Council of European National Top-Level Domain Registries

Report on ICANN72

Virtual Annual General Meeting

October 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

Why every ccTLD should care about the ccNSO guidelines review

Until a few years ago, one needed to climb an impossibly steep learning curve when engaging in the country code Names Supporting Organisation (ccNSO).

These days, thanks to the excellent work of the secretariat, it is much easier to join the discussions. There are now good prep materials, live note-taking and perfectly supported online meetings and recordings. All the information we need is at our fingertips.

But still, the activity ratio within the ccNSO membership remains low.

At the last members' vote in July, heaven and earth was moved just to reach the quorum that allowed a vote on the retirement of country codes. And the two files that are coming up next are important enough to merit every single ccTLD's attention.

First, there is the Review Mechanism Working Group which will recommend a policy for review mechanisms for decisions by the ICANN Board that affect ccTLDs. These decisions are: the delegation, revocation and retirement of ISO 3166-1 listed countries and territories. It's hard to imagine that there is even one ccTLD that wouldn't care about a mechanism that might decide on its mere existence.

And secondly, there is work being undertaken on the selection and deselection of IDN ccTLDs. For more than a decade the ccTLD community has been relying on the IDN fast track mechanism, which introduced new top level domains long before the new gTLD round took place in 2004. The group defines the criteria, process and procedures for (de)selecting Internationalised Domain Name country code Top Level Domain strings. The results of this work will eventually replace the IDN ccTLD Fast Track Process.

So, how is it possible that ccNSO members seem not to care enough to vote?

The ccNSO has grown significantly since it developed its own internal rules in 2004. The ccNSO currently has 172 members (up from 45 in 2004) and it has become more and more difficult to get the necessary quorum and votes to move forwards on some of the crucial positions.

Of those members, only a small group is actively engaged and knowledgeable enough about the procedural issues at stake to cast a vote confidently and in a timely manner. And this isn't just a problem for the few policy development processes mentioned above. Since 2004, the ccNSO has also been named in new ICANN processes such as the accountability framework where the role of the ccNSO as a decisional participant is specified.

At ICANN 72, the ccNSO Guidelines Working Group presented their proposal (version 7, 14 October 2021) to address this procedural issue without creating a democratic deficit.

In a well-attended session, the working group presented their proposals for change and took the temperature of the room. The proposals include a review timeline for the internal rules, establish procedural minimum timelines and set out principles that should govern the relationship between the ccNSO council and the ccNSO Community. They also include a list of decisions that the Council can take without being subject to members' votes, transparency and publication obligations and fine tuned electronic voting procedures. Finally they suggest revised quorum rules for members' votes. Overall their proposals were broadly supported and set the course for the dearly needed review.

Let's keep our fingers crossed that enough members will see the need to support this change when the final proposal is subjected to their vote. The irony of failing to do so would signal systemic failure.

DNS Abuse discussions shifting gears

The DNS Abuse topic was omnipresent at ICANN 72. Webinars in prep week (At-Large Advisory Committee and ICANN Board workshops) set the stage and the tone for intense but overall balanced discussions.

In this post I am trying to capture the main lines of thought and initiatives that came out of what must have been 15 hours of meetings and as many hours of zoom chats.

Executive summary

This is picking up speed fast.

What is this about?

The DNS Abuse discussions are not new. After a decade of arguing over ICANN's scope to deal with this topic, most parts of the community now seem to have accepted that ICANN can be a place to discuss technical DNS Abuse. Despite the lack of formally accepted definition of technical DNS Abuse, in all discussions the following is understood to be captured by this term: phishing, pharming, botnets, malware and spam if spam is used as a delivery channel to one of these four harmful activities.

The limitation to these activities seems to have been stable for the last couple of meetings, despite calls to reject it as a starting point for the discussions from some parts of the ICANN community (e.g. gNSO Business Constituency). Having originated and been fine-tuned in the contracted parties' Abuse Working group, this list has now found its way into all conversations. For instance in the ccNSO, there seems to be an agreement that possible incremental improvements to this definition do not seem to outweigh the extra lost time for yet another review.

