DNS
RESEARCH
FEDERATION

Habits of excellence: why are European ccTLD abuse rates so low?

Emily Taylor, Alex Deacon, Nathan Alan

August 2023

DNSRF.ORG

"We are what we repeatedly do. Excellence, then, is not an act, but a habit."

(attributed to Aristotle)

Executive summary

European Union country-code Top Level Domain registries (EU ccTLDs) as a group have strikingly low levels of domain names associated with spam, phishing and malware. This study asks whether the data accuracy practices of European Union (EU) country code Top Level Domain (ccTLD) registries contribute to those low levels of malicious domain names within EU ccTLDs.

Voluntary and contractual norms within the domain name industry have emphasised the need for accurate, up to date and publicly accessible domain name registration data, but fulfilling that requirement while remaining in compliance with privacy laws and expectations has been a challenge.

For more than two decades the multistakeholder policy debates within ICANN surrounding the publication of registration data on WHOIS have remained unresolved. When EU privacy law, the GDPR, led to the WHOIS 'going dark', even though ICANN contracts required publication of registration data, it was clear that there was a lack of a legal obligation in EU legislation to mandate the collection, maintenance and publication of WHOIS data.

In late 2022, the European Union ratified the NIS2 Directive, which seeks to bridge that gap by imposing legal obligations on domain name registries and registrars to collect, maintain, make publicly available and verify domain name registration data[1] in line with 'best practices within the industry.'[2] This study asks to what extent can the data quality practices of EU ccTLDs demonstrate effective practices within the industry'?

The EU ccTLDs are not bound by ICANN consensus policies, but adopt policies and procedures to reflect local priorities. Their diverse approaches can provide insights into the effectiveness of different data accuracy and verification practices.

[1] NIS2, Article 28

[2] NIS2, Recital 111

This study, after providing background on the WHOIS and how it was affected by EU privacy laws, then steps through the relevant provisions in the recently-published NIS2 Directive with regard to WHOIS and data verification. Next, it introduces the EU ccTLDs as a group, before describing our methodology and disclaimers, data and analysis in answering four research questions (RQ) set out in the introduction. RQ1 is about comparative abuse rates; RQ2, abuse rates and market share; RQ3 the impact of demonstrated effective practices, and RQ4 considers other factors that might explain EU ccTLDs' low abuse levels.

Drawing on data and analytical tools within the DNS Research Federation's DAP.LIVE platform, along with desk-based research, this study brings that quantitative data together with an analysis of EU ccTLD data practices documented by CENTR in a recent report[3].

The data shows that **EU ccTLDs have the lowest abuse rates of any TLD bloc within the global market**. As a group, the EU ccTLDs accounted for only 3% of malicious use compared to their global market share of 15%. **The data indicates a correlation between EU ccTLD low abuse rates and the widespread adoption of diverse data quality measures among the EU ccTLDs.** The majority of EU ccTLDs take ad hoc, proportionate action to tackle problems as they arise, and a minority are experimenting with automated identity checks on registrants. The picture that emerges is that the combination of measures - such as automated data syntax validation and ad hoc measures - are likely to be the defining factors that make the difference for EU ccTLDs and help to explain their strong performance as a group. Yet, abuse rates are low right across the EU region, suggesting that the **combined measures demonstrate effective practices in mitigating malicious use of domains.** When considering other factors that may apply, the study highlights the mature economic and cybersecurity environment in the EU, and other quality markers in EU ccTLDs, such as high renewal rates. Our analysis indicates that EU ccTLDs are able to combine **high market penetration and low pricing with data assurance practices.**

[3] Registration data accuracy in European national domain registries: existing practices and challenges, CENTR, 2022 https://www.centr.org/news/news/data-accuracy-paper.html

Acronyms

The report uses the following acronyms, which are explained in the table below.

Acronym	Meaning
ccTLD	a country code Top Level Domain, such as .de (Germany), .uk (United Kingdom) and .fr (France).
CENTR	The Council for European National Top Level Domain Registries, the regional organisation for European ccTLDs (see centr.org)
DAP, DAP.LIVE	The DNS Research Federation's DNS Analytics Platform.
DNS	The Domain Name System, part of the Internet's system of unique identifiers
DNSRF	The DNS Research Federation (www.dnsrf.org)
EPDP	Expedited Policy Development Process on the Temporary Specification for gTLD Registration Data (see https://icannwiki.org/Expedited_Policy_Development_Process_on_the_Temporary_Specification_for_gTLD_Registration_Data)
EU	The European Union
GDPR	General Data Protection Regulation, the European Union's privacy law
ICANN	The Internet Corporation for Assigned Names and Numbers, coordinates policy for the Internet's unique identifiers ie domain names and IP addresses
IANA	The Internet Assigned Numbers Authority, a function of ICANN, which keeps the root database for Top Level Domains (see www.iana.org).
ISO	The International Standards Organisation, a standards development organisation with 169 country members https://www.iso.org/about-us.html
ITU	The International Telecommunication Union, a specialist

agency of the United Nations. The ITU has three main areas of responsibility: management of radio spectrum; development in the area of telecoms and ICTs; and developing standards for telecommunications.

NIS
The European Union’s original Network Information Security Directive 2016/1148. As a Directive, the NIS required transposition into EU Member State law. The NIS has been updated by the NIS2 (see below).

NIS2
The European Union’s updated Network Information Security Directive 2022/2555 (known as NIS2), which entered into force in October 2022, replacing Directive (EU) 2016/1148. Member States are required to transpose NIS2 into their national laws by October 2024.

OECD
The Organisation for Economic Cooperation and Development, an international organisation with 38 Member countries, founded in 1961 to stimulate economic progress and world trade (www.oecd.org)

SIDN
The ccTLD for the Netherlands (www.sidn.nl)

SSAC
ICANN’s Security and Stability Advisory Committee, part of the ICANN community (for more, see https://www.icann.org/community)

UDRP
The Uniform Dispute Resolution Policy, an administrative process for the resolution of disputes between trademarks and domain names. The UDRP was adopted as a consensus policy by ICANN in 1999.

WHOIS
A look up service that enables a user to find out the contact details of a domain name registrant, as well as certain technical information relating to a domain name. WHOIS data refers to the data relating to a domain name registration that is, or used to be, displayed as part of a WHOIS result.

Contents

Introduction

This study was commissioned by the ICANN Business and Intellectual Property Constituencies, to understand to what extent there are correlations between demonstrated effective practices of country code Top Level Domain (ccTLD) registries within the European Union (EU) and levels of malicious use of domain names within those ccTLDs.

The backdrop for this study is the finalisation in December 2022 of the text of Directive 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). As a Directive, NIS2 requires transposition into each of the EU Member States' domestic law by 17 October 2024[4].

This study seeks to identify possible linkages between three variables: **malicious activity relating to domain name registrations; registration data accuracy practices; and pricing** in the ccTLDs of the 27 EU member states plus .eu, normalised to the size of the ccTLD's domains under management. The output is a risk score (high, medium, low) for each ccTLD in the study, which combines the data practices, normalised instances of abuse, penetration rates and pricing. The risk score can be read alongside each ccTLD's data practices (where available), enabling a reader to understand possible correlations between data practices and abuse scores.

In approaching this study, we formulated the following research questions to guide our enquiries:

RQ1: **Comparative abuse rates** What are the rates of malicious use in European ccTLD compared with other market comparators (legacy gTLDs, new gTLDs, other ccTLDs - together 'TLD blocs').

RQ2: Abuse rates and market share How do the rates of malicious use by TLD blocs compare with the relative market share of each TLD bloc?

RQ3: Impact of demonstrated effective practices What is the correlation between registration data accuracy measures as documented in the recent CENTR Report (https://centr.org/library/library/download/10478/7435/41.html) (the CENTR Report).

[4] NIS2, Article 23(11)

RQ4: Other factors Could there be other explanations for lower than average rates of malicious use of domains in EU ccTLDs?

Before setting out our methodology, results, findings and conclusions, this report has a substantial background section to explain key concepts, developments in the regulatory landscape, and the context for European country code Top Level Domains (ccTLDs). The report begins with an explanation of WHOIS, the domain name registration look-up service, and the links between accurate registration data and better cybersecurity outcomes. It then describes European privacy regulations and their impact on WHOIS. There follows an overview of the recently published NIS2 Directive, and analyses the sections relating to WHOIS, both Article 28 and the recitals that help to understand the legislative goals.

After considering the impact of regulation on WHOIS, the report introduces European country code Top Level Domains (EU ccTLDs). After briefly explaining what a ccTLD is, the European context for digital development and the characteristics of EU ccTLDs are set out.

The report then progresses to the evidence-based analysis which forms its unique contribution to the debate. After setting out methodology and disclaimers, it then presents findings, answers to the four research questions, an analysis of pricing and market penetration, and a brief consideration of good practices outside the EU region, before setting out its conclusions. The appendices contain full data tables to complement the analysis.

WHOIS and the impact of European Regulation

WHOIS

For many years, the DNS community has recognised the requirement for domain name registration data to be **up to date and accurate**. For example, the obligations on gTLD registrants to provide accurate, reliable and up to date registration data have been in place since 1999[5]. Access to data is described by ICANN's Security and Stability Advisory Committee (SSAC) as 'essential for a variety of legitimate purposes, especially the identification and mitigation of various types of Internet abuse and technical problems,'[6] making the link between the public availability of data and the mitigation of cybersecurity and technical issues.

