19 MAY 2025 • *Brussels, Belgium*

CENTR Comment on the European Democracy Shield

Summary of CENTR key recommendations

- The EU has an extensive legal framework that prescribes clear obligations on all digital services within the information ecosystem when it comes to responding to harmful content. There is no justification for creating a different set of standards for disinformation, while lowering rule of law safeguards available in democratic society.
- Only competent public authorities, including judicial authorities, are adequately equipped to judge over the level of harm posed by disinformation campaigns and instruct digital service providers, such as ccTLD registries, to take action, based on a clear legal basis available at national and EU level.
- Disputes over domain ownership and instances of illegitimate brand impersonations can be resolved in judicial proceedings and Alternative Dispute Resolution (ADR) procedures offered across European ccTLD registries and beyond.
- In line with the simplification agenda of the European Commission, the EUDS should steer clear of additional burden for digital infrastructure actors and not duplicate existing cybersecurity measures already found in other EU legislation.
- The EUDS must recognise the importance of and promote voluntary private-public partnerships in educational initiatives aimed at internet safety and increased digital literacy skills.

Introduction

CENTR is the association of European country code top-level domain registries (hereinafter ccTLDs). All EU Member State and EEA country ccTLDs (such as .de for Germany 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 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 – commonly thought of as the "phone book of the internet". It provides a navigation function to map user-friendly domain names to numeric IP addresses. ccTLDs only hold information enabling users to navigate the internet but do not store, transmit or enhance any content online[1].

As technical operators of the essential internet infrastructure, CENTR members wish to highlight the following in the context of the upcoming European Democracy Shield (hereinafter 'EUDS').

Countering disinformation and foreign information manipulation and interference

Legal status of disinformation

One of the key objectives of the EUDS is to counter disinformation and foreign information manipulation and interference online.

The European Commission[2] defines disinformation as "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Public harm comprises threats to democratic political and policy-making processes as well as public goods such as the protection of EU citizens' health, the environment or security". The legal status of the disinformation in the EU is not clearly defined as 'illegal content' per se, albeit it can be covered by a criminal liability in individual Member States, if certain conditions are met[3].

Most importantly, if the significant public harm to citizens' health or security is identified as 'illegal content', both national (e.g., penal code) and EU legal instruments (e.g., the Digital Services Act or the Regulation on Terrorist Content Online[4]) may be applicable.

[1] CENTR, "Domain name registries and online content" (2022).
[2] European Commission, Communication on "Tackling online disinformation: a European Approach", COM(2018) 236 final; similar definitions are provided in the European Parliament resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation (2020/2268(INI)); and European Commission, Communication "On the European democracy action plan", COM(2020) 790 final.
[3] In several Member States the criminal law covers, as a general rule, the deliberate dissemination of disinformation in case it poses a threat to peace or the public order (e.g., Croatia, Cyprus, the Czech Republic, Greece, Hungary, Slovakia, Romania).
[4] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, PE/19/2021/INIT.

The EU Digital Services Act[5] (hereinafter 'DSA') clarifies the responsibilities of digital services in responding to illegal activities and obliges all relevant digital services to act upon the orders of public competent authorities.

Under the DSA, the public competent authorities can take action against certain items of online content only in cases when it can be considered illegal. This is in line with the international human rights law that justifies the restriction of freedom of expression in exceptional circumstances, while prohibiting the forms of most egregious speech[6]. According to the UN Secretary General, states should avoid adopting general prohibitions on the dissemination of information based on vague and ambiguous concepts, including "false news"[7].

Role of ccTLDs in tackling harmful content

When it comes to the actions available for ccTLDs to take in response to any illegal content, it is worth highlighting that domain names (e.g., 'wikimedia.org') cannot be equated with websites (e.g., www.wikimedia.org). Publishing any content on a website, platform or an application associated with a domain name requires services that are offered by a variety of other intermediaries, e.g., hosting service providers and online platforms[8].

