Council of European National
Top-Level Domain Registries

Report on ICANN68

Virtual Policy Forum

22-25 June 2020

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

Contents

Executive summary

For this virtual ICANN meeting, the ccNSO spread its meetings beyond the confines of the ICANN schedule. The ccTLD news sessions were held at the beginning of June (the recordings can be found here and here). Additionally, the ccNSO organised an informative session for the GAC related to the DNS in COVID-19 times. The recordings of that session can be downloaded here. The summaries in this report cover the sessions of the virtual ccNSO members meetings held on 23 and 24 June.

Some of the main topics on the GAC agenda which are notable for ccTLDs included the increased attention towards DNS abuse and the need to address this high-priority topic within the ongoing policy development processes, such as the New gTLD Subsequent Procedures PDP and the Expedited Policy Development Process on access to WHOIS.

The GAC ICANN68 Communiqué is available here.

ccNSO Report

ccTLD governance models

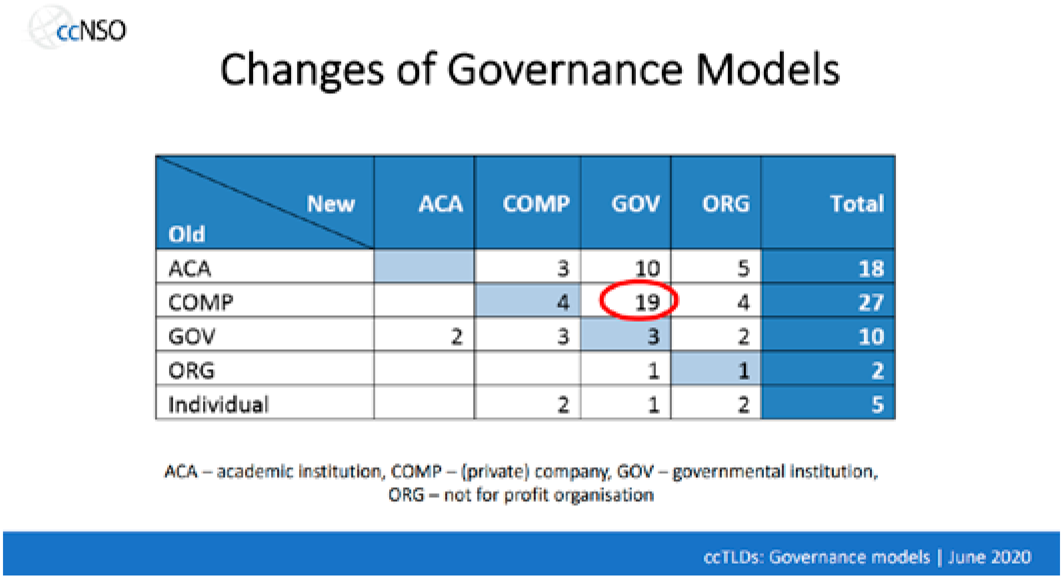
In this session, four ccTLDs presented their governance models (.be: not-for profit; .jp: for profit; .mx: academic; .bw: governmental department) and discussed the impact of having a specific model on issues such as budget control, their capacity to innovate or political influencing.

To kick off this session, Katrina Sataki presented a few interesting datasets. Since 2003, 63 ccTLDs have been transferred. These transfers were geographically distributed as follows: Africa = 21 (33%), Asia-Pacific = 22 (35%), Europe 14 (22%) and Latin America and Caribbean = 6 (10%).

There is a clear trend in the effect of these transfers on governance models. Just over half (34/63) were transferred to a manager that qualifies as a governmental institution while 14 were transferred to a not-for profit organisation.

Over half of the managers that were part of an academic institution and 19 out of 27 managers that were a private company were transferred to a governmental department.

