ICANN | GAC
Governmental Advisory Committee

ICANN 68
VIRTUAL POLICY FORUM
22–25 June 2020

DNS Abuse Mitigation

Sessions 2, 8

Contents

Session Objectives

The GAC will discuss recent developments related to DNS Abuse, in particular in the context of the COVID-19 crisis, in connection with a Cross-Community Plenary session planned on this topic during ICANN68. This session will also be an opportunity to review and discuss relevant developments in the prevention and mitigation of DNS Abuse and Security Threats.

Background

Malicious activity on the Internet threatens and affects domain name registrants and end-users by leveraging vulnerabilities in all aspects of the Internet and DNS ecosystems (protocols, computer systems, personal and commercial transactions, domain registration processes, etc). These nefarious activities can threaten the security, stability and resiliency of DNS infrastructures, and that of the DNS as a whole.

These threats and malicious activities are generally referred to as "DNS Abuse" within the ICANN Community. DNS Abuse is generally understood as including all or part of activities such as Distributed Denial of Service Attacks (DDoS), Spam, Phishing, Malware, Botnets and the distribution of illegal materials. While everyone appears to agree that DNS abuse is an issue and should be addressed, there are differences of opinion as to whose responsibility it should be. Registries and Registrars in particular are concerned about being asked to do more, as this affects their business model and bottom line.

As part of this discussion, it should be noted that even the exact definition of "DNS Abuse" is a subject of debate[1].

Nonetheless, some progress has been made in the past years. Here is a summary of previous efforts undertaken in the ICANN Community to address DNS Abuse, some of which have benefited from GAC involvement:

- ICANN's **Generic Names Supporting Organization (GNSO)** setting up the Registration Abuse Policies Working Group in 2008. It identified a set of specific issues but did not deliver policy outcomes, nor did a subsequent discussion of non-binding best practices for Registries and Registrars (including workshops during ICANN41 and ICANN42).

- **As part of the New gTLD Program,** ICANN Org adoption of a series of new requirements[2] per its memorandum on Mitigating Malicious Conduct (3 October 2009). ICANN's Report on New gTLD Program Safeguards (18 July 2016) assessed their effectiveness in preparation for the bylaws-mandated Competition, Consumer Choice and Consumer Trust (CCT) Review which delivered its recommendations on 8 September 2018.

- Prior to the creation of the GAC's Public Safety Working Group (PSWG), **representatives of Law Enforcement Agencies (LEA)** played a leading role in the negotiation of the 2013 Registrar Accreditation Agreement[3], as well as in the development of GAC Advice related to Security Threats which led to new provisions in the Base New gTLD Agreement that outlined responsibilities of registries. These provisions were later complemented by a non-binding Framework for Registry Operators to Respond to Security Threats (20 October 2017) agreed upon between **ICANN Org, Registries and the GAC PSWG**.

[1] As evidenced during the DNS Abuse and Consumer Safeguards discussion during the GDD Summit (7-8 May 2019).

[2] Vetting registry operators, requiring demonstrated plan for DNSSEC deployment, prohibiting wildcarding, removing orphan glue records when a name server entry is removed from the zone, requiring the maintenance of thick WHOIS records, centralization of zone-file access, requiring documented registry level abuse contacts and procedures

[3] See Law Enforcement Due Diligence Recommendations (Oct. 2019) and the 12 Law Enforcement recommendations (1 March 2012)

- **The Security and Stability Advisory Committee (SSAC)** issued recommendations to the ICANN Community in particular in SAC038: Registrar Abuse Point of Contact (26 February 2009) and SAC040: Measures to Protect Domain Registration Services Against Exploitation or Misuse (19 August 2009).

- **The ICANN Organization,** through its **Security Stability and Resiliency (SSR) Team** regularly train public safety communities and assist in responding to large scale cyber incidents, including through the Expedited Registry Security Request Process (ERSR). Most recently, ICANN's **Office of the CTO** has developed ICANN's Domain Abuse Activity Reporting (DAAR) and produces monthly Abuse Reports. This tool has been actively supported both by the GAC and by a number of Specific Review Teams as a way to create transparency and identify sources of problems, which could then be addressed through compliance or - where needed - new policy.

Issues

Past initiatives have not yet resulted in an effective reduction of DNS abuse; rather, it is clear that much remains to be done. Despite ICANN Community attention and existing industry best practices to mitigate DNS Abuse, GAC-led community engagements as well as the CCT Review's Statistical Analysis of DNS Abuse in gTLDs (9 August 2017), have highlighted persistent trends of abuse, commercial practices conducive to abuse and evidence that there is "*scope for the development and enhancement of current mitigation measures and safeguards*" as well as potential for future policy development[4].

