Council of European National Top-Level Domain Registries

Report on ICANN69

Annual General Meeting

October 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

Highlights from ICANN69 3

ICANN69 ccNSO Report 4

ccNSO Members meeting on ccNSO Governance 4
Internet Governance Liaison Committee (IGLC) 4
ccTLD news session – COVID-19 impact 5
European perspectives on ICANN and Internet Governance 5
ccNSO Strategic an Operational Planning Standing Committee 6
ccNSO Tech Day 6

ICANN69 GAC Report 7

DNS Abuse 7
- Background and recent developments 7
- Discussions on definitions and scale of the problem 9
- Exchange with the Public Safety Working Group 10
- GAC concerns with the EPDP Phase 2 (SSAD) 10
- Community statements during the session on WHOIS post-GDPR and its impact on end-users and public safety 11

Highlights from ICANN69

ICANN is currently facing a structural challenge: how can it reconcile the need for intersessional work with the necessity of transparency and cross-community debate in its virtual meetings, aspects which were such an integral part of ICANN's fabric at a time when it held three physical meetings every year?

This online ICANN meeting seems to have increased the differences in meeting formats and interaction in the different Advisory Committees and Supporting Organisations. While at the ccNSO it was mainly 'business as usual', the GAC has adapted quite differently to the way the ICANN community interacts these days.

In general, this ICANN meeting was less transparent and less open than the previous meeting (one example being the need to register even before the meeting agenda could be consulted). However, in the GAC even the meeting dynamic changed. As a substantial part of the work is now done intersessionally (and not open to the public), the public GAC meetings have become more similar to one-way downloads and as a result they lack interaction. This intersessional work could also lead to the different parts of the ICANN community operating in silos.

This ICANN meeting was also spread out over three weeks. More and more participants are signalling that this is a stretch that becomes hard to reconcile with their day jobs.

The ccNSO sessions were generally informative, reasonably interactive and thoroughly prepared. The best ccNSO sessions were - as usual - those where ccTLDs exchanged experiences (from COVID's impact to Internet Governance).

One issue that came up during the ccNSO meeting is that as a result of ICANN's increased policy efforts (such as writing letters to the European Data Protection Board) it is creating confusion and possible collateral damage for ccTLDs. In its communication, ICANN does not make a clear distinction between ccTLDs and gTLDs when communicating to external parties. ICANN needs to urgently and consistently specify in all its public communication that neither ICANN Org, nor the ICANN community sets policies for ccTLDs.

The topic that is now omnipresent in ICANN discussions is 'DNS Abuse' in its many shapes and shades. This topic was mainly discussed during the GAC and ALAC session, but is also an essential part of the gNSO discussions on the next round of new gTLDs or the discussion on WHOIS access and data accuracy. Adding to the existing complexity, contradictory data showed both an increase and decline in 'DNS Abuse' trends.

In the GAC, DNS abuse has truly become the cross-cutting issue within ICANN discussions. The discussions around what can be called DNS abuse, its scale, and which responsibilities are borne by whom, including ICANN Org itself are an underlying part of the GAC's priority topics. These topics are 1) The GNSO New gTLD Subsequent Procedures PDP WG (SubPro PDP WG); 2) Registration data and WHOIS, including data accuracy discussions.

Nigel Roberts (.je/.gg) indicated that he will not run for re-election as an ICANN Board member and Katrina Sataki (.lv) is the only candidate for seat 12 on the ICANN Board. It is a shame to see the former, an extremely strong contributor leave the ICANN community and also to lose such a fabulous ccNSO Council Chair to the ICANN Board. With Katrina's departure to the ICANN Board, Irina Danelia (.ru) volunteered to join the ccNSO Council and to fill the vacant European seat, and it is great to see an experienced Board Member step up and join the ccNSO Council. Thanks and congratulations to all!

ICANN69 ccNSO Report

ccNSO Members meeting on ccNSO Governance

The ccNSO held an interesting discussion on how it should and could improve its governance mechanisms to make it fit for today's environment.

