for DNS service providers to qualify as essential or important entities is not feasible, since this has already led to fragmentation by the inconsistent implementation of the NIS Directive by the Member States. More technical security measure requirements could be specified in ENISA guidelines.

The authors also consider that the obligations imposed regarding the accuracy of and accessibility to the domain name registration information (WHOIS data) are essential for maintaining and guaranteeing the DNS secure, stable and resilient. Accuracy can be obtained by strict registrant identification e.g., through KYBC procedures and cross-checks in publicly available data bases. As for data accessibility, a centralized system for the submission of registration data requests is ought to be set up. The minimum information necessary to process such requests is to be identified and the reaction time of the DNS service providers is to be defined.

The **Proposal for DSA** acknowledges that the due diligence obligations have to be adapted to the type and nature of the intermediary service concerned, thus setting out basic obligations applicable to all providers of intermediary services, and additional obligations for providers of hosting services, since *“providers of hosting services play a particularly important role in tackling illegal content online, as they store information provided by and at the request of the recipients of the service and typically give other recipients access thereto, sometimes on a large scale”*. However, as mentioned by the authors above, in certain cases, where there is overlap between malicious content and infrastructure related abuses, DNS service providers (TLD registries and registrars) ought to be required to take action in order to effectively address the abusive activities.

The reason for the necessity of taking action by those intermediaries too is explained by the following example of phishing: a malicious actor registers a domain name to launch a phishing campaign to deceive potential victims into disclosing passwords to their bank accounts. The fake website uses the official logo of the bank to look more trustworthy. Both the hosting provider and a DNS service provider ought to react in such a case. As long as the hosting provider removes the malicious content, but the malicious domain is not suspended, the malicious actor can purchase another hosting service from another provider and reuse the maliciously registered domain name. Suppose only the registrar or the TLD registry operator removes the domain name from the zone file. In that case, the malicious actor may reuse the hosting and register a new domain name with another operator to continue malicious activities. While, as in the example given, mitigating the abuse at the hosting or domain name level interrupts the malicious actions of the attacker, mitigating the problem at both the hosting and DNS levels ought to be required because both the hosting and DNS technical infrastructures are being abused. Such a mitigation approach also leads to increased cost for the malicious actor and thus barriers to DNS abuse.

In another example, a malicious actor compromises a legitimate website using a vulnerable content management system and uploads malware to distribute it and infect end users. The domain is registered by a benign user and abused (the site is hacked). In this case, the illegal content should be removed and the hosting infrastructure (vulnerability) patched by the webmaster or hosting provider (depending on whether the hosting is managed or unmanaged). Generally, in such cases, DNS service providers should not intervene at the DNS level, since suspending a benign domain name might cause collateral damage and disrupt legitimate activities of the domain owner and its users.

However, in some cases (e.g., distribution of CSAM), even if the DNS operator concludes that the malicious user is not abusing the DNS infrastructure, the DNS operator ought to inform the intermediaries involved in hosting (e.g., the website operator, domain owner, or hosting provider) and should (temporarily) suspend the domain name if the content is not promptly removed (duty of care). If, on the other hand, the DNS service provider concludes that CSAM material is being distributed using a maliciously registered domain name (DNS infrastructure abuse), the domain shall be suspended by the DNS service provider and the content removed by the hosting provider.

Therefore, DNS service providers also ought to be required to put in place user-friendly notice-and-action mechanisms that facilitate the notification of specific items of information that the notifying party considers to be illegal content to those providers concerned, pursuant to which those providers can decide whether or not they agree with that assessment and wishes to take action (suspend the domain name). Likewise, requirements of setting up internal complaint-handling system (possibly harmonised between providers), Know Your Business Customer (KYBC) procedures and establishing and enhancing collaboration with trusted notifiers ought to be extended also to them. Establishing and enhancing structured collaborations with trusted notifiers might be beneficial also for TLD registries and registrars by reducing the burden of these latter to assess the alleged illegality of content.

ICANN level. After having reviewed a certain amount of ICANN reports released by different working groups, review teams and stakeholder groups, etc., the authors note that among the ICANN stakeholders there has been a significant diversity of views for years on the definition of DNS abuse, its magnitude, the effectiveness of measures put in place to fight it, and the enforcement of existing contractual obligations of the contracted parties (registries and registrars). Such views have not been successfully brought closer but rather stakeholder groups stick to their position, making it difficult (if not impossible) moving forward at ICANN level which is based on consensus-driven policy making.

The contractual obligations in place for gTLD registries and registrars (and their resellers, if any) have been found unachieved, ineffective, and/or unenforced by periodic reviews mandated by ICANN Bylaws. The scope of the specific reviews mandated by ICANN Bylaws is to evaluate whether ICANN achieves its mission to ensure the stable and secure operation of the Internet's unique identifier systems. Reviews should also contribute to ensuring that, further to maintaining effective the multistakeholder model, ICANN serves the public interest.

The CCT Review Team Final Report's recommendations (based on the SADAG report) to include provisions in the Registry Agreement to incentivise the adoption of anti-abuse measures (Recommendation 14), to prevent systematic use of specific registrars of registries for DNS abuse, including thresholds of abuse at which compliance inquiries are automatically triggered and consider a possible DNS Abuse Dispute Resolution Policy (Recommendation 15), the improvement of research on DNS abuse (Recommendation 16), the improvement of WHOIS accuracy (Recommendation 18), and effectiveness of contractual compliance complaints handling remained unimplemented by ICANN.

The same can be said about the SSR1 Review Team's recommendations as highlighted in the SSR2 Review Team Final Report. ICANN Board's recent resolution on SSR2 Review Team's recommendations also makes it clear that most of the concerns raised by the SSR2 Review Team will likely not be addressed and the resolution of the issue (mitigating effectively DNS abuse) will be postponed for an indefinite period.

Moreover, due to the ongoing discussions on ICANN's remit, no significant actions will likely be taken at ICANN level to enhance to fight against DNS abuse (comprising the development of a consensus definition) in a holistic way.

Self-regulation. 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 does 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 harmonised 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 harmonised and transparent notice-and-action procedures. Some stakeholders suggested strengthening the collaborations with authorities, hotlines, and trusted notifiers.

While the authors share these views, they also highlight that there are several good practices adopted by intermediaries (see in details under Section 10) that ought to be expanded to other DNS service providers, in particular to gTLD and ccTLD registries and registrars.

From this derives the importance of the voluntary domain industry-led initiatives and the role of the associations and organizations promoting such initiatives (e.g., CENTR, eco – Association of the Domain Industry, I&JPN, DNS Abuse Framework). Some of the initiatives mentioned above (I&JPN's Operational, Approaches, Norms, Criteria, Mechanisms and Toolkit, DNS Abuse Framework) still have their limitation in assuming that abuses can be clearly distinguished as infrastructure (security) or content-related, which is, according to the authors is often not possible (e.g., phishing, malware distribution, etc.). However, legislators and regulators ought to support such voluntary initiatives by involving, among other, stakeholders representing public interest groups to maintain the regulatory system flexible and the stakeholders' interests well-balanced. For example, establishing a centralized registration data disclosure system and/or an abuse reporting platform would simplify and improve abuse reporting and handling both for the affected parties and the intermediaries.

10. Good practices in mitigating DNS abuse

The authors have identified a broad set of good practices adopted by gTLD and ccTLD registries and other services providers aimed to prevent and mitigate DNS abuse and to enhance the collaboration with other actors.

The good practices analyzed below comprise the practices adopted by:

- a. gTLDs:
 - 1. Public Interest Registry
 - 2. Donuts
 - 3. Other service providers
- b. ccTLDs:
 - 1. .eu
 - 2. .dk
 - 3. Other ccTLDs

a. gTLDs

Public Interest Registry (.org)

Public Interest Registry (PIR)³³¹, a not-for-profit organization created by the Internet Society (ISOC), is the registry operators of .org TLD since 2003. .org is among the largest TLDs with over 10.4 million registrations.³³²

Within the New gTLD Program, PIR applied for the management of .ngo and .ong domain extensions. PIR also applied for the creation and management of four internationalized domain names (IDNs) recognized as “organization,” “org” or “institution” in non-Latin-based scripts: .ॐॐॐॐ (in Devanagari - Hindi script), .opr one (in Cyrillic); .机构 and .组织机构 (in simplified Chinese). The first three of the IDNs were launched in May 2014. The Sunrise period for .ngo & .ong domain names began on 17 March 2015. Limited registration for organizations who have already submitted an Expression of Interest began on 21 April 2015.

The registration of .org domains are regulated by the Registration Policy of PIR.³³³

According to the **Anti-Abuse Policy** of PIR, abusive use(s) of .org, .opr, .机构, and .ॐॐॐॐ domain names should not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrars and registrants, as well as for users of the Internet. In general, PIR defines abusive use of a domain as the wrong or excessive use of power, position or ability, and includes, without limitation, the following:

- Illegal or fraudulent actions
- Spam
- Phishing
- Pharming
- Wilful distribution of malware
- Fast flux hosting

³³¹ <https://thenew.org/>

³³² https://www.verisign.com/en_US/domain-names/dnib/index.xhtml

³³³ <https://thenew.org/org-people/about-pir/policies/org-idn-policies/registration-policy-org-idn/>

- Botnet command-and-control
- Distribution of Child Sexual Abuse Materials (CSAM)
- Illegal Access to Other Computers or Networks

It is to be noted that there is no further definition provided for the category “illegal or fraudulent actions”. PIR is one of the registries that has coordinated the work resulted in the **DNS Abuse Framework**, adopting thus the narrower definition of DNS abuse, limited to the so-called technical threats.

Abusive uses, as defined above shall give rise to the right of PIR to take the followings actions under PIR’s Registry-Registrar Agreement (RRA) in its sole discretion: to deny, cancel or transfer any registration or transaction, or place any domain name on registry lock, hold or similar status, that it deems necessary, at its discretion; (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of PIR, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement or (5) to correct mistakes made by PIR or any Registrar in connection with a domain name registration. PIR also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.

PIR has recently introduced an **appeal mechanism** against the suspension under the Anti-Abuse Policy to a neutral third party.^{334 335} The appeal mechanism is administered by Forum (previously the National Arbitration Forum)³³⁶ according to the Appeal Process Rules³³⁷. While Forum charges USD 1,200 per case, PIR subsidizes USD 700 and then reimburse the other USD 500 if the appeal is successful. As of April 2021, Forum reported that no appeal of PIR suspension were received.

PIR publishes quarterly its **abuse metrics and statistics** on the actions taken.³³⁸ As of 8 July 2021, the following data were published:

Figure 24: Suspensions (source PIR)

³³⁴ <https://thenew.org/responsible-domain-industry-needs-responsible-registrant-appeals-process/>

³³⁵ <https://domainnamewire.com/2020/09/10/org-launches-new-registrant-rights-appeal-mechanism/>

³³⁶ <https://www.adrforum.com/domain-dispute/registry-spec>

³³⁷ [https://www.adrforum.com/assets/resources/RegistrySpec/PIR/Appeal%20Process%20Rules%20FINAL.p](https://www.adrforum.com/assets/resources/RegistrySpec/PIR/Appeal%20Process%20Rules%20FINAL.pdf)
[df](https://www.adrforum.com/assets/resources/RegistrySpec/PIR/Appeal%20Process%20Rules%20FINAL.pdf)

³³⁸ <https://thenew.org/org-people/about-pir/resources/anti-abuse-metrics/>

Abuse and Suspensions (through July 8, 2021)**DNS Abuse**

Abuse Type	2017	2018	2019	2020	2021 YTD
SPAM	17,604	6,208	16,991	18,861	10,431
PHISHING	54	2,696	22,959	6,677	2,872
MALWARE	8	114	990	505	319
BOTNET C&C	1	73	550	350	144
OTHER*	25	12	31	53	12
ANNUAL TOTALS	17,692	9,103	41,434	26,466	13,778
SUSPENDED BY REGISTRAR	1,601	384	1,652	1,887	989
SUSPENDED BY REGISTRY	9,160	1,809	4,982	3,094	1,651
TOTAL SUSPENSIONS	10,761	2,193	6,634	4,981	2,640

* Hacking, Distributed Denial of Service (DDOS) attacks, other technical abuses

According to PIR, many of the domains flagged for abuse are actually compromised domains, when the domains are initially registered for non-abusive purposes, but the registrant's domain is put to abusive purposes without its consent. Since the suspension at the registry level is not the appropriate action to deal with a compromised domain, the registrar or host should work to get control of the domain back into the registrant's hands.