In the Q&A that followed, none of the presenters signalled undue pressure from their governments regarding domain take downs. When asked about financial independence, all signalled complete financial independence, with the exception of the governmental



ccNSO

Changes of Governance Models

New Old	ACA	COMP	GOV	ORG	Total
ACA		3	10	5	18
COMP		4	19	4	27
GOV	2	3	3	2	10
ORG			1	1	2
Individual		2	1	2	5

ACA – academic institution, COMP – (private) company, GOV – governmental institution, ORG – not for profit organisation

ccTLDs: Governance models | June 2020

model, as the minister needs to give final budget approval. The academic model seemed the best suited to deal with new technologies and innovation. .be signalled statutory restrictions, .jp indicated that they would require extra support from their shareholders (the largest Japanese tech companies) and .bw signalled the need for a parliamentary resolution. Most managers confirmed that they could accept donations but that this had not occurred yet. If the opportunity arose they would carefully assess how this would affect their independence. Only the governmental department (.bw) could not accept donations without governmental approval. Finally, on the topic of governmental changes and their effect on the ccTLD manager, unsurprisingly the governmental department indicated that the impact would be significant, but others flagged that the shift in policy priorities between governments could have marginal effects on their operations.

The DNS in times of COVID-19: the ccTLD experience

The first part of this session saw a presentation of the TLD-OPS business continuity and disaster recovery playbook. This playbook contains a disaster recovery and business continuity tabletop exercise which was tested for the first time in the Montreal meeting. The playbook will be updated with the lessons learned during the COVID-19 pandemic.

The manager for .cl (Chile) illustrated how they managed to run their ccTLD throughout a multi-layered crisis. This period started with significant disruption and chaos on October 2019 (public transport hubs were destroyed, riots and even adjacent office buildings were burnt down) and, though working conditions were severely impacted, the domain name resolution services were not at risk at any point in time. The experience gained during this time of political instability proved to be very useful when adapting to the COVID-19 situation. Registry and registrar services were distributed across several data centres, most staff worked from home and the registry issued daily announcements. The internal and external communications were key to managing the crisis.

Pierre Bonis (AFNIC), in his capacity as Chair of the Internet Governance Liaison Committee (IGLC), provided an overview of a recent survey on capacity building. 85% of the responding ccTLD managers indicated that they were involved in local or regional capacity building. Key initiatives mentioned were cybersecurity training, online presence (website building) training and initiatives related to fighting online abuse. One of the key take-aways was that in times of fear, ccTLDs are generally seen as a neutral and professional source of expertise.

In the second part of this session, ICANN and the Regional Organisations provided their perspectives on the impact of COVID-19 and what the expected effect of the pandemic would be on upcoming policy discussions. ICANN presented the results of their analysis of the COVID-themed domains that were registered between 1 January and 1 June. In this period 662 111 domains were identified as being related to COVID-19. The stepped approach to zoom in on the domains that were actually being used for malicious purposes showed that of the 600K names, only a few hundred were reported for further investigation and only a few dozen presented sufficient evidence to trigger a take down.

The discussion with regional organisations showed that the expected impact of the COVID-19 pandemic on public policy discussions ranged from ‘no expected impact’ in the African region to ‘high impact’ in the European region. The most notable impact on ccTLD registration policies was the finetuning of data accuracy policies and related response times. Another common theme seems to be that lists of new registrations or even entire zone files are shared with authorities. In Europe the pandemic created the perfect stress test for collaboration between ccTLDs and consumer protection authorities, showing what works and what does not, and what a ccTLD can do and cannot do.

ccTLDs across the world often struggled to educate their communities and to explain how ccTLDs could help in these extraordinary times while at the same time staying out of content moderation or content-based decision making.

The most important lesson learned was that close local cooperation with law enforcement, health or consumer protection authorities is the most efficient way to help local internet communities tackle these issues.

ICANN policy work during COVID times

ICANN has been doing an excellent job in turning physical meetings into online meetings. Most supporting organisations and advisory committees have adapted well, some even signalled an increased efficiency. Another important effect is that there has been more cross-community interest in sessions that would typically have only appealed to a specific community. Two challenges remain, and they will be hard to overcome: firstly it is not possible to bring together a global community across all time zones in a way that allows equal participation and secondly, these online meetings work for those who already have an established network within the ICANN community. For newcomers, this bends the already steep learning curve even further up, and makes real engagement in ICANN's policy work close to impossible. The way forward will be based on community input. ICANN has published a draft exit strategy that suggests four stages. One of these stages suggests that regional meetings should be held in order to advance the policy work. In some of the discussions in the margin of this plan it was noted that regional (ccNSO) meetings would not be useful and could unbalance the essential equality between ccNSO members.