Why now?

The trigger for these invigorated debates is the mounting despair by the rightsholders' community and the law enforcement agencies about the lack of publicly available WHOIS data.

Who should act?

There is an interesting problem on the table: the collective action problem. Where something impacts everybody, but there are a number of disincentives towards acting collectively, very little progress is made. This explains the increasing role of organisations outside ICANN who are filling this gap: The DNS Abuse Institute and the Internet and Jurisdiction Policy Network have become leaders in knowledge exchange, and in the case of the former even take a proactive role in helping the industry tackle DNS Abuse. The institute plans to launch a Centralised Abuse Reporting Tool by Q3 2022.

Another phenomenon has also unlocked the whole conundrum: registries and registrars are taking steps to individually or collectively address some of the challenges outside of ICANN in order to avoid the fences put up by the ICANN mandate. The Registries and Registrars stakeholder group's Abuse Working Group recently published a paper that provides guidance and a framework for working with trusted notifiers.

In these discussions and activities, they go way beyond the limitations set by the definition discussed earlier. Content-based action is no longer shied away from. We see this in the way large US-based operators have started to work with Trusted Notifiers and accept their reports about infringing content as a basis for deleting a domain. Rather than relying on the legal system and due process, they enforce decisions by third parties. As one participant noted: "We are very happy for them to deal with this rather than us having to waste resources". While most ccTLDs are probably wary of that approach, this trend might create even stronger expectations to review current stances on third party notifications. To illustrate the different approach to this problem: the above-mentioned framework for trusted notifiers finds that a low false positive rate is acceptable.

Preaching to the choir?

The fundamental flaw in the logic in most of the discussions is this: those that are ready to engage in these conversations or accept ICANN's (e.g. DAAR) or the DNS Abuse Institute's help are already taking

action and have typically good track records and cleaner zonefiles.

For instance, when it comes to spam, yet another large scale study leads to the clear conclusion that this problem is not so much with the ccTLD zones, but with a small group of actors, both in the nGTLD groups and with specific registrars. In some TLDs 90% of the identified abuse was registered through 1 registrar.

Yet, any regulation (think NIS2 art. 23) will have an effect on the whole industry. At several points during the discussions it was pointed out that proactive measures (such as identity verification) will create unavoidable friction in the sales channel, affecting 99% of well intended registrants while hardly slowing down the bad actors.

Elephants

And this is probably still the elephant in the room: ICANN continues to fail to deal more forcefully with these bad actors. ICANN's compliance process needs more teeth. Some of the contracts - the registrar accreditation agreement in particular - need a review to make that work. Rather than shifting this discussion to ccTLDs - who are consistently rating better in abuse studies - or all contracted parties, the low hanging fruit should be picked first.

As a consequence of ICANN's incapacity to tackle this, the whole DNS industry will be jumping through a never ending series of hoops.

While some of these efforts by ccTLDs will have an impact, they come at a cost that might be too high for their marginal effect. Again the NIS2 data accuracy obligation is a prime example here: accurate registrant data in ccTLDs will not reduce the number of DDoS attacks, malware or state sponsored hacking. Anyone who keeps on making these claims is willingly spreading misinformation.

What should the ccNSO be doing on DNS Abuse?

The ccNSO held a long and interactive session to find out what - if anything - the ccNSO should do in the context of these discussions.

A range of speakers (4 ccNSO Members, 1 Public Safety Working Group Member and a Contracted Parties Abuse WG member) presented ideas for ccNSO actions which were then voted upon. Some of the ideas were way outside the scope of the ccNSO (audits on abuse mitigation, maintaining centralised lists of abusive domains), and others will for sure be controversial with ccTLDs (a voluntary Code of Conduct drafted by the ccNSO). As all participants in this open session took part in the voting, the results are not reliable as a base for ccNSO actions (only about 20% of participants were ccTLDs). It was an excellent kick start of the debate on the role of the ccNSO, but by no means an endpoint. The ccNSO Council will now prepare a proposal for discussion with ccNSO Members at ICANN 73.

ccTLDs might be just too different for a regional - let alone global - approach on this complex issue.