PIR also publishes the number of domains subject of suspension or seizure upon court order or law enforcement initiatives divided in the categories: botnets, not-botnets, intellectual property enforcement.

Figure 25: Court ordered actions (source PIR)

Court Ordered Actions on Domains (through July 8, 2021)**Court Ordered Law Enforcement Actions – Botnets**

(Botnet domains either suspended or seized by Law Enforcement Agencies)

Year	Number of Domains
2017	30,267
2018	13,927
2019	13,694
2020	86,240
2021 YTD	0

Court Ordered Law Enforcement Actions – Non-Botnets

(Non-Botnet domains either suspended or seized by Law Enforcement Agencies)

Year	Number of Domains
2017	30
2018	2
2019	1
2020	2
2021 YTD	14

Court Ordered Civil Intellectual Property Enforcement

Year	Number of Domains
2017	534
2018	1,128
2019	391
2020	91
2021 YTD	86

Moreover, PIR takes action (suspension) in limited cases of website content abuse (child sexual abuse material – CSAM, sites dedicated to the distribution of opioids online, incitement to violence, domains dedicated to fake Covid-19 “cures,” sites dedicated to the buying and selling of stolen credit card information).

Figure 26: Content-related abuse (source PIR)

Child Sexual Abuse Material

Year	2018	2019	2020	2021 YTD
URLs referred from the Internet Watch Foundation	447	834	1,327	1,292
Number of Domains included in those URLs	41	54	63	36
Domains suspended by PIR	13	8	8	5
Domains where content was promptly removed	28	46	55	31

Opioid Websites

(Sites that are dedicated to distribution of opioids online)

Year	Number of Domains
2019	3
2020	0
2021 YTD	0

Other Limited Content

(This category includes incitement to violence, domains dedicated to fake Covid-19 "cures," sites dedicated to the buying and selling of stolen credit card information, etc.)

Year	Number of Domains
2020	9
2021 YTD	2

With reference to CSAM, PIR has **collaborations** in place with the UK-based Internet Watch Foundation (IWF) and the US-based National Center for Missing and Exploited Children (NCMEC). Upon notification from the IWF or NCMEC (link containing the abuse), PIR sends a "de-fanged" or broken version of the URL in question to the registrar and give them a short window to ensure that the offending material is removed. In the vast majority of cases, the registrars or registrants act swiftly and the content is removed. If they do not, PIR suspends the domain name. PIR also co-founded the Child Sexual Abuse Material Referral Discussion Group, a forum for registries and to share ideas and identify the very good practices to combat CSAM via the DNS.

In 2017, PIR developed a policy to address systemic, large scale copyright infringement, the Systemic Copyright Infringement Alternative Dispute Resolution Policy (SCDRP), modelled on UDRP and similarly priced, with Forum providing arbitration services. The key difference was that instead of trademark infringement in the domain, it dealt with copyright infringement on the associated web site. However, further to the concerns expressed by the Electronic Frontier Foundation (EFF) and the Internet Commerce Association (ICA), the initiative was not launched by PIR.³³⁹

340

In June 2020, the U.S. Food and Drug Administration (FDA) and National Telecommunications and Information Administration (NTIA) launched a 120-day pilot program with the participation of PIR, Registry Services (formerly Neustar) and Verisign to curb illegal online sales of opioids. As part of the program, the FDA served as a trusted notifier to alert PIR and other partner registries, to websites that were illegally selling opioids. PIR acted on these names after having determined that the primary purpose of the site attendant to the domain was the distribution of opioids online. As the result of the pilot, nearly 30 websites illegally offering opioids for sale became inaccessible to the public. In February 2021, the FDA announced that it would continue the collaboration to help prevent illegal online opioid sales.³⁴¹

Furthermore, in May 2019, PIR introduced the **Quality Performance Index (QPI)** to measure the quality of individual registrar .org namespace and incentivize "healthy" (e.g., non-abusive) domain name registrations.³⁴² QPI is calculated by analysing data for each registrar based on a number of core Key Performance Indicators (KPIs)—abuse ratings, renewal rates, domain usage, DNSSEC enabled, SSL encryption usage, and the average term life of a domain name registration. The weighted scores are then combined to form a single QPI score. Of these factors, abuse is the primary metric; if a registrar fails on abuse, it will not qualify for QPI no matter its scoring in the other criteria. As a result, QPI incentivizes .org registrars to make domain health a priority and identify and remedy abuse such as botnets, malware, phishing, and

³³⁹ <http://domainincite.com/21564-pir-slams-brakes-on-udrp-for-copyright>

³⁴⁰ <https://onlinedomain.com/2017/02/24/domain-name-news/org-registry-pir-pausing-development-udrp-copyright/>

³⁴¹ <https://www.fda.gov/news-events/fda-brief/fda-brief-fda-continues-efforts-curb-illegal-availability-unapproved-opioids-online>

³⁴² <https://thenew.org/public-interest-registry-proudly-introduces-its-new-quality-performance-index/>

related spam. QPI was designed to: 1) recognize and reward those registrars who are aligned with and committed to the PIR mission of maintaining and growing trust in the .org domain, 2) identify areas of improvement so PIR can work with registrars to raise their scores, and 3) promote the overall quality of the domain name space and the internet as a whole. According to PIR, QPI serves as a “carrot” to registrars that meet our QPI criteria and a “stick” for those that do not, as they do not receive incentives their competitors receive. In March 2021, PIR announced that would expand the QPI and make it available at no cost to all registries.³⁴³ QPI was also mentioned as registry best practice by ICANN GAC Public Safety Working Group.

DNSSEC is implemented with all TLDs managed by PIR, including .org, .ngo & .ong, .opr, .机构, and .□□□□□.³⁴⁴

In February 2021, PIR launched the **DNS Abuse Institute**. Its stated objective is to create initiatives that will establish recommended practices, foster collaboration, and develop industry-wide solutions to combating abuses such as malware, botnets, phishing, pharming, and spam. It seeks to build upon the foundations laid by the DNS Abuse Framework and the Internet & Jurisdiction Policy Network’s Domains & Jurisdiction Program.³⁴⁵

Donuts

Donuts Inc. is a US-based registry operator managing the largest portfolio of new gTLDs with over 240 extensions, among which domains for use as business identifiers (such as .ltd, .company), navigation (such as .careers, .support, or .social), in vertical markets (such as .photography, .cafe, or .games) or in generics (such as .life, .world or .live).³⁴⁶

Donuts partners with numerous registrars.³⁴⁷ Name.com³⁴⁸, offering registration and hosting services as well, is part of Donuts Inc, although the latter shall not exercise functional control over such registrar in accordance with Specification 9 of the Registry Agreement.³⁴⁹

According the **Acceptable Use Policy**, Donuts reserves the right, at its sole discretion and at any time and without limitation, to deny, suspend, cancel, redirect, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status as it determines necessary for any of the following reasons:

- To protect the integrity and stability of one of its registries;
- To comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process;
- To avoid any liability, civil or criminal, on the part of Donuts, its affiliates, subsidiaries, officers, directors, contracted parties, agents, or employees;
- To comply with the terms of the applicable registration agreement and Donuts’ policies;
- Where registrant fails to keep WHOIS information accurate or up-to-date;
- Domain name use is abusive or violates the Acceptable Use Policy, a third party’s rights or acceptable use policies, including but not limited to the infringement of any copyright or trademark;

³⁴³ <https://thenew.org/pir-expands-qpi-initiative/>

³⁴⁴ <https://thenew.org/org-people/about-pir/policies/org-idn-policies/dnssec-policy-org-idn/>

³⁴⁵ <https://dnsabuseinstitute.org/about-the-dns-abuse-institute/>

³⁴⁶ <https://donuts.domains/what-we-do/top-level-domain-portfolio/>

³⁴⁷ <https://donuts.domains/what-we-do/accredited-registrars/#become-a-registrar>

³⁴⁸ <https://www.name.com/>

³⁴⁹ <https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm>

- To correct mistakes made by a registry operator or any registrar in connection with a domain name registration; or
- As needed during resolution of a dispute.

Abusive use of a domain is described as an illegal, disruptive, malicious, or fraudulent action and includes, without limitation, the following:

- Distribution of malware;
- Dissemination of software designed to infiltrate or damage a computer system without the owners informed consent, including without limitation, computer viruses, worms, keyloggers, trojans, and fake antivirus products;
- Phishing, or any attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication;
- DNS hijacking or poisoning;
- Spam, including using electronic messaging systems to send unsolicited bulk messages, including but not limited to e-mail spam, instant messaging spam, mobile messaging spam, and the spamming of Internet forums;
- Botnets, including malicious fast-flux hosting;
- Denial-of-service attacks;
- Child abuse imagery;
- Promotion, encouragement, sale, or distribution of prescription medication without a valid prescription in violation of applicable law;
- Illegal access of computers or networks;
- Cyber-bullying, harassment, or other forms of abuse to individuals or groups;
- Incitement to violence or other unlawful actions;
- Failure by registrant of a two-character second level domain to take steps to ensure against misrepresenting or falsely implying that it is affiliated with the corresponding government or country-code manager, if such affiliation, sponsorship or endorsement does not exist; and
- Holding oneself out as a licensed medical practitioner in a .doctor domain name when such license doesn't exist.

Donuts was also one of the principal drafters and original signatories of the **DNS Abuse Framework**, according to which DNS abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for the other forms of DNS Abuse).

Donuts provides an **abuse point of contact** through an e-mail address posted on its website (currently: abuse@donuts.mail) and also a web form for the submission of abuse reports.³⁵⁰

Donuts adopts a **transparent abuse handling process** and takes the following actions in case of detected or reported abuse:

1. Phishing, pharming, botnets, malware and spam:

- Completes a review of the evidence of detected and reported abuse to determine: 1. if there is a valid instance of DNS abuse, and 2. to identify the relevant registrar.

³⁵⁰ <https://donuts.domains/report-abuse/>

- Raises the query to the registrar to make them aware of 1. the type of abuse, 2. provides corresponding evidence, and 3. requests the registrar to review, take action and respond within a given time period, depending on the severity, type, and subjective review of the individual circumstances.
- Depending on the action and explanation provided by the registrar, Donuts 1. further liaises with the registrar if it investigates the matter and requires further time, or 2. takes action to suspend a domain or close the query based on Donuts' independent review and analysis.

2. Immediate Harm or Threat to life and Cyber Bullying:

Whether advised by third parties or as identified as part of daily tasks and workflows which may evidence any immediate harm or threat to human life or cyber-bullying would be immediately escalated to the Senior Manager of Compliance. Appropriate action is taken on a case by case basis as it may involve contacting and liaising with the registrant, the registrar, law enforcement authorities and other bodies and institutions as the issue requires.

