



06 February 2026 • *Brussels, Belgium*

CENTR Board Statement on EU action plan on fighting online fraud

Summary of CENTR Key recommendations

- EU ccTLDs are consistently being recognised as the zones with the lowest levels of abuse.
- EU ccTLDs' low abuse rates can be attributed to a variety of practices in place across EU ccTLDs, tailored to each individual ccTLD and applicable regulatory framework. There is no 'one size fits all' approach to tackling abuse online.
- Domain-level action to counter online fraud perpetrated through associated services can only be considered by competent public authorities in exceptional circumstances, where no other effective means are available.
- To ensure consistent application of the existing rules across the single market, the European Commission should develop guidelines for competent authorities on assessing proportionality criteria when involving DNS service providers and ccTLDs.
- EU ccTLDs are already governed by a wide range of EU regulations aimed at tackling online abuse. Introducing additional fraud-prevention requirements for EU ccTLDs is therefore unnecessary, given their already low levels of abuse and the fact that the EU regulatory framework applicable to the DNS space is still relatively new.
- EU ccTLDs cooperate with authorities and take a range of voluntary measures, within their technical remit, including broader educational activities to warn end-users of how to stay safe online. Voluntary cooperation between EU ccTLDs and public competent authorities should be encouraged, and where possible, facilitated by making additional resources available to authorities for their capacity-building activities.

Introduction

CENTR is the association of European country code top-level domain registries (ccTLDs). All EU Member States and EEA country ccTLDs (such as .fr for France and .no for Norway) are members of CENTR.

CENTR members are at the core of the public internet, safeguarding its stability and security. The majority of European ccTLDs are non-profit organisations or SMEs, providing an internet infrastructure service in the interest of and in close cooperation with their local internet communities (e.g., end-users, CSIRTs, law enforcement and other competent authorities).

Domain names are the foundational pieces of internet infrastructure necessary for many online services (e.g., website, application, platform) to be accessible online. ccTLDs are responsible for operating and maintaining the technical Domain Name System (DNS) infrastructure for their top-level domain.

The DNS is a well-established network protocol at the heart of the internet infrastructure. It provides a navigation function to map user-friendly domain names to numeric IP addresses. ccTLD registries maintain a domain name registration database that contains technical and administrative data necessary to provide DNS services, as well as identity and contact information of domain name holders. ccTLDs are considered “essential entities” under the NIS 2 Directive.¹

ccTLDs only hold information enabling users to navigate the internet but do not store, transmit or enhance any third-party content online.² ccTLDs are only one of several internet infrastructure actors that enable users to reach content or send emails. ccTLDs enable domain names to point to an IP address on which these services (e.g., a website or an email server) are hosted.

In the context of the EU action plan on fighting online fraud, CENTR wishes to highlight the following input to form the evidentiary basis for any future EU action within this area.

Evidentiary basis for tackling “DNS abuse”

The European Commission’s call for evidence for fighting online fraud highlights that “[a]buse of the Domain Name System (DNS) is often how online fraud is committed”, and that “phishing, farming, botnet attacks and spam distribution are also growing in scale and frequency”.

When considering any further action to tackle the issue of “abuse of the DNS”, CENTR urges the EU policymakers to carefully assess the need for further interventions at the EU level, taking into consideration existing voluntary efforts taken by ccTLDs, the global multistakeholder discussions, as well as the rich EU legislative body from cybersecurity, consumer protection to financial regulation that is already governing safety and security issues within the EU domain space.

¹ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (‘NIS 2 Directive’).

² CENTR, “[Domain name registries and online content](#)” (2022).

Abuse of the DNS and online fraud

The internet's essential infrastructure, such as the DNS, is necessary for many online services to be made available online, e.g., website, platform, email server, etc. However, these services are connected to and offered on top of a domain name and are provided by other intermediaries (such as web hosting companies, mail service providers, etc).

It is difficult to clearly draw the distinction between abuse of the DNS and abuse perpetrated through the use of DNS, because any activity online, legal or otherwise, typically requires a domain name and the rest of the DNS infrastructure to be set up before it can reach end-users. As a result, it has been challenging to establish a coherent and universally recognised “DNS abuse” definition. The European Commission’s DNS Abuse Study recognises this difficulty and proposes a broader definition that essentially equates “DNS abuse” with any cybercrime.³ However, such broad definitions can easily lead to false assumptions and misleading promises that cybercrime or online fraud can be solely mitigated or prevented at the DNS level, or via actions taken by DNS operators, such as TLD registries and DNS service providers. This view disregards the complexity of the internet’s infrastructure ecosystem, the variety of actors responsible for making services and content available online, and the collective responsibility of all stakeholders and parties (infrastructure, industry, competent authorities, policymakers) to increase online trust and ensure a safe space for users.

