Council of European National Top-Level Domain Registries

Report on ICANN66

Montréal
2-7 November 2019

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

GAC Report 10

Executive Summary

At this ICANN66 meeting, one of the top subjects in the GAC was DNS Abuse, which was discussed on numerous occasions. Furthermore, the on-going work within the EPDP (and beyond) to comply with the GDPR continues to be a high-priority topic for the GAC. There was also another update on the Dot Amazon file, though no further GAC advice on this topic was issued in Montréal.

Link to the GAC Montréal communiqué

The ccNSO held an excellent table-top exercise to test ccTLD disaster recovery and business continuity planning. The Strategic and Operational Planning Committee (SOPC) is reviewing its charter and warns of volunteer fatigue.

Discussions with the ICANN Board underlined that the community is struggling with the concept of DNS Abuse. It is to be expected that this discussion will remain high on the ICANN agenda and those of the different constituencies.

Registry updates on abuse prevention, auction processes and platform migration showed that the ccTLD industry is innovating at a fast pace.

The PTI sessions confirmed that PTI is doing an excellent job. Additional review mechanisms are not seen as a priority.

The Internet Governance session provided a good overview of the different ways in which ccTLDs contribute to local and global Internet Governance initiatives.

The ccNSO is running an election process for an ICANN Board Member to replace Chris Disspain at the end of his term. There are three candidates for the seat: Patricio Poblete, Calvin Browne and Nigel Phair.

ccNSO Report

All session overviews and presentations are available via the ccNSO meeting website.

The DNS and the Internet of Things (IoT)

In this excellent presentation, Cristian Hesselman (SIDNLabs) and Jacques Latour (CIRA) gave an overview of the challenges and opportunities for ccTLDs in the area of Internet of Things. The main differences with "traditional" applications is that IoT continually senses, interprets and acts upon the physical world without users being aware or involved (passive interaction). There are between 20 and 30 billion devices "in the background" of people's daily lives. They are widely heterogeneous (hardware, OS, network connections) and have longer lifetimes (sometimes decades). They are typically not or poorly maintained. IoT promises a safer, smarter, and more sustainable society, but IoT security is a major challenge. The Mirai (IoT powered) DDoS attack was a wake-up call for the Internet and DNS industry.

The DNS could provide answers to some of the major security challenges and allow users to gain back control over what information they share. It could also be used to avoid re- or misdirection of traffic through DNSSEC for example. There are also risks for the DNS itself. One of the main issues stems from the risk of being used as amplification for DDoS attacks from IoT devices. CIRA and SIDN presented some models in which the DNS helps mitigate these risks. Close collaboration with vendors of IoT devices and telecommunication operators will be needed.

Potential opportunities for ccTLDs include:

- acting as IoT trust anchors (cf. CIRA's secure IoT registry);
- initiating collaborative security efforts (e.g., a national DDoS clearing house);
- initiating IoT security mechanisms for which there is little commercial interest as of yet (e.g. secure home gateways);
- carrying out research on IoT security;
- leveraging the mature DNS infrastructure to support ongoing security of IoT devices.

Presentation

Meeting with the ICANN Board

This session covered three topics:

The Special IANA Functions Review. This review would be an extraordinary process to follow if the Board failed to adequately respond to a request to fix an IANA Functions systemic operational issue. It is the last resort and the very end of the escalation path. It would be triggered following serious and repetitive breaches of the service level agreement (SLA). The Board considers this a rather hypothetical question as we have never needed to take the first step on an escalation path so far. It should be noted that IANA is performing at the highest standards.

The second topic discussed was how the priorities highlighted by the CEO fitted into ICANN's 5-year strategic priorities' plan. The Board responded that these are set in consultation with the Board and the Board ensures they are linked to the approved plans.

The third topic was DNS abuse, and the Board was asked to give their views on this issue. The Board responded that the scope and definition of what constitutes 'abuse' is up to the community. The Board also acknowledged that some issues are currently being included in these ongoing discussions, and that not everyone in the community would agree that these issues fit in there. It was noted that ccTLDs could enrich the debates on this issue with their experience. The Domain Abuse Activity Reporting (DAAR) project is now open to ccTLD participation and those that are interested should contact David Conrad (ICANN).

Debriefing ccNSO workshops

SOPC workshop debriefing

Giovanni Seppia (EURid) gave participants an update on the Strategic and Operating Plan Committee (SOPC) of the ccNSO, notably the workshop that took place on 3 November. The first part of the workshop was a presentation by the ICANN finance team of what is in the pipeline. This report will be published on 17 December and will be followed by a two-month comment period. Further coordination with the gNSO was also discussed during this workshop. For the first time there was a decision to have a joint session,

starting with ensuring that common topics of interest are mentioned in the comment produced by the ccNSO SOPC and the equivalent gNSO working group.

Giovanni also explained that they had discussed the working group methodology, observing that there is a certain amount of multistakeholder fatigue. To combat this, they discussed how they could work differently and started with a course held in September in preparation for the meeting in Montréal.