The ccNSO has changed significantly over the last 15 years. Membership has increased by 200% since the ccNSO bylaws were approved. The goal of this session was to explore how the ccNSO can continue to function effectively in the light of the new circumstances. A few rules were discussed such as the current 10% blocking minority and term limits for council members. The most controversial discussion was about rules versus guidelines.

A significant part of the ccNSO's operations follow guidelines rather than the bylaws as specific issues or circumstances had not been foreseen at the time those bylaws were written. However, whilst rules are carved into the bylaws and can only be changed by the members, guidelines can be changed by the Council.

There is a tendency to park procedural issues as guidelines, if only to avoid a cumbersome procedure to change the bylaws. Guidelines seem to circumvent checks and balances and create a democratic deficit. The question remains of how the ccNSO can remain agile and not lose its transparent, predictable and democratic process. This discussion served as a good first step in what will be a long and interesting journey.

Internet Governance Liaison Committee (IGLC)

The IGLC is a group established by the ccNSO with the objective to share and discuss topics related to Internet Governance. During this session, members of the group presented local developments. The Armenian registry (.am) and its local ISOC chapter organised the fourth school on Internet Governance (IG), where it is noteworthy that more than half of the participants were teachers.

It was reported that the online edition of the Italian IGF was very well attended and showed a strong interest in IG issues. Some sessions had 13 000 (!) participants. The main reasons for this success are its compelling program, a close link with the business community through collaboration with the Chamber of Commerce and the timeliness of the topic at a time when everyone is working online.

.nl, .pt, .it and .fr shared their experience during the COVID pandemic and illustrated their commitments to supporting the local internet community.

In New Zealand, the local IGF (NetHui) was held completely online. The number of attendants was comparable to face-to-face meetings. The two hot topics were misinformation and the global challenges on encryption. The five eyes intelligence alliance (US, UK, NZ, CA and AU) recently published a document on this topic.

The group also discussed the issue of digital sovereignty. Across the globe, digital sovereignty concerns are increasing (e.g. TikTok in the US, GaiaX in Europe, general digital strategies across the world). These discussions touch on the economic and security aspects of reduced national control. This is not a new topic though; there have already been initiatives from the World Summit on the Information Society (WSIS) and the International Telecommunication Union (ITU), national internet proposals from Russia and China and the concept of digital colonialism in France.

However, political discourse is now no longer shy of supporting a strong independent digital national industry. It is no longer only used in the context of human rights.

ccTLDs have been regarded as assets for national digital sovereignty, but they still manage to operate in a collaborative way on an international level. ccTLDs should advocate this successful example where national and global go hand in hand. In Senegal for example digital sovereignty discussions led to the national ccTLD being considered part of the national critical infrastructure. The pandemic made the theoretical discussion very concrete.

The discussion in the group concluded by a split vote on the question of whether 'digital sovereignty' is a threat to the global internet or not. This probably illustrates the complexity of the issue. The IGLC will continue to observe this area and report to the ccNSO.

ccTLD news session – COVID-19 impact

Patrick Myles (CENTR) presented a global TLD market update. The domain market saw a significant surge in domain registrations. The European market notably saw an average 20% YoY growth, with deletes stable or slightly down. The retail price has slightly decreased. Across the ccTLD CENTR members, creation rates are trending up whilst deletion rates are stable, even trending down slightly. The number of COVID related domains was small (0.08%) and these COVID-themed domains show a lifecycle that is similar to non-COVID related domains. The pandemic pushed businesses online, and Patrick reported that user experience on many retail sites is improving. Finally, there are indications of greater preference for ccTLDs.

Alex Corenthin (.sn) presented the impact of COVID on the Senegalese ccTLD, .sn. Senegal saw a surge of offers on data and connectivity, as well as an uptake in e-commerce, logistics and deliveries. The number of e-education initiatives increased. There were, however, also significant negative effects such as the pause of structural project investments, loss of revenue, increased national debt and difficulties for the digital economy due to missing out on state aid. The ccTLD responded by offering free domains, improving the resilience of the infrastructure and highlighting the importance of digital sovereignty. In terms of the impact on registrations, there were 50% more registrations compared to the same months in 2019.