3. Child Sex Abuse Material (CSAM):

- Donuts only escalates CSAM issues received from a trusted advisor, to include, the Internet Watch Foundation (IWF) and the National Center for Missing and Exploited Children (NCMEC).
- If it receives a complaint or information which relates to CSAM from a third party, it sends the evidence to the above and request them to determine and advise if there is a CSAM issue.
- It does not under any circumstances investigate or view the alleged abuse as it relies on the IWF or NCMEC to confirm the nature and type of the abuse.
- It raises the query to the registrar to make them aware of 1. the type of abuse, 2. provides corresponding evidence, and 3. requests the registrar to review and respond within a given time period.
- Depending on the action and explanation provided by the registrar, Donuts 1. liaises with the registrar if it investigates the matter and requires further time, or 2. takes action to suspend a domain or close the query based on Donuts' independent review and analysis.

4. Rogue Pharmacy:

Donuts completes a review of the domain, to include using sources such as LegitScript to determine the nature and basis of the abuse as it applies to the supply and distribution of pharmaceuticals. Based on the research and analysis, action will be taken to 1. advise the registrar, and/or 2. advise law enforcement authorities and/or, 3. request further information from the reporting party.

5. Other:

Donuts reported that when evidence supports action, it shall be prepared to take action, so long as it can ensure transparency in its process, and proportionality in its actions. It will never take action, where such action is not objectively justifiable, and it shall not engage in arbitrary action.

Where there is physical evidence (screenshot) of attempted phishing, Donuts insists on registrar action; where such action is not forthcoming, or it disagrees with the response of the registrar, it intervenes. Donuts has also pointed out that it receives a number of reports of 'phishing' that do not provide any indicators of phishing, but are in effect escalations that purely consist of IPR infringement allegations. According to Donuts, as a registry, it is not a competent party to assess IPR infringement. In such matters it defers to the rights protection mechanisms that are available and indeed intended for such determinations (e.g., URS, UDRP, court procedures).

Donuts does continue to retain discretion, where evidence presented may not specifically identify phishing content, but there presents an abundance of additional evidence - infrastructure indicators (e.g., age of domain, IP address, trusted notifications, etc.), lexicographical peculiarities, inclusion of additional 'red flag' keywords, that would support escalation - these remain subjective and Donuts relies on its analysts to ensure a solid justification for escalation exists on a case by case basis.

Although CSAM is a content issue, Donuts has almost zero tolerance approach to the use of any domain in connection with CSAM. All IWF verified report must be actioned. However, in CSAM escalations the registrant may not always be responsible for the content and, therefore, the action in this instance is the removal/disruption of the CSAM content, and not the entire domain.

Currently, Donuts' principal **trusted notifiers** include:

- IWF
- NCMEC
- Motion Picture Association (MPA)
- Recording Industry Association of America (RIAA)
- National Crime Agency (UK).

Donuts also maintains close relationships with representatives of a number of **law enforcement authorities** (LEA), in particular, the FBI, Interpol and the National Crime Agency (UK).

The average **turnaround time** of Donuts to respond and/or mitigate abuse complaints is as follows:

- Response: the average turnaround is 1 day. All reports are responded to and Donuts aims to escalate any 'reported' abuse on the same day.
- Mitigation is not straightforward as it is highly subjective: however, the expected timelines of Donuts are generally as follows:
 - Phishing: 24/48/96 hours, based on the nature of the evidence and the urgency attached
 - Spam: 96 hours
 - Malware: 24/48/96 hours, based on the nature of the evidence and the urgency attached
 - CSAM: 96 hours, based on the advice of IWF
 - Botnets: usually based on court orders, therefore action is within the stated court established timeframe

- Botnets reported/detected: 24/48/96 hours, based on the nature of the evidence and the urgency attached
- Pharming: 24/48/96 hours, based on the nature of the evidence and the urgency attached.

Donuts, through its registrars, offers, for a fee, the **Domains Protected Marks List programs**, (DPML and DPML Plus), to preventively block registrations of validated trade marks without requiring defensive purchases in each of Donuts' 241 TLDs³⁵¹:

- DPML is a five-year block for an exact match second level domain (SLD) across standard-priced Donuts TLDs;
- DPML Plus is a ten-year block for an exact-match SLD across all Donuts TLDs that includes the ability to block three additional strings that contain the mark or are misspellings of the mark, and more than three "contains" or misspelled strings can be added for an additional fee.

However, in order to adhere to DPML/DPML Plus, trade marks should be validated by Trademark Clearinghouse (TMCH), as detailed in the TMCH guidelines.

Donuts also offers a service (TrueName) that automatically **blocks registrations of homographs of registered domains**.³⁵² When a registrant registers a Donuts TLD such as .guru, .money or .live, Donuts will block registrations of lookalike domain names that substitute letters or numbers with characters from Latin, Greek, and Cyrillic script tables for the purpose of malicious activity.

As for **registration data accuracy**, Donuts, as a registry operator, does not maintain the direct contractual link with the registrant and, thus, it relies on its registrar partners to review any complaints relating to claims of inaccurate registration data in the first instance. Donuts accepts and escalates, as appropriate, complaints relating to claims of inaccurate registration data as per the terms of its Acceptable Use Policy and the provisions of the Registry-Registrar Agreement (RRA).

Donuts does not currently offer any specific incentives to deploy **DNSSEC** for its registrar partners.

Whilst on the one hand Donuts adopts some good practices identified above, on the other hand, as data shows (Appendix 1 – Technical Report, Section 9.2), there is need for implementing further good practices that contrast the phenomenon of DNS abuse within its TLDs.

Other providers

Other providers also offer, for a fee, **preventive blocking services**^{353 354}. Most of these blocking services are based on trade marks entered in the TMCH repository. .club Trademark Sentry is based on US trade mark registrations. UNR (formerly known as Uniregistry) currently offers Extended Protection Service (EPS) and is planning to launch Unified Block (UB) in coalition with participating domain registries (ccTLDs and gTLDs). Under this latter, rightholders might submit blocking requests through contracted registrars in the same manner as registering a domain name. UB will extend the protection originally provided by the TMCH by accepting trade marks

³⁵¹ <https://donuts.domains/what-we-do/brand-protection/>

³⁵² <https://truenamename.domains/security/>

³⁵³ <https://adultblock.adult/>

³⁵⁴ <https://trademarksentry.club/about/>

registered in it, but also trade marks not included in the TMCH, and other IPR and names. Rights eligible for UB will comprise:

- Company Name: Name of the legal entity as registered in the company register or business register
- Trademarks
- Trade Name/Fictitious Name/Assumed Name/Doing Business As (DBA)
- Celebrity names
- Official person name.

b. ccTLDs

.eu

The .eu, the ccTLD for the European Union, is one of the largest ccTLDs with over 3.6 million registrations.^{355 356 357}

End-users of .eu include individuals, businesses from different industry sectors³⁵⁸, and other entities, as well as EU institutions, agencies, and bodies. In April 2021, .eu Registry crawled 100,000-domain names, out of which 80% had active web service and 15% were DNSSEC signed. Out of those names, more than 44% resolved into a structured website. The websites were classified according to the categories as defined by NACE, the statistical classification of economic activities in the European Community, and agreed by the members of CENTR.

As of 2 August 2021, registration of a .eu domain name can be requested by any of the following:

- A citizen of one of the European Union Member States, Iceland, Liechtenstein or, Norway, independent of their place of residence;
- A natural person who is not a citizen of one of the European Union Member States, Iceland, Liechtenstein, or Norway, but who is a resident of a European Union Member State, Iceland, Liechtenstein, or Norway;
- An undertaking that is established in a European Union Member State, Iceland, Liechtenstein, or Norway;
- An organisation that is established in a European Union Member State, Iceland, Liechtenstein, or Norway without prejudice to the application of national law.

The European Commission is responsible for the .eu TLD. The .eu Registry is entrusted by the Commission with organising, administering, and managing the .eu TLD, including maintenance of the corresponding databases and the associated public query services, registration of domain names, operation of the registry of domain names, operation of the registry TLD name servers and dissemination of TLD zone files.³⁵⁹ The purpose of the .eu TLD is to help enhancing the EU identity and promote EU values online through good

³⁵⁵ As of 30 June 2021, the total number of .eu domain name registrations was 3,731,298 with 212,228 new registrations in Q2 - https://eurid.eu/media/filer_public/b2/fe/b2fe65b5-7ae0-43ce-9c01-7e6c29ea16b0/quarterly_report_q2_2021.pdf

³⁵⁶ https://media.nominet.uk/wp-content/uploads/2021/05/The-Online-World-2020.pdf?_ga=2.208900692.715335191.1627204478-835102325.1621419253

³⁵⁷ https://www.verisign.com/en_US/domain-names/dnib/index.xhtml

³⁵⁸ EURid's .eu website categorization: <https://eurid.eu/en/news/uptake-of-eu-use-for-the-trade-and-it-sectors/>

³⁵⁹ Article 2 of [Regulation \(EC\) No 733/2002](#)

management, values such as multilingualism, respect for users' privacy and security and respect for human rights, as well as specific EU priorities.³⁶⁰

The .eu TLD is regulated by:

- Regulation (EC) No 733/2002 implementing the .eu ccTLD;
- Commission Regulation (EC) No 874/2004, laying down public policy rules concerning the implementation and functions of such TLD, amended by Commission Regulation (EC) No 1654/2005, Commission Regulation (EC) No 1255/2007, Commission Regulation (EC) No 560/2009 and Commission Regulation (EU) No 2015/516;
- Regulation (EU) 2019/517 on the implementation and functioning of the .eu top-level domain name and amending and repealing Regulation (EC) No 733/2002 and repealing Commission Regulation (EC) No 874/2004.

The latter was adopted on 19 March 2019, entered into force on 18 April and will be effective starting from 13 October 2022, except for Article 20 (eligibility criteria), which is effective as of 19 October 2019.

The .eu domain name is also regulated by the .eu Registry's terms and conditions (**Terms and Conditions**) and the registration policy (**Registration Policy**).³⁶¹ As of 2 August 2021, new Terms and Conditions and Registration Policy entered into force.

The European Registry for Internet Domains (EURid), is a private, independent, non-profit organisation existing under Belgian law. EURid has been designated by the Commission as the .eu Registry since 21 May 2003.³⁶² For that purpose, the Commission entered into a service concession contract with EURid. The current service concession contract of EURid with the Commission has been extended until 12 October 2022.

The .eu Registry must observe the rules, policies and procedures laid down in the cited Regulations and the contract with the Commission.

Among other obligations (Article 2 of Regulation (EC) No 733/2002), the .eu Registry shall organise, administer and manage the .eu TLD in the general interest and on the basis of principles of quality, efficiency, reliability and accessibility, and to ensure the integrity of the databases of domain names. Article 10 of Regulation (EU) 2019/517 requires the .eu Registry to organise, administer and manage the .eu TLD in the general public interest and ensure in all aspects of the administration and management of the .eu TLD, high quality, transparency, security, stability, predictability, reliability, accessibility, efficiency, non-discrimination, fair conditions of competition and consumer protection, and ensure the availability and integrity of the databases of domain names.

Furthermore, the .eu Registry is required to adopt policies and implement measures against speculative and abusive registration of domain names, as this is fundamental to maintain a high level of trust in the .eu TLD.³⁶³ According to Article 21 of Commission Regulation (EC) No 874/2004 the term speculative and abusive registration is related to prior rights identified by Article 10(1).

