Dynamic Coalition on DNS Issues (DC-DNSI) 2023 Annual Report Background information about the DC

The Dynamic Coalition on DNS Issues (DC-DNSI) has been working within the Internet Governance Forum since 2018. The DC-DNSI was created with the aim of providing an open avenue through which such issues may be discussed and debated at the IGF. Stakeholders can convene under the IGF's multistakeholder mantle to share information and exchange best practices on DNS-related policy challenges and, if desired, produce non- binding, more tangible outputs in line with the recommendation of the CSTD Working Group on IGF improvements.

The DC-DNSI has contributed to building a constructive, informed dialogue on DNS issues at IGF that complements work undertaken by the crucial organizations that develop the standards for and manage the DNS. Prior coalition work has focused on building support for the universal acceptance of Domain Names and internationalized Domain Names; promoting and raising awareness around Domain Name Security Extensions (DNSSEC); reviewing mechanisms to minimize Internet fragmentation from emerging regulations such as those on privacy, data localization, and data access; and canvassing the challenges faced by policymakers and decisionmakers when deciding to implement universal acceptance.

The DC-DNSI has also reactivated its mailing list to keep stakeholders informed and engaged through the year.The DC-DNSI was less active during the pandemic and was successfully revived in 2023 through the collaborative efforts of the DNS Research Federation, with support from Verisign and other partners.

Activities conducted in 2023

a) Activities within the IGF

With the reactivation of the DC , the coalition devoted a significant portion of 2023 developing a pragmatic approach to tackle emerging threats that impact the functionality of the DNS. To this end, the DC has begun to lay the groundwork for establishing a cohesive group of various stakeholders from the multistakeholder community to discuss and promote responsible best practices in securing the DNS.

Luminary representatives of the DC's membership participated in various conversations during the 2023 IGF in Kyoto discussing issues around development of DNS policies and standards, highlighting good practices within the industry that use evidence to inform policy choices, and different approaches to data-based decision-making. As part of this roundtable discussion- IGF 2023 DC-DNSI Closing the Governance Gaps: New Paradigms for a Safer DNS - participants had an opportunity to join a lively conversation. The session focused on discussing governance gaps and limitations in responding to DNS-related online threats within the internet ecosystem, including inadequate coordination among stakeholders and emerging vulnerabilities from technologies like

blockchain domains. Participants aimed to identify these gaps and propose actions for enhanced multistakeholder cooperation to address DNS-related harms effectively. These conversations laid the basis for proposed actions for 2023 and beyond.

The DC held a session on Day 0 at EuroDIG 2023 in Tampere, Finland. The title of session: "Mind the governance gap! Broadening the multistakeholder response to DNS-related cybersecurity threats." The goal of this session was to discuss ways to broaden multi-stakeholder responses to DNS abuse and identify potential governance gaps. The DC presented a roundtable discussion to explore these complex issues, and foster European multistakeholder responses, which ultimately fed into the coalition's updates at the IGF in Kyoto, Japan, and annual DC activity report for 2024.

b) Priorities/Objectives for the following year

The DC-DNSI priorities for 2024 include (but are not limited to):

- The DC-DNSI recognizes that challenges remain, and others have emerged since the coalition's inception. During 2024, the DC plans to revisit its action plan, and re- focus its efforts to ensure the work being performed over the next year also addresses policy conversations around the WSIS+20 review. Coalition participants and the IGF community will continue to convene under the IGF's multistakeholder mantle to share information and exchange best practices on DNS-related policy challenges and, if desired, produce non-binding outputs.

The DNSRF proposed to submit (or submitted) workshop requests to the following IGF meetings:

- EURODIG, June 17–19. Vilnius, Lithuania. This has been already submitted and accepted.
- UK IGF, estimated for July. London, UK
- US IGF, estimated for either July or September, location TBC.
- Global IGF, December 15 -19. Riyadh, Saudi Arabia
- One IGF in Global South to include either:
    - APrIGF, August 21 -23. Taipei, Taiwan
    - LACIGF, estimated for December 2024. Location TBC

The goal for the DC-DNSI in 2024 is to continue facilitating conversations on governance gaps in addressing online harms, particularly as it pertains to the role of proxy and hosting providers. The actions outlined below intend to broker industry

agreements on the diagnosis of the issue, and uncover areas for cooperation and action.