David Curtin (.ie) shared the Irish experience. 65% of the Irish workforce is employed by SMEs. Traditional SMEs are typically slower to digitise their business, with only 26% able to take payments online, and only 30% able to take online orders. Registrants need to have a link with Ireland to register a .ie domain name. Compared to the same months in 2019, increases in domain registrations ranged from 21% to 62% between May and August 2020. There were no promotions at this time but IEDR gave a 36% discount on new registrations to improve registrar margins. IEDR also engaged in co-marketing efforts with registrars. Finally, IEDR activated a registrar service failure protocol that could be used to migrate portfolios to another registrar in case of financial problems.

Additionally, they activated a registrant protection fund and launched an informative website to help SMEs get online. The government chipped in with financial support for SMEs, grants for bigger retailers and online trading vouchers (worth 5 000 Euros) that can help SMEs get advice on how to move their business online. Consumer behaviour has changed, and SMEs will have no other choice than to join the digital evolution. COVID is the catalyst and the government's support is the accelerant.

In Taiwan, the pandemic had an impact on TWNIC operations, leading to flexible working hours, VOIP customer service and an increased use of VPNs. Given the low infection rates, the impact on society was small. This is reflected in the domain registration trends; they remained mostly flat across 2019 and 2020.

In Guatemala the .gt registry extended expiration dates for government websites, for demands from registrants who had trouble paying for their extension and started a one-year-for-free promotion from May to July. As a result, the registry saw significant growth over that period.

An interesting panel discussion following the presentations touched on:

1. The success of price-based promotions (historic research shows no long-term impact, but the impact on goodwill for a suffering community can be significant);

2. Expected trends in domain registrations in the next 12 months (if the pandemic continues, business failures will have an impact on the positive growth trend);

3. The future of the pandemic situation and the impact on ccTLDs (the next 6 months look bleak from a societal point of view, ccTLDs will manage).

European perspectives on ICANN and Internet Governance – EURALO stakeholder table

The ICANN Board Chair signalled the recent work on prioritising ICANN's workplan to implement the accountability recommendations, whilst the ccNSO Chair signalled the increasing complexity of what is done at ICANN.

The Security and Stability Advisory Committee (SSAC) flagged DoH, DoT and the European discussions on abuse as the most relevant discussions at European level. Tatiana Topina (Non-Commercial Stakeholder Group) picked data accuracy as the key European topic.

Chris Mondini (ICANN) spoke about talent acquisition and the challenges in the online workplace.

Michele Neylon (GNSO) pointed out that privacy was being trampled, but that the GDPR had made us take it seriously. As a result, the WHOIS changed. Abuse has increased, but not related to the WHOIS change. The real issues are impacting businesses and users in Europe. We need to focus on digital transformation.

Jorge Cancio (BAKOM) pointed out that broad and diverse participation is the essential requirement for ICANN to be successful. The different levels of engagement is worrisome, and the cost of meaningful participation compared to its possible impact is too high. He underlined that we need to radically rethink the complexity of this community.

Natalia Filina (EURALO) signalled that the biggest issue is the lack of participation of European individual users in ICANN's work. The At-Large community provides legitimacy to the process by bringing in the voices of end-users into the PDP process.

Elena Plexida (ICANN) named the DSA as the most important policy initiative in the EU. This initiative will impact the discussions on WHOIS and will be applicable to companies with headquarters in the EU. She added that ICANN had responded to the public consultation.

CENTR referred to a range of initiatives (such as the NIS directive and data access discussions) in addition to the DSA which are of particular importance. CENTR's response to the DSA consultation can be found here.

CENTR also produced a video on the role of registries in the context of the online content discussions which is available here.

ISOC shared their concerns and announced the launch of a toolkit for governments to assess the impact of potential regulation.