Additionally, concerns with the ability to effectively mitigate DNS Abuse have been heightened in law enforcement, cybersecurity, consumer protection and intellectual protection circles[5] as a consequence of the entry into force of the European Union General Data Protection Regulation (GDPR) and ensuing efforts to change the WHOIS system - a key crime and abuse investigation tool - to comply with the GDPR. More recently, the COVID-19 global health emergency proved an illustration of existing challenges as related domains registrations spiked, including a small percentage[6] in support of various opportunistic fraudulent purposes.

ICANN's Advisory Committees, in particular the GAC, SSAC and ALAC, and various affected third parties have been calling upon ICANN org and the ICANN Community, to take further action[7].

Such further action would require that the ICANN community come to some form of consensus around a number of open questions. Discussions of abuse mitigation and potential policy work in the ICANN Community generally revolve around:

[4] See GAC comment (19 September 2017) on the Final Report of the Statistical Analysis of DNS Abuse in gTLDs.

[5] See Section III.2 and IV.2 in the GAC Barcelona Communiqué (25 October 2018) pointing to surveys of impact on law enforcement in section 5.3.1 of the Draft Report of the RDS Review Team (31 August 2018) and in a publication from the Anti-Phishing and Messaging Malware and Mobile Anti-Abuse Working Groups (18 October 2018)

[6] As reported by Registrar Stakeholder Group leaders to the GAC on 9 April 2020

[7] See DNS Abuse and Consumer Safeguards discussion during the GDD Summit (7-8 May 2019)

- **The definition of DNS Abuse**:
  What constitutes abuse considering the purview of ICANN and its contracts with Registries and Registrars ?
- **The detection and reporting of DNS Abuse (awareness and transparency perspective):**
  How to ensure that DNS Abuse is detected and known to relevant stakeholders, including consumers and Internet users ?
- **Prevention and Mitigation of DNS Abuse (effectiveness perspective)**:
  What tools and procedures can ICANN org, industry actors and interested stakeholders use to reduce the occurence of abuse and respond appropriately when it does occur ? Who is responsible for which parts of the puzzle, and how can different actors best cooperate?

The GAC, in its efforts to improve security and stability for the benefit of Internet users overall, might wish to be actively involved in advancing the discussion on these issues (documented in detail in this briefing) so that progress can be made towards more effective abuse prevention and mitigation.

Leadership Proposal for GAC Action during ICANN68

1. **Review lessons learned** so far **from COVID-19 related DNS Abuse** as reported by concerned parties, including public authorities, registrars, ccTLD Operators and ICANN org (see p, 10 of this briefing), **and prepare for engagement of the ICANN Community as appropriate,** starting with the Cross-Community Plenary Session on DNS Abuse and Malicious Registration During COVID-19 planned on 22 June 2020 as part of ICANN68.

2. **Deliberate on possible next steps for addressing overarching public policy issues related to DNS Abuse** as identified in previous GAC contributions, and **in particular consider following-up** with the GNSO Council, ALAC, ccNSO and possibly the ICANN Board **on possible avenues to address CCT Review Recommendations on DNS Abuse before the launch of subsequent rounds of New gTLDs** consistent with the GAC Montréal Communiqué Advice (6 November 2019).

3. **Discuss the status** of consideration and implementation **of recommendations pertaining to DNS Abuse issued by the CCT and RDS-WHOIS2 Reviews,** in light of ICANN Board Action as reported in:
    a. Board Action Scorecard on CCT Review Recommendations (1 March 2019)
    b. Board Action scorecard on RDS-WHOIS2 Review Recommendations (25 Feb. 2020)

4. **Consider progress of key DNS Abuse Mitigation Efforts more generally, in the ICANN Community** and in particular by Contracted Parties, ccTLD Operators and ICANN org, including with a view to promote elevated standards in practices and contracts:
    a. **Implementation of voluntary measures by gTLD Registrars and Registries** per the industry-led Framework to Address Abuse
    b. **Implementation of proactive anti-abuse measures by ccTLD Operators** that could inform gTLD registry practices
    c. **Contractual Compliance Audit of Registrars** regarding DNS Security Threats which was expected to follow the conclusion of a similar audit of Registries
    d. Improvements of ICANN's Domain Abuse Activity Reporting (DAAR) as previously discussed by Registries, the GAC and SSAC

