Council of European National Top-Level Domain Registries

Report on ICANN70

Virtual Community Forum

March 2021

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

Contents

Executive Summary

At the ICANN70 meeting, there was a sense of frustration amongst the ICANN community with the issue of DNS abuse. Several constituencies, including the Governmental Advisory Committee (GAC), the At-Large Advisory Committee (ALAC) and the Business Constituency (BC) expressed their concerns regarding the lack of DNS abuse recommendations within the Subsequent Procedures Policy Development Process (SubPro PDP). They believe that before the new gTLD round can be opened again, the DNS abuse issue needs to be addressed. However, numerous issues still prevail, according to the other block of voices within the ICANN community, such as ICANN Contracted Parties and the Non-Commercial Stakeholder Group: i.e. a lack of definition of DNS abuse, ICANN's limited remit, the difficult relationship with ICANN compliance, and the tension between mandatory vs. voluntary public interest commitments. ICANN70 was another manifestation that DNS abuse is the pain point for current policy development processes at ICANN, including the EPDP designed to address the impact of the EU GDPR on registration data and its accessibility.

The ccNSO only held a limited number of sessions at ICANN 70. It kicked off the review of its internal procedural rules and organised a debate on the future of ccTLDs. It also had an informal chat with the ccNSO-appointed ICANN Board Members on the future of ICANN meetings, the impact of ICANN reviews and the lack of a prioritisation process within ICANN. The Internet Governance Liaison Committee discussed sovereignty-related internet governance issues and how ccTLDs have been contributing to achieving public policy goals in this context.

Katrina Sataki (.lv) stepped down as Chair of the ccNSO to take up an ICANN Board seat later this year. Alejandra Reynoso (.gt) takes over the reins, supported by Jordan Carter (.nz) and Pablo Rodriguez (.pr) as vice-chairs.

ICANN70 GAC report

The GAC ICANN70 Communiqué is available here.

DNS abuse

There was a sense of frustration amongst the members of the ICANN community who were present at the ICANN70 meeting when it comes to tackling the issue of DNS abuse. Several constituencies, including the GAC, ALAC and BC expressed their concerns at the lack of DNS abuse recommendations within the SubPro PDP: before the new gTLD round can be opened again, the DNS abuse issue needs to be addressed, these voices are calling. However, numerous issues still prevail, according to the other block of voices within the ICANN community: i.e. the lack of definition of DNS abuse, ICANN's limited remit, the relationship with ICANN compliance, and public interest commitments (voluntary v mandatory). ICANN70 was another manifestation that DNS abuse is the pain point for current policy development processes at ICANN, including the EPDP designed to address the impact of the EU GDPR on registration data and its accessibility.

Recent developments

Second Security, Stability, and Resiliency (SSR2) Review Team Final Report

On 25 January 2021, the second Security, Stability, and Resiliency (SSR2) Review Team submitted its final report to the ICANN Board. The report is now open for public comment to inform Board action on the SSR2 Review Team's final recommendations.

The SSR Review is a Specific Review mandated by ICANN's Bylaws to review "ICANN's execution of its commitment to enhance the operational stability, reliability, resiliency, security, and global interoperability of the systems and processes, both internal and external, that directly affect and/or are affected by the Internet's system of unique identifiers that ICANN coordinates".

Specific Reviews are inter alia used to demonstrate how ICANN delivers on its commitments and identifies areas where it can improve.

The SSR2 Review Team Final Report contains 63 full consensus recommendations in the following areas:

- SSR1 implementation and intended effects.
- Key stability issues within ICANN.
- Contracts, compliance and transparency around Domain Name System (DNS) abuse.
- Additional SSR-related concerns regarding the global DNS.

The GAC comment (from 3 April 2020) on the previous draft version of the report endorsed many of the recommendations, and in particular those pertaining to improving Domain Abuse Activity Reporting (DAAR) and the strengthening of a compliance mechanism.

The Final report includes several recommendations that required the GAC's attention during the ICANN70 meeting. Namely, Recommendations 8-15 that have direct DNS abuse implications.

To date, comments on the SSR2 Final report have been submitted by the Registry Stakeholder Group (RySG), PIR and Verisign. Both the RySG and PIR have objected to Recommendation 8 that requires abuse and security experts participating in ICANN contract renegotiations to "represent the interests of non-contracted entities" in the benefit of "SSR of the DNS for end-users, businesses and governments". The RySG and PIR have also objected to Recommendation 14 that requires ICANN Org to create a Temporary Specification for Evidence-based Security improvements, requiring contracted parties to keep their percentage of abusive domains below a "reasonable threshold" and create financial incentives to portfolios with less abuse, according to the briefing to the GAC.