During the workshop, the SOPC also reviewed the SOPC Charter, which was established in 2008 and revised in 2017, when they decided to change the group from a working group to a standing committee within the ccNSO. The charter is divided into four sections: the scope of the SOPC, its activities, participation and membership. They have noticed that on average only 50% of the membership is active and so are developing an action plan, which includes improvements in the working group methodology and tasking each proactive WG or committee member to reach out and find new members before the next meeting in Cancun.

Giovanni ended by highlighting a recent achievement of the ccNSO community; exactly 10 years after the IDN ccTLD Fast Track Process was launched, .eu managed to have .eu in Greek delegated. The process took longer than expected but they never gave up, thanks to support of community and to many of those who participated in different working groups. It will be launched on 14 November, and Giovanni thanked all the ccNSO community, highlighting some members in particular.

TLD-OPS update and workshop debriefing

Jacques Latour (CIRA) and Régis Massé (Afnic)

Jacques explained the background behind deciding that there was a need to work on Business Continuity and Disaster Recovery (DR) within the community, which started with a workshop at ICANN63. During Sunday's workshop, they held a table top exercise and tested the BCP to see if it worked or not, concluding that it was a successful experiment. The success of the playbook was partly due to the volunteers, and Dirk Jumpertz (EURid) was recognised as the DR/BCP Drafting team's fearless leader. The feedback from this exercise was excellent!

The scenario used in the exercise was the security breach of a registry, and participants had a set of cards to help them identify the appropriate response. For the exercise, participants were given a DR playbook, a made-up registry (.ok registry) and then they had templates to work from. In the first part of the session they went through the document to see how to define things, how to build a plan etc, after which they applied the plan during a crisis. About 30 different ccTLDs were in the room and what was interesting is that even in controlled environment, everyone handled the situation differently. Jacques highlighted that everyone has different approaches and priorities so when working on a BCP, it is important to make sure that everyone is on the same page. Furthermore, the point of a BCP is to test it often in order to get used to it

The next steps are that the documentation will be made available for everyone. The cards will also be made available. The exercise might be repeated at one of the next ICANN meetings or at the CENTR Jamboree.

More info about the TLD-OPS group.

Registry updates

APEWS

EURid presented its Abuse Prevention and Early Warning System (APEWS). This is a system that aims to predict whether a domain name will be used abusively or not at the time of registration. It calculates similarities between past malicious registrations and clusters the resulting values. Proximities of values to these clusters have a high predictive value for future fraudulent activity. The system is continually being finetuned, but it already has an 80% accuracy. Currently domains are not blocked from registration if they receive a high-risk score, but they are manually verified. As a result, abusive registrations have already started to drop.

More information can be found on the EURid website.

Moving 2.8 million names

Alyssa Moore (CIRA) presented CIRA's project to move to a new registration platform. The main reasons for this change were a need to improve operations, get closer to gTLD standards and generally make life easier for Registries and Registrars. The list of requirements (operational and policy) are available in the presentation. The migration took 2 years of planning and 8 hours of migration, during which 2.8

million names were transferred. Key lessons learned included: be ruthless with messaging, make room for innovation during migration and opt for more generic platform features.

Direct Registrations under .za

Peter Madavhu (ZADNA) provided an overview of the .za Domain Name Authority and its plans for second level direct registration. The presentation is available here.

The greatest .ee innovation

Maarja Kirtsi (The Estonian Internet Foundation) presented the new auction process for deleted names in .ee. Until recently, when a name was not renewed it was deleted, and after a random delay of up to 24 hours, it was released for registration. Now the 24 hours following the deletion will be used to auction the name to the highest bidder. This should solve the inequality between registrations that result from drop catching. This is a blind auction and bidders need to register before the auction starts. They can do so via eID or mobile verification mechanisms. The mechanism is considered to be very successful, with about 14% of the deleted names being registered through the auction process.

IANA Naming Function session

Public Technical Identifiers (PTI) Board update by Chair Lise Fuhr

Until now, PTI has been taking its priorities from ICANN's strategic plan. The PTI Board is now developing a PTI strategy and will clarify PTI's mission statement. The main advantage of such a plan is that it will take into account PTI's specific needs. One of the ways this plan will differ is that ICANN has a 5-year strategic plan, and the PTI will have a 4-year plan. Key areas that will be included are focusing on customer needs, keeping up operational excellence, maintaining trust and demonstrating value and usability, and meeting security requirements. This plan will be aligned with ICANN's strategic plan, but will also include additional objectives, such as SLAs and consumer experience.

A public consultation is planned for April – May 2020.

Presentation

IANA update by Kim Davies

The 2020 IANA budget request holds no major changes and is shortly to be approved by the PTI Board. The IANA budget is around USD 10 million which comes down to roughly USD 4000 per TLD in the rootzone. After the PTI Board's approval it will be rolled into ICANN's budget.

The 2018 KSK rollover was widely considered to have been successful. IANA is currently proposing a future method of doing these rollovers. The proposal is to change the key every 3 years. They are also looking into increasing the capability to use a pre-generated key for an emergency rollover.