Disabling a domain name, effectively the only action available at ccTLD level to respond to any unwanted behaviour online, means disabling the underlying DNS infrastructure, which is **a drastic measure reserved to exceptional circumstances**.

The suspension of a domain name prevents it from resolving on the public internet. All subdomains (i.e., common.wikimedia.org) and services related to it (i.e., email addresses and webpages) are no longer functional. It also disables users' ability to navigate lawful content on websites linked to the domain, while the effects of such action is global, irrespective of users' location or applicable jurisdiction.

Furthermore, disabling underlying DNS infrastructure does not effectively remove content from the internet, as it can be moved and duplicated in other TLDs or digital services.

Consequently, **addressing ccTLD registries in response to illegal and unwanted content available online cannot be considered as an appropriate tool to handle problematic content**. Acting at the DNS level can only be considered when it can be reliably determined by a public competent authority that the domain itself is used with a clear intent of significant harm.

In addition, as the suspension of a domain has a global impact, it is necessary to apply a proportionality criteria when such action is considered. Only a particularly high level of harm can potentially justify resorting to such a

[5] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), PE/30/2022/REV/1.
[6] E.g., propaganda for war or advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (Article 20(2) of the International Covenant on Civil and Political Rights).
[7] Report of the UN Secretary-General on "Countering disinformation for the promotion and protection of human rights and fundamental freedoms", A/77/287, 12 August 2022.
[8] For an overview of different intermediary services and their technical functions, see Internet Society, "A Policy Framework for Internet Intermediaries and Content", January 2025.

measure. This principle is already explicitly codified in the EU consumer protection acquis[9] and should remain as the guiding principle for any EU policy making involving potential interference at the domain level.

For these reasons, **the action at TLD level cannot be considered as an intermediate or a quick response to disabling the availability of any unwanted and illegal content**. In this regard, it is worth mentioning that TLD registries are explicitly exempted from the obligations stemming from the EU Regulation on Terrorist Content Online, including from responding to 1-hour removal orders from the competent authorities. The EU regulators have recognised the importance of keeping the right balance between the needs to "effectively address the dissemination of terrorist content online, while ensuring respect for the private life of individuals"[10]. As a result, the Regulation solely applies to hosting service providers.

Only public competent authorities, including judicial authorities, are able to adequately assess the levels of harm and instruct a ccTLD registry to resort to such a dramatic measure as disabling a domain name. TLD-level action in response to a significant harm posed to the end-users can only be considered as a measure of last resort, after all other more effective means of action involving intermediaries closer to the content have not yielded any results.

Private interest groups and third parties are not suitable for making appropriate judgment calls regarding the level of harm posed by disinformation. This is the task that must stay exclusively with competent public authorities who in return can also mandate an appropriate action to be taken by service providers. Private interest groups and third parties, including fact-checkers and non-governmental organisations active in the disinformation space cannot act as quasi-authorities circumventing appropriate rule of law safeguards.

Any trust in democratic institutions and processes is rooted in rule of law and respect for legislative frameworks that already offer adequate levels of legal certainty for all actors involved in the information ecosystem, including digital service providers.

Consequently, **CENTR calls on EU policymakers to adhere to the proportionality criteria and the adequacy decisions by public competent authorities regarding the necessary interference each digital service provider is able to offer**, following the DSA and EU consumer protection acquis.

There is no justification for creating a different set of standards for disinformation than existing EU rulebooks concerning illegal content, considering its many forms of manifestations, ranging from health information to political processes, and unclear legal status. **The level of harm of each disinformation campaign must be evaluated by a competent public authority, equipped to balance public interest concerns**.

[9] Article 9(4) of the (EU) 2017/2394 Regulation on Consumer Protection Cooperation provides a hierarchical order of measures available for public authorities to respond to a serious consumer infringement to "avoid the risk of serious harm to the collective interests of consumers", including as a measure of last resort and "where no other effective means are available" to order domain registries or registrars to delete a domain name.