The European Commission reiterated their support for the multistakeholder model.

Pierre Bonis (Internet Governance Liaison Committee) reflected on the relevance of digital sovereignty and how it impacts ccTLDs. The term has been recycled and is now accepted as reflecting national digital independence. ccTLDs manage to serve their local internet community and still cooperate on a global level.

RIPE NCC sees an acceleration of the regulatory processes impacting the internet. Coordination amongst the internet infrastructure providers is crucial. ICANN and the GAC echoed this by calling for closer cooperation across communities and across borders.

The narrative needs to be driven by interdependence. Understanding the priorities and what we need to engage in is crucial. This can only be achieved through collaboration between the organisations.

In a poll at the end of the session, the majority (64%) of attendants indicated that they regarded Internet Governance in the age of digital sovereignty as the most important upcoming topic that will impact ICANN. The top three was completed by challenges for the ICANN multistakeholder governance model and the Digital Services Act.

ccNSO Strategic an Operational Planning Standing Committee

ICANN is on track to replenishing its reserve fund to 100% of one year of operational expenses. This has happened within two years rather than the envisaged eight years. The CFO expects there to be no need for additional allocations to the reserve fund.

ccNSO Tech Day

The ccNSO tech day agenda and materials can be found here.

CIRA and CENTR/InfoNetWorks both presented novel applications of registry technologies to new problem areas: IoT and air space management. DNS registry technology would, in these fields, anchor identities to electronic SIM cards or similar solutions in devices that need to be identifiable or connected to a particular actor or person.

NIC.AT has taken further steps to prepare CERTs for a future with registration data access protocol. The extensibility of this 2015 innovation for registrant data storage could help ensure less friction in discussions about registries and data protection, domain name abuse management and the role of public authorities vested with the responsibility to protect the public from abuse.

Finally, CZ.NIC has made further performance enhancements in its KNOT DNS software – now allowing UDP traffic maximization by stopping traffic

from passing directly through the Linux kernel. These changes were put into production at the beginning of September with smaller updates towards the beginning of October. No major disturbances have been reported on the CZ.NIC e-mailing lists since the entry into effect of these changes.

ICANN69 GAC Report

The GAC ICANN69 Communiqué is available here.

DNS Abuse

DNS abuse has truly become the cross-cutting issue within ICANN discussions. The discussions around what can be called DNS abuse, its scale and which responsibilities are borne by whom, including by ICANN Org itself are an underlying part of each priority topic of the GAC. These topics are 1) The GNSO New gTLD Subsequent Procedures PDP WG (Sub Pro PDP WG); 2) Registration data and WHOIS, including data accuracy discussions.

It seems that the balancing act between privacy vs security is increasingly prevalent at ICANN: preventing and mitigating the issue of DNS abuse is the underlying reason for the continued work on the GDPR implementation within ICANN contracted parties (i.e. gTLD registries and registrars), manifested in the discussions on the EPDP post-Phase 2.

Background and recent developments

Competition, Consumer Trust and Consumer Choice Review Team recommendations

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". The CCT Review Team has also issued recommendations for ICANN to take in order to increase safety within its contracted parties' zone. Some of these recommendations include financially incentivising the adoption of proactive anti-abuse measures; inserting contractual provisions aimed at preventing systemic use of specific registries and registrars; adopting thresholds of abuse at which compliance inquiries are automatically triggered; and requiring the publication of entire chains of ownership.

The ICANN Board has not accepted most of the CCT Review Team's recommendations. On 1 March 2019, the ICANN Board considered these recommendations and either placed them in pending status or to be considered for further input when appropriate (e.g. the recommendation to publish the chain of parties responsible for registrations).

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 had been identified as "prerequisites" or "high priority". This includes for example adding the financial incentives to Registry Agreements to adopt proactive anti-abuse measures.

In the GAC ICANN68 Communiqué the GAC called 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.