There is a new and improved authorization mode. IANA identified a material change needing feedback: the consent mechanism for 'shared glue'. When two ccTLDs share the same nameserver, all impacted ccTLDs are currently being asked for formal consent. The plan is to relax this requirement and ask for normal consent only.

Presentation

Customer Standing Committee (CSC) update

Outgoing chair Byron Holland (CIRA) shared some ideas and suggestions on the future of the CSC. The success of the CSC is based on its very limited scope and it operates on a strict 100% quorum rule. The attendance rate of committee members is very high and they all contribute fully. Going forward, Byron's advice is that "if it ain't broke, don't fix it". The CSC needs to keep reaching out to all stakeholders and partners. The ccNSO has a serious responsibility for the well-functioning of the CSC as it nominates 50% of the voting members.

Incoming Chair Lars-Johan Liman (Netnod) provided a brief update. Two members had to step down which led to a limited decision-making capacity. Current members of the CSC are Gaurav Vedi (Dominion Registries) and Dmitry Burkov (RySG- gNSO) and Brett Carr (Nominet) and Alejandra Reynoso (.gt) from the ccNSO. Three of the SLAs will need changing:

- Technical checks;
- New SLA for publication of IDNs;
- ccTLD delegation/Transfer: validation and reviews (currently in public comment phase).

PTI performance is extremely good – some minor metrics are missing, but there is no customer service impact nor operational problems. The process is working very well. The major challenge to CSC's continued success is ensuring community engagement.

Presentation

Session with ccNSO Board Members

This whole session was based on a very simple question: "What has, in the Board's view, changed since Marrakech?"

Danko Jevtović noted that abuse has become a topic of high interest. This has been triggered by the consumer trust report and raised through the community. A fundamental question is still what is in ICANN's remit. The subsequent procedures are moving forward, and the competition and consumer trust team report highlighted it as an issue that needs to be solved, as is the lack of availability of registration data. The Consumer Trust Review team asked for empirical data to clarify the debate.

Danko also noted that since Marrakech, root servers governance has landed on the agenda. The main question here is what the process is if one of the root server operators wants to step out or if new operators want to join.

Chris Disspain underlined that ICANN needs to fix WHOIS. It is critical that the EPDP group finds a way to access WHOIS data in a way that is compliant with the GDPR. He questioned why we have WHOIS, and what it should do. He added that governments must to be explained that WHOIS needs to be legislated if they want to have access to it.

Becky Burr suggested that regulation will creep into the ccTLD space. People are starting to realise that half of the domains are in the ccTLD space. Registry managers need to improve the way they explain what they do. Furthermore, the number of issues has exploded and this is not sustainable for Board Members, leading to an urgent need to prioritise.

Policy Sessions

Work Track 5 – New gTLD Subsequent Procedures Policy Development Process Working Group.

The subsequent procedures policy development working group is preparing the future rounds of new gTLDs. They have split the work into 5 work tracks.

Work Track 5 (WT5) is a working group that was tasked to review existing policy and implementation related to the topic of geographic names at the top level, determining if changes were needed and recommending revised or new policy and implementation guidance as appropriate.

This WT5 group has now submitted a consensus document to the full subsequent procedures policy development working group. The conclusion of WT5's work, after three years and 52 meetings, is that:

- the gNSO policy recommendations will be updated to be consistent with the 2012 Applicant Guidebook, bringing the gNSO policy in line with current implementation;
- two-character ASCII codes will continue to be reserved as ccTLDs ;
- The ISO3166-1 standard of long and short form names will continue to be protected.

The country code Policy Development Process (ccPDP) retirement working group

The ccNSO attendants were asked to provide input on the following topics:

- Oversight policy for the retirement process;
- Review mechanism to be developed by 2nd WG under this PDP;
- Exceptionally-reserved codes reserved by the ISO3166 maintenance agency (4 in total). Trigger event: if the maintenance agency makes a change to a two-letter code, the IANA Function Operator must consider if this change requires RETIREMENT. If so, this triggers a regular retirement process;
- Trigger event for retirement IDN ccTLDs will be identified under the PDP for IDNs.

All proposals received full support from attendants, and the next step is to stress-test the proposed policy.

The Chair of the group also provided a very thorough onboarding presentation to the GAC.

IDN Policy Development Process (PDP4)

This PDP is needed to fill the gaps left by the IDN PDP. For instances, the ICANN bylaws need some changes as they do not refer to ccTLD IDN managers and their role in ICANN processes. There are a few open questions that need to be addressed. E.g. How should IDN ccTLDs be represented in the ccNSO? One of the key elements to that answer is to change the ccNSO membership definition to: "A ccTLD manager is the organisation or entity responsible for managing an ISO 3166 country-code top-level domain or a later variant and referred to in the IANA Root Zone Database under the current heading of ccTLD Manager."

All presentations from this session will be published here.

Internet Governance Session

Internet Governance Liaison Committee

Pierre Bonis (Afnic) gave an overview of the goals and activities of the Committee. This Committee was established to coordinate, facilitate and increase the participation of ccTLDs in Internet Governance (IG) processes. The group launched a survey asking for ccTLD activity in IG, which confirmed the IG initiatives.