Other developments across the ICANN community in regard to DNS abuse mitigation:

- ICANN agreed with Verisign on an amendment to the .com Registry Agreement incorporating language consistent with Specification 11 Section 3(a)/(b) of the Base Registry Agreement.
- SSAC is working on a paper to propose strategies and processes to address DNS abuse identification and mitigation.
- ALAC has been discussing the definition of DNS abuse.
- ICANN compliance has been auditing registries and registrars regarding DNS abuse related obligations.
- Contracted parties are participating in voluntary initiatives such as the DNS Abuse Framework, DNS Abuse Institute, and the Internet and Jurisdiction Policy Network.

For next steps to mitigate DNS abuse, the GAC is considering the following:

Possible cross-community work to identify specific issues with certain levels of consensus and discuss potential policy development if appropriate.

- Financial incentive programs to reward effective prevention and mitigation.
- A trusted notifier program.
- The closure of discussions on DNS abuse.
- Making DAAR reporting actionable.
- The adoption of ccTLD best practices in the gTLD space (.dk and .eu were explicitly mentioned as ccTLDs with proactive measures to tackle abuse).

Contracted parties

The Registry Stakeholder Group (RySG) presented its progress on abuse work during a session with the GNSO. The RySG has developed an output document, "Registry Operator Available Actions", that explains the technical options available to registries to mitigate DNS abuse. The RySG is currently working on a joint document with the Public Safety Working Group on a new framework that is targeted at malware and botnets at scale.

The Registrar Stakeholder Group (RrSG) is currently working on several white papers: Incentivisation Programs, Registrant Protections, Approaches to business email compromise (BEC) scams. The RrSG is currently considering future work on a central resource for registrants dealing with DNS abuse.

During the session with the GNSO, several community members made statements regarding their views on the issue.

Brian Cimbolic (RySG) stressed that DNS abuse is limited to those types of misconduct where registries and registrars can take action, without the need for further investigation and specialised knowledge, like in the case of ID theft. The RySG is also considering having a cross gTLD and ccTLD group to look into practices and processes that are implementable across the DNS ecosystem.

James Galvin (Donuts) stressed the need to look into ICANN compliance and the enforcement mechanism within to address problems with those actors that do not take the DNS abuse issue seriously. He also highlighted the fact that the ecosystem is much broader than ICANN's contracted parties, and there are other players involved, like ccTLDs. He also argued that phishing can be performed in different ways, including ways that do not involve domain names. Phishing and spam can be considered DNS abuse when there is a cross-section with domain names, according to James Galvin.

Rowena Schoo (Nominet) highlighted that .uk has the benefit of being linked to the specific geographic location and a respective jurisdiction: whatever is illegal under English and Welsh law is passed to Nominet, irrespective of whether it is solely technical abuse. Nominet has a trusted notifier relationship with different law enforcement agencies. There is an arrangement where law enforcement agencies notify Nominet of illegal activity, and the domain name is either suspended or users are redirected to a warning page.

The Security and Stability Advisory Committee

The Security and Stability Advisory Committee (SSAC) issued a Report on an Interoperable Approach to Addressing Abuse Handling in the DNS, where it proposes a general framework of best practices processes to streamline reporting on DNS abuse. The following areas are inter alia covered by the report: a primary point of responsibility for abuse resolution, escalation paths, reasonable time frames for action, a proposed path forward towards harmonising efforts to address abuse incident reporting and handling, etc.

In its joint meeting with the ICANN Board, the SSAC highlighted that the report aims to tackle the issue of interoperability that is not common to the DNS. There are many different rules in place across the ecosystem, i.e. with regard to gTLDs, ccTLDs, registrars, web hosters etc. Interoperability is an issue that could be addressed across the ecosystem.

To this end, the SSAC finds that the lack of coordination leads to inconsistent approaches to DNS abuse management. Therefore, there is an opportunity to create a single entity – a Common Abuse Response Facilitator - to independently provide clarity and predictability to all stakeholders in the DNS ecosystem. The SSAC recommends that the ICANN community continues to work together in an effort to "define the role and scope of work for the Common Abuse Response Facilitator.

The Public Safety Working Group

The Public Safety Working Group (PSWG) presented its progress on the PSWG Work Plan 2020-2021, as endorsed by the GAC in March 2020.