³⁶⁰ <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0517>

³⁶¹ <https://eurid.eu/en/other-information/document-repository/>

³⁶² <https://eurid.eu/en/about-us/>

³⁶³ Article 5 of Regulation (EC) No 733/2002 and Article 9 of Commission Implementing Regulation (EU) 2020/857

The term of abuse, introduced by Commission Regulation (EU) 2015/516, is broader and is linked to the registrant's breach of the registration terms contained in Article 3 of Commission Regulation (EC) No 874/2004, including but not limited to material inaccuracy in the registration data as well as bad faith registration and infringement of third-party rights.

Regulation (EU) 2019/517 makes references to speculative and abusive registrations in recitals (7)³⁶⁴ and (17)³⁶⁵ and in Article 16 and to abusive registrations in recitals (18)³⁶⁶ and (20)³⁶⁷ and in Article 11(c)³⁶⁸ and speculative registration in Article 11(b)³⁶⁹. In the light of Article 14(1)(d), the registrations unsupported by rights or legitimate interests and the registrations used in bad faith are to be considered abusive registrations of domain names.

The Commission Implementing Regulation (EU) 2020/857 of 17 June 2020 laid down the principles to be included in the contract between the European Commission and the .eu top-level domain Registry in accordance with Regulation (EU) 2019/517.³⁷⁰

Under Article 2 of the Implementing Regulation, the .eu Registry shall contribute to enhancing the Union identity and promoting the Union values online. In particular, the .eu Registry, through its policies and its interactions with registrars, registrants and other stakeholders, shall promote openness, innovation, multilingualism and accessibility, freedom of expression and information, respect for human rights and the rule of law and shall take measures to promote users' security online and to respect users' privacy.

In accordance with Article 6 of the Implementing Regulation, the .eu Registry shall:

1. Ensure a high level of security for the network and information systems that it operates when managing the .eu TLD. In doing so, it shall put in place specific policies and comply with state-of-the-art cybersecurity risk management practices.

³⁶⁴ The Commission should promote cooperation between the Registry, the European Union Intellectual Property Office (EUIPO) and other Union agencies, with a view to combating the speculative and abusive registrations of domain names, including cybersquatting, and providing simple administrative procedures, in particular for small and medium-sized enterprises (SMEs).

³⁶⁵ The alternative dispute resolution (ADR) procedures to be adopted should comply with Directive 2013/11/EU of the European Parliament and of the Council and take into account the international best practices in this area and in particular the relevant recommendations of the World Intellectual Property Organization, to ensure that speculative and abusive registrations are avoided as far as possible. Those ADR procedures should respect uniform procedural rules that are in line with those set out in ICANN's Uniform Domain Name Dispute-Resolution Policy.

³⁶⁶ The policy on the abusive registration of .eu domain names should provide for verification by the Registry of the data that it receives, specifically data concerning the identity of registrants, as well as revocation and blocking from future registration of domain names considered by a final decision of a Member State court to be defamatory, racist or otherwise contrary to the law of the Member State. The Registry should take the utmost care to ensure the correctness of the data that it receives and holds. The revocation procedure should allow the domain name holder a reasonable opportunity to rectify any breach of the eligibility criteria, registration requirements or outstanding debts before the revocation is to take effect.

³⁶⁷ The Registry should adopt clear policies aiming to ensure the timely identification of abusive registrations of domain names and, where necessary, should cooperate with competent authorities and other public bodies relevant to cybersecurity and information security which are specifically involved in the fight against such registrations, such as national computer emergency response teams (CERTs).

³⁶⁸ A policy on abusive registration of domain names and a policy on the timely identification of domain names that have been registered and used in bad faith, referred to in Article 4

³⁶⁹ Requirements and procedures for registration requests, a policy on the verification of registration criteria, a policy on the verification of registrants' data, and a policy on the speculative registration of domain names

³⁷⁰ <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32020R0857>

2. Adopt a business continuity and recovery plan with prior written agreement of the Commission. The .eu Registry shall periodically revise the plan, with the prior written agreement of the Commission.
3. Provide registrars and registrants with state-of-the-art tools and technologies to protect themselves against cybersecurity threats and employ advanced methodologies to prevent abusive registrations.

EURid has accordingly stated that its mission is to create a trusted .eu space for the end-users in a sustainable way through operational excellence, all the while offering outstanding quality of service to its accredited registrars. In the past few years the focus has been put on quality instead of quantity.

.eu domain names can only be registered through a registrar accredited by the .eu Registry. Filing a request for domain name registration directly with the .eu Registry is not allowed. Therefore, the accredited registrars, via contract with EURid, provide domain name registration services to the registrants. There are over 700 registrars accredited by EURid.³⁷¹

The .eu Registry shall ensure both the **security and stability** of the .eu TLD and the **correctness of the WHOIS data** that it receives - and holds - from the registrar. According to the Terms and Conditions, the registrant has the following obligations:

- To keep its contact information accurate, complete, and up-to-date, both with the registrar with which the registrant has entered into an agreement and with the .eu Registry (via the registrar);
- Any email address communicated to the .eu Registry shall be a functioning e-mail address;
- To use the domain name in such a way that does not violate any third-party rights, applicable laws, or regulations, including discrimination on the basis of race, language, sex, religion, or political view;
- Not to use the domain name in bad faith or for any unlawful purpose.

Pursuant to the provisions of the registrar agreement (Registrar Agreement) (Article 4.1), the registrar shall ensure and document that each registrant for whom it registers a domain name has accepted the rules in effect at the time the registration is carried out and complies with all requirements set forth in all Regulations and rules applicable to the .eu, Registration Policy, Terms and Conditions, the WHOIS policy, the ADR rules and the ADR supplemental rules (jointly, Rules), including but not limited to the confirmation by the registrant that, to its knowledge, the request for domain name registration is made in good faith, does not infringe the rights of any third party and will not be used for unlawful purposes.

The .eu Registry:

- Shall block the domain name, where it is informed that an ADR procedure or legal proceedings are pending, until such proceedings are terminated and the .eu Registry has been notified of the relevant decision; in this case the domain name cannot be transferred to a new registrant and/or to another accredited registrar, and the registrant cannot change its contact information with respect to the blocked domain name;
- Shall revoke any domain name following a decision to that effect of a panel in an ADR procedure or court order;
- May revoke the registration of a domain name on its own initiative and without submitting the dispute to any non-judicial settlement of conflict procedures, on the grounds of non-fulfilment by the registrant of the eligibility criteria or breach of the Rules by the registrant (e.g., inaccuracy of the registration data).

³⁷¹ <https://eurid.eu/en/register-a-eu-domain/find-a-registrar/>

The .eu Registry enters into the same accreditation agreement with all registrars, thus the identification requirements are the same for all registrars. However, the way they apply any identification mechanism at their end is discretionary. By contract, the registrars shall provide EURid with accurate and up to date registration data. All documentation received by the .eu Registry is expected to be genuine and correct.

The .eu Registry has recently implemented a **Know Your Business Customer (KYBC) procedure**³⁷²:

- Verification via electronic identity card (eID): currently only for registrants with a Belgian electronic identity card;
- Verification via MRZ scan and SMS: for domain name holders with a mobile phone and an identity document with a Machine-Readable Zone from one of the European Union Member States, Iceland, Liechtenstein, or Norway.

To comply with its obligation of guaranteeing the security and stability of the .eu TLD and the correctness of the data, EURid carries out **verifications**. Thus, such verifications are related to the necessity of maintaining data accuracy and preventing illegal activities which could pose cyberthreats. Registrants with bad intentions likely use inaccurate data to hide their identity. Accurate registration data can help law enforcement authorities to actually identify the domain holders responsible for illegal activities and go after them via appropriate channel.

The .eu Registry performs different verifications of the registration data in relation to all newly registered domain names or already registered domain names for which the contact data has been updated.

EURid employs an **automated process** to check if the registration data mentions a valid physical address to which a letter could be delivered. The checks are made against official postal address databases from 240 countries around the world by a single partner with which EURid has a contract until the end of its mandate in 2022. The address validation checks take place on a daily basis.

In case the registrant is a company, EURid may check the company data against KBO (Belgian Companies Register) or EU national databases to verify if the company is validly registered. EURid has the possibility of carrying out such **cross-checks**.

EURid also checks newly registered domain names against the Domain Generation Algorithm (DGA) archive, a repository of domain names generated by algorithms. These domains are used in botnets and other DNS abuses in most cases.

EURid does not check all newly registered domain names manually before they are delegated, but with the help of a predictive algorithm. The **Abuse Prevention and Early Warning System (APEWS)**³⁷³, developed by EURid in collaboration with the University of Leuven, checks all newly registered domains in an automated way and uses machine-learning algorithms.

The general goal of such system is to reduce the amount of cyberthreats by detecting and preventing malicious domains upon registration. APEWS is an innovative and award-winning methodology based on evaluating patterns of domain name registrations. It predicts whether a domain name may potentially be used for malicious activities (spam, phishing, malware, botnet command-and-control). The current focus of such system is only on such kind of abuses. The legal basis for EURid developing

³⁷² https://eurid.eu/en/register-a-eu-domain/data-quality/#nav_kyc_project

³⁷³ https://eurid.eu/en/register-a-eu-domain/data-quality/#nav_apews

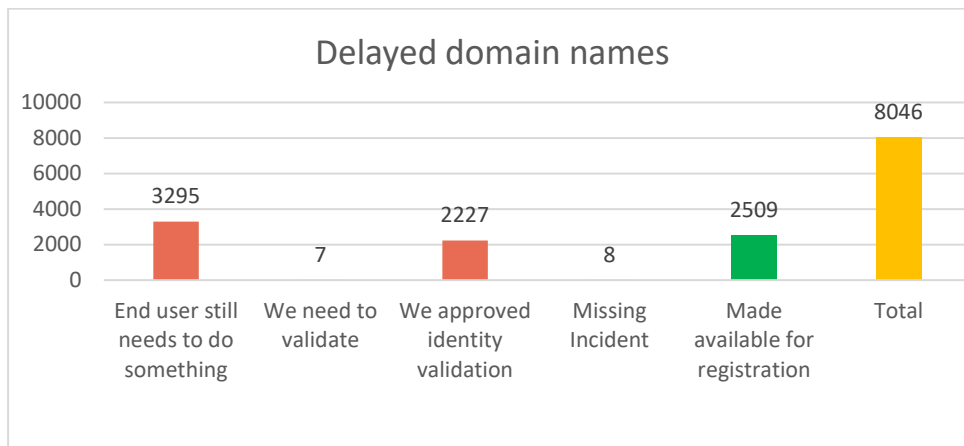
and using such system is Article 3(3) as amended by Commission Regulation (EU) 2015/516, according to which the verification on EURid's part of the validity of the registration applications takes place prior and not only subsequently to registration at the initiative of EURid or pursuant to a dispute for the registration of the domain name in question.

The system can be summarised as follows. APEWS uses the registrant data (domain name, registration time, registrant's contact information, registrar, nameserver information, IP address geolocation data) as part of its detection strategy combined with clustering to make similarity-based predictions, as well as traditional machine-learning techniques to perform reputation-based classification (public blacklists of malicious domains). First, parts of the 3.6 million .eu domain names were matched against blacklists of reputation providers, containing lists of domain names associated with Internet-based attacks. Every detail of the matching domain names was then used to train the predictive model. This resulted in a comprehensive scoring model. Every newly registered domain name is scored by APEWS on these predictive indicators. If the score is too low and, thus, the domain name is identified as potentially linked to abuse, its delegation in the .eu zone file is delayed and its status in the web-based WHOIS shows 'Server Hold'. The domain name is registered. However, any service linked to it (such as a website, email or any other service) will not function until EURid's verification procedure is completed. Moreover, post-delegation APEWS looks into the domain names registered in the last 24 hours and does the necessary check to detect suspicious activities. In 75% of the cases where the system flagged a domain name, the prediction was confirmed by third-party abuse indicators.