- They are often involved in the organisation or funding of IG initiatives;
- They focus on cybersecurity, capacity-building and regulation.

Legislative and Regulatory Tracking Initiative

Mandy Carver, VP for Government Engagement, presented a new ICANN initiative which will provide an overview of legislative and regulatory activity which could have a direct impact on ICANN's mission and remit. The goal of this overview is to identify the opportunities and needs for providing neutral technical information to inform the regulatory process. ICANN is asking ccTLDs to contribute to this initiative by sharing local knowledge. CENTR underlined the need to synchronise any outreach activity towards regulators. Currently, an overview is being published on a quarterly basis with abstracts from that regulatory overview. There is currently no mechanism to feed information into that database.

DENIC presented an overview of its Internet Governance related activities, divided in 3 categories "attending & presenting", "sponsoring & steering" and "creating & enabling". Each of these supports DENIC's vision of an "open, free and secure internet".

The Coordination Center for TLD .RU gave a presentation on 10 years of Russian IGF. They had a particularly difficult start as multistakeholderism was not a household concept. However, the initiative grew to become very successful, and has some unique features such as a focus on youth.

Presentations will be made available here.

GAC Report

DNS Abuse

Background

The topic of DNS abuse was one of the primary focusses on the ICANN66 agenda. Cross-Community discussions on the issue had been requested by the Public-Safety Working Group on at least one occasion during the previous ICANN65 meeting in Marrakech. In between the two meetings, on 19 August, the Registries Stakeholder Group (RySG) sent out an Open Letter to the Community on this topic. On 18 September the GAC issued its Statement on DNS Abuse where it was reiterated that "protecting the public from security threats and DNS Abuse is an important public policy issue." The GAC also restated its previous continuous attention to the topic that was reflected in the issuing advice, providing guidance and comments, organising cross-community discussions, and advocating for "stronger contractual provisions to safeguard the public". Pre-ICANN66, the GAC has called for "best practices" that can be found in the ccTLD world and that are directed towards "pro-active anti-abuse measures to address DNS-facilitated crime" to be implemented by gTLD registries and registrars. Namely, stronger authentication methods, including identity checks (.dk) and/or the use of data-based fraud prediction models which combine data registration and infrastructure metrics to identify and predict domain registrations made for harmful purposes (.eu).

The definition of what constitutes DNS abuse is subject to discussions across the ICANN community. The Competition, Consumer Trust and Consumer Choice (CCT) Review team has previously noted that "consensus exists on what constitutes DNS Security Abuse, or DNS Security Abuse of DNS infrastructure": these forms of abuse include more technical forms of malicious activity, such as malware, phishing, and botnets, as well as spam when used as a delivery method for these forms of abuse. The CCT Review Team also referred to DNS Abuse in its Final Report (8 September 2018) as "intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names." The CCT Review Team has also issued its recommendations for ICANN to take in order to increase safety within its contracted parties' zone. Some of these recommendations include incentivising the adoption of proactive anti-abuse measures; inserting contractual provisions aimed at preventing the systemic use of specific registries and registrars; adopting thresholds of abuse by which compliance inquiries are automatically triggered; and requiring the publication of entire chain of ownership. The ICANN Board has not accepted most of the CCT Review Team's recommendations.

Joint meeting between the GAC and RySG

In Montréal, DNS abuse was discussed during the joint meeting between the GAC and the RySG. During this session it was noted that there are number of different interpretations across the ICANN community on what constitutes DNS abuse. However, there are several initiatives and practices that are already being done by registries to tackle DNS abuse within their zones that need to be taken into account when the definition of DNS abuse is being discussed.

Brian Cimbolic (PIR) specified that the Advisory, New gTLD Registry Agreement Specification 11(3)(b) lays down the foundation for registries to conduct periodic technical analysis of its registrations for security threats. Spec 11(3)(b) does not specify what it means by "periodic", and ICANN Org has clarified that this type of technical analysis should be done at least once a month. However, according to Brian, most registries are doing much more than that. PIR (.org) for example conducts daily checks for security threats. The joint Framework for Registry Operator to Respond to Security Threats developed together with the PSWG specifies that referrals of abuse should be responded to within 24 hours and that referrals from law enforcement authorities should be given priority.

Furthermore, there are limited tools available for registries when addressing DNS abuse. At registry level, the only appropriate measure available to respond to DNS abuse is the suspension of domain names because it allows for the decision to be reverted in case the suspension is made by mistake. Deletion, for example, means that a domain name can be re-registered again. According to Brian, because registries cannot look

into content and furthermore can influence only one part of the website, any discussion on DNS abuse and registries' role needs to be appropriately framed. The suspension of domains names can have collateral damage.

Finally, PIR publishes quarterly reports on the number of suspended domains as per their anti-abuse policy.