As part of its Work Plan, the PSWG has been looking into best practices across the ccTLD space with the aim to adopt similar best practice in the gTLD space. The PSWG has also assessed the impact and risks of DNS encryption on DNS abuse mitigation.

The PSWG expressed its concern with the enforceability of ICANN contract provisions. Registry Agreement Specification 11 Section 3(b) requires registries to periodically conduct a technical analysis and assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware and botnets. Registries are also required to maintain statistical reports on the number of security threats identified and actions taken as a result of the periodic security checks. However, according to the PSWG, there are gaps at registry level, as Specification 11 Section 3(b) does not specify what type of actions need to be taken to respond to security threats. Furthermore, ICANN compliance experienced challenges in obtaining detailed information from certain registries on this topic during the registry audit for addressing DNS security threats in 2019.

On 12 February 2020 the ICANN Board, in response to Business Constituency (BC), signalled that ICANN compliance cannot enforce certain contract provisions. Namely, ICANN compliance does not have an enforcement right against registrars who fail to include the required language in their agreements. Instead, the Registry Agreements Specification 11 3(a) provides registries and registrars with a mechanism to take action against prohibited activities. Finally, ICANN Org has no contractual authority to instruct registrars to delete or suspend domain names.

The PSWG sees the next round of gTLDs as an opportunity for improved contract provisions on DNS abuse. The PSWG is also seeking the closure of the discussion on the definition of DNS abuse, as there are already resources across the ICANN community that attempt to provide a definition:

- Competition, Consumer Trust, and Consumer Choice Review Team (CCT Review Team): "intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names". DNS security abuse "refers to more technical forms of malicious activity, such as malware, phishing, and botnets, as well as spam when used as a delivery mechanism for these forms of abuse".
- ICANN contracts prohibit registrants from distributing malware, operating botnets abusively, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activities that are contrary to applicable law.

During the GAC meeting with the ICANN Board, Göran Marby (ICANN Org) clarified that the definition of DNS abuse belongs with the GNSO and is for the community to decide on.

New gTLD Subsequent Procedures PDP

DNS abuse also remains a pain point for the GAC in the New gTLD Subsequent Procedures PDP (SubPro PDP). The SubPro Working Group published its final report after over five years of community work on 1 February 2021.

GAC members continue to harbour "serious concerns" on the lack of policy recommendations on DNS abuse mitigation within the SubPro PDP WG final report.

In Montreal, the GAC advised the ICANN Board not to proceed with a new round of gTLDs until after the complete implementation of the recommendations of the CCT Review Team that were identified as "prerequisites" or "high priority", for example including financial incentives in Registry Agreements to adopt proactive anti-abuse measures.

The At-Large Advisory Committee (ALAC) issued a minority statement on 18 January 2021, opining that "in declining to make any recommendations on DNS abuse mitigation for subsequent procedures, the WG is foregoing a valuable opportunity to incentivize existing registry operators in voluntarily adopting desirable changes to their Registry Agreements (including any provisions that affect their registrars) in order to bring about ultimate beneficial consequences to individual end-users". In principle, the ALAC voices out similar concerns to the GAC.

During the joint meeting between the GAC and the ALAC, Alan Greenberg (ALAC) voiced out his concern with the wish of contracted parties to work on non-binding guidelines and best practices instead of consensus policy. He expressed his hope that the SubPro PDP work had not been done in vain, in light of the recently proposed EU NIS 2 Directive that might require the ICANN community to reconvene again in order to reflect the changes proposed by the upcoming EU legislation.

Public interest commitments and registry voluntary commitments

In March 2013, after the 2012 round of new gTLDs, ICANN finalised Base Agreement Specification 11 containing mandatory and voluntary public interest commitments (PICs). Mandatory PICs included the technical analysis of security threats and regulated/sensitive strings PICs. Voluntary PICs may include anti-abuse policy, abuse mitigation commitments, child protection and additional geographic name protections.

The SubPro Final Report recommends adopting mandatory PICs and requires ICANN to allow applicants to submit registry voluntary commitments in their applications. ICANN compliance is ultimately responsible for the oversight and enforcement of all provisions contained in the Registry Agreement.

An ICANN70 plenary session was dedicated to ICANN's enforcement of PICs.

Kathryn Kleiman stressed that ICANN is not in the position of policing content on the internet. Website content is not part of ICANN contracts, and content is as such outside of Specification 11 enforcement.

Jamie Hedlund (ICANN Org) stressed that registry voluntary commitments are voluntary, to the point they have become part of a contract.