Relevant Developments

Overview of Recent Developments

- **The COVID-19 crisis has led to engagements between the GAC and affected stakeholders**, which have brought into light various **efforts to respond and coordinate the response** against fraudulent and criminal activities:
    - **The GAC Leadership** reported on a discussion (9 April) requested by leaders of the Registrar Stakeholder Group (RrSG), and discussed the matter further in a joint leadership call (3 June 2020) in preparation for the ICANN68.
    - As part of their response to potentially fraudulent COVID-19 activities, **Registrars** report challenges in assessing fraudulence in relevant jurisdiction and sought assistance from public authorities. The RrSG has documented shared Registrar approaches to the COVID-19 Crisis for the benefit of its membership.
    - **GAC Members have been invited to share relevant resources** put in place by their respective public authorities such as those shared by law enforcement agencies (US FBI, UK NCA, Europol) and consumer protection agencies (US FTC)
    - The **European Commission** reported ongoing efforts in collaboration with EU Members-States, Europol, ccTLD and registrars to facilitate reports, their review and their referral to relevant jurisdiction through the adoption of a standardized form to report domain/content related to COVID-19 and the establishment of single point of contacts for relevant Members States authorities.
    - **Operators of ccTLDs** around the world are due to brief the GAC (4-5 June 2020) on the lessons they learned from their operations during the crisis
    - A brief of the GAC by **ICANN's Office of the CTO** (OCTO) being planned before ICANN68 is expected to illustrate ICANN initiatives and resources dedicated to supporting the contracted parties' response

- In the meantime, **Contracted Parties, ICANN's Security and Stability Advisory Committee (SSAC) and ICANN org have initiated new work** related to addressing Security Threats:
    - As reported by the GAC Public Safety Working Group during ICANN67 meeting, the **Registrar Stakeholder Group** published a Guide to Registrar Abuse Reporting
    - The Framework to Address DNS Abuse (17 October 2019) proposed as a **voluntary initiative by leading stakeholder of the DNS Industry**, now records 56 signatories as of 29 March 2020.
    - The **SSAC** initiated a Working Party on DNS Abuse in which a representative of the PSWG has been invited to take part.
    - **ICANN org**, as part of the implementation of the FY21-25 Strategic Plan, announced the launch of a DNS Security Facilitation Initiative Technical Study Group (6 May 2020) to *"explore ideas around what ICANN can and should be doing to increase the level of collaboration and engagement with DNS ecosystem stakeholders to improve the security profile for the DNS"*. Recommendations are expected by May 2021.

- Since the ICANN66 meeting. several **ICANN community processes have considered new recommendations related to DNS Abuse**, some of which have received GAC input, and some may be subject of GAC follow-up:
    - Following the **RDS-WHOIS2 Review Team** Final Recommendations (3 September 2019) the relevance of which to the mitigation of DNS Abuse was highlighted in a GAC Comment (23 December 2019) were considered by the ICANN Board per the Board Action scorecard (25 February 2020) and as part of its resolutions 2020.02.25.01 – 2020.02.25.06: 15 recommendations were accepted, 4 placed in pending status, 2 passed through to the GNSO and 2 were rejected.
    - **The SSR2 Review Team** delivered a Draft Report (24 January 2020) with a significant focus on measures to prevent and mitigate DNS Abuse. The GAC Comment (3 April 2020) endorsed many of the recommendations and in particular those pertaining to improving Domain Abuse Activity Reporting (DAAR) and the strengthening of compliance mechanisms. Final recommendations of the SSR2 RT are now expected by October 2020 (according to recent deliberations)
    - **The GNSO Policy Development Process Working Group on New gTLD Subsequent Procedures r**ecently reported (29 April 2020) that it is "*not planning to make any recommendations with respect to mitigating domain name abuse other than stating that any such future effort must apply to both existing and new gTLDs (and potentially ccTLDs)".* This is despite relevant recommendations addressed to it by the CCT Review Team, further supported by ICANN Board Action on these recommendations, as well as GAC Montréal Communiqué Advice (6 November 2019) and further GAC input as recorded in the GAC ICANN67 Communiqué (16 March 2020). A recent GNSO Council meeting (21 March 2020) discussed the possibility of initiating a Cross Community Working Group (CCWG) and possibly a subsequent GNSO PDP should new contractual requirements be needed. It did not discuss an informal proposal by the GAC Leadership (12 May 2020) to consider a Birds of a feather discussion among relevant experts, including ccTLD operators, to scope any future policy effort.