To perform this task, Top Level Domain registries and registrars provide a **WHOIS service,** making publicly available certain data relating to domain name registrations[7]. **WHOIS data** is the information that registrants provide when registering a domain name, such as their contact details, and other technical information relating to the domain name. ICANN's base agreement with gTLD registries requires the collection, 'maintenance of and access to accurate and up-to-date information concerning domain name registrations.'[8]

A distinction is made between 'thick' WHOIS and 'thin' WHOIS. For the majority of gTLDs, ICANN requires the registry to collect and maintain domain name registration data. A similar model is seen across all EU ccTLDs, where – despite differences in data practices – all registries operate a 'thick' WHOIS model.[9] The exception in the DNS industry is .com (the largest TLD), .net and .jobs, which operate a 'thin' WHOIS, in which the registration data is collected and maintained by registrars, and not held by the registry. In 2017, the ICANN community adopted a consensus policy requiring the transition of .com, .net and .jobs to a 'thick' WHOIS model, but implementation has been deferred[10].

The structure of the domain name market implies that registrars, not registries, are the responsible party for the initial collection of registration data. While ICANN's standard terms require registrars to terminate or suspend domain names where the

[5] ICANN Registrar Accreditation Agreement 1999, https://archive.icann.org/en/nsi/icann-raa-04nov99.htm. Relevant sections are II (F) (4) and II(J(7) which require the publication of WHOIS data and provide sanctions for registrants that wilfully provide inaccurate data.

[6] SAC 101, at page 3.

[7] For a detailed discussion on the definitions of WHOIS, see WHOIS Policy Review Team report, May 2012 https://www.icann.org/en/system/files/files/final-report-11may12-en.pdf , Key definitions section at p22 ff.

[8] ICANN Registry base agreement 2023, para 1.3.4, https://www.icann.org/en/registry-agreements/base-agreement;

[9] See CENTR report, Annex I - data referenced in NIS2 as collected by EU ccTLDs on 8/9/2022.

[10] See Thick WHOIS Transition Policy for .com, .net and .jobs https://www.icann.org/resources/pages/thick-whois-transition-policy-2017-02-01-en as updated on 7 November 2019

registrant has wilfully provided 'inaccurate or unreliable contact details,'[11] the obligations to provide accurate data flow down to the registrants. Prior to the advent of GDPR in 2018, privacy and proxy services were widely used to protect the identity of registrants from being displayed in the public WHOIS. Despite the widespread redaction of registration data from public WHOIS since 2018, privacy and proxy services remain in widespread use. The CENTR Report provides a useful explanation of the role of registrars and proxy providers.

While EU ccTLDs are not subject to ICANN consensus policies or contracts, WHOIS services have been provided by EU ccTLDs (and other ccTLDs beyond Europe) for many years. The CENTR Report notes that 70% of EU ccTLDs make a distinction between domain name registrations made by **legal entities and natural persons**. For natural persons, CENTR reports that 100% of the surveyed members collect the registrant full name and email address, and for legal entities, 100% of surveyed members collect the organisation and/or company name and email address[12].

The EU ccTLDs also recognise the link between accurate domain name registration data and improved cybersecurity outcomes. For example, the ccTLD for the Netherlands, SIDN, has announced a ban on proxy registrations from October 2023, noting that 'For SIDN and for other people and organisations, having the true registrant's details in the register is important mainly for preventing abuse.[13]

European privacy regulation and the impact on WHOIS

EU law has protected personal data since the mid 1990s, through the 1995 Data Protection Directive[14]. In the twenty years that followed, the global digital revolution placed increased emphasis and strains on the rights of privacy and data protection. The EU's updated privacy law, the General Data Protection Regulation (GDPR), came into force in May 2018. Several aspects of the GDPR had a direct impact on WHOIS:

[11] Para 5, RDDS Accuracy program specification, appended to the Registrar Accreditation Agreement 2023, at page 40. https://www.icann.org/resources/pages/registrars/registrars-en. The registrant's obligations to provide accurate and reliable contact details, and correct and update them within seven days of any change are set out at para 3.7.7 of the Registrar Accreditation Agreement 2023.
[12] CENTR study, at page 10.
[13] SIDN, Privacy and proxy services prohibited from .nl after 1 October, 19 July 2023, https://www.sidn.nl/en/news-and-blogs/privacy-and-proxy-services-prohibited-from-nl-after-1-october
[14] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

- Extra territorial effect
- Revenue based fines
- Increased obligations for data processors

Given the GDPR's extraterritorial effect, the loss of public WHOIS data was felt beyond the geographical region of the EU. In response to a Temporary Specification adopted by the ICANN Board in May 2018, WHOIS data for both organisations and individuals – or in legal jargon, both legal and natural persons– was removed from the public WHOIS for all generic Top Level Domains (gTLDs)[15]. The wholesale redaction of WHOIS data, even for legal persons, flowed into some ccTLDs too, while others maintain the publication of WHOIS results for organisations[16].

The WHOIS debate within the ICANN community has persisted for more than 20 years, and is beyond the scope of this report. Prior to GDPR, the publication of WHOIS registration data relating to individuals was highlighted as problematic by several civil society groups and European data protection experts[17]. Since the advent of GDPR in 2018, the loss of WHOIS data had a profound impact on the operational capabilities of public safety, brand protection and cybersecurity communities[18].

Despite substantial work within the ICANN community since 2018, including the cross-community Expedited Policy Development Process (EPDP), one of the issues viewed as preventing the publication of WHOIS data by TLD registries and registrars worldwide was the lack of a specific **legal obligation** in European law to collect,

[15] ICANN Temporary Specification for gTLD registration data, effective as of 25 May 2018. https://www.icann.org/resources/pages/gtld-registration-data-specs-en

[16] See, for example, WHOIS result for bbc.co.uk https://www.nominet.uk/lookup/?domain=bbc.co.uk (redacted for privacy), accessed 9 August 2023, and for gap.eu https://whois.eurid.eu/en/search/?domain=gap.eu (registrant organisation is displayed as Gap (RHC) B.V., along with an email address for contact), accessed 9 August 2023.

[17] See for example, Article 29 Working Party opinion 2/2003 on the application of the data protection principles to the Whois directories, 2003, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp76_en.pdf

[18] For a summary of the impact, see ICANN, GDPR and the WHOIS: A users survey - three years later, M3AAWG and APWG, Laurin B Weissinger, Dave Piscitello and Bill Wilson, 2021 https://www.m3aawg.org/WhoisSurvey2021-06, and Security professionals mourn the loss of Whois data post GDPR, DomainTools survey says https://www.domaintools.com/company/press/press-releases/security-professionals-mourn-the-loss-of-whois-data-post-gdpr-domaintools-s, Domain Tools, 2018, and SAC101, SSAC Advisory regarding access to domain name registration data states "Reliable, consistent, and predictable access to domain name registration data (via Registration Data Directory Services, or RDDS) is essential for a variety of legitimate purposes, especially the identification and mitigation of various types of Internet abuse and technical problems." ICANN Security and Stability Advisory Committee, June 2018 https://www.icann.org/en/system/files/files/sac-101-en.pdf

maintain, verify and make publicly available any portion of that data. NIS2 has stepped into bridge that gap.

NIS2: new legal obligation to collect, maintain, verify and provide access to WHOIS data

The original Network Information Security Directive (NIS) came into force in 2018. Beyond recognising the role of EU ccTLDs as providing critical infrastructure, it imposed few specific obligations on them.

The updated Directive, NIS2, was adopted in late 2022. NIS2 seeks to add legislative clarity into the international WHOIS debate, by providing legal obligations with respect to registration data. Those obligations apply to both registries and '*entities providing domain name registration services',* a defined term meaning 'a registrar or an agent acting on behalf of registrars, such as a privacy or proxy registration service provider or reseller (Article 6(22)). So, NIS2's WHOIS obligations apply to both registries and registrars.

Under NIS2, registries and registrars must '***collect and maintain accurate and complete domain name registration data** in a dedicated database with due diligence in accordance with Union data protection law as regards data which are personal data*' (Article 28). So, the NIS2 text requires the collection and maintenance of registration data to be consistent with data protection law. It also makes a connection between accurate and complete registration data as '*contributing to the security, stability and resilience of the DNS.*' (Article 28(1)).

Article 28(2) sets out the data points that comprise '*the **necessary** information to identify and contact'* domain name registrants:

(a) the domain name;
(b) the date of registration;
(c) the registrant's name, contact email address and telephone number;
(d) the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.

Article 28(3) imposes a new requirement on registries and registrars to have 'verification procedures' to ensure accurate and complete registration data, as follows (emphasis added):

Member States shall require the TLD name registries and the entities providing domain name registration services to have ***policies and procedures, including verification procedures,*** *in place* ***to ensure*** *that the databases referred to in paragraph 1 include* ***accurate and complete information****. Member States shall require such policies and procedures to be made publicly available.*

Article 28(4) requires TLD registries and registrars to make registration data **publicly available**, other than personal data, and to provide **disclosure of registration data** upon lawful and duly substantiated requests by legitimate access seekers (Article 28(5)).