Gregory Shatan (ALAC) highlighted that ICANN enforces contractual provisions on general terms and does not intervene in any particular cases of infringement, which is for the individual registry or registrar to enforce.

Anne Aikman-Scalese (IPC) suggested establishing auditable processes that could bring ICANN compliance into the area of content. She argued that there are already mechanisms in place that touch upon content, without making ICANN a regulator. Mandatory PICs should be enforced by ICANN compliance.

GAC Communiqué:

On DNS abuse: DNS Abuse should be addressed in collaboration with the ICANN community and ICANN org prior to the launch of a second round of New gTLDs. The GAC supports the development of proposed contract provisions applicable to all gTLDs to improve their responses to DNS Abuse. The GAC also emphasized the importance of taking measures to ensure that Registries, Registrars and Privacy/ Proxy Services providers comply with the provisions in the contracts with ICANN, including audits. The GAC welcomes the recently-launched DNS Abuse Institute and encourages community efforts to cooperatively tackle DNS Abuse in a holistic manner.

On PICs: If a subsequent round of New gTLDs occurs, additional mandatory and voluntary PICs should remain possible in order to address emerging public policy concerns. ICANN's mandate is clearly contemplating contract requirements such as voluntary and mandatory PICs, that promote the security, stability, reliability and resiliency of the DNS.

Data accuracy and access to WHOIS

Expedited Policy Development Process

After the GDPR entered into force, the ICANN community initiated the Expedited Policy Development Process (EPDP), as part of emergency measures to comply with the data protection rules under the EU GDPR when it comes to registration data.

Phase 1 (August 2018 - February 2019) of the EPDP laid out the foundation of a new policy framework and Phase 2 (May 2019 - July 2020) focused on a System for Standardised Access/Disclosure (SSAD). Phase 2 was concluded with the Final Report on 31 July 2020, to which the GAC submitted a minority statement, along with the ALAC, BC, IPC, SSAC. Phase 2A started in December 2020 focusing on issues not addressed on Phase 2: the treatment of data from legal entities and pseudonymised emails.

In its minority statement from 24 August 2020, the GAC expressed its public policy concerns in the way in which the EPDP recommendations:

- Currently conclude with a fragmented rather than centralised disclosure system.
- Do not contain enforceable standards to review disclosure decisions.
- Do not sufficiently address consumer protection and consumer trust concerns.
- Do not currently contain reliable mechanisms for the SSAD to evolve in response to increased legal clarity.
- May impose financial conditions that risk an SSAD that calls for disproportionate costs for its users including those that detect and act on cybersecurity threats.

On 9 March, the Intellectual Property Constituency (IPC) requested that the ICANN Board halts their consideration of the EPDP Phase 2 recommendations due to the lack of consensus, public interest issues and emerging regulations to be taken into account, such as the EU NIS 2 proposal.

The ICANN Board is due to consider launching an Operational Design Phase of the SSAD, which aims to assess the operational impact of the implementations of the GNSO recommendations.

The GAC is continuously concerned over the lack of differentiation between legal and natural persons when it comes to publicly available registration data in the EPDP recommendations. The EPDP Team is expecting legal input from Bird & Bird on the levels of risks associated with the proposed safeguards; and whether the .eu Regulation, the WHOIS practices of the .eu registry EURid and RIPE NCC, together with the recent EU NIS 2 proposal "create precedent that could reduce risk in case of publication of a legal person's registration data", even if it contains personal information.

During ICANN70 the European Commission highlighted the proposal from the GAC in respect of the differentiation of legal v natural persons that is "fully compliant with the GDPR", according to the Commission's GAC representative. The GDPR, according to the European Commission, does not protect legal persons, including their name and contact details. However, there might be instances when a legal entity's data contains personal data. To address this, the GAC suggests a "two-step approach". As a first step, the contracted parties should distinguish between natural and legal persons when collecting and publishing registration data, and in the case of natural persons keep registration data non-public. In the case of legal entities, a further distinction should be made for registration data that contains personal information: only non-personal data should be made public. Contracted parties can go further than this minimum requirement by allowing registrants to choose whether they want their personal data to be published. Similar concerns with the availability of registration data, especially when it comes to legal entities, have been taken into consideration in the NIS 2 proposal. Namely, that non-personal registration data needs to be public, according to the European Commission representative.

The GAC discussions highlighted the importance of registration data accuracy for DNS security, stability, and resilience, as stated in the SSR2 Review Final Report. According to the RDS/WHOIS Review report (2019) the data inaccuracy rate is 30-40%. According to an Interisle study from 2021, 13.5% of domains have an actual registrant identified in the WHOIS.