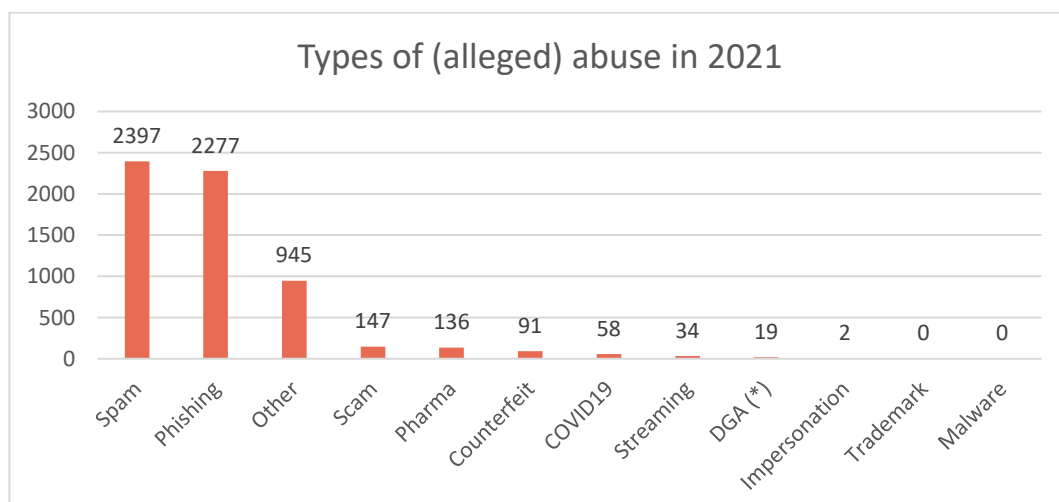
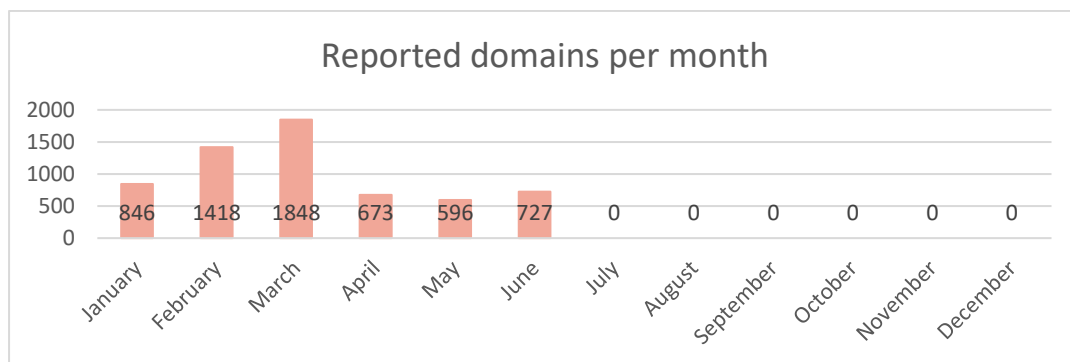
If any issue arises from the above verification, EURid carries out a **WHOIS accuracy procedure**, which consists of the following steps:

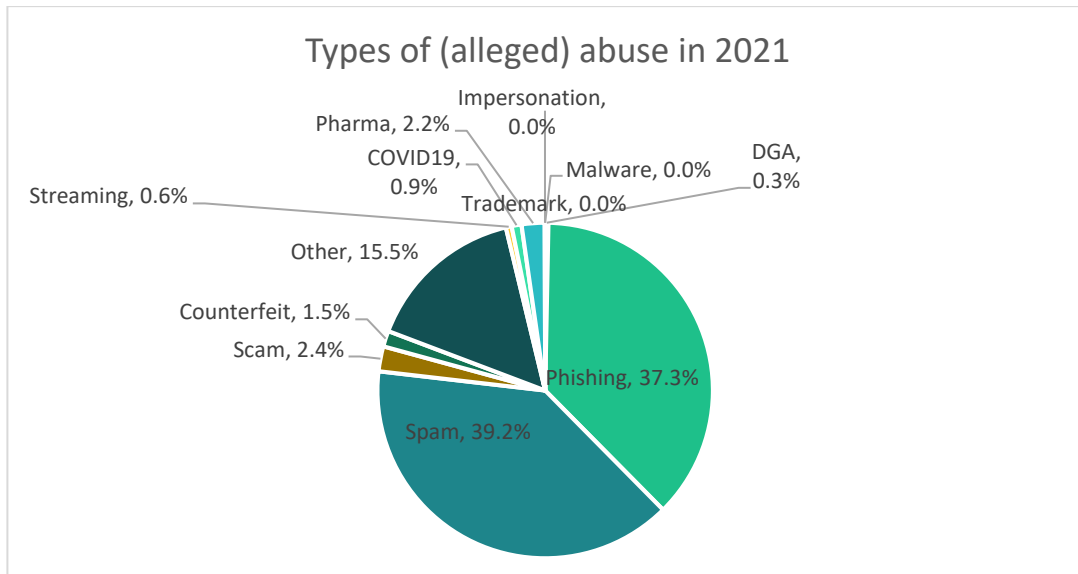
- An email notification is sent to the registrant requiring to provide (within 14 calendar days) documentary evidence that the registration data is accurate;
- If no satisfactory response is received in due time, the .eu Registry may suspend the domain name;
- In some cases, where potentially malicious activity is related to the domain name (e.g., domain name is part of a known malware campaign), EURid may shorten that reply period to 3 calendar days or even shorter, depending on the severity of the abuse and the potential impact on consumers. This fast track procedure is exceptional and requires approval from EURid's Managing Director for notifications less than 3 days.

As mentioned above, malicious actors have also exploited the COVID-19 pandemic to perpetrate scams and victimise Internet users. Indeed, a significant rise of new domain registrations associated with the pandemic has been encountered under all TLD extensions. The .eu TLD has also been affected by such phenomenon. In response to such emergency situation EURid, in agreement with the European Commission, has adopted measures in order to prevent bad faith registration of domain names relating to the pandemic. EURid has amended its APEWS system, by performing additional checks on the registration data of both existing registrations and newly-registered domain names that contain keywords such as Corona, COVID, Dexamethasone, Hydroxychloroquine, Interferon, Monoclonal, Pandemic, SARS-COV, Vaccine, Virus. For suspicious domain names detected by APEWS, EURid carries out a WHOIS accuracy procedure, requiring the registrants to validate their data and to submit a statement confirming that their domain name was registered in 'good faith' within 7 calendar days. The delegation of any domain name containing one of the agreed key words is delayed within the APEWS system framework. The daily number of delayed domain names containing one of the keywords above from 1 April 2020 until 1 July 2021 is as follows:

Figure 27: Delayed COVID-19-related domains (source EURid)

EURid also cooperate with law enforcement authorities reporting suspicious COVID-19-related domain names. The overall statistics of domain names reported to CERT.be, Belgian Federal Public Service Economy and Europol in 2021 is as follows (**Figure 28-30** – source EURid):





APEWS is considered a useful and innovative AI-driven proactive suspension system for malicious domain names, in particular those involved in the distribution of malware, phishing, spam, botnet command-and-control. It is not used to prevent (directly) domain names infringing IPR. IPR holders might use other measures to learn about possible abuses (Whois lookup, EUIPO's availability check and alert) and it will be up to them to take (reactive) action (e.g., .eu ADR).

Finally, EURid employs other technologies to reduce potential fraudulent domain name usage (e.g., **Domain Name System Security Extensions - DNSSEC, Registry Lock**³⁷⁴). EURid provides **discount on registration fee** for DNSSEC enabled domain names. Moreover, the .eu Registry has in place the so-called **DNSQuality Score**. The DNSQuality score is a feature developed by EURid and it is a visual reflection of the quality of the DNS (Domain Name System) setup of a given domain name.³⁷⁵ EURid performs weekly, technical checks on every active domain name, calculating a new DNSQuality Score each week via a sequence of tests. These tests are performed for every domain name which has at least one linked name server and an 'In Use' status. Each test allocates a certain number of points, and the total number of points is calculated to obtain a DNSQuality score expressed as a percentage. Tests include:

- Whether a domain name is reachable over IPv4 and IPv6;
- Whether all of the name servers linked to the domain name are responsive;
- Whether the domain name is enabled with the 'Domain Name Security Extensions' (DNSSEC).

Domain name holders can look-up the DNSQuality scores of domain names that they have registered via their account.

As for content monitoring, EURid runs daily **manual content checks** on domain names 24 hours after the registration, as well as 53 days after the registration (to give some time to registrants to set up a web site), looking for keywords such as brands, bank names, drug names. The checks are based on past experience with brands subject to abuse or originate from daily de visu checks. The daily checks may reveal a specific brand subject to abuse on a specific day, thus adding to a growing list. For practical reasons, not all brands or trade marks are added to such list, as it would contain millions of brands. Such list is limited to the ones spotted on a daily basis. EURid also crawls the above-mentioned domain names and collects the main page

³⁷⁴ <https://eurid.eu/en/my-eu/>

³⁷⁵ <https://eurid.eu/en/my-eu/>

of the website to which the domain name resolves (if it exists). Then, the page content is analysed, looking for webshops. The identification of keywords corresponding to well-known trade marks or typos of well-known trade mark is random and based on EURid's knowledge, not related to any cross-checks in trade mark databases. If the .eu Registry considers a domain name suspicious, it initiates a WHOIS accuracy procedure which can result in the suspension and withdrawal of the domain name. Additionally, EURid might **report suspicious domain names** to the competent authorities, such as Europol and CERT.

These regular checks are also run ad-hoc whenever needed on specific lists of suspicious delegated domain names. At present content monitoring is still in the research phase with a mix of manual and automated procedures. To date, on a daily basis EURid detects 10-20 dubious domain names and the legal department of EURid initiates the WHOIS accuracy procedure on such domain names. If the identity is proven by the registrant but the data is suspicious, the results of EURid's scans are shared with **relevant parties who can take further actions** (e.g., Europol, sectorial representative such as ASOP). The long-term objective of EURid is to introduce an automated procedure. However, classifying websites as suspicious remains challenging. The final assessment as to whether the domain name is abusive falls outside EURid's mandate and shall be made by the competent authorities and by entities with which EURid has collaborations.

Within the WHOIS search, EURid implemented the **functionality of searching** for possibly similar registered domain names, based on visual resemblance and using a similarity score. Such functionality enables .eu domain name holders to check if possibly infringing domain names are registered. Within the similarity score zero means that no visual difference exists in practice between the original domain name and the one with that score in one of the possible ways it could be written (capitals or lowercase). For example, ikea (Latin) and ικέα (Greek) may look quite different, but if it is written in capitals IKEA (Latin) and ΙΚΕΑ (Greek), then the difference is much smaller, explaining the low score.³⁷⁶ The holder of a .eu domain name (for example, ikea.eu) may request and receive from EURid the full list of registered domain names that share striking similarities with its domain name.