[10] See recital 13 of the Regulation (EU) 2021/784 on Terrorist Content Online: "[...]Providers of 'mere conduit' or 'caching' services, as well as of other services provided in other layers of the internet infrastructure, which do not involve storage, such as registries and registrars, as well as providers of domain name systems (DNS), payment or distributed denial of service (DdoS) protection services, should[...] fall outside the scope of this Regulation".

Empowering media outlets to protect their brand online

Disinformation can reach a significant user base, leveraging networks effect of social media and online communication services, but it can also mislead end-users by masking as a legitimate media outlet's domain[11].

If a domain name itself is used to confuse end-users by using an established media brand within its character string (e.g., sueddeutsche-news.de) and is used to impersonate a well-established media brand, **the brand owners are able to challenge the ownership of these domain names within judicial proceedings and the Alternative Dispute Resolution (ADR) procedures** established across ccTLDs in Europe and beyond[12].

Media outlets should be encouraged and empowered to challenge the ownership of misleading domains that impersonate their brand and reputation online, leveraging existing dispute resolution mechanisms available across the TLD space.

If lookalike domains are used to spread other types of harm, such as phishing or consumer scams in addition to spreading disinformation, competent public authorities (including national CSIRTs[13]) are equipped to act upon them leveraging existing EU and national legal frameworks, including by ordering suspension of domain names if it is necessary and proportionate with the level of posed harm (as stated in the previous chapter).

Ensuring the fairness and integrity of electoral processes and the strengthening of democratic frameworks

Increased cybersecurity of essential infrastructure

Reliable and secure functioning of the DNS is an essential prerequisite for a trustworthy online environment. The DNS infrastructure is essential for many online services, from accessing media online to e-government services. The criticality of the DNS is also recognised in the EU legislation, as the NIS 2 Directive[14] considers ccTLD registries and DNS service providers as "essential entities". The NIS 2 Directive places extensive obligations on the ccTLDs, including detailed cybersecurity risk-management measures[15] and requirements on maintaining an accurate and complete registration data of domain name holders.

European ccTLDs are cognisant of the critical role they hold in the information society and invest significant efforts into keeping their TLD zone safe and secure. As a result, European ccTLDs are consistently being

[11] Technical Report on an Analysis by the Federal Foreign Office (Germany), "Germany Targeted by the Pro-Russian Disinformation Campaign "Doppelgänger" (2024).
[12] EU Disinfo Lab, "Doppelganger media impersonation: Leveraging domain name dispute resolution", 27 November 2024.
[13] For example, in Estonia national CERT-EE has the legal authority to request the removal or restriction of harmful online content when malicious domains pose risks to public security or trust.
[14] Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union ('NIS 2 Directive').
[15] 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.

recognised as operators of TLD zones with the least amount of abuse[16]. No instances of European media impersonation used within foreign disinformation campaigns were reported within EU ccTLDs[17].

In addition, CENTR members further support the integrity and security of the DNS by adopting and promoting the latest security standards, relevant for the infrastructure they are managing (e.g., DNSSEC[18]).

CENTR members have demonstrated their commitment to upholding the highest measures of cybersecurity standards. Roughly 95% of European ccTLDs are certified under the well-recognised international information security standards, such as ISO 27001 and/or ISO 9001. In addition, the maturity of the European ccTLD sector is evident from the activities within the European Top-Level Domain ISAC, where CENTR members identify emerging security trends, share threat intelligence, and develop proactive measures to prevent and mitigate cyber-attacks.

In line with the simplification agenda of the European Commission, aiming to reduce administrative burden stemming from European legislation on private sector and consequently improve the competitiveness of the European economy, the EUDS should **not duplicate the already-existing cybersecurity measures found in EU legislation, especially concerning essential digital infrastructure.**

Integrity of the governmental online infrastructure

Conscious of the additional challenges faced by public sector online, CENTR members are supporting their governments in running second-level governmental and other public sector domains (such as .gob.es, .gov.cz, .police.uk) that are essential for offering e-government services to the general public, taking advantage of the established cybersecurity measures across European ccTLDs[19].