Article 28(6) provides that compliance with the obligations set out in Article 28 '*shall not result in a duplication of collecting domain name registration data. To that end, Member States shall require TLD name registries and entities providing domain name registration services to cooperate with each other.'* This provision may be intended to recognise the .com registry's 'thin' WHOIS model as potentially compliant.

NIS2 imposes a new requirement for EU ccTLDs to have data '**verification procedures**'. No definition of 'verification procedures' is given in the Directive, but some guidance is contained at recital 111 (emphasis added):

Those procedures should ***reflect the best practices used within the industry*** *and, to the extent possible, the progress made in the field of* ***electronic identification****. Examples of verification procedures may include* ex ante *controls carried out at the time of the registration and* ex post *controls carried out after the registration. The TLD name registries and the entities providing domain name registration services should, in particular, verify at least one means of contact of the registrant.*

This report does not attempt to identify what the 'best practices used within the industry' are, but rather highlights the diverse practices of the group of EU ccTLDs as examples of **demonstrated effective practices**.

The NIS2 Directive carries implications for EU based TLD registries and registrars and to the global industry, thanks to its **extra-territorial effect**. Under Article 26(3) Member States may take legal actions against registries and registrars that provide services in their jurisdiction, regardless of whether or not the entity is established or has a point of contact in that territory.

The unique context for European ccTLDs

What is a ccTLD?

There are two types of Top Level Domain (TLD), generic Top Level Domains (gTLDs) and country code Top Level Domains (ccTLDs). Generic Top Level Domains such as .com, .net, .org and others have global markets. Consensus policies for gTLDs are coordinated through the ICANN multistakeholder community, and ICANN operates a system of standard contracts for gTLD registries and accredited registrars.

Country code Top Level Domains are different. There are approximately 200 ccTLDs worldwide, as identified in the IANA database. Any two letter country code identified in the ISO-3166 list[19] has the potential to be a ccTLD identifier.

The policies and practices of ccTLDs throughout the world are developed independently, rather than through ICANN. As a result, the global group of ccTLDs is highly diverse, and tend to be tightly bound to their country or territory[20]. Many have developed close ties with local law enforcement, consumer protection and other public safety authorities[21]. Several ccTLDs operate the ICANN-developed Uniform Dispute Resolution Process and others have adapted the UDRP to reflect local conditions and priorities[22]. In common with the gTLD registries, a majority of global ccTLDs operate a registry-registrar model.

[19] https://www.iso.org/obp/ui/#search

[20] For the exceptional case of out-of-territory operated ccTLDs, see Samuel Bashfield & James Mortensen (2023) Self-regulation, internet domains and Indian Ocean territories, Journal of Cyber Policy, DOI: 10.1080/23738871.2023.2238723

[21] See, for example, Afnic New public consultation to facilitate access to registration data for authorized authorities, September 2022 https://www.afnic.fr/en/observatory-and-resources/news/new-public-consultation-to-facilitate-access-to-registration-data-for-authorized-authorities/

[22] https://www.wipo.int/amc/en/domains/cctld/

The European context for digital development

The continent of Europe is economically successful, with four G7 members[23] and 26 of the 38 OECD members are European countries[24]. The European Union is the largest trading bloc in the world and is the principal trading partner for more than 80 countries[25]. Europe's economic strength is reflected in the maturity of its digital and Internet development. Twenty European countries have a score of more than 90% in the International Telecommunication Union's (ITU) Global Cybersecurity Index[26]. According to the ITU[27], Europe as a region has the highest number of countries with both data protection and breach notification regulations, with comprehensive national computer emergency response programs. Europe has strength in National Cybersecurity Strategies, cybersecurity training for government officials, information sharing and capacity development[28].

Therefore, the EU ccTLDs are operating in an environment of comparatively mature cybersecurity institutions and regulatory environments.

Introducing European country code Top Level Domains

Our study group comprises the 27 EU ccTLDs and .eu, comprising 50 million domain name registrations. Overall, the EU ccTLDs represent 15% of global market share and the individual registry sizes range from just under 20,000 (Malta, Cyprus) to more than 17 million (.de, Germany).

Not for profit models are the norm for EU ccTLDs, with 84% being private non-profit organisations, or public sector (eg, university) run[29]. Some ccTLDs are self-regulating, while others have specific regulation.

[23] https://www.cfr.org/backgrounder/what-does-g7-do
[24] https://www.oecd.org/about/members-and-partners/
[25] https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/eu-position-world-trade_en#:~:text=The%20EU%20is%20the%20largest,of%20manufactured%20goods%20and%20services
[26] https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
[27] ITU, Overview of Global Cybersecurity Efforts: Current Gaps, March 2022 https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Overview_of_Global_Cybersecurity_Efforts_Current_Gaps.pdf

[28] *ibid*
[29] Patrick Myles, "From measuring the market to understanding it", CENTR 20th anniversary publication): https://centr.org/library/library/download/9466/5928/41.html

EU ccTLDs have other quality markers:

- high renewal rates (CENTR reports an average of 84%)
- healthy domestic market share (the median for the group is 53%)
- a high level of 'developed web content', compared with gTLD counterparts[30]

As a group, the EU ccTLDs offer registrations at relatively low cost prices, i.e. the prices charged to registrars. The average cost price of the EU ccTLDs, based on their published pricing, is similar to that of .com at just under $9.

Unlike their counterparts outside Europe, since 1995 EU ccTLDs have been providing public access to WHOIS data while also being subject to EU privacy laws and regulations. While the GDPR did change some of the publication practices of many EU ccTLDs, the data protection principles remain consistent with the 1995 Data Protection Directive.

Methodology and disclaimers

So far, this study has set out the background to the WHOIS, the impact of EU privacy laws on the availability of registration data, and new legal obligations on registries and registrars brought in by NIS2 to collect, maintain and publish registration data. It has then provided a brief background on European ccTLDs, the socio-economic background in which they operate and –while acknowledging their independence and diversity– some common characteristics shared by the majority of EU ccTLDs.

The remainder of this paper describes the evidence driven analysis performed by the research team, beginning with a methodology, disclaimers and limitations of the study, results and the answers to our four research questions. The study then briefly flags good practices outside of the European Union, and highlights the low levels of abuse in .au (Australia) and .uk (United Kingdom), before setting out our conclusions.

For the purposes of this study, the DNSRF research team leveraged data acquired from three main sources. First was the DNSRF Data Analytics Platform's (DAP.LIVE) collection of abuse reporting feeds, encompassing phishing, malware and spam.

[30] Source: CENTRstats Global TLD Report, Edition 4 2022, CENTR https://centr.org/library/library/download/10681/7680/41.html

Second, we performed a desk-based collection of publicly available data relating to metrics associated with TLDs in general, with a focus on EU ccTLDs. Finally, we consulted studies published by CENTR, ICANN and other authoritative sources[31].

In our analysis, we included reports of abuse (described in more detail below) for the time period between January 1, 2022 and December 31, 2022. We have analysed the twelve months of data as a whole versus on a month-by-month or week-by-week basis. This ensures a sufficiently large and robust data set that will account for seasonal spikes and dips and other anomalies that typically occur.

The data at hand contains information for all TLDs from around the world. For the purposes of this study, we have categorised the TLDs into the following four categories.

- Legacy gTLDs (.com, net, org, info, biz)
- New gTLDs (From the 2013+ rounds)
- EU ccTLDs (All ccTLDs from EU Member states plus .eu)
- Other ccTLDs (all non-EU ccTLDs from the rest of the world)

This reflects the approach taken by CENTR in its white paper on data accuracy, and enables like-for-like comparisons between this study and that of CENTR. Other relevant literature, such as the European Commission's study on domain name system (DNS) abuse 2022[32] (the Fasano study), drew a distinction between EU ccTLDs and other European ccTLDs. We have not adopted this approach, but note that the group of 'other ccTLDs' contains ccTLDs that are members of the European Economic Area (Iceland, Liechtenstein and Norway) are members of the European single market (Switzerland) or have recently exited the European Union (United Kingdom). The data from these other European ccTLDs is similar in character to that of the EU ccTLDs, and we note that these additional European countries can also provide sources of demonstrated effective practices on data handling. Where we differ in approach from the Fasano study, is that we do not categorise as part of this European group the Russian Federation and other non-EU countries that fall within the United Nation's

[31] Registration data accuracy in European national domain registries: existing practices and challenges, CENTR, 2022 https://centr.org/library/library/download/10478/7435/41.html, and CENTRstats Global TLD Report Edition 4/2022, CENTR, 2023, https://centr.org/library/library/download/10681/7680/41.html
[32] Study on domain name system (DNS) report, Annex 1, Technical Report, European Commission 2022 https://op.europa.eu/en/publication-detail/-/publication/d9804355-7f22-11ec-8c40-01aa75ed71a1

category of Eastern Europe[33], due to the differences in legal frameworks and traditions.

