Council of European National Top-Level Domain Registries

Report on ICANN71

Virtual Policy Forum
14-17 June 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

CENTR reporting moving on to the next phase 3

Impact of Regulatory Developments on ICANN Policy Topics 3

The problems 3
The solutions 4

ccTLD governance models - why one size does not fit all 5

ICANN71 and DNS Abuse 6

Definitions? 6
Facts? 6
Legislation? 7
The role of ICANN? 7
Is the internet going to fall? 8

Data accuracy obligation and EPDP - what's next? 8

Distinction between legal and natural persons 9
Accuracy 9
Data is still missing 10
Or is it really missing? 10

In other news 11

The SSAC publishes a recommendation on abuse handling in the DNS 11
Subsequent Procedures (SubPro) aka Future gTLDs Update 11
ICANN 72: sleepless in Seattle or in the home office? 11
Important heads-up 12
ccNSO Policy session 12

CENTR reporting moving on to the next phase

In recent years ICANN Org and the ICANN community have significantly improved the accessibility of information and the coverage of ICANN meetings and processes. Both the live reporting from the ccNSO and the gNSO briefings are outstanding examples of thoroughness and timeliness. Where CENTR has filled an information gap by writing ICANN guides and reports for the last 20 years, we concluded that this is no longer needed.

Therefore, after covering about 65 ICANN meetings and more than 1000 pages of reporting, we decided to shift gears and bring a different type of coverage.

Rather than cover all sessions in the GAC and ccNSO, we will pick the most relevant themes from the ICANN meeting, keep an eye on longer term trends and offer an analysis where relevant for ccTLDs.

We'd like to thank our loyal readership and hope you'll enjoy our new approach to covering this complex, often frustrating, sometimes exciting but always fascinating organisation.

Impact of Regulatory Developments on ICANN Policy Topics

Since 2016 the ICANN community has been struggling with the relationship between its multistakeholder model and the reality of regulatory developments. Often these regulatory developments overrule the outcome of the multistakeholder discussions or impact its delicate status quo. A session at ICANN 71 on the impact of regulatory developments on ICANN policy topics touched on a number of aspects, but tip-toed around the really difficult questions.

I see three problems to this, with two possible solutions.

The problems

First, there is the issue of timing. The EU NIS 2 Directive proposal provides a perfect example here. Despite European legislators not being known for the high speed of their processes, the ICANN Community is struggling to keep up with the impact of finalised legislation. Where the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data is in essence a response to the 2016 GDPR, the ICANN Board is still considering the final report on phase 2 (the distinction between legal vs natural persons as registrants). However, in the meantime, the European Commission has published a proposal for an updated Network and Information Security Directive (NIS 2). This proposal includes an article that deals with data accuracy requirements for registries and registrars (i.e. Article 23). While it is tempting to see this as a solution in the current EPDP discussions, recent advice from the European Data Protection Supervisor (EDPS) signals it might not bring any relief.

The key question is: should ICANN wait for the conclusion of this regional regulatory process or base its future discussions on the assumption that the draft proposal will stand the test of the trilogue?

Secondly, there is the issue of representation. ICANN's multistakeholder community provides ICANN with its main strength: diversity-driven consensus. However, when ICANN consensus outcomes are fed into regulatory processes, they become just one of many different submissions. ICANN's response to the Digital Services Act consultation was one of the whopping 2863 responses received. NIS 2 is currently being discussed in the European Parliament and is likely to raise a similar interest. At the same time, regional and national instruments might be of high relevance to the global ICANN community, but that interest might not be parallel to the interest of local ICANN community members (Law Enforcement, Governments or countrycode registries). So even if the ICANN community reaches a consensus, how is ICANN Org going to advocate that consensus in regional or national legislative processes?