Moreover, the 'Tools' functionality within the WHOIS search enables users having a complaint or issue with a registered domain name to file such complaint:

- Inaccurate registrant data: anybody spotting wrong data may inform EURid with the aim of bringing further investigation;
- Dispute registration is meant to inform those who think their rights have been infringed and explain possible solution to them;
- The 'Request an authorisation code' feature was introduced to help the registrant of the domain name to transfer his or her domain name from the current registrar to another one. Normally, the registrar shall execute such request, but in case there is any kind of conflict between the registrant and his or her registrar, the registrant may request a transfer code directly from EURid to avoid that he or she (or rather the domain name) is held hostage by the registrar. EURid monitors the release of authorisation codes on a regular basis to detect possible macro issues at the registrar level.

The website of EURid provides **general information** is provided on how to contact the domain name holder and on the .eu ADR.^{377 378}

³⁷⁶ <https://whois.eurid.eu/en/search/?domain=ikea.eu>

³⁷⁷ <https://eurid.eu/en/other-information/faq/i-wish-to-register-a-eu/#someone-registered-a-domain-name-that-i-want-or-that-i-have-a-better-claim-to-than-its-current-holder-what-do-i-do>

³⁷⁸ <https://eurid.eu/en/register-a-eu-domain/domain-name-disputes/>

Third parties with legitimate interests may request the disclosure of the personal data of a .eu domain name holder by submitting the **personal data disclosure form**.³⁷⁹

The request form should mention:

- The domain name for which the request is completed;
- The legitimate interest regarding the disclosure of personal data;
- How the requested data is intended to be used.

The request form for disclosure of personal data is to be sent to EURid by email or fax. The form is reviewed by EURid and, if data is disclosed, it usually takes a couple of days, up to a maximum of 30 days.

The .eu Registry has in place the following **collaborations**:

- European Union Intellectual Property Office (EUIPO)
- Europol³⁸⁰
- Belgian Customs (against counterfeit websites)
- Belgian Prosecutors and law enforcement authorities (against cybercrime)
- Association for Safe Online Pharmacy (ASOP) (against rogue pharmacies)
- International AntiCounterfeiting Coalition (IACC) (against counterfeit websites)
- eCommerce Foundation (against fake e-shops)
- Anti-Phishing Working Group (APWG) (against phishing)
- Belgian Computer Emergency Response Team (CERT).

EURid's collaboration with the EUIPO consists in:

- Availability check through EUIPO: at the time of filing of a European Union trade mark (EUTM) application, EUTM applicants can check if an equivalent .eu domain name is available and, if so, register it with the accredited registrars;
- Alert through EUIPO: EUTM applicants and holders can opt-in to receive alerts as soon as a .eu domain name is registered that is identical to their EUTM (application);
- Information (link to EUIPO) within EURid's Whois search regarding EUTM availability and registration.

EURid's collaboration with ASOP consists in:

- Based on examples of rogue pharma websites that are provided to EURid by ASOP EU (with the support of ASOP Global), EURid detects similar "suspicious" websites hosted at .eu domains;
- EURid shares with ASOP EU new suspicious cases that have been identified, and seeks its advice (based on feedback from an expert group within the National Association of Boards of Pharmacy – NABP) where the suspicious website is either confirmed as rogue pharma site or dismissed as legitimate;
- If ASOP EU informs EURid about a rogue pharma site that has not been detected (or created after EURid checks), EURid starts the ID check and integrates the ASOP EU findings into the detection system;
- Using the website page examples, EURid creates a list of trade mark and keywords to investigate if domains containing them host rogue pharma;
- In any of the cases listed above, EURid starts a registrant ID check process. If registrant does not answer or cannot prove its ID, the domain is suspended. Indeed, EURid does not have the mandate, nor the authorisation to suspend domains based on website content, only on inaccurate Whois data.

³⁷⁹ <https://eurid.eu/en/about-us/document-repository/>

³⁸⁰ <https://eurid.eu/en/news/eurid-joins-nmr-project/>

- The EURid detection system works automatically but there is always a human check on suspicious cases. This double check system enables learning to take place with continual improvement via adaptations.

.dk

The total number of the .dk registrations is 1,330,606.³⁸¹

The .dk domain name is regulated by the Danish Act on Internet Domains (Domain Names Act)³⁸², enacted in 2014 and administrative orders related to such act. The administrative orders are issued by the Danish Business Authority which supervises the .dk Registry. The law no. 436 on network and information security for domain name systems entered into force in 2018. The Terms and Conditions (version 10) is effective since 1 March 2019.³⁸³

The .dk TLD is administered by DK Hostmaster. DK Hostmaster comes from a sole registry tradition, and even if registrars³⁸⁴ have always been able to sell .dk domain names and are authorised to manage domain names on behalf of registrants, DK Hostmaster still maintains a direct relation with the registrants. Partly to protect the registrant's consumer rights and also to uphold accountability and data accuracy measures towards them.

There is no eligibility criteria for the registration of .dk domain names.

Pursuant to Article 18 of the Domain Names Act, DK Hostmaster has to ensure an **accurate, updated and public WHOIS database**, containing information about registrant's name, address, and telephone number (both for natural and legal persons). The purpose of this provision is to establish a high-quality system with as much transparency as possible. Anyone should be able to find out the identity of a registrant and thus the person behind a specific domain name.

The registrant must provide accurate contact information. In order to secure accurate and updated registration data, DK Hostmaster performs the **verification of the registrant's identity and contact information**. Danish domain registrants are required to identify themselves using NemID, a system of electronic identification used by Danish banks, government websites, and other private companies. DK Hostmaster also cross-checks the registrant data of Danish residents with national databases of Civil Registration System (CPR) and Central Business Register (CVR). Foreign registrants are subject to a risk assessment, which will determine whether they receive a request to provide proof of identity before registration - high risk - or up to 30 days after registration - low risk (no-risk customers are not required to provide proof)³⁸⁵. When a high risk of inaccurate registrant data exists, delegation must await the approval of requested documentation. The approval process takes 24 hours from the receipt of the documentation. If the domain holder cannot or will not provide proof of his or her identity, the domain name is suspended and subsequently deleted. Data and ID checks has been carried out for each domain name registration request since November 2017.

³⁸¹ https://media.nominet.uk/wp-content/uploads/2021/05/The-Online-World-2020.pdf?_ga=2.208900692.715335191.1627204478-835102325.1621419253

³⁸² <https://www.retsinformation.dk/eli/ta/2014/164>

³⁸³ <https://www.dk-hostmaster.dk/en/terms>

³⁸⁴ https://selvbetjening.dk-hostmaster.dk/registrar_list

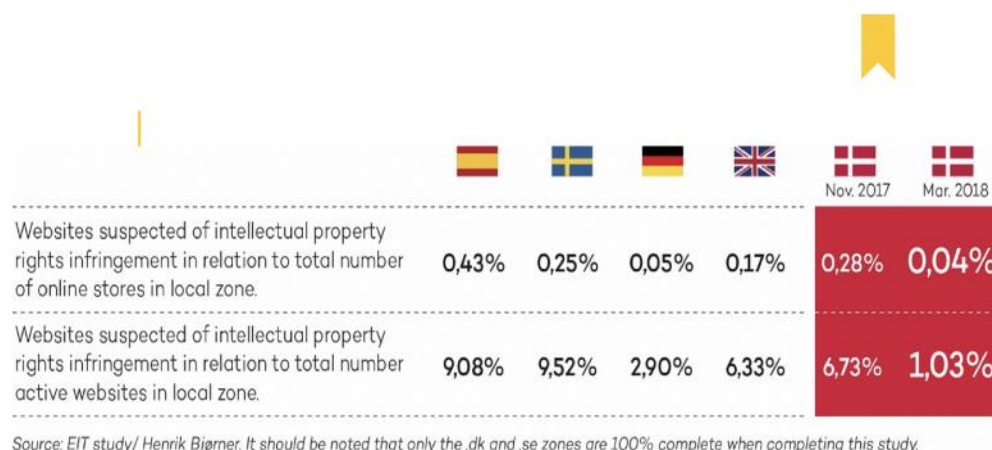
³⁸⁵ [https://www.dk-hostmaster.dk/sites/default/files/2017-12/Procedure for kontrol af kontaktoplysninger og id for reg med bopael udenfor DK EN.pdf](https://www.dk-hostmaster.dk/sites/default/files/2017-12/Procedure%20for%20kontrol%20af%20kontaktoplysninger%20og%20id%20for%20reg%20med%20bopael%20udenfor%20DK%20EN.pdf)

DK Hostmaster uses **algorithms** in the automated risk assessment on registrant data, which are part of any registration from an applicant outside Denmark. Some of these algorithms are designed to respond to registration characteristics associated with domain name registrations linked to fake webshops, e.g., illogical data combinations, how quickly a domain name is re-registered and the registrar. This changes as time goes on and other characteristics might become more relevant. The reasoning behind the algorithms is that online criminals tend to use inaccurate registrant data, but, in any case, DK Hostmaster only looks at data and patterns relating to the registration of a domain name.

If .dk Registry receives a notification regarding reasonable suspicion that the identity information of a registrant in the WHOIS is not correct .dk Registry shall **investigate the accuracy of the WHOIS information** and delete the domain name registration if the information is incorrect and not corrected.

Article 18 of the Domain Names Act and DK Hostmaster's strict ID-verification together has contributed to the significant decrease of illegal websites, since registrants cannot be anonymous.

Figure 31: Percentage of fake webshops in Denmark 2017-2018 (source DIFO)



Source: EIT study/ Henrik Bjørner. It should be noted that only the .dk and .se zones are 100% complete when completing this study.

Source: DIFO

DK Hostmaster does not monitor the content of websites, since this does not fall under its mandate as registry and can be done better and in compliance with due process safeguards implemented by law enforcement authorities (LEA). The .dk Registry **collaborates** with different police authorities, consumer protection authorities and the national information security authority. Information is readily accessible on how to lodge an abuse report.³⁸⁶

In 2020, the Danish Business Authority introduced certain obligations on the .dk Registry concerning **DNSSEC**. Article 12 of the Executive Order (BEK nr 44 af 14/01/2020 (Gældende) provides that the .dk Registry's systems must be able to support the introduction of Domain Name System Security Extensions (DNSSEC) and be arranged in such a way that the system provides a quick and easy access to DNSSEC signing of domain names under .dk. The .dk Registry must require registrars who offer domain names under .dk to support DNSSEC not later than 1 January 2021 and offer DNSSEC signing to registrants. If the registrar does not offer a name server

³⁸⁶ <https://www.dk-hostmaster.dk/en/how-complain-about-website-content>

service, the registrar must inform the registrant where DNSSEC signing can be carried out. In order to facilitate the deployment of DNSSEC, the .dk Registry may charge differentiated rates for maintaining a domain name registration, depending on whether or not the domain name is DNSSEC signed.

Other ccTLDs

Other European ccTLD registries also have in place practices and measures similar to those of the registries mentioned above (.eu, .dk), which contribute to reduce malicious activities on the Internet. These measures range between preventive and reactive measures.

DNS Belgium, the registry operator of **.be**, also performs **preventive automated checks on registration data** as soon as the domain name is registered, but before activation (delegation).³⁸⁷ This procedure consist of the following steps:

- An automated system checks the registrant data of a domain name during registration. When a number of parameters determine that something is wrong with the data, the domain name is not yet activated.
- The registrant and registrar will receive an email from DNS Belgium requesting proof that the registrant data are correct.
- The registrant send by email a document to verification@dnsbelgium.be that shows that the registrant data are correct.
- DNS Belgium evaluates the documents and activates the domain name within 5 working days if the documents are sufficient.
- If the documents do not provide sufficient proof that the registrant data is correct, DNS Belgium requests more information. The domain name remains registered but it cannot be used.
- If the necessary documents are not sent to DNS Belgium, the domain name remains registered but it cannot be used.