DAP.LIVE abuse data, queries and dashboards

The DAP.LIVE platform currently hosts, and makes available to authorised users, 70 data feeds spanning 18 separate categories. In this research, the following data feeds were utilised:

Feed	Description
DAP: Phishing Combined	This feed contains all of the Phishing URLs reported and available on both the OpenPhish and APWG phishing feeds. The data in this feed is updated once an hour and the URLs are de-duplicated within a time window of one day (e.g. URLs reported by both providers on the same day are de-duplicated.)
URLhaus: Complete Data Set	This feed contains all malware URLs reported to the abuse.ch URLhaus Project. The data in this feed is updated every few minutes.
Spamhaus: Domain Block List	This feed contains a list of domains on Spamhaus' domain block list. It is updated once an hour.

In order to properly analyse the data, 52 separate data queries were created and used to generate the findings in this study.

The data is displayed across public dashboards, which accompany the publication of this report, enabling users to review the data and visualise the results.

[33] See ' Eastern European States' in Regional Groups of Member States (ND), United Nations Department for General Assembly and Conference Management https://www.un.org/dgacm/en/content/regional-groups.

Finally, to prevent spikes in the data (i.e. very high apparent abuse rates, relating to very small data sets), we removed from the analysis the following TLDs with total registrations under 1000:

- gle, goog, aws, krd, juegos, ki, moi, storage, mp, gw, ltda, aw, td, sarl

Desk-based Research

The research team collected the following data points from publicly available data sources. The desk-based research gives us:

- **Registration figures as of 31 December 2023** for EU ccTLDs and some other ccTLDs from Domain Tools. We corroborated the data for EU ccTLDs by consulting the registry websites. The majority of EU ccTLD registries publish registration figures as well as historic registration figures. A minority do not: Bulgaria, Cyprus Greece, Malta, and Romania. For these we corroborated from the 'Online World' study by Nominet for 2020[34]. The registration data assisted us in determining relative **market share** and **market penetration** when compared with population size. We filled in gaps with domain counts from Domain Tools, but we noted in one case (.pt) substantial differences between the registry published data and that provided by Domain Tools, owing to differences between registered and active domains as noted on the registry website.
- **Population Size.** We have collected data on population size for each of the EU Member States from the World Bank[35] to help us understand the **market penetration** of individual ccTLDs. The market penetration gives a sense of the uptake of each EU ccTLD across Member States normalising for populations that vary from half a million (Malta) to more than 83 million (Germany). Where market penetration is low, policies referenced in this study may have little impact on the overall market because they only affect a very small registry.

[34] The Online World, Nominet, 2021 https://nominet.uk/wp-content/uploads/2021/05/The-Online-World-2020.pdf?_ga=2.148134647.1512727290.1685527633-638319410.1685527633

[35] The World Bank, Data, Population - All countries and economies (ND, accessed April 2023) https://data.worldbank.org/indicator/SP.POP.TOTL

- **Pricing.** We obtained the cost price for 1 year's new registration, published by the majority of EU ccTLDs[36]**.** The cost price is converted to a single currency (US Dollars, or USD) to aid comparisons, using the applicable conversion rates on xe.com on 31 May 2023. Exchange rate fluctuations will lead to differences in the conversion rate.

Quantifying Abuse - Methodologies Used

A recent Exploring DAP blog published by the DNS Research Federation described and analysed three methodologies used to count and quantify abuse. When analysing the data for this study, we used all three methodologies, but focused our findings on the number of unique domain names associated with each form of abuse (phishing, malware and spam). This is because our area of interest is the sphere of influence of ccTLD registries. Other methodologies are valid, particularly when considering the roles and responsibilities of registrars and/or hosting providers.

Counting the unique number of domain names used to mount attacks against users during the 12 month time period allows us to calculate an overall abuse rate for each TLD. To do this we use the following formula:

```
(# of Unique Domain Names used in Phishing Attacks
                        +
  # of Unique Domain Names used in Spam Attacks
                        +
# of Unique Domain Names used in Malware Attacks)
                        /
 Total Number of Registered Domain Names in 2022
```

This formula results in a normalised abuse rate for each TLD. We use this rate to determine the extent/scope of abuse associated with each TLD.

From the range of abuse rates in the data set, we divided the TLDs into three segments and labelled them high, medium and low risk. The Risk Score is calculated based on abuse rates that fall into the following brackets:

Low:	0.0 to 0.2
Medium:	0.2 to 0.9

[36] We were unable to find the registry cost price for .hr, .bg, .lt, .at, .ie and .de.

```
High: 0.9 and above
```

We calculated several 'global average' measures, which took account of the relative market share of each TLD bloc.

Disclaimers and limitations of this study

Approaches on measuring malicious use of domain names.

There is no single, accepted way of defining or measuring the malicious use of domain names. There has been extensive work done within the ICANN community and others, such as the Internet and Jurisdiction Policy Network, to define DNS Abuse. The approach is to limit the definition to include only those types of malicious use that lie within the scope and responsibilities of registries and registrars[37].

Not all segments of the community accept this narrow definition, favouring more expansive approaches. For example, the Fasano study defined DNS Abuse as 'any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity' and included the distribution of malicious content within that definition[38]. Moreover, the ICANN Security and Stability Advisory Committee observes that 'new types of abuse are commonly created, and their frequency waxes and wanes over time', and for this reason recommends that ICANN establish a cross-community working group to 'establish a process for evolving the definitions of prohibited DNS abuse, at least once every two years.'[39] Our own analysis notes that different definitions and measurement approaches lead to different results[40].

This current study does not attempt to resolve the controversies surrounding definitions or measurement, and our methodology is adopted for the reasons stated

[37] See, for example, Internet and Jurisdiction Policy Network, Domains and Jurisdiction Program Toolkit, 'DNS Level Action to Address Abuses' https://www.internetjurisdiction.net/domains/toolkit

[38] Bayer et al, Study on Domain Name System (DNS) Abuse, Appendix 1 - Technical Report, European Commission, 2022 at page 16 https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1/language-en/format-PDF/source-search

[39] Security and Stability Advisory Committee, SAC115, SSAC Report on an interoperable approach to addressing abuse handling in the DNS, at page 13 https://www.icann.org/en/system/files/files/sac-115-en.pdf.

[40] Alex Deacon, DNS as a vector for phishing attacks, different victims, different methodologies, different results June 2023, DNSRF https://dnsrf.org/blog/dns-as-a-vector-for-phishing-attacks--different-victims--different-methodologies--different-results/index.html

above, rather than as a contribution to the debate on definitions and measurement approaches[41], or an acceptance of any one of the available approaches.

Limitations of this study

The obvious limitation to this study is the lack of a full data set on EU ccTLD data accuracy practices. The CENTR study provides a welcome overview and aggregated data, but in many cases does not provide a per ccTLD drill down. We have derived the information relating to data practices presented below from the CENTR Report, but of the 27 member states and .eu, we only have specific information on data accuracy practices for 14 of those ccTLDs.

In any complex system, there can be multiple causes for a particular behaviour or outcome. This study identifies correlations between EU ccTLD practices relating to data accuracy and low levels of abuse in those TLDs. Numerous industry sources identify complete and accurate registration data as an essential part in maintaining a secure and stable DNS. Common sense suggests that the variety of data accuracy practices reviewed in this study, and the CENTR study that preceded it, do appear to have a positive impact in reducing malicious or abusive use of domains. Beyond observing the correlation, the proliferation of data accuracy practices, and the low abuse levels, this study cannot definitively state that it is *only* those practices that have led to such an outcome. This study briefly considers other factors relating to ccTLDs that, in the views of the authors, may *also* contribute to the impressively low levels of abuse across the EU ccTLD sector. That said, it is unlikely that the data accuracy practices of European ccTLDs adversely impact levels of abuse - the results strongly suggest the opposite.

[41] For a thorough review of the approaches to measurement of phishing, see https://dnsrf.org/blog/dns-as-a-vector-for-phishing-attacks--different-victims--different-methodologies--differe https://dnsrf.org/blog/dns-as-a-vector-for-phishing-attacks--different-victims--different-methodologies--different-results/index.html; and for a contrasting view, see https://dnsabuseinstitute.org/dns-abuse-if-we-cant-measure-it-does-it-exist/

Results and analysis

European ccTLD rates of malicious domains - market comparison

Our analysis indicates that EU ccTLDs comprise only 3% of global combined abuse reports, far lower than the percentage of their 15% market share.

Why do we consider market share? If all things were equal, then we would expect the distribution of bad domains to be equally spread across the market in proportion to market share.

If the EU ccTLDs' level of malicious domains is lower in proportion to market share than other comparators, then it may be a result of good practices in relation to data quality, or it could be a result of other factors.