Strategic and Operational planning committee

The ccNSO SOPC is a group that provides input on behalf of ccTLD managers on the ICANN strategic and operational plans. It submits comments on behalf of the ccNSO and organises regular Q&A sessions with ICANN's financial team.

The current FY20-21 plan was adapted by ICANN to take into account the impact of the COVID pandemic and, contrary to the regular process, it did so without community consultation. Even though these changes did not affect the planned support for ccNSO policy development, the ccNSO has formally questioned this decision. Additionally not all of the comments from this group to ICANN on the Operating Plan FY20-21 were reflected in the updated plan.

Despite much more positive outlooks signalled in all industry reports, ICANN still expects a negative impact on its FY21 revenue but plans to regularly provide updated projections. The ICANN CFO underlined that they are not planning to be right on the mark, but will make very conservative financial plans. The FY21 revenue is therefore projected to be 6% lower compared to FY20 forecasts. The economic impact is projected to affect ICANN org funding beginning in FY20-Q4. Personnel costs are projected to increase by 5% due to inflationary increases and a modest increase in headcount. On a total headcount of 400 this will bring the average cost per ICANN staff member to 190 000 USD. Any FY20 and FY21 surplus would be used to replenish the reserve fund.

GAC Report

DNS Abuse

Background and latest developments

The discussions on DNS abuse are becoming increasingly prominent across the ICANN community and especially regarding a concrete definition that could still fall within ICANN's remit.

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 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", which essentially calls for a broader definition of DNS abuse than the currently existing consensus. The CCT Review Team has also issued its recommendations for ICANN to follow in order to increase safety within its contracted parties' zone (i.e. gTLD registries and registrars). Some of these recommendations include financially 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 at which compliance inquiries are automatically triggered; and requiring the publication of the entire chain of ownership. The ICANN Board has not accepted most of the CCT Review Team's recommendations.

In the GAC Montreal Communiqué, the GAC advised the ICANN Board not to proceed with a new round of gTLDs until after the complete implementation of the recommendations of the CCT Review Team that were identified as "prerequisites" or a "high priority", for example including the financial incentives in the Registry Agreements to adopt proactive anti-abuse measures. The GNSO New gTLD Subsequent Procedures PDP WG (hereinafter SubPro PDP WG) reported on 27 April 2020 that it is not planning to make any recommendations with respect to mitigating domain name abuse other than stating that any such effort must apply to both existing and new gTLDs (and potentially ccTLDs).

In its contribution to the SubPro PDP WG, per the GAC ICANN67 Communiqué, GAC members expressed concern with this approach, highlighting the importance of the CCT Review Team's recommendations and the need to implement them.

The GAC leadership suggested consulting experts and expects the GNSO Council to propose a "framing document" laying out procedural options for future work.

The Stability, Security, Resilience (SSR2) Review Team delivered a Draft Report (24 January 2020) with a focus on measures to prevent and mitigate DNS abuse. The GAC endorsed many of the recommendations and in particular those pertaining to improving Domain Abuse Activity Reporting (DAAR) and strengthening the compliance mechanism. The final recommendations of the SSR2 Review Team are expected in October 2020.

In addition, the Security and Stability Advisory Committee (SSAC) Work Party on DNS Abuse was established. The group is expected to discuss the reliable data sources of malicious activities and review effective practices currently in place within the industry, including "innovative practices" amongst ccTLDs. The SSAC Work Party will also consider and make relevant recommendations for ICANN for these innovative and effective practices to be more widespread amongst ICANN community. The SSAC will not provide a formal definition of abuse but will provide a framework for different parties to utilise in abuse handling and prioritisation. The Work Party is currently progressing on an escalation framework to mitigate abuse victimisation. This is aimed at actions taken on domain names for their swift takedown in order to reduce the number of people being victimised by the continuation of abuse on these domain names.

Meanwhile, contracted parties, such as the Registry Stakeholder Group (RySG) and Registrar Stakeholder Group (RrSG) adopted a definition of DNS abuse on 17 June 2020, as "composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam when it serves as a delivery mechanism for the others".