Presentation from the PSWG

Gabriel Andrews (FBI) presented the perspective of law enforcement and highlighted the challenges that law enforcement is facing in conducting their investigations because of the impact of the GDPR on the availability of WHOIS data. According to Gabriel, WHOIS is a tool that is used by law enforcement and cybersecurity researchers on a daily basis and it is a key tool in addressing DNS abuse, while the latter remains a #1 public safety priority. The global cost of cybercrime is growing exponentially and there has been a notable increase in the circulation of child sexual abuse material (CSAM) content. Additionally, "business email compromise" (BEC) is a global epidemic with a significant financial cost.

Gabriel also highlighted the numerous existing practices across registries and registrars that are directed towards tackling DNS abuse. He stressed more preventative measures that are addressed at making sure that DNS abuse does not occur, highlighting the registrant identity checks done in the .dk zone and EURid's Abuse Prevention system that is aimed at "pre-emptive blocking of registrations based on patterns recognition". He welcomed the practices used within the ccTLD space.

Gregory Mounier (Europol) picked up the baton from Gabriel Andrews to highlight the fact that the existing practices within ccTLD space could and should be more widely accepted, including for gTLDs. The fact that some ccTLDs have adopted these measures within their zones shows that it is possible and not necessarily expensive, according to Gregory. He also supported the idea of registries providing financial incentives for registrars to take proactive measures to address DNS abuse. Additionally, the "trusted notifier" programme can allow registries to take measures without entering into complicated legal discussions, according to Gregory.

Laureen Kapin (US Federal Trade Commission) highlighted the numerous existing DNS abuse definitions across the ICANN community and beyond. For example, she also referred to the definitions provided by the Internet & Jurisdiction Policy Network that make a distinction between technical abuse and website content abuse. According to I&J work (that remains voluntary) "action on DNS level may be justified against both types of abuse with higher threshold for content abuse".

Laureen also expressed her regret that the ICANN Board has not accepted most of the CCT Review Team's recommendations to address DNS abuse. She pointed out the need to introduce a so-called "3-strike rule" that can be used to address the systemic abuse of specific registries and registrars as an "effective response if an actor continually engages in bad behaviour" and does not abide by its contract terms. In addition, the full chain of domain name ownership should be collected by the registries and registrars, including information on any possible resellers in between. According to Laureen, there is an informational gap that needs to be closed in the official records with regards to the ownership of a domain name, as the law enforcement authorities simply "do not know where to go".

Chris Lewis Evans (UK National Crime Agency) reiterated previous GAC advice on the issue (e.g. Beijing Communiqué) that stressed the need to implement the CCT Review Team's recommendations. He also stressed the need to learn from the ccTLD community and promote the good practices within that can provide pointers towards "upping up" the baseline on how to tackle DNS abuse across ccTLDs and gTLDs.

During the Q&A round with the GAC members, Switzerland raised the question of ICANN's role in addressing other abuse instances, like fraud, and the types of action that can be taken by ICANN in order to promote measures that can make it difficult for bad actors to abuse the DNS.

Gabriel Andrews (FBI) provided the response by stressing the need to verify the identity of registrants in order to prevent DNS abuse before it can even occur. By "taking away the anonymity", one takes away the comfort from bad actors out there to carry on, according to Gabriel.

Joint meeting between the GAC and the ICANN Board

The GAC asked the Board to elaborate on the operational steps it intends to take to:

1. Promote "a coordinated approach to effectively identify and mitigate DNS security threats and combat DNS abuse"? And

2. Maintain itself a "source of unbiased, reliable, and factual information on DNS health", in particular with regard to:

   a. increased transparency about actors responsible for systemic abuse (DAAR and ICANN Compliance complaints)

   b. Convene discussions on new contractual provisions in ICANN's contracts, consistent with the CCT Review Team's recommendations.

Becky Burr (ICANN Board) highlighted the results of a recent audit by the Compliance Group that assessed registries' compliance with their obligations to do scans for DNS security threats. She also highlighted the fact that ICANN is still looking for effective tools and that the Board consdiers the topic of DNS abuse to be a top priority. When it comes to the CCT Review Team recommendations, Becky stressed that many of these are policy recommendations that need to be addressed in policy development processes, such as the one conducted by the GNSO and in their work in the new gTLD subsequent procedures policy development process. However, the Board reserves its right and obligation to ask and make sure, once the GNSO work is completed, that the CCT Review Team's recommendations are fully considered by the subsequent procedures policy development process. Additionally, the ICANN Board cannot oblige the policy development process to adopt recommendations that come from different parts of community. However, it is part of Board's obligation to evaluate whether the "global public interest is being served".

Göran Marby (ICANN CEO) welcomed the work that has been done in connection to DAAR. He also expressed his happiness over some of the conversations that the ICANN Org has been having with some of the ccTLDs that "want us[read: ICANN] to be part of the same system".

Belgium stressed the importance of the topic of DNS abuse to governments. According to Belgium, there is an urgent need to come to a certain position with regards to the CCT Review Team's recommendations and proceed to implement them in order to adequately react to the growing threat posed by DNS abuse.