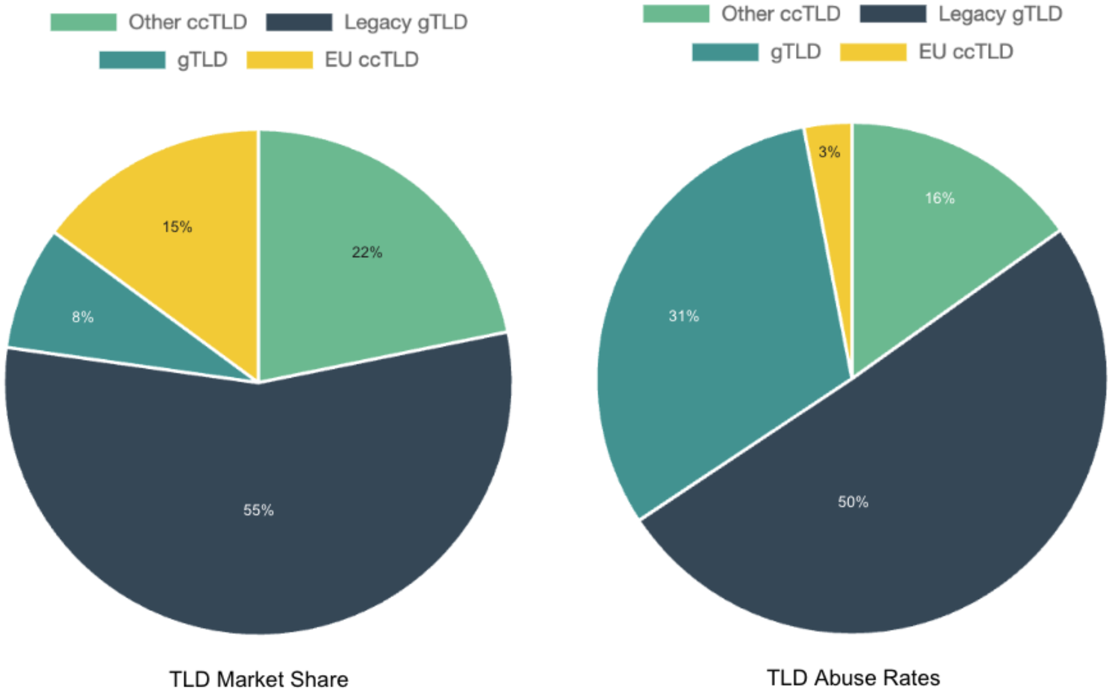


Figure 1 Global TLD market share compared with abuse rates

This finding correlates with that of the Fasano study for the European Commission (2022), which concludes that 'EU ccTLDs are the least abused in both absolute and relative terms to market share.'[42] Our research also shares the Fasano study's observation that in relative terms, new gTLDs are the most abused group, comprising an 8% market share, but representing 31% of abuse reports on our analysis.

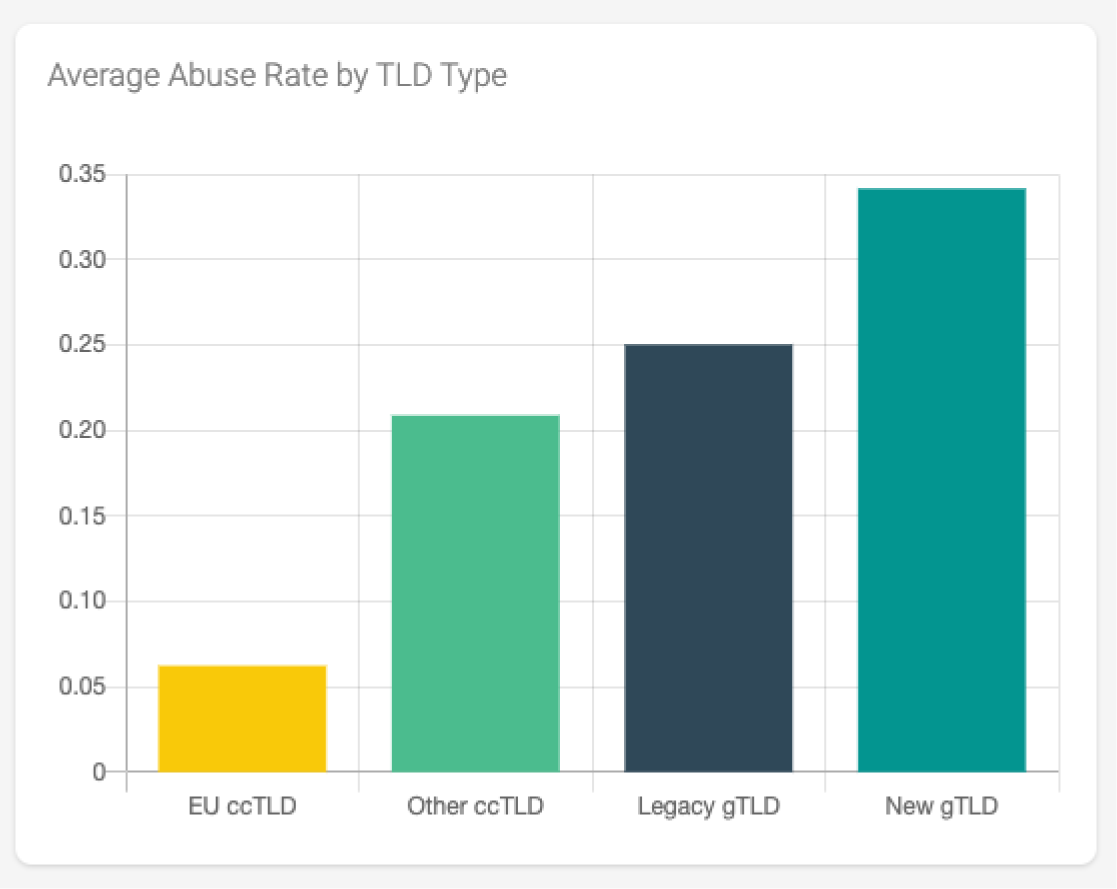
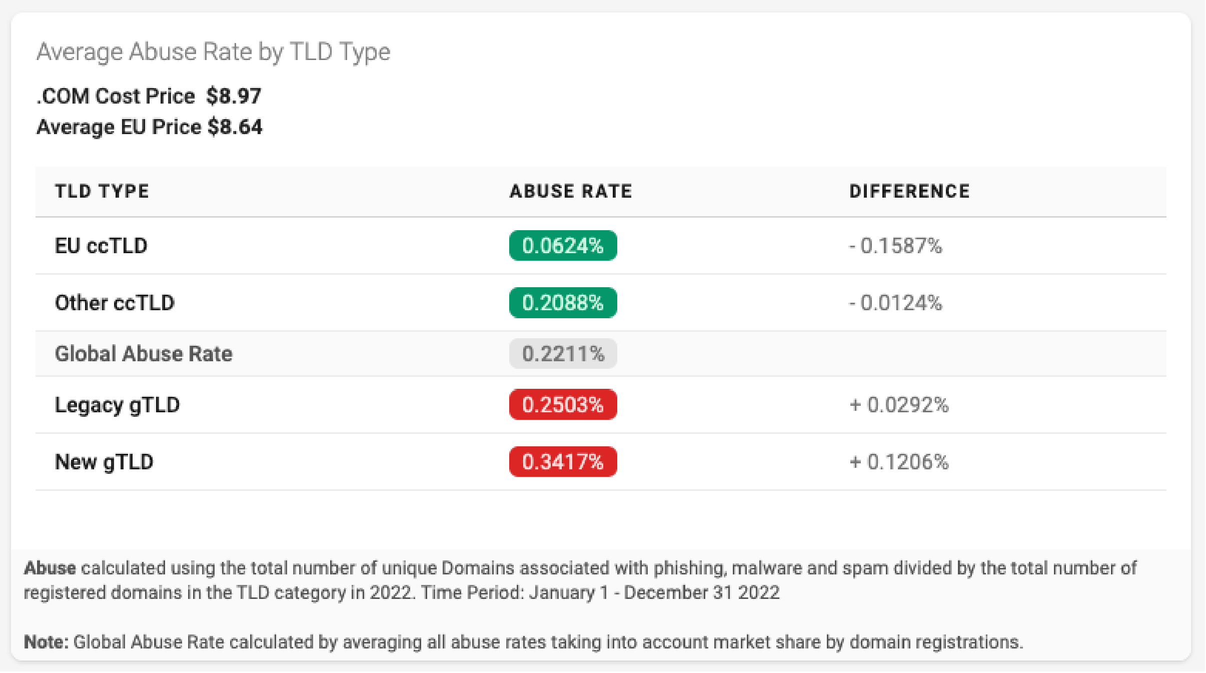


Figure 2: average abuse rate by TLD type

A comparison of the average abuse rates by TLD type highlights the different profiles of each TLD bloc. Again, the EU ccTLDs have the lowest average abuse rate of the four at just over 0.06%, followed by other ccTLDs (0.21%). The legacy gTLDs have an average abuse rate of 0.25% and the new gTLDs an average of 0.34%.

[42] Bayer, J. et al, Study on Domain Name System (DNS) Abuse, Annex 1 Technical Study, at page 26 https://op.europa.eu/en/publication-detail/-/publication/d9804355-7f22-11ec-8c40-01aa75ed71a1, European Commission 2022,



Average Abuse Rate by TLD Type

.COM Cost Price $8.97
Average EU Price $8.64

TLD TYPE	ABUSE RATE	DIFFERENCE
EU ccTLD	0.0624%	- 0.1587%
Other ccTLD	0.2088%	- 0.0124%
Global Abuse Rate	0.2211%	
Legacy gTLD	0.2503%	+ 0.0292%
New gTLD	0.3417%	+ 0.1206%

Abuse calculated using the total number of unique Domains associated with phishing, malware and spam divided by the total number of registered domains in the TLD category in 2022. Time Period: January 1 - December 31 2022

Note: Global Abuse Rate calculated by averaging all abuse rates taking into account market share by domain registrations.