GAC Discussions on the CCT Review Team recommendations

In its compilation of Individual Input on the SubPro PDP WG recommendations from May 2020, GAC members mostly converged on noting that DNS abuse mitigation should be included in the Subpro PDP WG recommendations. A few GAC members mentioned that the approach to address DNS abuse should be holistic. As reinstated by the GNSO Council on 21 May 2020, no policy recommendations are expected with respect to mitigating DNS abuse as a result of the SubPro PDP, and any future effort should be holistic and must apply to both existing and new gTLDs (and potentially ccTLDs).

Switzerland raised the point about the issue of DNS abuse needing a faster resolution through contractual rules.

Jeff Neuman (Co-Chair of the SubPro PDP WG) expanded on the GNSO council conclusion, saying that it would be more appropriate to deal with the question of DNS abuse in a separate track from the SubPro PDP, as it requires a more "holistic approach". The SubPro PDP has no jurisdiction over any of the current and legacy operators, while new registries are unlikely to enter contracts before 2023 after being selected in the next round of new gTLDs. Additionally, the higher rates of DNS abuse mostly affect legacy TLDs from 2004. Implementing anti-abuse obligations in new contracts will not solve this issue as legacy TLDs will not be affected by these new measures.

The GAC still considered the topic of DNS abuse in SubPro PDP discussions to be a priority and noted that the GAC is waiting for the GNSO Council to come up with concrete proposals on how to deal with the topic in a holistic fashion.

During the joint meeting between the GAC and the ICANN Board, Pakistan raised a question about ICANN Org's vision in cooperating with governments that are particularly affected by DNS abuse and the malicious traffic it generates. Maarten Botterman (Chair of the ICANN Board) stressed the need to define the focus of DNS abuse discussions and that ICANN will continue enforcing measures in the contracts. Göran Marby (ICANN CEO) stressed the usefulness of DAAR in this regard and the fact that a number of ccTLDs are also participating in it and receiving access to the reporting.

The Public Safety Working Group

The Public Safety Working Group (PSWG) gave an overview to the GAC about recent DNS abuse-related developments within the ICANN community, especially in connection to the COVID-19 pandemic.

The PSWG acknowledged the numerous presentations and webinars held in connection to COVID-19 and its impact on the DNS, as presented by ccTLD managers and contracted parties. The reported impact of COVID-19 on the DNS has been limited, and the figures reported by ccTLDs and gTLDs have been consistent: the levels of reported COVID-19 related abuse remained low across ccTLDs and gTLDs.

The PSWG also noted the industry-led voluntary Framework to Address Abuse, highlighting that many signatories of the framework had made a noticeable effort to engage in conversations with law enforcement. The PSWG also noted reports by contracted parties of domain name blacklists developed by security firms that were much more aggressive than necessary and included legitimate websites that ended up being flagged as malicious.

When it comes to law enforcement activities during the COVID-19 pandemic, the data used by law enforcement to go after malicious actors was different from the datasets used by contracted parties, according to Gabriel Andrews (FBI). The FBI started with a much smaller dataset of domain names that had been reported as being used for abusive purposes, such as fraud, malware distribution and phishing. The FBI worked with datasets received from trusted private parties, such as Microsoft, PhishLabs, ScamSurvivors. The FBI noted the importance of partnering up with cybersecurity practitioners and third parties to receive reliable data. Once the websites were identified, referrals with screenshots of the websites were sent to registrars together with preservation letters asking registrars to preserve registrant's data. These referrals were sent to registrars on a weekly basis. The FBI noted that the peak for these referrals was on 17 April.

The peak of FBI referrals was compared to the statistics shared by the ICANN Office of the Chief Technology Officer (OCTO), that identified the peak of COVID-19 related registrations in the gTLD space to be around the end of March. Gabriel Andrews speculatedthat there might be a correlation between the peak in COVID-19 related registrations, as reported by ICANN Org, and the peak of referrals sent to registrars after the abuse was reported to the FBI. Gabriel Andrews speculated that it might take about three weeks for a cycle to be completed: from a domain name being registered by a bad actor, to be used in criminal activity, to being reported by a victim and for the FBI to send out the referral to the registrar. However, this speculation was not supported with any further data or analysis.