Thirdly, different parts of the ICANN community are in rather a different shape when it comes to dealing with public interest issues. Let's take the elephant in the room as an example: so-called DNS Abuse. As regulatory processes try to remedy regional or national issues, the way they target 'the DNS' or 'domain name registries and registrars' is often pretty blunt. In the - laudable - name of maintaining the level playing field, those parties with low DNS abuse stats will be affected in the same way as those with high stats. When the European Commission is aiming to "[contribute] to the security, stability and resilience of the DNS" by demanding data accuracy (NIS 2, art 23), it is unclear how additional requirements for registries and registrars with low DNS abuse stats would help achieve this.

The solutions

In the session, many participants identified the need to set up an early warning system for regulatory developments. This can only work as a joint effort. For example, CENTR publicly provides monthly regional updates (see e.g. for May 2021). Through the GAC (and ccNSO) ICANN has an incredible source for news about legislative initiatives at its fingertips. ICANN should further explore these avenues and provide a curated and regular feed to its community.

Legislative processes are best navigated after synchronisation with the local internet community and the local ICANN community participants. Before engaging in a process, ICANN should inform and sync with those entities. Here the GDPR provides an excellent example. European ccTLDs adapted pretty swiftly to the new circumstances, as they were compliant with their national data protection regimes long before the EU GDPR came into force. The change in accessibility of the WHOIS database has led to very few issues. Maybe more could have been learned from these local processes...

Think globally, but act locally in close partnership with the locals.

ccTLD governance models - why one size does not fit all

ccTLD governance models[1] are often a source of confusion and concern. How is it possible that there is no standard governance model for one of the most visible operators of the Domain Name System (DNS)? Why are they different? Which one is the best?

For anyone associated with the ccTLD industry these are not new questions. The topic of ccTLD governance models even made it to the 2005 Tunis agenda for the Information Society[2] and has been the subject of a series of (slightly outdated but still relevant) OECD reports.

All of these questions and more were answered in an outstanding presentation by Katrina Sataki (former ccNSO Chair, future ICANN Board Member) during a session at ICANN 71 organised by the At-Large Advisory Committee.

The findings and conclusions from the ccNSO research were nicely illustrated by a wide range of case studies from around the world.

Given the different legal frameworks, local customs and differences in local public policies, there really is not a single governance model that would fit more than a few ccTLDs.

This is visible in the company structure of the ccTLD managers. Different regions seem to show a preference for different models, e.g. the most common model in Europe is a dedicated not-for-profit private company whilst in the Latin-American and Carribean region ccTLD managers are often academic institutions.

The different models have different strengths and weaknesses.

For example, government based models are associated with clear responsibilities and rights of registrants and good oversight over the implementation of public interest into the domain name registration policies.

Not-for-profit models are associated with efficiency and the agility to respond to changes.

Governance models that are based on multistakeholder input seem to work best.

Some ccTLDs have carefully balanced boards, others have advisory councils, some are membership based or have oversight, typically by the government.

One thing that all ccTLDs have in common is that they serve their local internet community.

That community is not restricted to its registrants, but includes government agencies, businesses, the telecom industry and internet users who have not registered a domain.

ccTLD managers are a prime example of how diversity leads to the structural strength of the system. There is no single organisational weakness that could impact this important function, they are not interdependent, either financially or technically.

1 The ccNSO defined a ccTLD governance model as a collection of mechanisms, processes and relations of the ccTLD Manager and others, to control and operate the ccTLD.
2 The Tunis Agenda for the Information Society was a consensus statement of the World Summit on the Information Society, adopted on November 18, 2005 in Tunis, Tunisia. It called for the creation of the Internet Governance Forum and a novel, lightweight, multistakeholder governance structure for the internet.

The numerous exchanges between the ccTLD managers - regardless of their structure - in the ccNSO, regional organisations such as CENTR, or even in standards development organisations such as the Internet Engineering Task Force, mean that the different models can continuously learn from each other and implement best practices which come more naturally to other models.

The diversity of different models is a feature, not a bug

ICANN71 and DNS Abuse

The so-called "DNS Abuse" continues to be the prevalent cross-cutting issue across the ICANN universe. Discussions on the need to consider public interests when it comes to the numerous on-going policy development processes, along with the question of ICANN's role in the multistakeholder ecosystem seems to be driven by the pressing issue of the darkened WHOIS post-GDPR, and as a result the inability of law enforcement and other third parties to address DNS abuse in an effective and timely manner. Let's try to dissect this complex issue by looking into the challenges for the ICANN community to move forward.