On 21 September, the GNSO New gTLD Subsequent Procedures PDP WG (SubPro PDP WG) issued its Final Draft Report where it acknowledged ongoing important work in the community on the topic of DNS abuse (e.g. the CCT Review Team recommendations) and stated its belief in the need for a holistic solution to account for DNS abuse in all gTLDs (and potentially ccTLDs).

On 30 September, the GAC issued a Collective Comment to the Sub Pro Final Draft Report, urging the GNSO Council to trigger holistic effort in order for the "conditionality expressed in the GAC ICANN66 Communiqué[sic. Montreal advice] to be met". The GAC stressed the importance of the CCT Review Team's recommendations to be implemented before the beginning of the next round of gTLDs. Notably, in its collective comment the GAC also makes a point about avoiding the reference towards ccTLDs in these efforts, as "they do not fall under ICANN's remit but operate under national legislation".

It is also notable that ICANN Org considers the policy work on DNS abuse to be of special importance as the rationale for extending ICANN President and CEO Goran Marby's contract in July 2020, and explicitly mentions Marby's work in "Community discussions on DNS Abuse that could lead to policy recommendations".

SSAC

The Security and Stability Advisory Committee (SSAC) Work Party on DNS Abuse was established to discuss reliable data sources of malicious activities and review effective practices currently in place within the industry. The SSAC Work Party consists of representatives across the ICANN community, including the Public Safety Working Group (PSWG) and ICANN's contracted parties. Since its creation, the SSAC Work Party has been working on a report that intends to outline a strategy to address the methodologies, practices and cooperation necessary for reducing DNS abuse. The report is intended to be published in the coming weeks.

Jeffrey Bedser (iThreat, SSAC Work Party on DNS Abuse) highlighted a few key points expected to be reflected in the upcoming report. The report will encourage the development of standard definitions of abuse, while at the same time not aiming to establish new definitions but rather building upon the existing ones. In addition, the report will determine the appropriate primary point of responsibility for abuse resolution, identify best practices for the deployment of evidentiary standards, establish standardised escalation paths for abuse resolution and recommend the development of "notifier programs" amongst other things.

Contracted parties

In September 2019, several registries and registrars launched the Framework on DNS Abuse, to standardise definitions and set expectations for action. The Framework defined DNS abuse as malware, botnets, phishing and pharming, with spam listed as an attack vector. Since then the Framework has grown to over 50 signatories.

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", echoing the definition enshrined in the Framework.

WHOIS and registration data

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 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). The Final Report of Phase 2 was published on 31 July 2020.

The GAC submitted a Minority Statement on 24 August, along with ALAC, BC, IPC, SSAC. In the Minority Statement, the GAC withholds its support for certain recommendations in the Final Report of Phase 2 "which in their current form do not strike the appropriate balance between protecting the rights of those providing data to registries and registrars, and protecting the public from harms associated with bad actors seeking to exploit the domain name system". According to the GNSO Operating Rules and Procedures, "minority viewpoints" have no formal influence on subsequent deliberation of the GNSO Council.

It is unclear when the Interim Policy will be replaced by the Registration Data Policy, due to several outstanding issues still on the negotiation table.

Following several Minority Statements, the GNSO Council requested a consultation with the ICANN Board to discuss the issues surrounding the financial sustainability of the SSAD, including whether a further cost-benefit analysis should be conducted before the ICANN Board considers all SSAD-related recommendations for adoption.

In parallel, further policy work in the GNSO is expected to be initiated shortly:

1. The EPDP is expected to be reconvened in a new shorter phase (Phase 2a) to address the distinction between legal and natural persons and unique anonymised contacts.
2. A separate scoping effort will be initiated regarding data accuracy, including potentially initiating a new PDP in the future.

Discussions on definitions and scale of the problem

Despite many parallel efforts from different corners of the ICANN community (and beyond), there is no definition on what constitutes DNS abuse that is accepted by the community as a whole. As evident from the ICANN69 meeting, any attempt to define the issue of DNS abuse raises several overarching problems: the lack of consistent data on the scale of the problem, the issue of (non)separation of content moderation and internet infrastructure, and ultimately whether these discussions are even consistent with ICANN's remit, as enshrined in its Bylaws.