The FBI noted the difficulties in obtaining registrant data when registrars redact it due to the Privacy/Proxy service. According to law enforcement reports during ICANN68, most registrants of domains involved in COVID-19 related fraud, phishing or malware have employed Privacy/Proxy services to hide their identity. In order to obtain that data from registrars, a subpoena or a court order is needed. According to Gabriel Andrews, where it once took 30 seconds to look into the data needed for an investigation, it now takes three weeks to obtain it from registrars. In order to ensure that the data is still available three weeks after the FBI gets a subpoena, the FBI needs to send a letter for preservation to registrars.

Additionally, the FBI provided statistics that identified more than 2,5 times as many cybercrime complaints received in April 2020 compared to April 2019. This justifies the extra vigilance law enforcement exercised during the pandemic, according to the PSWG.

Laureen Kapin (US Federal Trade Commission) welcomed the development of advancing on the definition of DNS abuse by the RySG and RrSG, noting that this definition could potentially be expanded even further. The definition adopted by the CCT Review Team also included "intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names". According to Laureen Kapin, the five categories mentioned in the definition adopted by the contracted parties do not include certain forms of “website content abuse” that are so egregious that the contracted party should act upon it when provided with specific and credible notice. According to Laureen Kapin, there is room for a broader discussion to widen the concept of DNS abuse.

Becky Burr (ICANN Board) asked for clarification on where the line can be drawn when we speak about DNS abuse and website content abuse. Laureen Kapin explained that her thinking is that “specific malicious activities and deceptions that were being conveyed through the use of a domain itself”, although they fall outside the core of DNS security abuse, could still be in the remit of ICANN as these exploit the DNS. According to Laureen Kapin, COVID-19 is a clear example of where law enforcement authorities have been cooperating with registrars and looking into domain names because these were used to deliver an inherent message of deception: e.g. vaccines and a cure for COVID-19.

Chris Lewis-Evans (UK National Crime Agency) reported statistics from the UK. Since the COVID-19 outbreak on 23 March, the UK has received reports of online shopping fraud totalling over 16 million GBP (although not all of those online shopping instances were COVID-19 related). 2 378 victims have lost a combined total of over seven million pounds to COVID-19 related scams (by June 2020).

Cathrin Bauer-Bulst (European Commission) reported on Europol’s activities. Throughout the pandemic, Europol published reports covering statistics on all types of crime, not necessarily linked to COVID-19. According to Cathrin Bauer-Bulst, Europol has a reputation for being a source of reliable and honest information. Together with the European Commission, Europol developed a request form to contact registrars about domain names engaged in criminal activity. The form was inspired by the Guide to Abuse Reporting Best Practices that was developed by the RrSG. When it comes to the definition of DNS abuse, Cathrin Bauer-Bulst supported her fellow colleagues in the PSWG by stating that the definition that had been adopted by the contracted parties should be a baseline for further discussion on the scope. She also considered registrars to be the “single swift point of entry” to take action, irrespective of the separation between DNS security abuse and website content abuse.

Registry Stakeholder Group

The Registry stakeholder group held an excellent webinar in preparation of the ICANN meeting. The webinar gave a cross community overview of COVID-themed registrations and abuse patterns. The recording can be viewed here.

SSAC activities

The SSAC submitted its response to the SSR2 Draft Report. It expressed its concerns about a number of recommendations made in the Draft Report and specifically with regard to their underlying rationale and their measurability. In general, the SSAC considered that the outcomes sought by SSR2 for some recommendations are not clear.

With regard to the SSAC Work Party on DNS Abuse and its future activities, Jeff Bedser (SSAC) indicated during the public meeting of the SSAC that the Work Party would try to further frame the issue of DNS abuse to reduce victimisation through the quick identification of a relevant party responsible for dealing with a particular type of abuse. The SSAC will look into the full ecosystem and beyond ICANN contracted parties, as there are a number of abuse types that registrars and registries typically do not respond to.

Stephanie Perrin (NCSG) raised a question about the statistics and reports available regarding the results of domain name takedowns, and the reliability of the metrics when abuse is not clearly defined. Jeff Bedser responded that the measurement of data about reported abuse is quite straightforward: data on actions is not collected, unless the domain name is removed from the zone. However, there are no reliable metrics on takedown actions at the moment. Rod Rasmussen (SSAC) clarified that there are limits to the type of abuse that is being recorded. Child sexual abuse material is not something that gets recorded, while phishing does. The SSAC wants to work on the framework that ensures that reports on different types of abuse go to the right actors, instead of arguing over semantics and differences between types of abuse.