Further comments from the community on DNS abuse

- During the Cross-Community session on DNS abuse, Graeme Bunton (Tucows) highlighted the contractual obligations available for registrars when addressing DNS abuse. These include a requirement for registrars to maintain abuse contact and take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse; an obligation to maintain dedicated law enforcement abuse contact 24/7 and review these complaints within 24 hours; and an obligation to publish an abuse handling process on their website. According to Graeme, many registrars do not have enough means to prevent abusive registrations. However, Tucows is "taking down 100 domains a day" but is not advertising this practice.

- Brian Cimbolic (PIR) highlighted the Quality Performance Index, a programme that is used within PIR, that looks into registrar abuse metrics and domain name usage. As a result, it creates economic incentives for registrars to perform better in terms of abuse. He highlighted the fact that SIDN (.nl) has a similar programme. Additionally, PIR is currently finalising an appeal mechanism for registrants to be able to object to the suspension of domain names unde nr anti-abuse policy with a third-party review process. Brian also provided concrete numbers when suspending domains names in PIR as a result of addressing DNS abuse: In Q3 of 2019 28 675 domain names were suspended, of which only 8 were related to content.

- Farzaneh Badiei (Non-Commercial Users Constituency) stressed the need to define DNS abuse in a limited technical manner. ICANN should not get involved in non-technical programmes that engage in tackling abuse that goes beyond technical abuse that has been already defined within the ICANN community. According to Farzaneh, the problem is not in the definition of abuse but in the fact that there is "a patchwork of solutions and inconsistent governance mechanisms". She also stressed the need to be careful with financially incentivising the suspension of domain names that can result in overzealous content removal.

- Mason Cole (Donuts) reiterated the statement which was recently published by the Business Constituency that defines abuse as an "action that causes actual and substantial harm or is a predicate of such harm and is illegal or illegitimate or considered contrary to the stated legitimate purpose". He also stressed the definition that in his opinion has captured the technical definition of abuse and consists of "distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices and counterfeiting".

- Elliot Noss (Tucows) pointed out the fact that the ICANN community has discussed this topic for 20 years. He stressed the fact that the issue needs to be solved at the level of contractual compliance.

- Dirk Krischenowski (.berlin) highlighted the results of a survey on DNS abuse conducted within 22 geographic names in the past 12 months. The survey results show that there is very little abuse in the geoTLD space. Only three respondents indicated that there had been more than 10 cases within the last year. Dirk concluded that in his view there is no need for further contractual obligations.

- Byron Holland (.ca) took the floor stressing the need for a clear definition that draws a clear line between technical and content abuse matters. The ICANN Bylaws are very clear, together with a well-defined remit. TLD operators need to be very cautious when deciding where to act and where to create policies. Byron also stressed the fact that judicial oversight is a precondition of the rule of law. The rule of law should not be abolished just because there is a pressure to act quickly.

- Pierre Bonis (.fr) noted that there is an increasing pressure from stakeholders outside of ICANN, pushing for the technical community to act upon abuse. According to Pierre, it is important not to impose responsibilities which come from hosting providers to the technical layer, who should not perform the tasks of judges or police on the internet.

GAC Communiqué: The GAC advises the Board not to proceed with a new round of gTLDs until after the complete implementation of the recommendations in the Competition, Consumer Trust and Consumer Choice Review that were identified as "prerequisites" or as "high priority".

Relevance to ccTLDs

ccTLDs and their practices in tackling abuse (that are primarily voluntary!) are continuously being considered the champions in keeping their zones secure and free from abuse within the ICANN community. More and more voices are calling for the adoption of similar measures in the gTLD space, by re-opening contracts and making these measures part of contractual obligations (read: mandatory). The discussions over the definition of DNS abuse are also increasingly moving towards "content" moderation, blurring the line between "technical" abuse and "content" abuse. While registries cannot adequately assess or control content abuse, it is evident that in the case of a broader DNS abuse definition, the role and impact of the so-called "trusted" notifiers would become increasingly prominent when addressing content abuse at DNS level, including in the ccTLD space.

WHOIS and Data Protection

Background

On 20 May 2019, the Temporary Specification on gTLD Registration Data (hereinafter Temp Spec), which was intended as a temporary policy in response to the EU General Data Protection Regulation (GDPR) was replaced by the Interim Registration Data Policy for gTLDs (hereinafter the Interim Policy), a consensus policy that implements (some) GNSO policy recommendations concerning data protection requirements for gTLDs. The Interim Policy requires gTLD registry operators and ICANN-accredited registrars to continue implementing measures that are consistent with the Temp Spec on an interim basis. The Interim Policy will be replaced by the Registration Data Policy effectively from 29 February 2020. It was already suggested at the last ICANN65 meeting in Marrakech that there would be delays in delivering the final Registration Data Policy by the end of February 2020, and at ICANN66 in Montréal, participants received confirmation that it would be delayed by a further six months.

In previous advice, the GAC noted on several occasions that the Temp Spec was failing to meet the needs of law enforcement, cybersecurity researchers and IP rightsholders. The needs of ensuring third-party access

to WHOIS data was not dealt with in the Final Report of the GNSO Council on the EPDP (in the so-called Phase 1). The adoption of the Final Report immediately set in motion the work of the EPDP Team on Phase 2 which aims to develop a system for standardised (and most likely distributed) access to non-public registration data.