In addition to using existing resources to share information and coordinate responses to disinformation campaigns across EU[20] governments must be ready to counter and prevent exploitation of its online infrastructure and resources (e.g., e-government platforms, official election information websites, etc.) by attackers, especially in preparation and during elections. Consequently, **governmental bodies must ensure they procure and deploy digital services that adopt the latest internet security standards, including DNSSEC**. High security standards of digital services used within the public sector must be an essential element in public procurement.

[16] European Commission, Study on Domain Name System (DNS) abuse (2022).
[17] Technical Report on an Analysis by the Federal Foreign Office (Germany), "Germany Targeted by the Pro-Russian Disinformation Campaign "Doppelgänger" (2024).
[18] DNSSEC adds an extra layer of security by adding a cryptographic signature to the DNS records making the DNS spoofing attacks more difficult. Using DNSSEC ensures that internet users receive the data they requested without any tampering from the side of a possible attacker.
[19] E.g., CZ.NIC (.cz) operates the system and infrastructure of the gov.cz domain. Nominet (.uk) is running critical domains for gov.uk.
[20] E.g., the EEAS Rapid Alert System that is set up among the EU institutions and Member States to facilitate the sharing of insights related to disinformation campaigns and coordinate responses.

Strengthening societal resilience and preparedness (including digital and media literacy, critical thinking, etc.)

European ccTLDs cooperate closely with their local internet communities, including governments. Besides liaising with their local authorities, CENTR members use their unique position in the internet ecosystem to contribute to the increased technological savviness of internet users. CENTR members offer and support educational resources aimed at youth and the general public to help them to navigate the internet safely, improve their critical thinking and digital literacy skills. Some notable examples include:

- Afnic (.fr) launched an initiative aimed at helping young people master their online presence and personal branding through school workshops.
- .PT registry (.pt) coordinates Ponto Digital platform that offers training initiatives, competitions, events, and news in the digital field, and has an API connection with the EU Digital Skills and Jobs Platform.
- CZ.NIC (.cz) developed a series of educational videos explaining how to use the internet safely.
- NASK (.pl) supports the Polish Safer Internet Center which helps young people safely navigate the internet.
- SK-NIC (.sk) launched a series of educational videos aimed at the general public on topics such as disinformation or online fraud.
- Nominet (.uk) supports digital skills training programme Click Start for people from disadvantaged backgrounds.
- Punktum dk (.dk) launched tjekpånettet.dk, where internet users can check if a website or link is scam, phishing or legitimate, and work to raise awareness together with large NGOs .
- The Estonian Internet Foundation (.ee) supports every year internet community projects that promote cybersecurity and help people stay safe online while developing essential digital skills. This also includes initiatives that tackle false information on the internet. In addition, the .ee registry organises the annual Internet Day to raise awareness about key internet-related issues, including online safety.
- Registro .it (.it) offers online resources and regularly organises courses devoted to young students (primarily targeting initial educational cycles) through the "Ludoteca" project, whose aim is to increase awareness on the internet ecosystem and promote safe usage of the internet by young people.
- Israel Internet Association (.il) regularly develops and distributes multilingual (Hebrew and Arabic) public tools, policy reports on disinformation resilience, and hands-on workshops that equip educators, students, and community leaders with practical digital-literacy and online-safety resources.

Despite their primary role in maintaining the internet's infrastructure, CENTR members actively approach the issue of strengthening societal resilience and preparedness from the whole-of-society perspective, recognising their potential in educating the broader public.

The EUDS must recognise the importance of and **promote voluntary private-public partnerships** in educational initiatives aimed at internet safety and increased digital literacy skills.