Comments from the community on DNS abuse during the Plenary and At-Large sessions

- Jim Galvin (RySG, Afilias) reiterated that the only measure available to a registry for doing anything about abuse is removing a domain name. This is a blunt and disproportionate tool for addressing most website content abuse. The COVID-19 related DNS abuse that RySG has identified in the last months was very limited: it was primarily content-related abuse, where the registries also took part by reaching out to registrars and hosting providers.

- Graeme Bunton (RrSG, Tucows) echoed the statement made by the RySG: no material DNS abuse was identified by the RrSG, and there was only a small number of abusive registrations. Graeme Bunton also called for more quality data and information on concrete attributes shared by bad actors before considering any tools to tackle the issue of DNS abuse.
- Peter Van Roste (ccNSO, CENTR) provided an overview of COVID-19 related DNS abuse within European ccTLDs. Only 0.08% of newly-registered domain names within 12 ccTLDs was COVID-19 related. The levels of associated abuse were consistently low. From the lessons learned, Peter Van Roste indicated that ccTLD collaboration with local national authorities, such as health and consumer protection authorities, worked well.
- Jonathan Zuck (ALAC) stated that according to DAAR, eight actors currently engage in systemic abuse. Any anti-abuse related efforts should focus on these eight actors.
- Mason Cole (BC) pointed out that, irrespective of external events, DNS abuse continues to grow steadily. A lot of abuse associated with cybercrime, such as rogue pharmacies, is rooted in domain names. According to the data provided by Microsoft, more than 30 000 domain names are COVID-19 related. According to Mason Cole, ICANN Org does not have the tools needed to combat the behaviour of rogue registrars and to hold these actors accountable.
- Brian Cimbolic (PIR) presented PIR's Quality Performance Index (QPI) that provides financial incentives for registrars with "good" registration patterns. The QPI is based on the following factors: abuse rates, renewal rates, domain usage, being DNSSEC enabled, SSL usage.
- David Conrad (ICANN Org) gave an overview of additional tools developed by ICANN Org that can help contracted parties with data: e.g. the Domain Name Security Threat Information Collections and Reporting tool that provides RAR with confidence reports for appropriate action, tracking and reporting outcomes. David Conrad also expressed the unwillingness of ccTLDs to participate in DAAR that in return will help to refine DAAR reports and offer more detailed data.
- Yrjö Länsipuro (ALAC) pointed out the existing discrepancies between levels of abuse reported by Europol and other law enforcement agencies and what has been presented by contracted parties to the ICANN community. He suggested that if content exists to aid and abet DNS abuse, it should also be treated as DNS abuse.
- Owen Smigelski (Namecheap) praised all the efforts made by registries and registrars to combat COVID-19 related online abuse. According to Owen Smigelski, the DNS industry has done a remarkable job during these difficult times and has taken steps to collaborate with law enforcement and other governmental agencies that should be a lesson learned for the future.
- Fabricio Vayra (IPC) noted that it is common practice for bad actors to take advantage of disasters, beyond COVID-19. He stressed the need to acknowledge the fact that bad actors will continue their criminal activity and that contracted parties should be more proactive in making sure that abuse does not happen. He underlined the need for the community to learn from the COVID-19 experience and include that in ICANN compliance activities.
- Göran Marby (ICANN CEO) noted that ICANN Org's role in the DNS abuse discussions is to support and facilitate these discussions within the community. ICANN Org is also supporting the community by providing it with tools, such as DAAR, health indicators and reputational feed available for contracted parties.

GAC Communiqué: The GAC believes that capacity building and training initiatives should be prioritised by ICANN Org, in terms of budgetary allocation and scheduling, for countries most affected and where the benefit would be the greatest. The GAC notes that new efforts to tackle DNS abuse should not replace, but rather complement existing initiatives to improve the accuracy of registration data, such as the Accuracy Reporting System, and to implement policies on privacy and proxy services, which are currently on hold despite having been recommended by a number of review teams and endorsed by previous GAC advice.

The GAC calls on the Board to implement existing advice and on the ICANN community to seize this opportunity and commit to its different work streams on DNS Abuse, aiming for security, safety and the protection of individual and public rights and freedoms.