Figure 3: average abuse rate by TLD type

Looking at the average abuse rates across the global set, we see that the EU ccTLDs on average have an abuse rate of 0.06%, significantly better (0.16% lower) than the global average abuse rate of 0.22%. At the other end of the scale, new gTLDs as a group have an abuse rate of 0.34%, higher by 0.12% than the global average. Both the legacy gTLDs and other ccTLDs are closer to the global average of 0.22% with scores of 0.25% and 0.21%, respectively.

The average abuse rates are useful for comparing large blocs of TLDs, but they disguise a varied picture in the underlying data. The most texture comes from within the new gTLD and Other ccTLD groups, where the standard deviation within each group is 0.63 and 0.23 respectively indicating a comparatively large difference between the TLDs with the highest and lowest abuse scores, as illustrated in the table below:

	EU ccTLD	new gTLD	Legacy gTLD	Other ccTLD
Number of domains	49,688,221	27,307,194	188,840,080	73,742,245
Average abuse rate	0.06%	0.34%	0.25%	0.21%
Standard deviation	0.04	0.63	0.17	0.23

Table 1: TLDs with highest and lowest abuse scores

Results for the EU ccTLD data set

The EU ccTLD set is more homogeneous than the global set, with a standard deviation of 0.04 indicating a closer clustering of the results around the average score for the EU group of 0.06%.

We ranked the abuse score of all 577 TLDs in our study (remember that TLDs with fewer than 1000 names were excluded from the data set under analysis), with 1 having the lowest level of abuse, and 577 having the highest. The EU ccTLDs were positioned within a range of 34 (.cy for Cyprus) to 366 (.ro for Romania) within the global abuse ranking. Applying our risk scoring to the EU ccTLDs, all were designated as low risk.

The full data sets are set out in Appendix 1.

Global Abuse rank (/577)	TLD	Country	Domain Count	Penetration of ccTLD by 1,000 of population	Abuse rate	Risk score
42	dk	Denmark	1,359,434	250	0.02%	Low
59	de	Germany	16,553,293	209	0.03%	Low
60	cz	Czech Republic	1,402,892	139	0.03%	Low
61	nl	Netherlands	6,027,494	359	0.03%	Low
92	be	Belgium	1,655,929	151	0.04%	Low

Table 2: Top 5 EU ccTLDs with more than 100,000 domains under management

Table 2 shows the EU ccTLDs in this study, the number of domains, market penetration rate, and abuse rate for the year in question (1 Jan 2022-31 December 2022). The final column is the risk score, described in the methodology.

The entire group of EU ccTLDs perform extremely well, all falling below the global average abuse rate, and all being ranked as low risk according to the parameters stated in our methodology.

Findings - Research questions 1 and 2

Our analysis indicates that the answers to our first two research questions are:

RQ1: **Comparative abuse rates** What are the rates of malicious use in European ccTLD compared with other market comparators (legacy gTLDs, new gTLDs, other ccTLDs - together 'TLD blocs')?

The EU ccTLD abuse rates are the lowest of any TLD bloc within the global market.

RQ2: Abuse rates and market share How do the rates of malicious use by TLD blocs compare with the relative market share of each TLD bloc?

The EU ccTLD abuse rates are significantly lower than the market share of the EU ccTLDs.

Correlation with anti-abuse measures

The CENTR Report[43] highlights diverse proactive and reactive measures taken by 26 EU based ccTLDs, ranging from proactive data quality checks, to implementing 'know your customer' measures that are familiar from the financial services sector.

According to the CENTR Report, ad hoc measures to ensure data accuracy are the most common approach among the EU ccTLDs, with 14 of the 26 EU ccTLDs who responded to CENTR's survey taking such an approach. The majority combined ad hoc measures with a variety of other measures. With abuse rates are low across the EU region, our analysis suggests that the **combination of data assurance measures demonstrate effective practices** in mitigating malicious use of domains.

A minority of the EU ccTLDs undertake checking prior to the point of registration (referred to in the NIS2 Directive as *ex ante* checking). These checks can include predictive technologies, but at the date of the CENTR Report neither the 'know your customer' nor predictive technologies were widely adopted through the region.

Key findings from the CENTR Report that are relevant to this study:

- Approximately **half of EU ccTLDs** surveyed by CENTR undertake automated **data syntax validation** on the creation of domain names. These are described as automated checks on reachability, syntax and other rule-based checks.
- Diverse measures are undertaken by EU ccTLDs to ensure data accuracy. The **most commonly adopted systematic identity verification checks are related**

[43] Registration data accuracy in European national domain registries: existing practices and challenges, CENTR, October 2022 https://centr.org/library/library/download/10478/7435/41.html

to 'legal entities' (eg, companies, organisations), with approximately 30-35% performing verification checks at registration.

- A minority, fewer than 20%, of the registries surveyed by CENTR undertook systematic identity verification for natural persons at the point of registration.
- The most commonly occurring measure was **ad hoc data checks** in response to complaints or reasonable suspicion.
- There is a **lack of standardised, pan-European electronic identity processes.** Only 5 out of 33 respondents were reported by CENTR to be using eID methods to verify registrant identities, of which three were highlighted in specific case studies. These were .eu for European Union with an abuse score of 0.07%, .be for Belgium with an abuse score of 0.04% and .dk for Denmark with an abuse score of 0.02%.

Reviewing the results of our quantitative analysis of malicious use of domains with the data practices described in the CENTR Report, we draw the following conclusions with regard to our third research question:

RQ3: Impact of demonstrated effective practices What is the correlation between proactive anti-abuse measures as documented in the recent CENTR Report on data practices[44]?

There is a correlation between the presence of data quality practices among EU ccTLDs and low abuse rates.

Approximately half the EU ccTLD group perform automated syntax validation - for example that a telephone number, email address, town/city or country conform to the expected format. Of the EU ccTLDs that provided information on their data quality practices, all undertook additional (often human-mediated) measures to ensure data quality. At the current time, the picture that emerges is that **the combination of measures - such as automated data syntax validation and ad hoc measures - are likely to be the defining factors that make the difference for EU ccTLDs and help to explain their strong performance as a group**.

Implementation of eID is still in early stages in the DNS industry, and as the CENTR Report points out, no pan-European solution currently exists. All three registries that have implemented eID also implement multiple other measures. While .dk is near the

[44] https://centr.org/library/library/download/10478/7435/41.html)

top of the European ranking, .at and .eu are more middle ranking within the EU group. It is therefore **too early to determine** the extent to which implementation of eID reduces malicious use of domain names.

Global Abuse rank (/577)	TLD	COUNTRY	Ad hoc measures	One or more other measures	eID
34	cy	Cyprus			
42	dk	Denmark	x	x	x
58	mt	Malta	x	x	
59	de	Germany	x		
60	cz	Czech Republic	x	x	
61	nl	Netherlands		x	
92	be	Belgium			
93	fi	Finland			
105	se	Sweden			
117	es	Spain			
120	ie	Ireland	x	x	
132	sk	Slovak Republic	x		
158	ee	Estonia	x	x	
165	at	Austria	x	x	x
179	it	Italy	x	x	
186	lu	Luxembourg			
192	eu	European Union	x	x	x
193	lv	Latvia	x	x	
207	lt	Lithuania			
217	bg	Bulgaria			
229	fr	France	x	x	
233	hu	Hungary	x	x	
240	gr	Greece			
273	si	Slovenia			
296	pt	Portugal	x	x	
299	hr	Croatia			

Global Abuse rank (/577)	TLD	COUNTRY	Ad hoc measures	One or more other measures	eID
301	pl	Poland			
366	ro	Romania	x	x	

Key: grey = no data; green = ccTLD has implemented eID.

Table 3: EU ccTLDs data assurance measures, ordered by global abuse rank

Full results showing the anti-abuse measures of EU ccTLDs for which we have data are set out at Appendix 2. Table 3 indicates the position within the abuse ranking of EU ccTLDs of those three registries that have implemented automated registrant identity checks (marked in light green). Greyed out rows indicate a lack of data.

We encourage all European ccTLDs to share their data accuracy practices, so that a fuller understanding of industry effective practices can emerge. For example, we have no information about four out of the top ten EU ccTLDs on their data practices and are thus unable to infer whether those practices have an impact on abuse.

What other factors might account for differences in rates of malicious domains?

Our fourth research question asked whether there may be **any other factors** that might impact the levels of malicious use of domains in the EU ccTLD environment. The EU ccTLDs have many advantages arising from the economic strength and maturity of domestic markets, with established cybersecurity institutions and regulatory frameworks. They have evolved within a data protection environment, requiring them to balance their legal obligations to safeguard individuals’ privacy with the demands of public safety and others. The majority are non-profits with a public purpose, and being tightly bound to their country or territory, have close links with a wide range of domestic stakeholders. There are significant other quality markers among the EU ccTLDs - high renewal rates, high levels of ‘developed web content’ and successful market penetration.

Other common factors among the EU ccTLDs are that they operate a ‘thick’ WHOIS model, and distinguish between legal and natural persons.

To what extent do data checks and pricing impact market penetration?

In an intensely competitive, global market, with notoriously low margins at the retail or registrar level, it may be supposed that adding friction to the purchase process of a particular TLD might have an adverse impact on growth and market penetration.

