Booklet of Innovations

A collection of projects and initiatives by ccTLD registries for Europe's digital future

CONTENTS

Introduction	4
Resilience	6
Interoperability	9
Online Safety and Security	12
Education and Awareness	15
Conclusion	18

INTRODUCTION

CENTR is the association for exchange, dialogue and innovation of country code top-level domain (ccTLD) registries in Europe, such as .ee for Estonia or .de for Germany.

It brings together the ccTLD registries of all the EU Member States, the European Economic Area countries and beyond. In total CENTR has 51 full and 10 associate members. Full members of CENTR manage 61% of all domains in EU countries, representing more than 76 million registrations.

ccTLDs operate and maintain 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 Internet Protocol (IP) addresses and is used by any service running on the internet, either visible to the end-users (e.g., website, email) or entirely behind the scenes (e.g., instant messaging, Voice over IP, and infrastructure management).

The role of a ccTLD registry is critical to the functioning of the information society, while European online identifiers are crucial for any individual or business wishing to establish an online presence.

ccTLDs are rooted in their national jurisdictions and collaborate closely with their local internet communities, including governments. As such, ccTLDs are an essential component of Europe's digital infrastructure and continuously strive to be champions of a resilient, stable and secure internet in Europe.

As shown in this booklet, European ccTLD registries can provide a wealth of experience and knowledge to policymakers, stemming from decades of providing internet services for the public benefit.

This booklet collects some of the best examples of the work of our members across four areas.

The examples reflect the crucial work of some of our members, yet are far from being exhaustive.

RESILIENCE

INTEROPERABILITY

ONLINE SAFETY AND SECURITY

EDUCATION AND AWARENESS

RESILIENCE

Europe's digital infrastructure faces growing pressure from geopolitical tensions and a cybersecurity threat landscape that is continuously evolving.

Increasingly sophisticated DDoS attacks and infrastructure dependencies are making resilience, diversification, and technological sovereignty more and more important for European internet infrastructure.

Protecting it and ensuring it can withstand and recover from disruption is a strategic priority, essential to safeguarding citizens' data and the services they rely on.

CENTR members sit at the front line of this effort. Across the continent, they are actively building and strengthening the resilience of Europe's digital space. The initiatives below reflect that work.

These projects support:

- EU Cybersecurity Strategy
- NIS2 and Cyber Resilience Act

FRANCE - Anticipating new pressures on the DNS

AFNIC (.fr)

Several Afnic projects study how the DNS needs to adapt to remain resilient as usage patterns and energy demands evolve.

The project "How do AI agents reshape the Internet?", developed with École Polytechnique and UCLouvain, measures how AI agents are changing internet traffic and contributing to the centralisation of infrastructure, and looks at how network and service providers can adapt. Researchers collect traffic data from multiple vantage points, including root servers and .fr management, using machine learning to identify behavioural differences and semantic techniques to correlate AI agent requests with task-oriented query patterns. The aim is to support the design of new protocols capable of handling generative AI traffic at scale.

The DECODES project looks at the resilience question from an energy angle, analysing the role of the DNS in data centre energy consumption. Although the DNS accounts for only a small share of global internet traffic, it depends on servers distributed worldwide, most of them hosted in data centres that run continuously to keep the internet efficient and available. DECODES explores how this footprint can be optimised without compromising that reliability.

Together, the two projects address infrastructure resilience from different angles: anticipating the traffic-side pressures of new technologies like AI agents, and reducing the resource cost of keeping the DNS running.

THE NETHERLANDS - Tapdance

SIDN (.nl)

Tapdance is a configurable, near real time authoritative DNS statistics collector based on dnstap. It runs alongside any authoritative DNS server to collect, aggregate and visualise query- and network latency statistics in near real time. SIDN developed this Free and Open-Source monitoring tool to automatically scale with their DNS infrastructure, without any manual intervention.

With Tapdance, .nl registry is able to further optimise its DNS anycast infrastructure and respond more quickly to cybersecurity threats such as DDoS attacks.

AUSTRIA - RcodeZero DNS

NIC.AT (.at)

For ccTLD registries, DNS availability is essential: an outage can affect an entire national namespace. For this reason, using multiple independent DNS providers reduces dependencies and strengthens operational resilience.

RcodeZero provides a globally distributed Anycast DNS infrastructure operated by a European provider with deep roots in the registry community, allowing TLD operators to add an independent and highly resilient DNS layer to their existing infrastructure. Traffic is distributed across the Anycast network and automatically routed to available nodes, helping maintain availability even if individual locations or network paths become unavailable. Beyond the technology itself, RcodeZero combines global infrastructure with registry expertise, 24/7 operational support and close cooperation with its customers. The service also demonstrates how expertise developed within a national registry can evolve into shared infrastructure that benefits the wider European and international domain community.

INTEROPERABILITY

The internet's success and scalability have been possible thanks to open standards and the widespread adoption and availability of Free and Open-Source Software (FOSS) solutions. Open standards are publicly available and developed through transparent processes open to broad participation. They enable interoperability, compatibility between different services, and promote user choice.