Definitions?

First of all, what is DNS abuse? It seems that different ICANN constituencies have different meanings of this notion. In 2018 the Competition, Consumer Trust, and Consumer Choice Review Team suggested that DNS abuse can be defined as "intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names". On the other hand, ICANN contracts prohibit registrants from engaging in activities such as the distribution of malware, botnets, phishing or intellectual property infringements. Contracted Parties (gTLD registries and registrars) have limited the definition to harmful activities involving the DNS, such as malware, botnets, phishing, pharming and spam as a delivery mechanism for other forms of DNS abuse. These limitations are based on the cases when registries and registrars should be able to act without seeking additional competence, like judging what can be considered an IP infringement.

Yet, there is no definite answer on what DNS abuse is or whether the aforementioned practices can or even should always be attributed to the technical layer of the internet.

Facts?

While there is no defining notion of what DNS abuse is, the facts and data presented to different constituencies keep pouring in to justify the 'urgency' to address it, before reaching any agreement on what to measure in the first place. During the GAC session on DNS Abuse Mitigation at ICANN71, the Messaging Malware and Mobile Anti-Abuse Working Group (M3AAWG) and the Anti-Phishing Working Group (APWG) presented their latest report from June 2021. The report was based on a survey of "cyber investigators and anti-abuse service providers" on ICANN's application of the GDPR and how it has impacted "anti-abuse work". According to the results of this survey, the many use cases of WHOIS are affected, and only 2.2% of the respondents think that ICANN's policy implementing the GDPR is working when it comes to access to registration data. The underlying conclusion of these findings is that non-publicly available WHOIS precludes addressing cybercrime online.

DNS abuse is increasingly being associated with everything that can be wrong on the internet (i.e. “cybercrime”).

Legislation?

The ICANN Board continues to stress that the policies around addressing DNS abuse, along with the definition itself should be left for the community in the appropriate policy development process, led by the GNSO. This makes other constituencies, like governments, nervous and impatient, as they might feel that their concerns are not being appropriately taken into consideration. As for the discussions in the Governmental Advisory Committee (GAC), if an appropriate solution to address the public interest concern is not achieved through the multistakeholder process, then governments tend to resort to the measures they know best: national or regional legislation and other multilateral fora. We see this already at EU and Council of Europe level (the NIS 2 Directive proposal and the 2nd Additional Protocol to the Budapest Convention respectively), with other governments and regions to follow. During the GAC session on DNS Abuse Mitigation Japan presented its proposal for guaranteeing that the operations of registries and registrars are in compliance with ICANN contracts. These measures include: a registration data accuracy obligation at the time of domain name registration; the verification of registrants’ identity; and requiring registries and registrars to provide evidence that proves that domain names are not “abusive”.

Meanwhile, ICANN Org is struggling to enforce its contracts with regard to data accuracy requirements on its Contracted Parties.

The role of ICANN?

Governments are increasingly becoming frustrated with their mere advisory role in the ICANN policy development process. It might have been a working solution a decade ago, when the internet infrastructure was not considered to be states’ critical infrastructure and the backbone of the economy. However, the world has evolved since then, while the role of ICANN has largely not. Could this be an opportunity for ICANN to reinvent itself? Or is it destined to play catch-up with the increasing level of national and regional legislation targeted its way? During the plenary session at ICANN71, Jovan Kurbalija stressed the need for ICANN to become a constructive participant in the global digital debate, including on DNS abuse.

As we noted in our previous blogpost, this call to action might be in vain, given the limitations for ICANN Org to represent the ICANN community and the possible clash with local interests. Legislative processes are best navigated in synchronisation with the local internet community and the local ICANN community participants.

However, from the public engagement activities, it seems that ICANN Org is increasingly prioritising the European Union as a strategically important regulator, with other regions being pushed to the sidelines. These sentiments were confirmed by e.g. the Caribbean region representative during the plenary session, who highlighted the fact that ICANN Org’s management has not met with the government officials in the region for years.