Consequently, instead of blanket and broad definitions of “DNS abuse”, it is advisable to take a more pragmatic approach and identify what types of actions, practices and mitigation measures are available for different intermediaries and technical infrastructure operators across the stack. If any mitigation and prevention measures are considered for each operator, these must be technically possible, proportionate and necessary in a democratic society, depending on the role of the operator, proximity to unwanted content or end-user, as well as the likelihood of unwanted collateral damage to the infrastructure or fundamental rights of end-users.

The role of ccTLDs in addressing abuse

Online fraud usually involves contact with the end-user and includes deceptive practices designed to extort information, money or property. According to the European Commission, online fraud is one of the categories of cybercrime, including “large-scale fraud” that “can be committed online through instruments such as identity theft, phishing, spam and malicious code”.⁴ By simply registering a domain name without creating a user-facing webpage, setting up a mail server to deliver unsolicited communications in the form of spam, or establishing a connected crypto-wallet, malicious actors are limited in their ability to deceive end-users. Therefore, online fraud can be largely categorised as “content abuse”, as it requires communication to end-users (e.g., spam), and/or lookalike or deceptive websites.

ccTLDs do not have the technical capacity to directly target unlawful content or behaviour online. They can only suspend the underlying technical infrastructure, i.e., the domain name, that will disrupt the functioning of all

³ CENTR [Comment on the DNS Abuse study](#), 30 March 2022.

⁴ European Commission, [“Cybercrime”](#), 31 October 2024.

associated services (such as website or email hosting). However, this drastic measure does not remove illegal content from the internet: the unlawful content remains reachable through other means (e.g. directly typing the IP address in the browser) or can move to a different infrastructure provider (e.g., domain hopping). The rule of thumb in mitigating content abuse, involving fraud that is primarily perpetrated through content and intermediary services connected to a domain name, is that intermediaries closer to the content (e.g., hosting service provider) are more equipped to address unwanted behaviour and take down unwanted content for good.⁵

Nevertheless, many EU ccTLDs consider fake and deceptive websites associated with the domain names within their zones as unwelcome behaviour, where a ccTLD registry can take action within its technical and legal limits. While the ccTLD registry cannot act against specific content, the use of a domain name for deceptive and fraudulent activity may be considered a violation of its Terms of Service⁶, or trigger additional domain name holder verification checks⁷. In addition, ccTLDs rely on the expertise of competent public authorities to identify and take actions against fraudulent activity associated with a domain name.⁸

As content abuse is not perpetrated through the infrastructure managed by a ccTLD registry, it is not reasonable to expect registries to proactively seek out any misconduct taking place via services offered by other intermediaries. However, when other intermediaries fail to act, and the significant harm to end-users persists, ccTLD registries can be approached by competent authorities and take action based on a lawful order. This is already codified in the EU consumer protection acquis⁹ and is in line with the Digital Services Act (DSA)¹⁰, both of which codify a proportionality criteria that must be followed when action at the DNS-level is considered. Recent financial regulation, specifically in the crypto markets space, follows a similar approach and includes a possibility for supervisory authorities to order deletion of domain names, “where no other effective means are available” to protect the interests of crypto-asset holders.¹¹

Due to domain-level action being a drastic intervention at the infrastructure level, following a mandatory proportionality assessment is a must for any response requiring intervention from ccTLDs in case of fraudulent activity involving domain names. Domain-level action to counter online fraud perpetrated through associated services can only be considered by competent public authorities in exceptional circumstances, where no other effective means are available. EU-level action can include helpful guidelines for authorities to assess

⁵ CENTR, “[Domain name registries and online content](#)” (2022).

⁶ For example, [Punktum dk](#) (.dk) can suspend a domain name if it is used for obviously illegal acts and where an attempt has been made to obtain a legal injunction or prohibition against the infringer or other technical intermediaries.

⁷ For example, EURid’s (.eu) [Abuse Prevention and Early Warning System](#) is designed to predict whether a domain name can potentially be used in an abusive manner.

⁸ For example, DNS Belgium (.be) [cooperates](#) with the Belgian authorities, so that upon receiving a request, it is authorised to suspend domain names that are connected to fraudulent webshops or phishing websites.

⁹ Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws (‘CPC Regulation’).

¹⁰ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (‘Digital Services Act’).

¹¹ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (‘MiCA’).

proportionality criteria when involving DNS service providers and ccTLDs, to help with its consistent application across EU single market.

Mitigation and prevention practices for tackling abuse

A variety of different actors and fora consistently recognise EU ccTLDs as the zones with the lowest levels of abuse¹². The consistently low levels of abuse across EU ccTLDs cannot be attributed to one or two overarching practices and stem from a variety of reasons, tailored to each individual ccTLD and applicable regulatory framework.