FOSS is central to the EU's push for digital sovereignty and technological independence. As Europe seeks to reduce reliance on non-European infrastructure and vendors, FOSS tools offer a practical path towards that goal, while also contributing security and resilience across the internet's core systems.

CENTR members actively contribute to this open ecosystem, as the internet's core infrastructure is designed around open standards and FOSS.

These projects support:

EU Open Source Strategy

Tech Sovereignty Package

CZECH REPUBLIC - FRED

CZNIC (.cz)

FRED (Free Registry for ENUM and Domains) is a Free and Open-Source domain name registry software. It provides the full stack a registry operator needs: an EPP server for registrars, Web WHOIS service, WHOIS & RDAP protocols for the public, a web and command-line interface administration interface for operators, and a zone generation pipeline – all distributed as packaged software.

The system was written from scratch in 2006, and the software has been continuously improved and updated since then. Notable features added recently are DNSSEC Automation, DNS hosting support and expired domain auctions.

Currently, thirteen ccTLDs from across the world rely on FRED. CZ.NIC is finishing changes so the system can be also used to host new gTLDs. Furthermore, ccTLD administrators deploying FRED may take advantage of other CZ.NIC tools developed and distributed as Free and Open-Source Software such as authoritative DNS server Knot DNS, recursive DNS server Knot Resolver or routing daemon BIRD.

SWEDEN, FRANCE

Zonemaster

Internetstiftelsen (.se), Afnic (.fr)

Zonemaster is a joint project between Afnic (.fr) and Internetstiftelsen (.se). It is a Free and Open-Source Software package that validates the quality of a DNS delegation.

The ambition of the Zonemaster project is to develop and maintain the software as a Free and Open-Source DNS validation tool, offering improved performance over existing tools and providing extensive documentation which could be re-used by similar projects in the future.

The Zonemaster tool helps DNS administrators, experts, and beginners alike check their DNS configuration, and anyone who wants to know whether the domain name they own or use has any issues. When a request to test a domain name is sent to Zonemaster, the program checks its health by traversing the DNS from the root (.) to the TLD and finally the DNS servers. If domain servers include configuration errors, Zonemaster generates a report to help users fix them.

UK - Nominet DNS Fund

Nominet (.uk)

The Nominet (.uk) DNS Fund invests in the security, resilience, and long-term viability of essential Free and Open-Source components of the DNS.

When DNS projects go underfunded, the risk is systemic, exposing millions of users to vulnerabilities, and threatening the stability and security of the entire internet.

The Fund focuses on this gap: Free and Open-Source critical infrastructure components relevant to the development, deployment, and operation of the DNS.

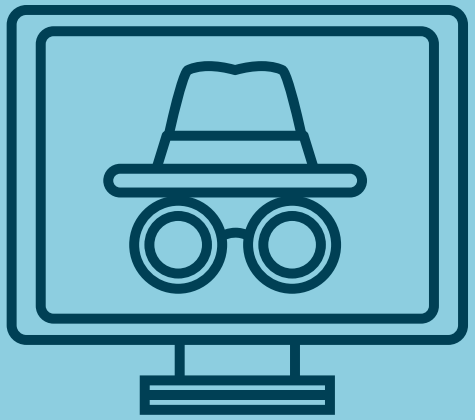
A robust and secure DNS is fundamental for the internet's continued operation and the public benefit it provides.

ONLINE SAFETY AND SECURITY

For all CENTR members, detecting and preventing abuse online is a top priority. Malicious use of domains, for example, for phishing or malware distribution, directly undermines the trust and safety that a resilient digital space depends on, and effective detection becomes a key line of defence in protecting citizens and businesses online.

European ccTLDs are consistently recognised as one of the safest domain spaces worldwide. The consistently low levels of abuse across EU ccTLDs stem from a variety of reasons, tailored to each individual ccTLD and applicable regulatory framework.

In the following section, we spotlight CENTR members' initiatives contributing to a safe space online, for example by using machine learning and AI to strengthen and refine their abuse prevention and detection mechanisms.



These projects support:

Action Plan on Fighting Online Fraud

Digital Services Act

EUROPEAN UNION - APEWS

EURid (.eu)

Abuse Prevention Early Warning System (APEWS) is an award-winning predictive system that analyses domain name registration data and patterns to identify potentially abusive domains before registration. It uses a machine-learning algorithm, developed by EURid (.eu) in collaboration with Leuven University, to predict in near real time whether a domain may be abused.

Integrated with the .eu Registration Platform, it triggers immediate suspension of new domains under EURid's Data Quality System. Deployed for years and proven effective, the pre-delegation checker is an essential building block for detecting issues before delegation and preventing abuse.

While APEWS' feedback loop and features focus on .eu domain registrations, APEWS is being tested for use by other registries. This setup improves performance and scalability, allowing the system to handle larger data loads.

The machine-learning training continuously improves abuse detection accuracy through shared data and cooperation with other registries.