Relevance to ccTLDs

The discussions over the definition of DNS abuse are increasingly moving towards content moderation, blurring the line between "technical" abuse and "website content" abuse. While registries cannot adequately assess or control content abuse, it is evident that there is more pressure to adopt preventive measures when addressing abuse on the DNS level. Additionally, more voices are calling for a "holistic approach" when addressing DNS abuse within the ICANN community, that seems to also encompass ccTLDs (although for now 'in parenthesis'). Previously, with their practices in tackling abuse, ccTLDs have consistently been considered to be the champions in keeping their zones secure and free from abuse within the ICANN community, while COVID-19 seems to have shifted this rhetoric towards 'how and where to get real data' in order to feed the debate. ICANN Org has also consistently voiced out the need to include more ccTLDs into DAAR for more consistent reporting during ICANN68, not providing any reasons 'why' ccTLDs should be part of a tool aimed at improving security in the gTLD space, nor indicating any incentives for ccTLDs to join. Relevance to ccTLDs

Without a secretariat providing the GAC with factual information about processes and rules of procedure, the GAC's work risks fragmenting and relying on fewer active GAC members that could take a more predominant role and promote a biased view on issues.

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 GNSO EPDP 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 is supposed to be replaced by the Registration Data Policy.

In its previous advice, the GAC has noted on several occasions that the Temp Spec fails to meet the needs of law enforcement, cybersecurity researchers and IP rightsholders. The need to ensure 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 access to non-public registration data (hereinafter SSAD).

On 7 February 2020, the Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team – Phase 2 was published, together with an additional Addendum on 26 March. The GAC provided Input on the Initial Report on 24 March 2020 and a Comment on the Addendum on 5 May 2020. The final Phase 2 recommendations are expected to be concluded by July 2020 (preliminary deadline).

GAC discussions

There were some extensive discussions on the SSAD during ICANN67. During ICANN68 the high-level assessment of the likely outcome of the EPDP Phase 2 presented to the GAC indicated that the EPDP deliberations on the SSAD can "conclude adversely to public policy interests".

Chris Lewis-Evans (UK National Crime Agency) outlined a possibility for the EPDP to continue into Phase 3 after the Phase 2 Final Report publication. The reasoning for Phase 3 includes a lack of decision-making on some important items like the application of data protection to legal persons compared to natural persons; the issue of privacy/proxy services and WHOIS accuracy. He stressed the importance of WHOIS accuracy that is also rooted in the GDPR: any personal data collected by data controllers and processors must be accurate for the purpose of data processing. Additionally, according to Chris Lewis-Evans, it is also important to equip ICANN's compliance team with the adequate tools to address disobedience with ICANN policies by contracted parties.

Laureen Kapin (US Federal Trade Commission) stated that previously the SSAD had been moving towards ICANN Org's originally proposed Unified Access Model (UAM) that was favourable to several public policy interests. However, according to Laureen Kapin, these interests are no longer being taken into consideration in Phase 2, and there is a risk of losing "the balance previously achieved on the SSAD".

Georgios Tselentis (European Commission) expanded on the public policy concerns not addressed by the current EPDP discussions on the SSAD that are at risk of not being aligned with GAC expectations:

- Accuracy of registration data for the purpose for which it is processed;
- Publication of legal entities' registration data;
- Centralisation and automation of disclosures;
- Evolution mechanism towards increased centralisation, automation and standardisation of disclosures;
- Ability for compliance enforcement against wrongful disclosure denials;
- Preventing double privacy shield for privacy proxy services.

The focus on further automation and the evolution mechanism is justified by the need for the SSAD to move from the current fragmented system with more than 2 500 approaches to access requests to non-public registration data, according to Laureen Kapin. The SSAD needs to be flexible, as the GDPR is a new and complicated legal framework that is subject to increased legal guidance over time through data protection authorities' advice and case-law. Therefore, there is a need to adapt to future guidance and for a potential increase in the categories for automation in the SSAD. The EPDP team is currently discussing whether a new separate PDP should be established for these new categories for automation in the future.

Chris Lewis-Evans stressed the need not to initiate a new PDP every time there is a new piece of data protection legislation and the fact that contracted parties need to retain some sort of flexibility in their ability to process data in a legally safe way.