Links to the main DNS Abuse related sessions:

- Board workshop on DNS Abuse
- At-Large session on Tackling DNS Abuse
- GNSO: CPH DNS Abuse Work Group Community Update
- ccNSO session on the role of the ccNSO in the DNS Abuse discussions Part I
- ccNSO session on the role of the ccNSO in the DNS Abuse discussions Part II
- GNSO: BRG - Regulation, DNS Abuse and the Next Round - dotBrand Perspectives

We need to talk about data accuracy

The topic of registration data accuracy is picking up again at ICANN. Be it due to the fact that the EU is negotiating the NIS 2 Directive and the corresponding registration data verification obligation put on registries and registrars. Or that data accuracy keeps coming up in the ongoing GDPR compliance discussions by ICANN contracted parties (e.g. gTLD registries and registrars) after more than three years of law enforcement authorities and rights holders claiming not to be able to investigate illegal activities online due to the "darkened WHOIS". One thing is sure: the data accuracy discussion underpins many current cross-community issues at ICANN, including 'DNS abuse', contractual compliance and public interest concerns.

Accuracy, what?

Although the idea of 'accuracy' when it comes to collected registration data by registries and registrars is not new and has apparently already been included in the registrar accreditation agreement dating back to 1999, it is only recently that the data accuracy discussion reached another level of 'urgency'. This coincides with the GDPR's impact on the *public* availability of registration data across gTLDs (the so-called 'darkening of WHOIS').

After the GDPR entered into force in 2018, ICANN responded with the Temporary Specification that moved most of the personal information of registrants within ICANN contracted parties (gTLD registries and registrars) to no longer being publicly available. This suddenly became a pressing issue primarily for law enforcement and rightsholders. After more than three years of discussions on a potential consensus policy on "WHOIS obligations" within the unprecedented Expedited Policy Development Process (EPDP), there is still no end in sight on how to reconcile the differences between all stakeholder groups. With a number of loosely connected issues popping up that the EPDP allegedly needs to solve, it is no wonder this is taking so long. All the EPDP should have addressed is how to make sure that contracted parties respect and adhere to data protection principles, and include processes and procedures to keep that data safe and secure. All the other issues, such as access to personal information, consumer protection issues and even public interest *beyond* data protection are essentially out of scope and merit their own separate legal basis.

Indeed, data accuracy is also part of the data protection principles. In fact, it is one of the fundamental principles under the GDPR, and puts an expectation on data controllers and processors to take "every reasonable step[...]to ensure that personal data which are inaccurate are rectified or deleted". As data protection is about protecting individuals, the data accuracy principle under the GDPR is about giving end-users control over their personal information. It is not about providing "efficient" access to third parties.

Accuracy *of* what?

The question of data accuracy is now a political question, as the EU is currently negotiating the revision of its cybersecurity rules that also include a very specific point on ensuring the accuracy of registration data. This obligation is a direct consequence of the alleged impact of the GDPR on the public availability of domain name registration data within gTLDs.

In fact, the EU NIS 2 proposal even borrows language from the GAC EPDP Phase 2 Minority statement, i.e. that the accuracy of domain name registration data is essential for maintaining a secure and resilient DNS. The issues that certain stakeholders, including governments and intellectual property rightsholder groups, have been raising within ICANN have all made it into the EU NIS 2: e.g. the obligation to publish all registration data concerning legal entities, and to provide access to non-public personal information of individuals to an unlimited group of "legitimate access seekers". Meanwhile, the GAC continues to underline that the EPDP recommendations are not striking "the right balance of protecting personal information and protecting internet users' safety and security", which is a consistent agenda point during the joint meetings between the GAC and the GNSO Council, responsible for overseeing the policy development work at ICANN.