Issues - Definition of DNS Abuse

As highlighted most recently during the GDD Summit (7-9 May 2019), there is **no Community-wide agreement on what constitutes 'DNS Abuse'**, in part due to concerns of some stakeholders with ICANN overstepping its mandate, impacts on the rights of users, and impact on the bottom line of contracted parties.[8]

There is, however, according the CCT Review Team, a **consensus on what constitutes 'DNS Security Abuse' or 'DNS Security Abuse of DNS infrastructure'** understood as including "*more technical forms of malicious activity*", such as malware, phishing, and botnets, as well a spam "*when used as a delivery method for other forms of abuse.*" [9]

Recently, **the ICANN Contractual Compliance Department has referred to 'Abuse of DNS Infrastructure' and 'Security Threats'** in its communications about audits of Registries and Registrars regarding their implementation of contractual provisions in the New gTLD Registry Agreement (Specification 11 3b) regarding "*security threats such as pharming, phishing, malware, and botnets*"[10] - and in the Registrar Accreditation Agreement (Section 3.18) - which refers to "*abuse contacts*" and "*abuse reports*" without providing a definition of the term 'abuse' specifically, but including 'Illegal Activity" within its scope.

From a GAC perspective, the definition of 'Security Threats' in the New gTLD Registry Agreement is in fact the transcription of the **definition given in the 'Security Checks' GAC Safeguards Advice** applicable to all New gTLDs in the Beijing Communiqué (11 April 2013).

Following the Board resolution (1 March 2019) directing ICANN org to "*facilitat[e] community efforts to develop a definition of 'abuse' to inform further action on this recommendation.*"[11], and building activities of the Consumer Safeguards function of ICANN org, **further discussions on the definition of abuse are expected before and during the ICANN66 meeting** in Montreal.

In particular, during a pre-ICANN66 webinar on 15 October 2019 **PSWG and Contracted Parties discussed current issues and industry practices**. In preparation for this webinar, the Registry Stakeholder Group had issued an Open Letter (19 August 2019) discussing the registries views on the definition of DNS Abuse, the limited options registries have to take action on security threats and theirs concerns with ICANN's Domain Abuse Activity Reporting. In response, the GAC issued a Statement on DNS Abuse (18 September), as well as the Business Constituency (28 October).

---

[8] Indeed, the definition of Abuse Mitigation may carry consequences in terms of the scope of activity overseen by ICANN policies and contracts. While governments and other stakeholders are concerned with the impact of DNS abuse on the public interest, including the safety of the public and the infringement of intellectual property rights, registries and registrars are concerned with restrictions on their commercial activities, ability to compete, increased operating costs and liability for consequences registrants may incur when action is taken on abusive domains. Non-commercial stakeholders on their part are concerned with the infringement of freedom of speech and privacy rights of registrants and Internet users, and share with contracted parties concerns about ICANN overstepping its mission.

[9] See p.88 of the CCT Review Final Report (8 September 2018) as highlighted more recently in the GAC Statement on DNS Abuse (18 September 2019)

[10] The Advisory, New gTLD Registry Agreement Specification 11 (3)(b) (8 June 2017) provides a definition of 'Security Threats' as including "*pharming, phishing, malware, botnets, and other types of security threats.*"

[11] See p.5 of scorecard of Board Action on the Final CCT Recommendations

Issues - Awareness and Transparency: Community Engagements on DNS Abuse

The GAC and its Public Safety Working Group (PSWG) have led several Cross-Community engagements at ICANN meetings over the past few years **seeking to raise awareness and explore solutions with relevant experts**. More recently, leaders of ICANN's Supporting Organizations and Advisory Committee (SO/AC), and the ALAC held well attended engagements on the matter.

- During ICANN57 in Hyderabad (5 November 2016), the GAC PSWG led a High Interest Topic session on Mitigation of Abuse in gTLDs which was designed as an exchange of views across the ICANN Community and highlighted:
  - the lack of a shared understanding of what constitute DNS Abuse;
  - the diversity of business models, practices and skills influencing approaches to mitigating abuse; and
  - the need for more industry-wide cooperation, to be supported by shared data on security threats.

- During ICANN58 in Copenhagen (13 March 2017), the GAC PSWG moderated a Cross Community Session Towards Effective DNS Abuse Mitigation: Prevention, Mitigation & Response which discussed recent trends in DNS Abuse, in particular Phishing, as well as behavior such as domain hopping across registrars and TLDs which may require more coordinated and sophisticated responses from the industry. The session also served to highlight:
  - the emerging Domain Abuse Activity Reporting (DAAR) initiative,
  - ongoing collaboration between ICANN org Contractual Compliance and SSR functions, and
  - the opportunity of leveraging New gTLD auction proceeds to fund the needs of Abuse mitigation

- During ICANN60 in Abu Dhabi (30 October 2017), the PSWG hosted a Cross Community Session on Reporting of DNS Abuse for Fact-Based Policy Making and Effective Mitigation to discuss the establishment of reliable, public and actionable DNS Abuse reporting mechanisms for the prevention and mitigation of abuse, and to enable evidence-based policy making. The session confirmed the need for publication of reliable and detailed data on DNS Abuse, as contained in the Domain Abuse Activity Reporting (DAAR) tool. The PSWG considered further developing possible GAC principles[12].