After activation (delegation), DNS Belgium may perform **checks of the accuracy of the registration data**, either on its own initiative, or following a complaint from a third party or the government. Registrants shall be required to cooperate actively in such checks and must share the necessary documents in support of the correctness of the data. If DNS Belgium has serious doubts about the accuracy of the registrant's contact data, it may suspend the domain name concerned (disable it) and then initiate an infringement procedure pursuant to Article 3.d of the Registration Terms and Conditions.³⁸⁸ The registrant has 14 days to correct the wrong or incomplete contact data. If he or she fails to rectify, the domain name is withdrawn. Besides the manual checks, there is a complaint form available to report problematic registrant data. Furthermore, DNS Belgium deploys several techniques to do their own research as well. The .be Registry has a set of parameters that are used to automatically evaluate registrant contact data: validity of Belgian postal codes, validity of telephone number format (e164), etc.

In December 2018, DNS Belgium established a **Notice & Action procedure** in collaboration with the Belgian Federal Public Service for Economy (FPS Economy) to block (suspend) .be domain names used for fraudulent webshops and/or hosting phishing websites.³⁸⁹ At the FPS Economy's request, the .be Registry applies the N&A protocol and makes the domain name inaccessible. The URL of the website redirects users to a warning page of the FPS Economy. The registrant has 14 days to react and provide his/her bona fide. After 6 months, the blocked domain name expires.

³⁸⁷ <https://www.dnsbelgium.be/en/internet-security/prevention>

³⁸⁸ https://assets.dnsbelgium.be/attachment/Enduser_Terms_and_Conditions_en_v6.1_1.pdf

³⁸⁹ <https://www.dnsbelgium.be/en/news/fraudulent-websites-offline>

Thanks to the procedures put in place by DNS Belgium, illegal practices involving .be domain names have decreased since 2019.³⁹⁰

SIDN, the registry operator for .nl, also uses **machine learning technology to automatically check all .nl domain name registrations** and to predict if they will be used abusively. The technology was developed to detect fake webshops as early as possible (at the moment of the registration, but before the website is activated). The same is also used to identify other forms of abuses, such as phishing and malware propagation. In case of detecting suspicious domain names, SIDN contacts the registrar. The registrar does its own checks and has the power to take down fraudulent sites. If a registrar is not willing to help, SIDN checks the registration data. The data linked to malicious activities is nearly always false. SIDN can delink the name servers if the registrant's identity is not confirmed within five days. Delinking has the effect of making the domain name and its website unreachable. SIDN reported that over 5,000 fake web shops were taken down in 2018³⁹¹ and nearly 4,500 in 2019³⁹².

Moreover, SIDN offers **Domain Name Surveillance Service (DBS)**³⁹³, a monitoring service that flags up typo squats and brand name abuse on the Internet and gives rightholders the option of taking immediate legal action.

In 2017, SIDN also established a voluntary **Notice and Take Down procedure**³⁹⁴ based on the Dutch Notice and Take Down Code of Conduct. The Code is intended for dealing with child pornography, plagiarism, discrimination and the sale of illegal or stolen goods, etc. A request can be filed with SIDN if the referral path (1. content provider, 2. website administrator, 3. registrant of the domain name, 4. registrar / hosting service provider) has been exhausted and the content has not been taken down by other intermediaries. Upon receipt of the request and further to assessment with the help of partners organisations (e.g., CSAM - Reporting Hotline for Internet Child Pornography), SIDN disables domain names with clearly criminal or unlawful content only as a last resort.

The current **.hu** Registration Rules and Procedures³⁹⁵ (Paragraphs 2.2.1 and 2.3.2), in force since 1 July 2021, require domain registrant to act with utmost care in choosing the domain name so as the application, the domain name, and its usage shall not violate the rights of other persons or entities (e.g. the right of exclusive names, the right of privacy, the right of reverence, the right of intellectual property, etc.). Domain applicants are expected to **check** the commercial register or major trademark databases before choosing the domain name.

Furthermore, the .hu domain name registration procedure provides for **delayed delegation** of all domain names, meaning that upon submitting a domain name registration request, the application is published at the .hu Registry (ISZT) website's announcements section.³⁹⁶ During the **announcement period** (8 days) the domain name applicant is granted the conditional right of using the domain name, meaning that the domain name is entered in the zone file, but remains undelegated to the applicant (Paragraph 1.2.3.7). Any third party who has a legal interest to state that the delegation of a domain name to a particular applicant infringes the rules may file an

³⁹⁰ <https://www.dnsbelgium.be/en/news/block-fraudulent-websites>

³⁹¹ <https://www.sidn.nl/en/news-and-blogs/fake-webshops-taken-off-line-much-sooner>

³⁹² <https://www.sidn.nl/en/news-and-blogs/nearly-4500-fake-webshops-taken-down-in-2019-following-detection-by-SIDN>

³⁹³ <https://www.sidn.nl/en/product/dbs>

³⁹⁴ <https://www.sidn.nl/en/nl-domain-name/complaining-about-the-content-of-a-website>

³⁹⁵ <https://www.domain.hu/domain-registration-policy/>

³⁹⁶ <https://www.domain.hu/domain-announcement/>

objection requesting the Consulting Board³⁹⁷ of the Alternative Dispute Resolution provider (Infomediátor³⁹⁸) to hear the dispute (Paragraph 9).

Norid, the registry operator of **.no**, requires the domain registrants be registered in the Norwegian National Registry (Folkeregisteret) if individuals or the Central Coordinating Register for Legal Entities (Enhetsregisteret) if corporations.³⁹⁹ Regular **checks** are carried out by Norid to verify the existence of domain holders and if an legal entity closes its operations in Norway (cancelled from the Central Coordinating Register for Legal Entities), the domain name is automatically removed from the root zone (except for the cases of transfer of the domains to individuals who have right to register a .no domain name).

The following ccTLD registries provide easy to access **information on how to report different types of abuses**:

- DNS Belgium (.be)⁴⁰⁰
- AFNIC (.fr)⁴⁰¹
- NIC.at (.at)⁴⁰²
- Nominet (.uk)⁴⁰³
- Norid (.no)⁴⁰⁴

c. Overview and assessment of gTLD and ccTLD good practices

The following table summarizes the good practices identified above:

Type	Good practices	Example
Preventive	Anti-abuse / acceptable use policy	PIR, Donuts, .eu, .hu
	KYBC procedure	.eu, .dk
	Employment of machine learning predictive technology to identify abusive registrations	.eu, .nl
	Delayed delegation	.eu, .dk, .hu
	Cross-checks in public databases	.eu, .dk, .no
	Incentive programs (discount) to promote healthy registrations	PIR, .eu
	DNSSEC deployment and other security solutions	PIR, .eu, .dk, .nl, .se, .cz, .no, .sk
	Preventive blocking services	Donuts, UNR
Reactive	Regular WHOIS accuracy verification	.eu, .dk, .be, .no, .hu
	Manual content check	.eu
	Surveillance / search service	.be, .nl
	Collaborations with LEA and trusted notifiers	PIR, Donuts, .eu, .dk, .be
	Notice & take down procedures	.be, .nl
	Appeal mechanism against suspension before third neutral party	PIR
Transparency and information	Publication of abuse metrics and statistics	PIR

³⁹⁷ <https://www.domain.hu/alternative-dispute-resolution/consulting-board/>

³⁹⁸ <https://infomediator.hu/>

³⁹⁹ <https://www.norid.no/en/om-domenenavn/regelverk-for-no/#link5>

⁴⁰⁰ <https://www.dnsbelgium.be/en/internet-security/reporting-web-misuse>

⁴⁰¹ <https://www.afnic.fr/en/domain-names-and-support/resolve-a-dispute/report-a-domain-name/>

⁴⁰² https://www.nic.at/en/good_to_know/security/stopline

⁴⁰³ <https://www.nominet.uk/complaints/#website>

⁴⁰⁴ <https://www.norid.no/en/konflikt-om-domene/ulovlig-innhold/>

	Foreseeable response time to abuse reports	Donuts
	Easy to access information on how to report abuse / abuse point of contact	Donuts, .eu, .be, .fr, .at, .uk, .no
	Adherence to voluntary / self-regulatory initiatives promoting collaborations among DNS service providers	PIR, Donuts

gTLDs' practices in contrasting DNS abuse vary significantly. While all gTLD operators have to follow ICANN consensus policies and fulfil the same obligations provided for by their contracts (RA), some of them adopt more proactive approach in contrasting malicious activities in their TLDs, by putting in place technical and contractual measures (e.g., price incentives and technical support for DNSSEC adoption, and incentives for "healthy" registrations), offering services to IPR holders, although for a fee (e.g., preventive registration blockings, surveillance and search), improving the transparency of abuse handling mechanisms, and building collaborations with trusted notifiers that all contribute in reducing malicious activities.

The measurements of the authors show that EU ccTLDs are by far the least abused in absolute terms and relative to market share (see Appendix 1 – Technical Report). Only 0.8 percent of all abused (compromised and maliciously registered) domain names were registered under EU ccTLDs.

Although specificities in the regulation and practices of the ccTLDs exist and might depend on their national legal frameworks, the harmonisation through the adoption of good practices available at the European and international market would enhance online security and EU citizens' and businesses' trust in the DNS and generally in the Internet.

Therefore, other gTLDs and ccTLDs should consider to adopt one or possibly more of the above-mentioned good practices in order to reduce and effectively mitigate DNS abuse.

11. Solutions and recommendations to mitigate DNS abuse

Based on the primary and secondary research conducted to measure the DNS abuse phenomenon (Section 7), and the extensive analysis of the regulatory framework (Section 9) and the good practices (Section 10), the authors propose the following set of recommendations.

Type(s) of abuse to be addressed	Which actor(s), DNS service provider / third-party addressee, should act?	Which institution(s) should impose the obligation or which entity should encourage collaboration?	Recommendation	Source / support
A. Better DNS metadata (for identifying resources and their attribution to intermediaries)				
Type 1 - Abuse related to maliciously registered domain names	ccTLD registries	European Commission, EU co-legislators, Member States technical standardization bodies, industry associations	1. Provide a scalable and unified way of accessing complete registration (WHOIS) information (in compliance with data protection laws), using the Registration Data Access Protocol (RDAP), necessary to attribute abused and vulnerable domain names to their respective registrars and obtain their contact information.	Appendix 1 – Technical Report, Section 6, p. 27
Type 2 - Abuse related to the operation of the DNS and other infrastructures	ccTLD registries	European Commission, EU co-legislators, Member States technical standardization bodies, industry associations	2. Publish DNS zone file data through DNS zone transfer or a system similar to the Centralized Zone Data Service (CZDS) maintained by ICANN.	Appendix 1 – Technical Report, Section 5, p. 26
Type 3 - Abuse related to domain names distributing malicious content				
B. Contact information and abuse reporting				
Type 1 - Abuse related to maliciously registered domain names	gTLD and ccTLD registries and registrars	ICANN, European Commission, EU co-legislators, Member States technical standardization bodies, industry associations	3. Display email addresses of registrants and domain name administrators that are otherwise not visible in the public WHOIS as anonymized email addresses to ensure the ability to contact domain owners and administrators directly to notify security vulnerabilities and domain name abuse.	Appendix 1 – Technical Report, Section 18.4, p. 79
Type 2 - Abuse related to the operation of the DNS and other infrastructures	Domain name administrators	ICANN, European Commission, EU co-legislators, Member States technical standardization bodies,	4. Maintain standard email aliases for given domain names (e.g., abuse, hostmaster, webmaster) to notify security vulnerabilities and domain name abuse.	Appendix 1 – Technical Report, Section 18.4, p. 79
Type 3 - Abuse related to domain names distributing malicious content				

		industry associations		
	All DNS operators and intermediaries	ICANN, European Commission, EU co-legislators, Member States technical standardization bodies, industry associations	5. Set up a standardized (and potentially centralized) system to access to registration data (WHOIS data), identifying the minimum information necessary to process disclosure requests. The reaction time to such requests shall be clearly defined.	Section 9.b, law enforcement authorities, cybersecurity investigators, network technology professionals, child protection organisations, patient safety organisations, consumer protection organisations, and anti-counterfeiting and anti-piracy organisations
	All DNS operators and intermediaries	ICANN, European Commission, EU co-legislators, Member States technical standardization bodies, industry associations	6. Set up a standardized (and potentially centralized) system for abuse reporting, identifying the minimum information necessary to process such report. The receipt of abuse reports is to be acknowledged. The reaction time to such reports shall be clearly defined and the abuse reporter should be provided with information on the actions taken. The DNS service providers shall provide for an appeal proceeding against their decisions to a third neutral party.	Sections 9.f-g, and 10.a, law enforcement authorities, cybersecurity investigators, network technology professionals, child protection organisations, patient safety organisations, consumer protection organisations, and anti-counterfeiting and anti-piracy organisations
	Computer Emergency Response Teams (CERT), security organisations	European Commission, EU co-legislators, ENISA, Member States and national authorities	7. Exchange information on threats between parties involved (e.g., CERTs, security organisations) using collaborative platforms such as Malware Information Sharing Platform (MISP) to report and mitigate abuse in a more effective and timely manner.	