We divided the number of registrations for each of our EU ccTLDs by the number of population in the country or territory represented by the ccTLD. This gave an average penetration rate of 105 domains per 1000 of the population. The lowest rate was 9, and the highest was nearly 360 per 1000.

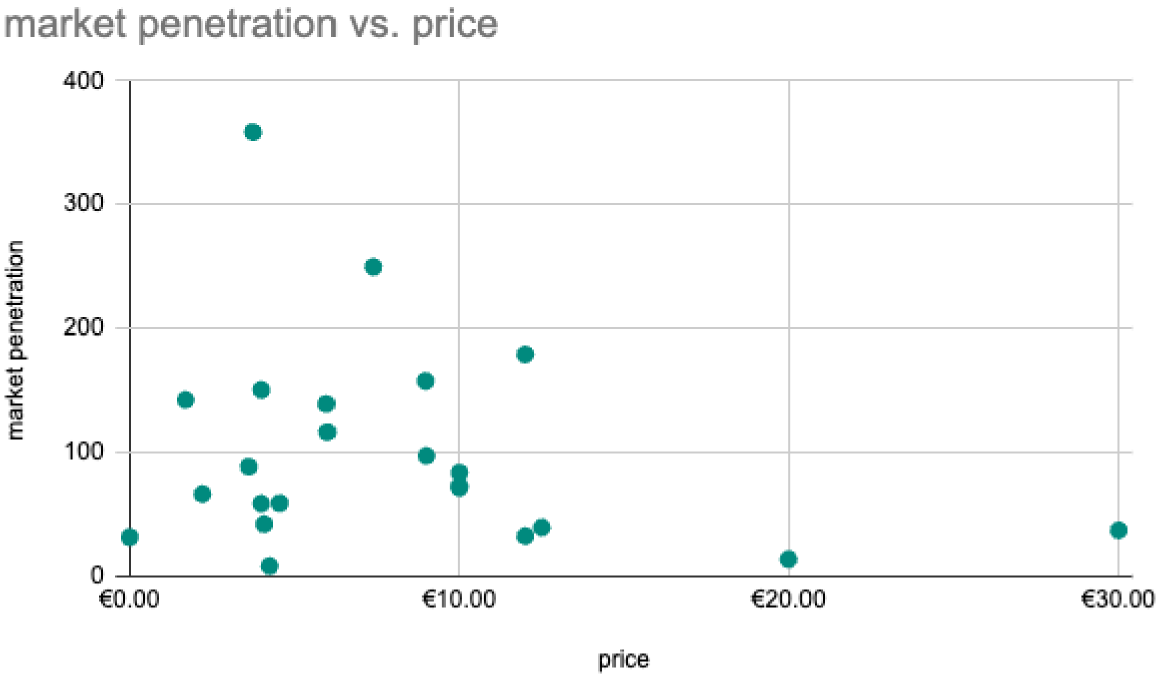


Figure 4: EU ccTLD market penetration vs registry trade price

Correlating market penetration with cost price (Figure 4) suggests that below the level of approximately €10.00, there is little impact on market penetration. Some of those EU ccTLDs with the lowest market penetration also have low pricing. Our conclusion is that price alone does not explain market penetration. While it might be expected that low pricing might attract criminal or abuse use, the evidence does not suggest this, and we conclude that **proportionate data quality practices in low price ccTLDs seem effective in mitigating risks of criminality or malicious domain name abuse.**

Correlating between the presence of data verification and validation practices outlined in the CENTR Report, we found that there was little or no correlation between data practices and market penetration (see table at Appendix 1). For example, Denmark had a market penetration of 250 per 1000 of population, while also having extensive data verification practices. Conversely, some of the registries with the lowest market penetration rates also undertake data verification steps.

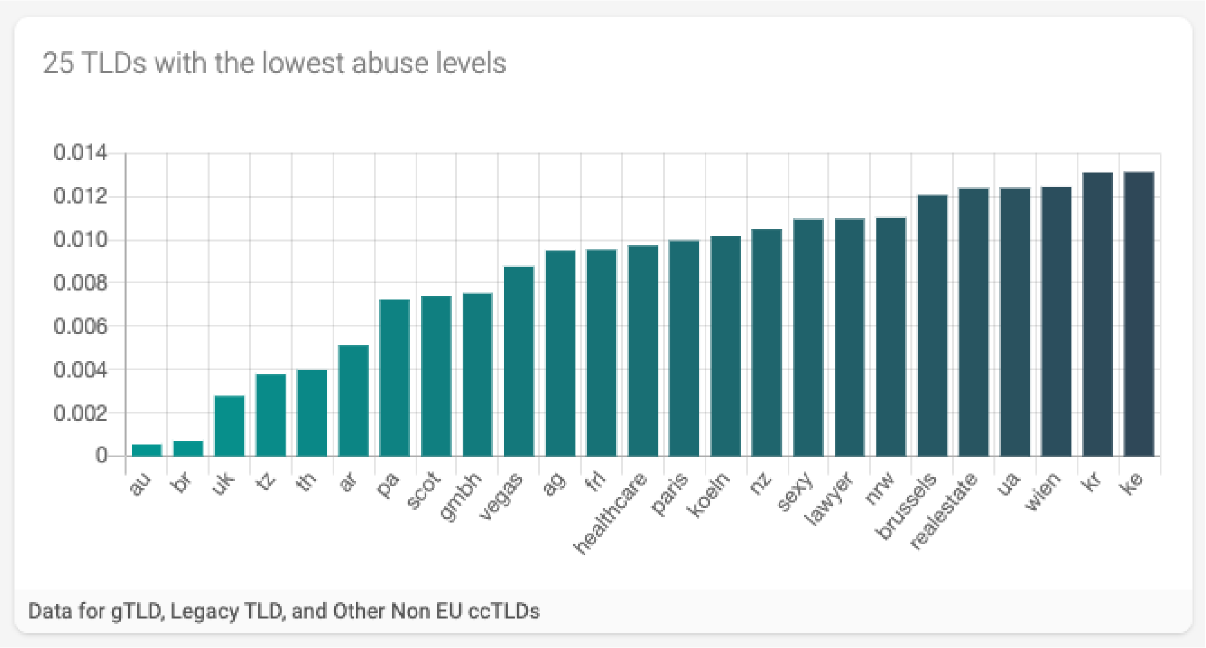
Good practices outside of the European Union

The European ccTLDs have diverse data quality practices and as a bloc have the lowest average rate of abuse globally, at 0.06%, compared with a global average of 0.2%.

	EU ccTLD	New gTLD	Legacy gTLD	Other ccTLD
Lowest abuse rate with >100,000 domains	.dk, 0.02%	.africa 0.03%	.org 0.1%	.au 0.0006%
Risk score	Low	Low	Low	Low
Highest abuse rate with > 100,000 domains	.ro, 0.17%	.cfd 3.3%	.info 0.5%	.ml, 0.9%
Risk score	Low	High	Medium	High

Table 4: Global rates of abuse (for TLDs with more than 100,000 domains)

As indicated by Table 4, if we exclude the smaller registries, with less than 100,000 domains, the highest abuse rate is found in .cfd at 3.3% of 275,000 domains. The lowest abuse rate in our data set was found in .au for Australia, at 0.0006% of 4 million domains. The ten TLDs with the lowest rates of abuse in our study, with a range of 0.001%-0.009% were .vegas, .gmbh, .scot (new gTLDs), and .pa for Panama, .ar for Argentina, .th for Thailand, .tz for Tanzania, .uk for United Kingdo m, .br for Brazil and .au for Australia (Other ccTLDs). Therefore, **data quality practices outside of the EU should be investigated to gain further insights into global good practice.**


25 TLDs with the lowest abuse levels

Data for gTLD, Legacy TLD, and Other Non EU ccTLDs

Figure 5: 25 TLDs with the lowest abuse rates.

The TLD with the lowest abuse rates in the world is .au, the ccTLD for Australia. With 4.25 million domains, .au has a market penetration of 166 domains per 1,000 of population. The cost price to registrars is equivalent to €5.10 per year. Under its legal policies, the .au registry auDA applies both eligibility criteria and identity validation at the point of registration. To satisfy the eligibility criteria, a registrant must have an Australian presence, and the domain must match the registrant’s name, acronym, or trademark, goods services or events, among other things [45].

Third place in the global ranking for low abuse rates is .uk. One of the largest TLDs in the world, .uk has open registration policies, meaning that there is no residency or eligibility criteria for registrants. With more than 11 million domains, the .uk TLD has a market penetration rate 165 per 1,000 of population. The cost price to registrars is equivalent to €4.50.

[45] For the validation, eligibility and residency requirements, see auDA’s domain name licence terms 2019, https://www.auda.org.au/policy/au-domain-administration-rules-licensing#audirect at clause 2.3 and 2.4

Nominet confirmed that data accuracy is a stated priority in both their registrar and registrant agreements. They occasionally take enforcement action against registrars for failure to comply with those data quality and validation requirements, but told us 'this is proportionate and usually through informal dialogue in the first instance or in annual compliance meetings.'