ICANN should continue to serve as an important venue for the global multistakeholder community to come together and come up with policies that are not only proportionate but also workable for all regions and operators across the world. Unenforceable contracts is one of the examples where policy aspirations clash with the legal reality.

Is the internet going to fall?

Both ccTLDs and gTLDs are working hard to keep the internet community safe, despite no clear definition on DNS abuse, without conclusive data to support the assumption that access to WHOIS is a panacea to everything that is wrong on the internet, and while still being GDPR compliant.

Numerous voluntary and solution-driven efforts are being taken already, as presented by the Contracted Parties House at ICANN71. Other venues to bring together relevant industry actors and share good practice have emerged, such as the DNS Abuse Institute and the Internet & Jurisdiction Policy Network to address some of these issues without a risk for increased liability and contractual changes at ICANN level. As evident from the session, Contracted Parties are steadily advancing on their discussions regarding so-called "trusted notifiers", improving registry-registrar cooperation and registrants' rights protection mechanisms. These initiatives might be setting new standards and will be setting new expectations. The whole domain name industry should pay close attention to what is happening in this constituency, including the ones who do not have contracts with ICANN.

Outside of the gTLD space, European ccTLDs are continuously considered champions when it comes to addressing abuse within their remit and means and tools available for DNS infrastructure operators, while being subject to the GDPR and national data protection frameworks. It would have been natural to seek guidance from the region that has decades-long experience in managing redacted WHOIS whilst still being able to address abuse.

Awareness of these good practices, including the careful consideration to not disproportionately affect internet users' overall accessibility to services working on top of the DNS infrastructure, needs to be more widely targeted at the ICANN community at-large, as well as specifically towards governments and their public interest concerns in "DNS Abuse" discussions. The DNS is an important protocol which makes the internet function, yet it does not provide a silver bullet to solve wide societal problems.

The role of the internet ecosystem and the numerous players active within needs to be addressed in a holistic approach, with a clear understanding of the effects of drastic actions taken on the infrastructure level,be it at ICANN, other IG fora or in legislation negotiations.

Only this way can we all make sure we have one global internet.

Data accuracy obligation and EPDP - what's next?

Three years after the EU GDPR entered into force, the ICANN community is still debating the emergency measures with regard to data protection of gTLD registration data. Before the GDPR, gTLD registration data was publicly available, but the accuracy of this data is an issue that the community was facing long before that. In 2021, the Expedited Policy Development Process (EPDP) moved on to Phase 2A, with one main issue in focus: the distinction between natural and legal persons in the domain name registration process. Meanwhile, the EPDP's previous Phase 1 and Phase 2 policy recommendations are facing further implementation

challenges: inter-dependencies between issues in different phases and disagreements on issues of importance to the Governmental Advisory Committee (GAC). On top of everything, other regulatory developments, such as the EU NIS 2 Directive proposal, could have a further impact on the outcomes of the EPDP, with some constituencies calling for a halt to the EPDP Phase 2 recommendations. Registration data accuracy discussions are also steadily picking up, in light of the EU NIS 2 proposal.

Distinction between legal and natural persons

The GAC is continually concerned over the lack of differentiation between legal and natural persons when it comes to publicly available registration data in the EPDP recommendations. According to the briefings that the GAC received at ICANN71, the registration data of legal entities is consistently claimed not to be protected by the GDPR (ignoring the CJEU case-law on the matter, which confirms it is more nuanced than such a simple distinction). The preliminary EPDP recommendation on the issue retains a mere possibility for registries and registrars to differentiate between registrations of legal and natural persons, but they are not obliged to do so. The GNSO has been asked to monitor relevant developments, including NIS 2, to determine whether any changes to the EPDP are necessary.

Contracted Parties, particularly registrars, are those who would need to bear the burden of implementing the required distinction between legal and natural persons, while still being subject to the GDPR and other national data protection frameworks. They have identified technical difficulties in making such a change which, though it seems simple on paper, the benefits of such a change remain unclear.