Phase 2

In Montréal, it was highlighted that EPDP Phase 2 continues to work on the building blocks of a standardised access model (SSAD) including defining groups of users, defining a central or decentralised model, and assigning liability. There is also an issue of accrediting privacy and proxy services regarding which the respective policy has already been developed but the implementation has currently been stalled. Issues deferred from Phase 1, such as the distinction between legal and natural persons, and the redaction of the city field is not considered to be a top priority and will be dealt with in parallel only if and where possible.

In parallel with the community work on Phase 2, the ICANN Org has established a so-called "Strawberry Team" that is working on exploring whether ICANN can take on liability and provide a "central gateway" to provide access to the WHOIS to interested user groups. One of the tasks of the "Strawberry Team" is to seek guidance from the European Data Protection Board on whether ICANN's assumptions on such a legal regime are consistent with the GDPR, and in particular whether providing such "central gateway" will actually shift liability away from the contracted parties. During the Montréal meeting, it was also highlighted that the efforts to seek advice from the EDPB are also meant to feed into the policy discussions in the EPDP. The outline of such a central gateway model that was sent to the EDPB by the "Strawberry Team" assumes that ICANN can take on responsibility and both hold the registration data in a centralised way and accredit the data access requests through the "central gateway".

This "central gateway" is necessary to address the "unintended consequences" of the GDPR, such as the absence of a "one-stop" for public authorities to get access to WHOIS information. Each contracted party (from 2000+) has its own interpretation of what constitutes a legitimate interest for requesting non-public WHOIS data and this is said to create further hurdles for law enforcement.

Work on the SSAD consists of two primary phases. First there is a need to agree on policy issues that are addressed in the EPDP. Second, there is a need to see how this type of model can be implemented, e.g. the question of verification and accreditation of public authorities (and be legally permissible under the GDPR).

The concrete building blocks of Phase 2 that will be used to form the draft policy recommendations by the EPDP Team include the accreditation of requestors, content of requests, response requirements, query policy, acceptable use policy, automation, logging, financial considerations.

The draft policy recommendations in the EPDP Initial Report are expected to be published in December 2019.

In Marrakech, members of the GAC volunteered to provide indicative lists of public authorities and other relevant parties requiring non-public registration data. The European Commission outlined in Montréal that it is coordinating with the EU Member States to identify law enforcement authorities that need access to non-public registration data.

In addition to public authorities, the GAC has previously expressed the need to ensure access to the WHOIS to non-accredited parties as well, such as cybersecurity researchers and IP rightsholders.

During the Q&A session with the RySG, Indonesia asked how the work in Phase 2 would accommodate the differences between countries and their own legal systems for data disclosure.

Alan Woods (Donuts, EPDP Team) responded that there is a need to develop a system that is agnostic to specific legal systems, and that certain basic principles of data protection that derive from international treaties should provide guidance on how to protect data subjects' rights in the most common way.

France brought up the issue of differentiation between legal and natural persons that needs to be ensured in the publicly-available registration data. The EPDP Team highlighted that there is a study on the issue, on the way to provide clarity, stressing the need to keep in mind that appropriate safeguards for the protection of individuals' privacy need to be in place.

During the Plenary session on EPDP Phase 2, several community members raised the question of 'who' would manage the "central gateway" and/or revise

all the incoming data disclosure requests. The answer from the EPDP Team was that it is "not yet determined". The policy discussions have not yet concluded whether one centralised entity should handle all disclosure requests or whether the decision should be made at the level of each registry/registrar.

Pearse O'Donohue (European Commission) stated that there would be no shift of liability from the contracted parties in the model of a "central gateway". ICANN will only receive additional liability and there are concerns over this in the European Commission. He reiterated that the GDPR had not been intended to have an extraterritorial effect, but it is clearly related to the personal data of EU citizens or to all personal data when it is processed within the EU. EPDP work is not about designing a new data protection law but to make sure that ICANN-contracted parties conform to privacy protection.

GAC Communiqué: With regards to Phase 1 of the EPDP, the GAC advises the Board to take all possible steps to ensure that ICANN org and the EPDP Phase 1 Implementation Review team generate a detailed work plan identifying an updated realistic schedule to complete its work and provide and inform the GAC on the status of its progress by 3 January 2020. With regards to Phase 2 and the conclusion of the EPDP, the GAC advises the Board to:

1. instruct the ICANN org to ensure that the current system that requires "reasonable access" to non-public domain name registration is operating effectively. This should include:
    - educating key stakeholder groups, including governments, that there is a process to request non-public data;
    - actively making a standard request form available, that can be used by stakeholders to request access based on the current consensus policy; and
    - actively making links to registrar and registry information available as well as points of contact on this topic.
2. instruct ICANN Compliance to create a specific process to address complaints regarding failure to respond to, and the unreasonable denial of requests for non-public domain name registration data, and monitor and publish reports on compliance with the current policy as part of their regular monthly reporting.