BELGIUM, THE NETHERLANDS

RegCheck

DNS belgium (.be), SIDN (.nl)

RegCheck is a tool designed to predict whether a new domain name registration is suspicious based on historical registration data and in a targeted manner.

The core of RegCheck is a machine-learning classifier that assesses the risk that the domain name will be used for malicious purposes based on characteristics known at the time of registration. Based on this assessment, it flags some registrations and requires them to undergo additional verification prior to the domain name being activated.

The system was developed collaboratively between SIDN (.nl) and DNS Belgium (.be) and has been deployed as a real-time system at .be registry since March 2024.

Since its deployment, .be registry has witnessed a decrease in the number of .be domain name registrations that have been revoked for breaching the terms and conditions, indicating a decline in the number of active malicious registrations.

SPAIN - AmaIA

RED.es (.es)

AmaIA is an information system, developed by Red.es (.es) whose purpose is to detect potentially malicious or fraudulent .es domains.

Through the use of artificial intelligence to identify risk patterns and enable early detection of potentially abusive domains within the .es namespace, it ensures that .es is more secure and of higher quality.

By strengthening DNS security, improving operational efficiency, and supporting regulatory compliance, amaIA contributes to a safer and more trusted internet.

EDUCATION AND AWARENESS

Resilience is not only about infrastructure and technical defences, it also depends on people.

Digital skills, literacy, and awareness of online risks are essential to building a safer, more trustworthy internet, and equipping citizens with these skills is a core pillar of the EU's Digital Decade targets for 2030.

CENTR members play an active role in this effort, helping citizens, businesses, and communities build the knowledge they need to navigate the internet safely.

The initiatives below showcase projects that go beyond the day-to-day work of running a registry, extending benefits to the broader community.

These projects support:

Union of Skills

Digital Decade Policy Programme

SERBIA - LOKALAC

RNIDS (.rs)

Talented children and young people, especially those pursuing science and research, often lack visibility, funding, and mentorship, while at the same time vulnerable groups in society need consistent support.

Lokalac connects the domain and internet community with these causes, using proceeds from campaign merchandise and related activities to fund both youth science initiatives and social welfare programmes.

One of the most significant examples is a donation to the Mathematical Grammar School in Belgrade. Proceeds from the merchandise collection were directed to the school, enabling its top students to visit CERN. The students took part in the campaign wearing Lokalac t-shirts, were accompanied to public appearances and interviews, and they are the project's greatest ambassadors.

RNIDS (.rs) keeps building inter-institutional partnerships with schools, research institutions and social organisations so that Lokalac grows into a recurring, recognisable model for how a ccTLD registry can create shared value beyond its core operations.

PORTUGAL - re_B00TCMP

.PT

The re_B00TCMP initiative is a one-day event that aims to raise awareness about the opportunities, challenges, and risks of the digital world. Young talents have the opportunity to deepen their digital skills through activities aligned with cybersecurity best practices.

re_B00TCMP involves police, organisations, businesses, and schools in developing a comprehensive programme that provides young people, their parents, and teachers with the knowledge and tools for a safer and more responsible online presence.

This initiative is the result of collaborative work aimed at promoting a culture of responsibility and ethical behaviour in the digital world. With the support of partners and local communities, including .pt registry, the Portuguese Criminal Investigation Police, the Public Security Police and CyberS3c, it aims to contribute to a safer, more reliable, and resilient cyberspace.

ESTONIA - Support programme

Estonian Internet Foundation (.ee)

The Estonian Internet Foundation (.ee) runs an open support programme to fund cybersecurity and DNS awareness projects in Estonia. It focuses on the most vulnerable parts of society: youth, the elderly and communities outside the main cities. Its goal is to help these groups understand and protect themselves online.

Most projects funded by the .ee registry are led by schools or civil society organisations. Activities include learning programmes and materials, challenges, competitions, events and seminars. Since 2022, the programme has supported 48 projects and reached approximately 35 000 Estonians.

The programme is funded by the proceeds of .ee deleted domain auctions, with a total available fund of €50 000 a year to be dedicated to innovative and impactful educational initiatives.

The programme began in 2018, when the registry started supporting a national cybersecurity challenge called "Küberpuuring", and has been open to everyone in Estonia since 2022.

CONCLUSION

As illustrated in this booklet, European ccTLDs are advancing resilience, security, and trust across the internet's core infrastructure. They strengthen the technical foundations of the DNS, contribute to a more open internet, champion online safety and security, and equip citizens with the skills and awareness they need online. These initiatives show that CENTR members are active contributors in shaping a safer, more resilient internet for all Europeans.

Continued dialogue between ccTLD registries and EU policymakers will be essential to ensure that future regulation builds on, rather than duplicates, the work already being done on the ground, allowing CENTR members to keep a secure, open, and trustworthy European online space.

Council of European National Top-Level Domain Registries

secretariat@centr.org | www.centr.org

Belliardstraat 20, 1040 Brussels

EU Transparency Register: 980834014781-65