C. Improved prevention, detection and mitigation of DNS abuse related to maliciously registered domain names

Type 1 - Abuse related to maliciously registered domain names	gTLD and ccTLD registries, registrars, and resellers	ICANN, European Commission, EU co-legislators, Member States	8. Verify the accuracy of the domain registrant (WHOIS) data, by employing KYBC procedures and cross-checks in publicly available databases.	Section 10 and Appendix 1 – Technical Report, Section 9.2, p. 35
	gTLD and ccTLD registries	Industry associations	9. Develop or improve existing similarity search tools or surveillance services to enable third-parties to	Section 10 and Appendix 1 – Technical

			identify names that could potentially infringe their rights.	Report, Section 11.2, pp. 44-45
	gTLD and ccTLD registries	Industry associations	10. Offer, directly or through the registrars/resellers, services allowing rightholders to preventively block infringing domain name registrations.	Section 10 and Appendix 1 – Technical Report, Section 11.2, p. 45, anti-counterfeiting and anti-piracy organisations
	gTLD and ccTLD registries	Industry associations	11. Use predictive algorithms to prevent abusive registrations.	Section 10, law enforcement authorities, cybersecurity investigators, network technology professionals, child protection organisations, patient safety organisations, consumer protection organisations, and anti-counterfeiting and anti-piracy organisations
	gTLD and ccTLD registries and registrars	ICANN, European Commission, EU co-legislators, ENISA, Member States and national authorities	12. Monitor abuse rates of TLD registries or registrars on an ongoing basis by independent researchers. Abuse rates should not exceed predetermined thresholds. If thresholds are exceeded and the abuse rates do not improve within a given time period, accreditation may be revoked.	Appendix 1 – Technical Report, Section 9.2, p. 37
	gTLD and ccTLD registries and registrars	ICANN, European Commission, EU co-legislators, Member States	13. Financially reward TLD registries and registrars with lower abuse rates, e.g., through a reduction in domain registration fees, to align economic incentives and raise barriers to abuse.	Appendix 1 – Technical Report, Section 9.2, p. 37
	gTLD and ccTLD registries	Industry associations	14. Maintain access to existing domain/URL blacklists. Identify the registrars with the highest and lowest concentrations and rates of DNS abuse in their ecosystems. Propose incentive structures to encourage registrars to develop methods to prevent and mitigate malicious registrations effectively.	Appendix 1 – Technical Report, Section 11.2, pp. 45-46
D. Improved detection and mitigation of DNS abuse distributing malicious content				
Type 3 - Abuse related to domain names	Hosting providers	European Commission, EU co-legislators,	15. Monitor the abuse rates on an ongoing basis by independent researchers.	Appendix 1 – Technical Report,

distributing malicious content		ENISA, Member States and national authorities	Abuse rates should not exceed predetermined thresholds. Study incentive structures to induce hosting providers to develop technical solutions that effectively curb hosting and content abuse.	Section 12.3, p. 52
	Free hosting and subdomain service providers	European Commission, EU co-legislators, ENISA, Member States and national authorities, industry associations	16. Employ advanced prevention and remediation solutions to quickly curb abuses of subdomain names and hosting infrastructure. They should proactively detect suspicious domain names containing keywords of the most frequently targeted brands and names and work closely with the most heavily attacked companies and develop trusted notifier programs.	Appendix 1 – Technical Report, Section 13, p. 55

E. Better protection of the DNS operations and preventing DNS abuse related to the operation of the DNS and other infrastructures

Type 2 - Abuse related to the operation of the DNS and other infrastructures	ccTLD registries	European Commission, EU co-legislators, ENISA, Member States and national authorities, industry associations	17. Sign TLD zone files with DNS security extensions (DNSSEC) and facilitate its deployment according to good practices.	Section 10 and Appendix 1 – Technical Report, Section 15.3, p. 60
	gTLD and ccTLD registries	ICANN, European Commission, EU co-legislators, ENISA, Member States and national authorities, industry associations	18. Require registrars to support DNSSEC signing for registrants. Domain administrators (registrants) should have easy access to DNSSEC signing of domain names within the TLD.	Section 10 and Appendix 1 – Technical Report, Section 15.3, p. 62
	gTLD and ccTLD registries	ICANN, European Commission, EU co-legislators, Member States, industry associations	19. Offer discounts for DNSSEC-signed domain names.	Section 10 and Appendix 1 – Technical Report, Section 15.3, p. 63
	Internet Service Providers operating DNS resolvers	European Commission, EU co-legislators, ENISA, Member States and national authorities	20. Configure DNSSEC validation to protect end users from cache poisoning attacks and ensure the integrity and authenticity of domain name resolutions.	Appendix 1 – Technical Report, Section 16, p. 67
	National governments and Computer Emergency Response Teams (CERT)	European Commission, EU co-legislators, ENISA, Member States and national authorities	21. Intensify notification efforts to reduce the number of open DNS resolvers (and other open services), which are among the root causes of distributed reflective denial-of-service (DRDoS) attacks.	Appendix 1 – Technical Report, Section 16.4, p. 71
	Security community		22. Intensify efforts to continuously measure the adoption of Sender Policy Framework (SPF) and Domain-based	Appendix 1 – Technical Report,

			Message Authentication Reporting and Conformance (DMARC) protocols. Correct and strict SPF and DMARC rules can mitigate email spoofing and provide the first line of defence against Business Email Compromise (BEC) scams.	Section 17.4, p. 76
	Network operators		23. Deploy IP Source Address Validation (SAV) not only for outgoing but also for incoming traffic at the edge of a network to provide an effective way of protecting closed DNS resolvers from different external attacks against DNS infrastructure, including possible zero-day vulnerabilities within the DNS server software.	Appendix 1 – Technical Report, Section 19, p. 80

F. DNS abuse awareness, knowledge building, and mitigation collaboration at EU level

<p>Type 1 - Abuse related to maliciously registered domain names</p> <p>Type 2 - Abuse related to the operation of the DNS and other infrastructures</p> <p>Type 3 - Abuse related to domain names distributing malicious content</p>	EU ccTLD registries	European Commission, EU co-legislators, Member States, industry associations	24. Harmonise / approximate the practices of ccTLDs by the adoption of the good practices available at European and international level	Section 10, law enforcement authorities, cybersecurity investigators, network technology professionals, child protection organisations, patient safety organisations, consumer protection organisations, and anti-counterfeiting and anti-piracy organisations
	All DNS operators and intermediaries	European Commission, EU co-legislators, Member States, industry associations	<p>25. Require the collaborate with EU and Member States' institutions, law enforcement authorities (LEA) and so-called trusted notifiers or trusted flaggers. Where collaborations exist but are informal, they are to be further strengthened and formal processes are to be set up for the parties to interact. In this regard, parties should identify the persons responsible within the entities in question and their respective deputies. An operations manual should be drawn up and outline:</p> <ul style="list-style-type: none"> the step-by-step process that each party must follow the method to identify the cases in which the parties should contact each other the means of parties' interaction (e.g., through a specific interface, email or other) and the expected response time (24h / 48h / 72h or other) the frequency of reports (if requested) on the activities 	Section 10, law enforcement authorities, cybersecurity investigators, network technology professionals, child protection organisations, patient safety organisations, consumer protection organisations, and anti-counterfeiting and anti-piracy organisations

			performed in accordance with such operations manual.	
	n/a	European Commission, EU co-legislators, Member States, industry associations	26. Raise awareness and promote knowledge-building activities to make consumers, rightholders, or other affected parties aware of existing measures tackling DNS abuse.	Section 10, law enforcement authorities, cybersecurity investigators, network technology professionals, child protection organisations, patient safety organisations, consumer protection organisations, and anti-counterfeiting and anti-piracy organisations.
	All stakeholders	European Commission, EU co-legislators, Member States, industry associations	27. Share knowledge and promote capacity-building activities between all intermediaries and stakeholders involved in the fight against DNS abuse.	Section 10, law enforcement authorities, cybersecurity investigators, network technology professionals, child protection organisations, patient safety organisations, consumer protection organisations, and anti-counterfeiting and anti-piracy organisations

12. Acronyms and abbreviations

ADR	Alternative Dispute Resolution
APEWS	Abuse Prevention and Early Warning System
APWG	Anti-Phishing Working Group
AS	Autonomous System
BEC	Business Email Compromise
C&C	Command-and-Control
ccTLD	Country code Top-Level Domain
CENTR	Council of European National Top-Level Domain Registries
CSAM	Child Sexual Abuse Material
DDoS	Distributed Denial-of-Service
DGA	Domain Generation Algorithm
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
DNSSEC	DNS Security Extensions
DRDoS	Distributed Reflective Denial-of-Service
ENISA	European Union Agency for Cybersecurity
EUIPO	European Union Intellectual Property Office
GAC	Governmental Advisory Committee of ICANN
GDP	Gross Domestic Product
GNSO	Generic Names Supporting Organization of ICANN
gTLD	Generic Top-Level Domain
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IDN	Internationalised domain names
IoT	Internet of Things

IP	Internet protocol
IPR	Intellectual property rights
ISP	Internet service and access provider
ISSP	Information society service provider
KYBC	Know Your Business Customer
LEA	Law enforcement authorities
OECD	Organisation for Economic Co-operation and Development
RDAP	Registration Data Access Protocol
RFC	Request for Comments
SAV	Source Address Validation
SPF	Sender Policy Framework
TLD	Top-Level Domain
UDRP	Uniform Domain Name Dispute Resolution Policy
URL	Uniform Resource Locator
URS	Uniform Rapid Suspension System
WHOIS	Protocol for querying databases that store the registered users or assignees of an Internet resource
WIPO	World Intellectual Property Organization

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696 or
- by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications at: <https://publications.europa.eu/en/publications>. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: <http://eur-lex.europa.eu>

Open data from the EU

The EU Open Data Portal (<http://data.europa.eu/euodp/en>) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