As a follow-up to the previous GAC advice, the GAC emphasises again that the Privacy Proxy Services Accreditation Issues (PPSAI) policy recommendations remain highly relevant and that implementation efforts should continue as appropriate, in parallel with the ongoing policy development work in the EPDP. The implementation of the PPSAI should not be deferred until the completion of the EPDP.

Relevance to ccTLDs

For decades, ccTLDs have successfully argued that their policies should only adhere to local laws. ICANN's ambitious parallel plans to build 1) a standardised access model that complies with as many regulatory frameworks as possible and 2) a centralised access system for the identification of law enforcement authorities and a wide range of other user groups might increase pressure on ccTLDs to revise their own governance models. Additionally, if the gTLD space were to be centrally managed and "unified/standardised" by ICANN under their interpretation of a regional law like the GDPR, it might also result in conflicting interpretations of the GDPR in the ccTLD space.

Dot Amazon

Background

In 2012 the US-based tech giant Amazon Inc. filed an application for the use of .amazon. Some of the GAC members, belonging to the Amazonian region (the Amazon Cooperation Treaty Organization - ACTO), objected to the .amazon application.

In the Abu Dhabi Communiqué, the GAC advice to the ICANN Board was to "continue facilitating negotiations between the Amazon Cooperation Treaty Organization's (ACTO) member states and the Amazon corporation with a view to reaching a mutually acceptable solution to allow for the use of .amazon as a top level domain name".

On 10 March 2019 the ICANN Board adopted a resolution regarding the .amazon applications in which it provided the ACTO countries and Amazon Inc. with the opportunity "to engage in a last effort" that allowed both parties to work towards a mutually-acceptable solution regarding the .amazon applications. The facilitation of the negotiations by the ICANN Board came to an end.

On 15 May 2019, the ICANN Board accepted the .amazon applications according to the policies and procedures of the New gTLD Program. The ICANN Board determined that there is no public policy reason why the .amazon applications should not be allowed to proceed and found that the submission made by Amazon Inc. was not inconsistent with the previous GAC advice on the matter.

In Marrakech, the GAC asked the ICANN Board to explain in writing whether and why it considered that its decision to proceed with the .amazon applications complied with GAC Advice.

Discussions in Montréal

Brazil continues to strongly oppose the Board's decision to support the .amazon application in favour of Amazon corporation. According to the statement made by the Brazilian ambassador, .amazon is a regional TLD that is "similar to a country TLD." According to Brazil, the difficult political context in the region has caused additional hurdles for ACTO countries to find consensus. Brazil also stressed the cultural importance of the Amazonian region for the identity of its people. Brazil requested that the ICANN Board assign an independent mediator in order to proceed with the aim to find a mutually acceptable solution for all parties. Brazil also expressed the view that it is not too late to reach that mutually-acceptable solution.

The US and Israel did not support any further advice on the matter and expressed their objection towards any further delay of proceeding with the .amazon applications.

China highlighted the high public interest for ACTO countries in this issue, where commercial interests are contradicting with public policy. China encouraged the ICANN Board to deal with this sensitive matter in a careful manner and to take on additional effort to find mutually acceptable solution.

The European Commission urged the ICANN Board to use caution when delegating significant geographic names due to cultural sensitivities. The European Commission stressed the need for an externally mediated and timebound final negotiation round between parties in order to attempt to find a mutually acceptable solution. Switzerland supported the statement made by the European Commission and reiterated the GAC advice in Abu Dhabi that sought a mutually acceptable solution between the concerned parties. Switzerland found that the best way forward is to exhaust all means available in the context of existing available procedures.

Portugal expressed concern over the "terrible precedent" that the .amazon case has established for confidence in ICANN proceedings. They stressed that geographic names with cultural and historic significance cannot be considered as "usual market assets".

Belgium reminded the GAC that .amazon was initially considered "a problematic geographic name", similarly to .spa. Several of these problematic applications of geographic names were resolved with an appropriate solution, and this should also have happened with .amazon.

GAC Communiqué: No further GAC advice on this issue was delivered in Montréal.

Relevance to ccTLDs

The DotAmazon case continues to be a contentious issue between ICANN and its governmental advisory committee, with no foreseeable end in sight. The Brazilian ambassador compared a geographic TLD to a ccTLD and referred to its significance in terms of identity of its people, history and culture. Yet, what constitutes a country, its country code, a region and its name - is and should be decided upon outside of ICANN and its discussions on Internet Governance. By approving the .amazon applications in favour of the tech giant, the ICANN Org seems to have made a decision on what does and does not constitute a geographic region on the internet, entering the domain of public policy debates reserved for governments. Considering the current on-going increased regulatory attention towards the internet, including its technical layer, the on-going debates on disregarding the governments' public interest in the case of .amazon does not contribute to strengthening the multistakeholder model of Internet Governance, where all parties should be on equal footing. Some governments strongly feel that business interests have prevailed in these discussions.

ICANN67 will be held on 7–12 March 2020 in Cancun, Mexico.

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 54 full and 8 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 ICANN66

(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