Accuracy

The GNSO leadership is currently looking to initiate a scoping exercise on registration data accuracy work within the community. Many questions for future work on accuracy are still open beyond its scope: e.g. team composition and the timing of when the work will be launched. The date for the scoping work to be initiated has been provisionally set to August 2021, after EPDP Phase 2A is concluded.

According to the GAC, "the accuracy of domain name registration data is fundamental for maintaining a secure and resilient DNS" (EPDP Phase 2 Minority Statement). A similar sentiment has been transposed to the EU NIS 2 Directive proposal, that echoes the GAC concerns within the EPDP: data accuracy, the distinction between natural persons and legal entities, as well as ensuring access to registration data to an undefined group of so-called "legitimate access seekers" (Article 23).

The European Commission's representatives have previously reassured the ICANN community that the NIS 2 Directive proposal (and specifically Article 23) is not meant to replace the multistakeholder process within the EPDP but rather help operators by creating a necessary legal basis for registries and registrars to keep collecting, processing and publishing domain name registration data (while mostly ignoring how the GDPR is implemented by European ccTLDs). During the joint session between the GAC and the GNSO, the European Commission representative clarified that legitimate access seekers in the context of access to registration data should include cybersecurity researchers and intellectual property rights "enforcers". The Commission representative also urged the ICANN community to address the accuracy

issue, as it is not solely linked to GDPR compliance but also to contractual obligations with ICANN.

It is questionable if technologically neutral and general regional legislation, coupled with the principle of subsidiarity (Directive vs Regulation) and the supremacy of EU primary law (EU Charter of Fundamental Rights) can bring relief to purely contractual enforcement issues within ICANN.

Data is still missing

During the GAC's joint session with the GNSO, there were calls for data on the existing accuracy levels, in particular, the current percentage of accurate registration data, as well as the needed threshold for the data to be considered accurate.

To get more clarity on the associated issue, the registrars are also working on a "Registrant WHOIS Experience" study to better understand the current reality and whether "unredacted registration data in the WHOIS/RDAP continues to contribute to harm, enable fraud, or increase abuse", as identified by the Security and Stability Advisory Committee. Back in 2007, the SAC023 concluded that the "appearance of email addresses in the WHOIS contributed to receipt of spam- virtually assuring spam delivery to these email addresses". The results of the study are expected to be presented at the ICANN72 meeting.

It is clear that a lot has changed since 2007. However, it is important to base any policy development process on facts and evidence, especially when that policy change could come with an increased liability risk and potentially a technical burden on operators (similarly, the introduction of Article 23 in the NIS 2 Directive proposal should also have been more clearly substantiated, beyond a general statement that it is better for security).

Or is it really missing?

Having observed the EPDP discussions for over three years, the ICANN community is struggling to reconcile the many interests at stake. Despite the fact that a lot of substantial work has already been done, the implementation of policy recommendations from previous phases has been slowed down by minority statements, calls for the ICANN Board to address public interest concerns in the GAC, and despite good intentions, by recent regulatory developments in the EU.

On the other hand, there are already existing practices and examples to follow from European ccTLDs who are already compliant with the GDPR and who, in fact, did not face many significant changes to their registration data availability policies when the GDPR entered into force, including questions on access. European ccTLDs do not have a unified approach to their registration processes either: it is deeply rooted in national specifics and jurisdictions and, as stated in our previous blogpost, diversity within ccTLDs is not a bug but a feature.

Perhaps, the policy recommendations coming out of the ICANN PDPs need to offer more flexibility to operators to consider national developments, needs and specifics as well, whilst the DNS is subject to increasing regulatory attention. So far this approach has worked for ccTLDs, and more can be learned from these experiences.

In other news

The Security and Stability Advisory Committee (SSAC) publishes a recommendation on abuse handling in the DNS

Recently, the SSAC published a recommendation on how abuse should be handled in the DNS, underlining yet again the growing importance of the topic.