At the point of registration, Nominet validates all new registrations, 'but higher risk phishing terms identified go through additional verification procedures.' Like the majority of its EU counterparts, the .uk registry responds to ad hoc complaints or issues of concern. It does not validate data periodically or use eID at present. It does conduct external verification using external data sets, but does not outsource this function. It performs ad hoc checks on postal or phone details where there are suspicious characteristics.

Conclusions

For more than two decades, the publication of WHOIS registration data has been highly contested within the ICANN multistakeholder community. With the advent of the EU's privacy law, GDPR, in 2018, the majority of WHOIS registration data 'went dark'. Policy processes identified a lack of a legal obligation in statute that required TLD registries and registrars to provide WHOIS. In December 2022, The European Union enacted the NIS2 Directive, with requirements that TLD name registries and registrars have policies and procedures, including verification procedures to ensure accurate and complete registration data.

Against this background, this study brought together an evidence-based analysis of abuse rates across more than 340 million domain names, to understand the impact of data practices among EU ccTLDs. Using the DAP.LIVE platform, we brought together multiple sources of data to understand the extent of phishing, malware and spam reports across the global set of TLDs. We created specific queries and dashboards to display the data. We also undertook desk-based research on registration figures, population size, and pricing among EU ccTLDs, as well as relevant laws, policy processes, and abuse studies. These are set out in the methodology, along with disclaimers and limitations to the study and its findings.

We posed four research questions, and the data demonstrated that **EU ccTLDs have the lowest abuse rates of any TLD bloc within the global market**. As a group, the EU ccTLDs accounted for only 3% of malicious use compared with their global market share of 15%. In contrast, the set of new gTLDs accounted for 31% of malicious domains, despite a market share of only 8%. **The EU ccTLD abuse rates are significantly lower than the market share of the EU ccTLDs**.

The data indicates there is a correlation between EU ccTLD low abuse rates and the EU ccTLDs efforts to verify registration data. Evaluating the impact on abuse rates of the data practices undertaken by EU ccTLDs, the **automated syntax validation and ad hoc, proportionate data checks done** in response to reasonable suspicion that a domain name is malicious are the most widely adopted practices across the EU ccTLD group.

As a group, **the EU ccTLDs have numerous advantages which could help to explain their low levels of abuse** - such as the economic strength and maturity of domestic markets, having evolved within a data protection framework, having close links with local stakeholders and operating a non-profit model. Interestingly, the presence of **data checks does not seem to impede market penetration** for this group, nor does the comparatively low cost price of this group seem to attract abuse - quite the opposite.

Acknowledgements

This research project was funded through the generosity of the Business and Intellectual Property Constituencies of ICANN.

The authors would like to thank Andrew Bennett of Netistrar for additional research, the peer reviewers for their constructive comments on the draft report, and in particular to Peter van Roste of CENTR for reviewing an early draft and answering our questions on EU ccTLDs.

Responsibility for the report’s conclusions and any errors remain with the authors.

APPENDICES

Appendix 1: abuse rates and risk scoring

Global Abuse rank (/577)	TLD	COUNTRY	DOMAIN COUNT	POPULATION 2021	Penetration of ccTLD by 1,000 of population	ABUSE REPORTS	ABUSE RATE	COST PRICE	RISK SCORE
34	cy	Cyprus	23,443	1,244,000	14	4	0.02%	€ 20.00	Low
42	dk	Denmark	1,359,434	5,857,000	250	275	0.02%	€ 10.00	Low
58	mt	Malta	19,631	519,000	37	5	0.03%	€ 30.00	Low
59	de	Germany	16,553,293	83,196,000	209	4301	0.03%		Low
60	cz	Czech Republic	1,402,892	10,506,000	139	370	0.03%	€ 6.00	Low
61	nl	Netherlands	6,027,494	17,533,000	359	1636	0.03%	€ 4.00	Low
92	be	Belgium	1,655,929	11,593,000	151	595	0.04%	€ 4.00	Low
93	fi	Finland	528,563	5,541,000	97	190	0.04%	€ 9.00	Low
105	se	Sweden	1,445,124	10,416,000	143	567	0.04%	€ 2.00	Low
117	es	Spain	2,011,540	47,416,000	42	837	0.04%	€ 4.00	Low
120	ie	Ireland	311,054	5,033,000	66	133	0.04%		Low
132	sk	Slovak Republic	451,708	5,447,000	84	203	0.04%	€ 10.00	Low

Global Abuse rank (/577)	TLD	COUNTRY	DOMAIN COUNT	POPULATION 2021	Penetration of ccTLD by 1,000 of population	ABUSE REPORTS	ABUSE RATE	COST PRICE	RISK SCORE
158	ee	Estonia	159,255	1,331,000	117	83	0.05%	€ 6.00	Low
165	at	Austria	1,484,924	8,956,000	164	836	0.06%		Low
179	it	Italy	3,163,350	59,110,000	59	1921	0.06%	€ 4.00	Low
186	lu	Luxembourg	103,703	640,000	179	65	0.06%	€ 12.00	Low
192	eu	Europe	3,640,454	443,200,000	8	2405	0.07%	€ 4.00	Low
193	lv	Latvia	128,523	1,884,000	73	85	0.07%	€ 10.00	Low
207	lt	Lithuania	222,413	2,801,000	81	160	0.07%		Low
217	bg	Bulgaria	76,760	6,878,000	9	58	0.08%		Low
229	fr	France	3,995,952	67,750,000	59	3199	0.08%	€ 5.00	Low
233	hu	Hungary	852,551	9,710,000	89	692	0.08%	€ 4.00	Low
240	gr	Greece	[ ]	10,641,000	39	406	0.08%	€ 13.00	Low
273	si	Slovenia	141,613	2,108,000	71	146	0.10%	€ 10.00	Low
296	pt	Portugal	390,376	10,325,000	158	434	0.11%	€ 9.00	Low
299	hr	Croatia	117,948	3,899,000	32	134	0.11%		Low
301	pl	Poland	2,370,612	37,747,000	67	2741	0.12%	€ 2.00	Low
366	ro	Romania	563,524	19,120,000	33	927	0.16%	€ 12.00	Low

Appendix 2: Data quality practices (source: CENTR)

Global Abuse rank (/577)	TLD	COUNTRY	At registration	Ad hoc	Periodically	Use eID	External verification services / checks	Require address in country / region	Checks on postal / phone details / bank account	Copy of registrant passport
42	dk	Denmark	X	X		X	X		X	
58	mt	Malta	X	X						
59	de	Germany		X						
60	cz	Czech Republic		X			X	X	X	
61	nl	Netherlands					X			X
120	ie	Ireland	X		X					
132	sk	Slovak Republic		X						
158	ee	Estonia	X	X	X					
165	at	Austria		X		X	X			

Global Abuse rank (/577)	TLD	COUNTRY	At registration	Ad hoc	Periodically	Use eID	External verification services / checks	Require address in country / region	Checks on postal / phone details / bank account	Copy of registrant passport
179	it	Italy		X	X					
192	eu	Europe		X		X			X	X
193	lv	Latvia	X	X	X					
229	fr	France		X						X
233	hu	Hungary	X	X						
296	pt	Portugal	X	X						
366	ro	Romania		X						X

Note that data is not available for all EU ccTLDs. Data in this table is partly derived from the text and partly from data / charts in the CENTR study.

Appendix 3 About the DNS Research Federation

The DNS Research Federation is a not for profit organisation dedicated to raising awareness of the domain name system's impact on cybersecurity, policy and technical standards. The DNSRF achieves its mission through education and research, improving access to data, and engagement in technical standards.

The DNSRF sits at the intersection of policy and technology. We fund research, engage in technical standards, and bring technical tools and objective data relating to the Internet's unique identifier systems ̄ especially the DNS ̄ to researchers, public safety and industry stakeholders.

Exploring the linkages between traditional Internet governance, the strategic importance of technical standards, and contemporary policy challenges, the DNS Research Federation connects up islands of scholarship and communities of expertise.

About the authors

Emily Taylor

Emily Taylor is a founder of the DNS Research Federation and CEO of Oxford Information Labs. A lawyer by training, Emily has worked in the Internet governance and cybersecurity environment for more than 20 years. Emily developed the WHOIS policy for Nominet and went on to Chair ICANN's first WHOIS review team. She also served on the first phase of the ICANN Expedited Policy Development Process on gTLD registration data. Emily is an associate fellow at Chatham House and editor of the Journal of Cyber Policy. She is a regular commentator on technology issues in news and broadcast media including the BBC and Sky News. Emily is a graduate of Cambridge University, and has an MBA from Open University.

Alex Deacon

Alex is a Senior Research Fellow at the DNS Research Federation and the founder of Cole Valley Consulting, where he works with large technical and media organisations to solve complex issues that bridge the worlds of Internet technology, infrastructure, policy, governance, standards and cybersecurity. Before establishing his consultancy, Alex held senior technical leadership positions at The Motion Picture Association, Neustar, Symantec and Verisign.

Nathan Alan

With 10+ years experience building and maintaining websites and mobile applications, Nathan is an expert in modern javascript frameworks, and has worked extensively with Angular, KnockoutJS, and Durandal. Nathan also has experience creating hybrid apps that work across multiple platforms for well known high street retailers, delivery companies, and domain registrars. Nathan is Director of Engineering for Oxford Information Labs and holds a BSC in IT from Oxford Brookes University.