Scale?

Data is key to underpinning the problem, but the numerous presentations during ICANN69 on the statistics regarding "DNS abuse" show the lack of consistent data in outlining the actual impact on end-users and businesses. The lack of definition causes another problem, as in the absence of what is needed to be measured, the differences in reported data and approaches to the topics are even greater.

ICANN69 meeting discussions were an illustration of Mark Twain's saying that "Facts are stubborn things, but statistics are pliable".

David Conrad (ICANN Org) presented the Domain Abuse Activity Reporting (DAAR) statistics showing that in the period from September 2019 to September 2020, there was a decrease in phishing, malware and botnets, but an increase in spam. The DAAR data comes from reputation service providers and it does not distinguish between different types of spam: as in 1) unsolicited email or 2) spam as a delivery mechanism for other types of abuse (like phishing and malware). Nevertheless, according to Conrad, overall DNS abuse is going down.

Mason Cole (Business Constituency) cited Interisle Consulting Group data from the study period of 1 May to 21 July 2020 that shows that phishing is on the rise. However, according to Cole, the phishing problem is bigger than reported and the exact size of the problem is unknown. According to Cole, the "over-redaction of WHOIS data is contributing to the under-detection problem".

Greg Aaron (Interisle Consulting Group) provided more information on the phishing landscape in 2020 based on the respective study. According to Interisle data, phishing is highly concentrated in certain domain registrars, hosting providers and TLDs. The detection and blocklisting of phishing domains are impacted by several factors, including a lack of WHOIS data. According to Aaron, Google browser data shows that phishing is going up, while malware is going down.

According to the SSAC Work Party on DNS abuse, "DNS abuse and resultant cybercrime continues to victimize millions annually".

Chris Lewis-Evans (UK National Crime Agency) cited data from the FBI's Internet Crime Complaint Center that identifies phishing to be the most frequently reported complaint. Global ransomware reports

increased by 715.08% according to the FBI.

Notably, several of the sources cited above do not differentiate between "content" abuse and DNS abuse (per definitions identified above).

James Bladel (GoDaddy) provided a glimpse into phishing reports to a registrar. GoDaddy reports a more modest year-over-year growth of 15% and nothing approaching a "surge" of abuse. Currently GoDaddy processes over 2000 phishing reports per day, however this data does not show the amount of phishing incidents. Most of these reports are not actionable (i.e are not related to domain names) or duplicated. GoDaddy data relating to COVID-19 scams also show mostly content-focused incidents that are more effectively mitigated at the webhost level, rather than at Registry/Registrar/DNS level. Additionally, registrars received a lot of pressure, including from regulators, to just block the registration of any COVID-19 related string and not to allow any COVID-19 related registrations. However, most of the harmful registrations seen by GoDaddy do not mention COVID-19 at all, making this measure simply unnecessary and ineffective.

Definitions?

Different stakeholder groups agree that common frameworks and definitions are needed in order to move this discussion forward. The Framework of DNS abuse adopted by different contracted parties has been cited as a good foundation for any future work on this matter. At the same time, some contracted parties are also calling for caution in initiating a new development process on the issue of DNS abuse, primarily due to ICANN's limited remit in addressing content moderation. Additionally, there is a need to explore whether any existing measure, such as contractual compliance, could be used to mitigate the problem before new policies are written.

During the Public Forum at ICANN69, ICANN CEO Göran Marby highlighted that when it comes to DNS abuse discussions, ICANN Org is only facilitating the community discussions on this. It will be for the community to decide on the actions, while ICANN Org develops systems to support fact-based discussions.

Exchange with the Public Safety Working Group

Chris Lewis-Evans (UK National Crime Agency) stressed during the Joint meeting of the Public Safety Working Group (PSWG) and the GAC that the issue of DNS abuse is not going to disappear. The debate needs to focus on the speed of response, accuracy of registration information and clear and enforceable contract provisions with consequences.