The DNSRF proposes to leverage the recent approval of the NIS2 Directive to facilitate the conversation. The organisation has launched a new project on the implementation of NIS2, intended to document the impacts of the directive, including extraterritoriality effects. The project is described in detail at the end of this document.

Specifically, the team proposes the following workshops in 2024:

EURODIG. Who is affected by the NIS2 Directive and what it means to the fight against online harms

In January 2023, the European Union's update to the Network and Information Systems Directive, now known as *NIS2,* became law. As part of the vision for advancing cybersecurity in the Union, Article 28 of the Directive creates legal obligations for domain registries and entities providing domain name registration services in relation to the WHOIS database.

In the context of EuroDIG, this workshop intends to shed light on the ecosystem that will be affected by Article 28 of the NIS2 Directive and what the NIS2 directive might mean for coordination of the diverse actors in the ecosystem in addressing online harms. As part of this exercise, stakeholders will be invited to reflect on current contributions from across the DNS value chain to mitigate online harms and what additional cooperation may be required.

The session will take a whole-ecosystem approach considering a broad spectrum of stakeholders (registries, registrars, resellers, as well as proxy, hosting, cloud computing and data centre service providers) and touch upon what roles and responsibilities may fall to these members of the ecosystem.

The conversation seeks to unpack what level of cross-industry collaboration is implied in the directive, and how stakeholders from the DNS value chain may be expected to collaborate. The discussions will build on prior dialogues by the DC-DNSI and highlight possible strategies for broad ecosystem cooperation in addressing various forms of abuse online.

Tentative speakers to include: Verisign (Klara Jordan or Keith Drazek), Thomas Rickert from ECO, Dirk Jumpertz from Eurid, Emma Caner from OVHCloud, ENISA /a representative from the European Commision

UK IGF. The Impact of NIS2 in the UK DNS Ecosystem

Building on the discussions from the EURODIG session, this workshop at the UK IGF will seek to shed light on the extraterritoriality effects of NIS2 on the EU's immediate neighbour, the UK. The session will discuss implications of the rollout of the NIS2 directive in the UK, and when the impact may be expected.

Tentative speakers will include: Emily Taylor/Georgia Osborn from the DNSRF; Nominet; Mark Hughes from DxC, Cloudflare TBC. Verisign, Keith Drazek.

Global IGF. Extraterritorial effect and Broad Ecosystem Approach: the impact of NIS2 in global responses to DNS abuse

The global IGF session will articulate the impact of the NIS2 directive beyond the EU, with a special focus on Global South regions. Long-arm European legislation such as GDPR have impacted Global South regions and generated compliance burden, in spite of these having no direct say in how the regulation gets crafted, and few opportunities to influence change in those regulations. The session will explore the extraterritorial impact of the NIS2 directive, as well as its embedded, broad ecosystem approach to improving the accuracy of domain name registration data, which entails action all the way to the level of proxy and hosting providers. The session will also draw on DNSRF efforts to uncover the broader ecosystem of entities affected by the NIS2 directive, and introduce from the organisation's mapping exercise, how the Global South is affected.

A fourth session either at APrIGF or LACIGF would draw on the extraterritoriality effects question with focus on the region in question.

Engagement DC-DNSI

Strategies to drive engagement on the list.

- New follow up with prior list members
- Printouts with QR code on onsite sessions
- Individual invites to sign up to list
- Social media posts

Strategies for regular meetings - two online sessions

- April 2024
    - Circulate blog with conclusions of DC-DNSI in 2023 (take form IGF session) + proposal for 2024
    - Coordinate call to discuss priorities + present plan → possibly line up a couple of interventions
- October 2024
    - Global IGF preparatory session

- Present IGF panel
- Discuss DC-DNSI 2024 output – Summary report from 2024 work