August 2024 • *Brussels, Belgium*

CENTR response to International Telecommunication Union survey on the developmental aspects to strengthen the internet

Summary of CENTR key recommendations:

- To ensure balanced and evidence-based policymaking that contributes to the global development of the Internet, CENTR encourages more dialogue between policymakers and the technical internet infrastructure community.
- All stakeholders should support and respect the multistakeholder governance of the DNS, which facilitates the development of common open standards and protocols supporting global interoperability.
- Policymakers must avoid addressing societal problems through interventions via the technical internet infrastructure, without a proper and publicly available impact assessment of these interventions on human rights and universal accessibility of essential digital infrastructure, such as domain names.
- Policymakers must refrain from introducing unnecessary and disproportionate barriers to the domain name registration process via national and international legislation. Universal accessibility of essential digital infrastructure, such as the DNS, must be maintained.

INTRODUCTION

CENTR submits the following answer to the open consultation on **the developmental aspects to strengthen the internet** as published by the ITU Council Working Group on International Internet-related Public Policy Issues (CWG-Internet).

CENTR is the association of European country code top-level domain registries (hereinafter ccTLDs). All EU Member State and EEA country ccTLDs (such as .nl and .no) 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. registrars, end-users, Computer Security Incident Response Team (CSIRTs), law enforcement and other competent authorities). ccTLDs are responsible for operating and maintaining the technical Domain Name System (DNS) infrastructure for their top-level domain (such as .de or .cz). 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. How relevant multilateral and multi-stakeholder processes, including but not limited to UN-based processes such as Summit of the Future, WSIS+20 and the IGF, could address aspects related to Internet development?

The DNS is an integral part of the internet, standing the test of time for almost 40 years. It performs the essential task of translating IP addresses to a human-readable domain names that are used by connected devices and services (smart phones, web browsers, e-mail exchanges). The DNS functions as a distributed, decentralised structure built with extra redundancy. This ensures that even in situations when a given server is unreachable or during periods of heavy workloads, the DNS remains operational as there is no single point of failure. Furthermore, the scalability of the system enabled the internet as a network of networks to grow seamlessly, making the global growth in internet access a success.

The success of the DNS and the internet in general stems from the policy and technical development process in organisations functioning on the multistakeholder approach. These fora include among others ICANN and RIPE NCC, as well as standards and protocols developing organisations such as the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C). The multistakeholder approach adopted within these fora, allows different stakeholder groups, e.g. governments, civil society, technical community, industry, and end-users to participate on an equal footing with each other.

The openness of the standard and protocol development process brings in a broad range of perspectives that altogether improve the overall quality and reliability of a chosen solution. **The preference for open standards**

and protocols improves the security and the resilience of the internet infrastructure, as it enables thorough scrutiny and prevents vendor lock-ins.

The efforts to further the development of the internet should acknowledge the intricate web of well-established multistakeholder processes. The processes such as the Global Digital Compact (GDC) and the upcoming WSIS+20 review should be seen as instruments to embolden such multistakeholder fora and reinvigorate the Internet Governance (IG) processes, rather than undermining them. **The multilateral processes should not duplicate or contradict the well-established processes for technical development of the internet**, for it to remain global and universal.

2. What are the challenges and opportunities, good practices and favourable policy environments to strengthen the Internet, including in areas such as:

Secure and resilient internet

The interoperable solutions (protocols/standards) that underpin the DNS have been chosen by the internet community through a multistakeholder process. Legislative interventions in the operation of the DNS may result in conflicts between policies and standards set by the global IG community and national legislation. As a result, fragmentation emerges in conflicting legal requirements which technical operators, such as TLD registries, must adhere to. Even well-intentioned legislative interventions may undermine global voluntary commitments and create technical conflicts (e.g., recent legislative efforts on Geographical Indicators in the EU, and the Sony v Quad9 case). **Any national or regional legislation should be proposed with a careful assessment of its potential interference with voluntary protocols and standards, in close consultations with the technical community.**

Policymakers must abstain from trying to resolve unwanted online behaviour through mandating disproportionate intervention at the technical level. These attempts are harmful to the integrity of the DNS and put unreasonable expectations on the DNS operators.

ccTLD registries do not store, cache or transmit any content online and as a result, have no insight into or control over the content associated with the domains. Ordering a TLD registry to delete or suspend a specific domain name to prevent access to a piece of content renders the domain name and any associated services, e.g. website, email service, inaccessible. However, it does not prevent users in reaching the actual content, as such content remains online and can be found by alternative means (e.g., by navigating to a different domain name, or the host server IP address).