Laureen Kapin (FTC) explained that there needs to be more clarity in identifying registries' obligations in response to DNS security and whether this entails monitoring DNS abuse. Hence, more work is needed to come up with specific proposals for enforceable contract provisions. In addition, according to Kapin, there are 8-10 problematic actors amongst contracted parties when it comes to the DNS abuse issue, and there should be a way to address this behaviour within the contract.

Laureen Kapin also raised the need to work together with all actors within the ecosystem, instead of debating on the statistics, as everybody agrees that DNS abuse and cybercrime are negative issues.

Susan Payne (Intellectual Property Constituency) highlighted the need for reliable data in order to measure whether any steps taken are effective and to be able to compare with other datasets.

Laureen Kapin explained that there is a difference between the figures reported by DAAR and the numbers claimed by the Intellectual Property Constituency (IPC). However, the IPC is not able to disclose details due to competition concerns. On measuring the effectiveness of the steps taken to mitigate DNS abuse, this is where contracted parties could help and shed light on whether any measures are having an impact on DNS abuse, according to Kapin.

GAC concerns with the EPDP Phase 2 (SSAD)

In its Minority Statement from 24 August, the GAC provided input on its public policy concerns with the Final Report of EPDP Phase 2. The GAC particularly highlighted the following criticism with the recommendations from the EPDP Phase 2 that:

- conclude with a fragmented disclosure system;
- do not contain enforceable standards to review disclosure decisions;
- do not sufficiently address consumer protection and consumer trust concerns;
- do not sufficiently contain reliable mechanisms for the SSAD to evolve in response to increased legal clarity;

- may impose financial conditions that risk creating an SSAD with disproportionate costs for its users, including those that detect and act on cybersecurity threats.

The GAC also expressed its continued concern that several highlighted key issues were not addressed in Phase 2, including data accuracy, masking data from legal entities not protected under the GDPR and use of anonymised emails. In addition, more clarity is needed on the status and role of data controllers and processors under the GDPR.

The US welcomed further work on priority issues like the distinction between legal entities and natural persons' data, as well as the need for data accuracy.

Russia stressed that the whole WHOIS issue resulted because of national legislation and that the WHOIS service is currently imbalanced, as it depends on the recommendations of individual states and the interpretation of local players. Russia stressed that states need to be more proactive on this issue and seek the international harmonisation of national regulations concerning access to WHOIS. Russia proposed drafting national recommendations for national registries and registrars to provide access to WHOIS data. In this regard, Russia highlighted the Domain Name Act in Denmark which requires the mandatory publication of registration data that could be considered as an example for other national states.

Community statements during the session on WHOIS post-GDPR and its impact on end-users and public safety

- Laureen Kapin (FTC) highlighted that access to WHOIS is needed for the public to conduct due diligence and find those responsible for conducting scams. According to Kapin, consumers have noted the missing information in WHOIS, assuming that businesses are dishonest because certain information is missing.

- Gabriel Andrews (FBI) noted the challenges in access to WHOIS for law enforcement. In pre-GDPR times it took 10 seconds to conduct a public source lookup. Since the GDPR entered into force, registrars have been responding to WHOIS-access requests differently: some respond to law enforcement requests; some only respond to local law enforcement authorities' requests; some will ask for a legal process, such as a corresponding court order and/or subpoena. There are also challenges posed by different jurisdictions, depending on available MLAT mechanisms. Depending on the legal process, it might take up to six months in order to get the needed access to WHOIS data.

- Greg Aaron (Interisle Consulting Group) highlighted the reasons why cybersecurity professionals need WHOIS data. Even if criminals register a domain name with fake information, it is still possible to run checks on this data and identify bad faith. Furthermore, criminals usually register domain names in batches, and by the time phishing is detected, most of the damage has already been done. According to Interisle data, 60% of domain names used in phishing attacks are registered by the phishers. A similar study conducted by .nl and .fr (the COMAR Project) found that 57% of domain names used on phishing are registered by the phishers. According to Aaron, registries and registrars must use the registration data available to them better to suspend malicious registrations.