Interestingly, back in 2014 a Study on the Misuse of WHOIS found that publicly available registration data has, amongst other things, also contributed to the "highly sophisticated planning to extract money, distribute malware, and[...]a phishing attack using WHOIS information". In other cases, registrant

information was used to register numerous domains for illegal purposes.

Clearly, the whole debate about third-party (incl. public) access to WHOIS being essential for combatting 'DNS abuse' is not that black and white in the end. Data protection on the internet, including within the domain name industry, is also a security-related matter that unfortunately goes largely unnoticed in the GDPR-compliance discussions at ICANN.

In parallel with the EU negotiations on imposing a "security"-related data accuracy obligation on TLDs operating in Europe, the discussions on *what accuracy is* in the context of registration data is also picking up within the ICANN Community. The newly-established Registration Data Accuracy Scoping Team is expected to look into existing accuracy requirements under ICANN contracts with registries and registrars and assess the measures used by ICANN Compliance to monitor, measure, enforce and report on the accuracy obligations as specified in these contracts. From the discussions taking place at ICANN72, it seems that registration data accuracy within the ICANN context has primarily been a syntactical and operational check to ensure that registrants provide contact details that are functional.

In principle it should be for the community to decide whether any additional elements to the concept of accuracy need to be added to the definition through a formal policy development process in the GNSO and after the Scoping Team finishes its mapping work. However, the proximity of EU legislation that does not take into account these community discussions on accuracy might make these efforts moot. The EU discussions on NIS 2 are leaning heavily towards a different definition of accuracy obligations that include additional ID verification checks that put all the burden on technical operators. Since the EU NIS 2 Directive is intended to apply to all TLD operators that offer their services in Europe, it will also affect ICANN contracted parties.

Access to non-public registration data

The discussions on accuracy can no longer be distinguished from the questions of who shall receive access to non-public personal information of domain name holders and when. While the EU is in the process of obliging TLDs to give it out to all "legitimate access seekers'', the ICANN community is still discussing the possibility of establishing a System for Standardized Access/Disclosure (SSAD) to "centrally handle requests for non-public registration data". To inform the deliberations on putting such a system in place, the ICANN Board has requested an Operational Design Phase (ODP) Assessment. Originally, the ODP Assessment was supposed to be completed by 25 September 2021. According to the project update given at ICANN72, the data collection activities have taken longer, and the data received has raised more questions, which merits more community discussions. In addition a proper cost-benefit analysis needs to be conducted before the ICANN Board can make a decision to proceed forward with the SSAD.

At the same time, another verification issue landed on the table: the verification of users who wish to use SSAD and request access to registration data. Ironically, the completion of the ODP Assessment phase has also been delayed by the fact that the GAC is not able to complete a survey on the accreditation of governmental entities, due to this being a "complex issue".

Verifying the identities of registrants and legitimate access seekers should be easy, no? Otherwise, why are we in the process of putting a data verification obligation on registries and registrars operating in the EU, expecting them to figure this out on their own in order to effectively comply with it? This remains a mystery for now that would need to be fleshed out in the implementation phase. Not only in the case of the still largely hypothetical SSAD, but also the speedily approaching NIS 2 Directive compliance.

The sense of urgency

Registration data accuracy is indeed an urgent topic within ICANN. However, this urgency is not coming from the looming threats to the security, stability and resilience of the DNS. The urgency of data accuracy is underpinned by individual governments and regional policymakers trying to "fix" an issue that is uniquely relevant only in the context of global internet governance. The NIS 2 Directive won't have an impact on contractual compliance by ICANN. However, it will have an effect on individual gTLDs, ccTLDs and registrars that will find themselves between a rock and a hard place trying to comply with unattainable standards.

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 10 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.

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 or LinkedIn