EU ccTLDs are already subject to a plethora of EU regulation, including strict cybersecurity risk management measures due to their status as “essential entities” within digital infrastructure¹³, registration data accuracy obligations with identity verification requirements¹⁴, content moderation framework under the DSA, e-Evidence access provisions for cross-border criminal investigations¹⁵, as well as considered one of the key actors within EU-wide consumer protection and financial regulation enforcement regime. As some of the aforementioned regulation is relatively recent or still in its transposition phase, its long-term effects, including its influence on non-EU actors who are subject to the same regulatory requirements as EU ccTLDs, will only become apparent in later stages. As a result, there is no urgency in addressing internet infrastructure, including ccTLDs, in the EU action plan on online fraud, as most of the DNS-relevant regulation with anti-abuse aspects has been adopted in recent years. More stringent or additional regulatory requirements applicable to EU ccTLDs in order to tackle abuse online are not justified, due to already low abuse rates and a complex regulatory environment that has not had a chance to be properly implemented yet and make a dent on non-EU actors.

In addition to regulatory obligations, EU ccTLDs have proven to be reliable and cooperative partners in tackling abuse online, also on a voluntary basis.

EU ccTLDs cooperate with authorities and take a range of voluntary measures, within their technical remit. For example, EU ccTLDs have established channels to exchange information with the police, consumer protection authorities or local Computer Emergency Response Teams (CERTs) on suspicious and potentially malicious

¹² European Commission, [Study on Domain Name System \(DNS\) abuse](#) (2022), DNS Research Federation, [Habits of excellence: Why are European ccTLD abuse rates so low?](#) (2023), World Economic Forum, [Fighting Cyber-Enabled Fraud: A Systemic Defence Approach](#) (2025).

¹³ Article 21 of the NIS 2 Directive, European Commission Implementing Regulation (EU) 2024/2690 laying down rules for the application of the NIS 2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures[...] with regard to DNS service providers, TLD name registries et al.

¹⁴ Article 28 of the NIS 2 Directive obliges TLD registries and entities providing domain name registration services to collect and maintain an accurate and complete database of domain registration data.

¹⁵ Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (‘e-Evidence’).

domain names.¹⁶ The registries also flag domain names with suspicious behaviour to the authorities, upon which the authorities can investigate further and take the appropriate action.¹⁷ Some EU ccTLDs also develop technical solutions to detect suspicious domain names based on criteria such as the previous patterns of historical domain abuse, choice of a registrar, date of registration, the domain name itself, etc.¹⁸

Important abuse prevention and mitigation measures also include general public awareness-raising campaigns and educational programmes targeting end-users that EU ccTLDs organise as part of their mission to serve their local internet communities. These educational efforts consist of guides on how to be safe online and avoid online fraud, how to seek help after being defrauded, and how to report illegal content to competent authorities.¹⁹

As voluntary cooperation between ccTLDs' public competent authorities has proven to be an effective way to increase safety online, these efforts should be encouraged, and where possible, facilitated with additional resources available for authorities for their capacity-building activities.

The EU action plan on online fraud aims to “significantly reduce the occurrence and impact of online fraud throughout the EU” by reinforcing coordination and improving cross-border and multistakeholder cooperation. At the global level, the discussions on mitigating and preventing DNS infrastructure abuse²⁰ take place, amongst others, in the multistakeholder setting of ICANN, where the technical community, private sectors, civil society, academia, and governments are actively participating in the deliberations on tackling abuse involving DNS infrastructure. In order to collectively tackle DNS infrastructure abuse at a global scale, the EU should continuously engage in the discussions and policy development processes in ICANN.

¹⁶ For example, SIDN (.nl) [cooperates](#) with the Police National Internet Fraud Desk by immediately disabling any domains identified as fraudulent by the Police. The Estonian Internet Foundation (.ee) [works](#) together with the Police and the national CERT for the prevention of malicious activity on the domain names.

¹⁷ For example, CZ.NIC (.cz) [operates](#) a DNS crawler that helps classify websites to detect unreliable online shops. A list of domain names connected to these potentially fraudulent websites is then shared with the Czech Trade Inspection Authority once a week for further investigation by the authority. CZ.NIC may also provide further information on specific domain names if requested by the Czech Trade Inspection Authority or other competent authorities.

¹⁸ For example, SIDN (.nl) and DNS Belgium (.be) have jointly developed a [tool](#) that automatically assesses suspicious characteristics of newly registered domain names based on historical registration data. Detected domain names are flagged for further manual verification.

¹⁹ For example, NIC.AT (.at) provides a [guide](#) on how to report illegal content online. Internetstiftelsen (.se) created dedicated educational websites for the [general public](#) and for [schools](#).

²⁰ ICANN [defines](#) “DNS abuse” as malware, botnets, phishing, pharming, and spam (when spam is used as a delivery mechanism for any of the other four types of DNS Abuse).