- Milton Mueller (NCSG) stressed that according to many privacy laws, registrants have a legal right to shield their registration data. Criminals can more easily misuse publicly and openly available personally identifiable information. Mueller cited Google Transparency Reports that show an overall decline in malware and phishing. According to Mueller, there is no direct link between the size of the problem for cybersecurity and the redaction of WHOIS data. Any SSAD effort needs to be compliant with the GDPR.

- Owen Smigelski (RrSG, Namecheap) stressed that data protection concerns stemming from international human rights law cannot be ignored because these might be inconvenient to some actors. All data protection principles enshrined in the European data protection laws, including data accuracy, are there in the interest of the data subject primarily and are not necessarily also in the interests of third parties. These principles do not provide any third party with the right to access personal data, nor do they create any obligation to disclose that data to third parties. Furthermore, the overall amount of abuse involving domain names is decreasing according to ICANN data. Unredacted WHOIS data provides attack vectors for domain hijacking, spam and phishing. Smigelski also shared

some figures of WHOIS access requests depending on requester type. According to Namecheap data, around 74% of all WHOIS access requests are filed by intellectual property rightholders.

GAC Communiqué:

On DNS abuse: the GAC appreciates the ICANN Board's recognition of the importance of further work on this issue. From the GAC's perspective, the momentum has been increasingly building for concrete action as the Community has progressively engaged in constructive dialogue to advance work on a shared goal, the mitigation of DNS abuse. Beginning with the recommendations from the CCT-RT and the SSR2 RT and continuing through several cross-community sessions and more recent work on the DNS Abuse Framework, the GAC believes there is now a solid expression of broad support for concrete steps to be taken to address the core components of effective DNS abuse mitigation. The GAC stands ready to work with the ICANN Board and the Community to advance this shared goal, including through proposals to improve policies and/or improve contract provisions and enforcement, in relation to curbing DNS abuse.

On the access to gTLD registration data: the GAC reiterates that registration data should be accurate. As the GAC noted in its Minority Statement on the Phase 2 EPDP registration data recommendations, "[t]he accuracy of domain name registration data is fundamental to both the GDPR and the goal of maintaining a secure and resilient DNS. The GDPR, as well as other data protection regimes and ICANN's Registrar Accreditation Agreement, require data accuracy and such accuracy is critical to ICANN's mandate of ensuring the security, stability, reliability, and resiliency of the DNS. [...] Consistent with [Article 5 of] the GDPR it is essential that data accuracy and quality is ensured to the purposes for which they [the data] are processed". The GAC reiterates its statement from the Abu Dhabi Communiqué that any successor to the WHOIS service must meet the needs of "businesses, other organizations, and users in combating fraud, complying with relevant laws, and safeguarding the interests of the public[.]"

Relevance for ccTLDs

The discussions over the definition of DNS abuse are increasingly moving towards content moderation, blurring the line between "technical" abuse and "content" abuse. While registries cannot adequately assess or apply an effective measure towards content abuse, it is evident that there is more pressure to adopt preventive measures when addressing any abuse at DNS level. Several community voices are calling for the adoption of measures without "arguing over statistics and definitions", turning the issue into justification for any policy or contract-change, be it the WHOIS access for third-parties, or new contractual obligations for gTLDs.

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 the champions in keeping their zones secure and free from abuse within the ICANN community. It is notable that the GAC was the one reminding the community and ICANN Org that ccTLDs are not part of ICANN's remit.

Furthermore, it is remarkable how the data accuracy principle enshrined in the GDPR to serve the interests of data subjects is turned on its head to protect the "legitimate interest" of third parties when requesting access to WHOIS in the discussions at ICANN, backed by the PSWG and the GAC. Any interpretation of the European legislation on a global level will put pressure on ccTLDs to align themselves with the global standard, irrespective of national nuances.

ICANN70 will be held on 20-25 March 2021.

CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. CENTR currently counts 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 ICANN69

(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