Milton Mueller (NCSG) pointed out that the NCSG has put forward a proposal about deciding on the issue of the evolving mechanism that needs to be done with full consensus. There is no room for a mechanism that will allow policy development without the GNSO Council and advisory committees, and it is necessary to make sure that this mechanism cannot be abused or taken advantage of, according to Milton Mueller.

Farzaneh Badii (NCSG) pleaded with the GAC not to put additional pressure on the EPDP and the GAC representatives within. There is a need to come to a consensus. The NCSG is not against the disclosure of registration data as such. According to Farzaneh Badii, the NCSG is against the disclosure of sensitive information to legitimate authorities.

Accuracy of gTLD Registration data

During the joint meeting of the GAC with the PSWG, Laureen Kapin highlighted the fact that in pre-GDPR times, the ICANN community was working on a WHOIS Accuracy Reporting System (ARS) that was suspended when the Temp Spec was adopted. She stressed that this project needs to be resumed in order to achieve the phase where it could measure and assess the accuracy of registrant identity data.

In September 2019, the RDS-WHOIS2 Review estimated that 30-40% of registration data was inaccurate and recommended resuming operations of the ARS or a comparable tool. The ICANN Board placed this recommendation in pending status until the EPDP Phase 2 had addressed the matter. The GNSO Council determined that WHOIS Accuracy is not on the critical path of Phase 2. According to the PSWG, "pervasive gTLD registration data inaccuracies continue to undermine the effectiveness of the gTLD registry directory service, including in meeting the legitimate needs of law enforcement and in promoting consumer trust".

During the joint meeting of the GAC with the ICANN Board, the GAC questioned the ICANN Board's intentions of restoring ICANN's ability to address gTLD registration data inaccuracies, including resuming the ARS identity validation.

Chris Dispain (ICANN Board) and Becky Burr (ICANN Board) both argued that the EPDP is not the place to hold these discussions. Nevertheless, the issue still needs the attention of the GNSO Council but preferably in a separate PDP. Furthermore, Chris Dispain noted that the discussions within the EPDP primarily focus on preserving the rights of data subjects, rather than benefitting those who wish to look into that data.

Georgios Tselentis (European Commission) argued that the European Commission's position is that both the rights of data subjects, as well as the rights of those with legitimate interest are equally important under the GDPR.

Chris Lewis-Evans (UK National Crime Agency) supported the position voiced by the European Commission and stressed that his understanding of data accuracy can be regarded from two aspects, one from the data subject and the other from the controller that must ensure that the data they are processing is accurate for their purpose.

Maarten Botterman (ICANN Board) also notified the GAC that the ICANN Org had consulted .dk and .fi on the issue of access and disclosure of non-public registration data.

GAC Communiqué: The GAC requests the Board to obtain an update from the GNSO, as soon as possible, on its progress towards developing a specific plan to continue the policy development process to address the unresolved issues related to distinguishing between natural and legal entities, and ensuring data accuracy. Such future policy efforts should start as soon as possible following the publication of the Phase 2 EPDP Final Recommendations and conclude where feasible six months after.

In line with its previous advice, the GAC observed the need to maintain WHOIS access to the fullest extent possible and noted that in its San Juan Communiqué it had advised the ICANN Board to instruct ICANN org to "distinguish between legal and natural persons, allowing for public access to WHOIS data of legal entities, which are not in the remit of the GDPR". The GAC reiterates that this advice still stands and should be considered.

Relevance to CENTR members

During ICANN68, WHOIS discussions were increasingly linked and handled together with the issue of DNS abuse, at times being almost inseparable. Issues of WHOIS accuracy and the distinction between the publication of legal and natural persons' registration data have also been considered as security issues that need to be handled within the EPDP. The GAC considers these two issues to be a matter of public interest due to the numerous complaints received from the law enforcement community, putting pressure on policy development processes within ICANN to advance on these issues as swiftly as possible. Finally, if any centralised and automated data access model, as inter alia also being promoted by ICANN Org itself (via its UAM) sees the light in the end of the process and manages to unify the 2500+ contracted parties, this will inevitably create pressure on ccTLDs to also unify their own data access and WHOIS policies, irrespective of national differences and nuances in the data protection regime.

ICANN69 will be held virtually on 17-22 October 2020.

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 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 ICANN68

(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