The goal of this report is to come up with an interoperable approach based on universal standards for DNS abuse handling. The SSAC recommends that each incident of DNS abuse should have a reporting entry point in the DNS ecosystem where the abuse is resolved through a predictable policy and process. These primary points can be registrars, registries, hosting service providers and other platforms, as well as domain name holders.

Those reporting abuse should have the responsibility of providing evidence and documentation, according to "objective standards".

The maximum time for escalation and remediation should be no longer than 96 hours.

The SSAC recommends that the ICANN community continues to work together with the extended DNS infrastructure community in an effort to examine and refine the proposal for a Common Abuse Response Facilitator to be created to streamline abuse reporting and minimise abuse victimisation.

Subsequent Procedures (SubPro) aka Future gTLDs Update

When will we see new gTLDs enter the root zone file? We don't know exactly but there are now indications that it is coming up.

While some parts of the ICANN community (such as the GeoTLD group) are getting frustrated with the slowness of the process, ICANN Org and the ICANN Board are moving forward with the draft operational plan that needs to deal with the hundreds of recommendations identified by the Cross Community working group back in 2020.

The next steps are:

1. the ICANN Board to decide on the Operational Design Phase trigger;
2. the ICANN Board to consider the PDP recommendations as adopted by the GNSO Council;
3. ICANN Org to begin implementing the policy recommendations. If all goes smoothly, ICANN Org could be expected to open a new round of applications for gTLDs tentatively around 2022-2023.

ICANN 72: sleepless in Seattle or in the home office?

In July, the ICANN Board will decide whether ICANN 72 (planned to take place in Seattle) can take place in person or whether it will be an online meeting. In a recent survey, the majority of respondents indicated an interest in returning to f2f meetings.

Some parts of the community flagged concerns on how this could affect representation and balance within the ICANN community. For example the discussions in the GAC reflected

the need to potentially reconsider the way a quorum is achieved for the GAC consensus advice. It will be essential to ensure that overall participation in GAC discussions does not disproportionately benefit those countries that have been advancing with their vaccination campaigns and therefore are able to participate in the f2f meetings. Likewise it will be important to ensure that remote participants can fully participate in GAC meetings, including its decision-making, in the same way as physically present members (in a hybrid setting). GAC members also expressed their concern over onboarding new GAC members that is currently lacking in the virtual environment.

Important heads-up

In the public part of the SSAC meeting, the "forced removal or transfer of a ccTLD" was raised as a possible topic of interest for future SSAC work. We will be keeping an eye on this.

ccNSO Policy session

It is easy to forget that the main reason for the existence of the ccNSO is to develop and recommend global policies relating to ccTLDs to the ICANN Board of Directors. Since its creation in 2003, it has only completed two such policy recommendations and is currently working on a third (PDP3 on the retirement of ccTLDs and appeal process) and fourth (PDP4 in IDN ccTLDs) recommendation .

The PDP3 answers the question as to what happens when a country code is removed from the list of country names ISO3166-1 or exceptionally reserved code list. This triggers a retirement process since the requirement of RFC1591 (the code is included in the ISO 3166 list) is no longer met. In case there is no agreement between the ccTLD operator and IANA, the ccTLD is retired within 5 years. If there is an agreement, the retirement plan can stretch over 10 years. Both processes end with the removal of the ccTLD from the DNS Root Zone file.

PDP3 also addresses the lack of appeal process for decisions from the ICANN Board that affect ccTLDs (such as decisions on the retirement, transfer, delegation or extension of retirement period of a ccTLD). The goal of introducing a review mechanism for such decisions is to increase the predictability and legitimacy of the process and to preserve the stability, security and operability of the DNS. Key considerations are that: the process needs to be low cost; it needs to be accessible, to be of limited duration and to increase the fundamental fairness of the decision making.

It is crucial that ccNSO members vote on this PDP3. Voting will be open in July.

PDP4 deals with IDN ccTLDs. While they have been around for about a decade, these are currently not recognised in the ICANN bylaws or in the ccNSO structure. The policy will also update the existing policy for the selection of IDN ccTLDs and spell out the principles underpinning the policy.

ICANN72 will be held on 23-28 October 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 ICANN71

(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