Technical action at the domain level to disrupt accessibility of online content should be only used as a measure of last resort, together with due proportionality checks, to avoid grave risks to end-users. Otherwise, the technical action could lead to violations of human rights, such as preventing end-users to exercise their freedom of speech or to conduct business. In general, without the appropriate proportionality test when DNS-

level action is mandated, the right to a fair trial and due process is jeopardised. States, as the primary duty bearers of human rights, must ensure an adequate level of protection of fundamental rights both online and offline. As a result, **a proper impact assessment and necessary balancing act between a technological solution and its impact on human rights must be conducted when DNS-level action is considered as legislative intervention**.

European ccTLD registries are committed to ensuring a high level of trust for all internet users. European ccTLD registries have consistently been recognised as operators of TLD zones with the least amount of abuse. This is done through adoption of a variety of different good practices, rooted within national context and consumer protection law regimes, among others. For example, there are a variety of registration data accuracy practices adopted by European ccTLD registries, that allow registries to take action (including suspending a domain name) based on inaccurate registration data, keeping registry action to its technical remit.

One of the most recent examples in proactive efforts to tackle security challenges faced by the ccTLD sector is the establishment of the TLD ISAC, an organisation aiming to strengthen the resilience and security of European ccTLD registries through information sharing, collaboration and promotion of best practices (founded by CENTR members).

Voluntary and community-led initiatives, along with sharing of good practices, should be further promoted and tested out before more drastic legislative interventions are considered.

Equitable access for all / fostering meaningful connectivity

The internet is not only about the ability to connect to others in a passive consumer role, it also about being an active participant in information society. Domain names enable individuals and organisations to establish their online presence (to develop a product or deliver an eGovernment service) through a unique technical identifier. European ccTLDs therefore invest greatly to ensure that domain names are accessible at a reasonable cost.

Since domain names are a limited resource and must be unique to technically function, they are provided at a "first come first served" basis. This principle allows anyone to establish their online presence without discrimination. Should a dispute over the legitimate interest to a domain name arise, it can be easily resolved through well-established out of court dispute resolutions procedures in place across TLDs (or be resolved in courts).

There have been instances when the "first come first served" principle was disregarded by policymakers. For example, the European Commission proposed a legislation that would subvert this principle and provide a privileged access to domain name registration to the benefit of intellectual property rightsholders, unnecessarily disadvantaging other legitimate beneficiaries. These imbalances erode the trust of the users in the DNS and make it more difficult to take full advantage of the internet. **Governments should avoid policy interventions with implications on the technical underpinnings of the internet without meaningfully consulting the technical community.** A keyway how to avoid interventions with potentially negative

consequences on the technical functioning of the internet is to prepare thorough impact assessments, in consultation with technical community.

3. How can we promote international multistakeholder cooperation on public policy issues that are focused on promoting the development aspects of the Internet?

While the multistakeholder approach can be adapted to respond to the newest challenges, it must be continuously supported by all stakeholders, by allocating enough resources to allow for its evolution. These resources include allocating experts, ensuring wide participation of stakeholders with different backgrounds, and taking a collective responsibility for its effectiveness as a result. The success of the multistakeholder model relies solely on its support from all stakeholders, including governments.

Due to criticality of the internet for society at large, and its status as a critical infrastructure (e.g., EU cybersecurity legislation) and nearly a human right (i.e., access to the internet), its further development must be rooted in multistakeholder approach, where many voices are heard and meaningfully participate in the decision-making process. Since public policy and critical internet technology are intertwined, while new technologies offer new challenges, the multistakeholder approach is needed more than ever, to avoid hidden harms and allow for continuous innovation.

Governments should continue their support for and participation in existing global and national multistakeholder processes around the IG. The continuous governmental support for these processes must also be included as a key commitment in the GDC and WSIS+20.