Laureen Kapin (PSWG) stressed the need for flexibility of the SSAD, as relevant legislation may change, e.g. the EU NIS 2 proposal as an existing example with a definite impact on the SSAD and the EPDP in general.

GAC Communiqué: Phase 2 EPDP is a step forward but the GAC has serious concerns relating to certain Recommendations and gaps in the Final Report of Phase 2 of the EPDP. The GAC advises the Board to consider the GAC Minority Statement and available options to address the public policy concerns expressed therein, and take necessary action, as appropriate.

Relevance for ccTLDs

It seems that security and DNS abuse issues are increasingly becoming inseparable from open WHOIS discussions across the ICANN universe. It also seems that the EU NIS 2 Directive proposal is already seen as a vector to counter-balance the GDPR effects on the accessibility and availability of public registration data, although it cannot be compared to the GDPR in terms of direct applicability across the EU Member States (Regulation v Directive) and the fact that NIS 2 is still in its nascent stages as a fresh legislative proposal. Data accuracy and EPDP progress discussions are also another example of governments stepping in by proposing regulation, if they feel that their public interest concerns are not duly taken into consideration within the multistakeholder process. To be continued.

ICANN70 ccNSO Report

The ccNSO only held a limited number of sessions during ICANN 70. As these sessions mostly dealt with ICANN related issues that do not impact ccTLDs directly, there is little news to report this time. You will find references to the session recordings below.

Noteworthy highlights:

- Katrina Sataki stepped down as ccNSO Chair in order to take up her seat at the ICANN Board later this year. Alejandra Reynoso (.GT) takes over the reins after having served as Vice-Chair and MPC Chair. She will be supported by Jordan Carter (.nz) and Pablo Rodriguez (.pr) who were elected as ccNSO vice-chairs. Here is the ccNSO Council Meeting recording.

- The ccNSO kicked off the process of updating its internal rules. These date back to 2002 and need to be adapted substantially to fit the increased size and changed participation dynamics in the ccNSO. Watch the recording.

- The ccNSO had an informal exchange with the ccNSO-appointed ICANN Board members on the current situation, the return to normal, the number of internal reviews and the need to prioritise the workload. Watch the recording.

- The ccNSO's Internet Governance Liaison Committee (IGLC) continued to shape the framework for exchanges on internet governance related ccTLD initiatives. It is seeking examples where ccTLDs have supported solutions to sovereignty-related policy discussions. Watch the recording.

- During a session on the future of ccTLDs, Olaf Kolkman (ISOC) shared his views on the five critical properties of the internet. In an excellent keynote speech, Olaf took us on a journey into the future. He invited participants to imagine this was 2031, we are still meeting virtually and still connecting. He gave us a very realistic taste of some potential scenarios (roaming fees, certificates...) and analysed how it came to this. In a dark scenario we could end up with a problematic situation of errors (sound cuts, digital borders, alert pop-ups etc) because of the small changes regulation has made to the functioning of the infrastructure. Governments are trying to address societal issues as they regulate the internet (fake news, privacy etc) but they are not considering the impact on the internet itself. Olaf highlighted the five critical properties of the internet (accessibility, open architecture, decentralised, common global identifiers and technological neutrality). If one of these properties is taken away, the system crumbles. He suggested that whenever there is a regulatory proposal, an internet impact analysis should be made so that the regulation does not negatively impact the critical infrastructure. In order to help with this analysis, ISOC published the internet impact assessment toolkit.

- Following this keynote, five ccTLD managers (.NG, .NL, .BR, .IN, .VI) explored the future of ccTLDs. There was general agreement that domains will not reach the end of their life cycle any time soon, that ccTLDs need to listen carefully to their local internet community in order to be successful and that the governments should be regarded as crucial partners when defining growth strategies for ccTLDs. Watch the recording.

ICANN71 will be held virtually on 14-17 June 2021.

CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. CENTR currently counts 53 full and 9 associate members – together, they are responsible for over 80% of all registered domain names worldwide. The objectives of CENTR are to promote and participate in the development of high standards and best practices among ccTLD registries.

Rate this CENTR Report on ICANN70

(Thank you for your feedback!)

☆☆☆☆☆

CENTR vzw/asbl
Belliardstraat 20 (6th floor)
1040 Brussels, Belgium
Tel: +32 2 627 5550
Fax: +32 2 627 5559
secretariat@centr.org
www.centr.org

To keep up-to-date with CENTR activities and reports, follow us on Twitter, Facebook or LinkedIn