- During ICANN66 in Montreal (6 November 2019), the ICANN Community held a Cross-Community Plenary Session on DNS Abuse. This session led to a call to action and identified several items for follow-up:
  - A call for registries and registrars to sign the Framework to Address Abuse

[12] See Attachment 1:Abuse Mitigation Principles in ICANN60 GAC Briefing on DNS Abuse and report of the session in the GAC Abu Dhabi Communiqué (p.3)

    - Work needed around creating a definition of DNS abuse from an ICANN perspective
        - Some speakers reiterated the need to be clear about the line between technical DNS abuse vs content abuse
        - Presentations highlighted language from Specification 11.3.b of the Base Registry Agreement, GAC advice, DAAR activity and CCT Review Team proposals
    - General agreement that ICANN is a suitable environment for sharing best practices
        - May need to develop improvements for identifying and contact those responsible for contact hosting and registrants
        - And to have appropriate appeal mechanisms in place for takedowns
        - There was some discussion (but no specific agreement) around incentives
    - General agreement that the community can help ICANN's Compliance Team be more effective (e.g. enforcing contracts where there is behavior that the community finds unacceptable).

- During the ICANN67 Virtual Meeting (9 March 2020), the ALAC held two sessions attended remotely by many participants of the ICANN Community, one providing an introduction DNS Abuse (including an educational video) and one reviewing in practice Contractual Compliance enforcement in response to typical DNS Abuse cases

- During the ICANN68 Virtual Meeting (22 June 2020), the ICANN Community is due to meet in plenary to follow-up on the ICANN66 discussion and specifically review stakeholders experience of the COVID-19 registration spike and associated DNS Abuse, fraud and cybercrime.
  Reports and lessons learned are expected to be consistent with pre-ICANN68 briefings on this matter given by ccTLD Operators (4-5 June 2020), by gTLD Registries and Registrars (11 June 2020), and by ICANN's Office of the CTO (12 June 2020)

Issues - Awareness and Transparency: DNS Abuse Studies

A number of DNS Abuse safeguards were built into the New gTLD Program through new requirements[13] adopted by ICANN org per its memorandum on Mitigating Malicious Conduct (3 October 2009) and GAC Safeguard Advice on Security Checks.

Building on ICANN org's assessment of the effectiveness of these New gTLD Program Safeguards (18 July 2016), to which the GAC had contributed (20 May 2016), the CCT Review Team sought a more comprehensive comparative analysis of abuse rates in new and legacy gTLDs, including statistical inferential analysis of hypotheses such as the correlations between domain name retail pricing and abuse rates.

The findings of this Statistical Analysis of DNS Abuse in gTLDs (9 August 2017) were submitted for Public Comment. Community contributions were reported (13 October 2017) as constructive, welcoming the scientific rigor of the analysis and calling for further such studies to be conducted.

In its comments (19 September 2017), the GAC highlighted, among other conclusions, that:

- The study made clear that there are significant abuse issues in the DNS:
    - In certain new gTLDs, over 50% of registrations are abusive
    - Five new gTLDs accounted for 58.7% of all of the blacklisted phishing domains in new gTLDs
- Abuse correlates with policies of Registry Operators:
    - Registry operators of the most abused new gTLDs compete on price;
    - Bad actors prefer to register domains in standard new gTLDs (open for public registration), rather than in community new gTLDs (restrictions on who can register domain names)
- There is potential for future policy development regarding:
    - Subsequent rounds of new gTLDs, in connection with evidence that risk varies with categories of TLDs, in addition to strictness of registration policy
    - The enhancement of current mitigation measures and safeguards against abuse, as informed by such statistical analysis
- ICANN should continue and expand upon the use of statistical analysis and data to measure and share information with the community information about levels of DNS abuse.

On 17 October 2019, a study of Criminal Abuse of Domain Names Bulk Registration and Contact Information Access was released by a consultancy (Interisle Consulting Group) which has direct relevance to ongoing community discussions and explored:

- How cybercriminals take advantage of bulk registration services to "weaponize" large numbers of domain names for their attacks.
- Effects of ICANN's interim policy redacting Whois point of contact information to comply with the GDPR on cybercrime investigations
- Policy recommendations for ICANN org and community considerations

[13] Vetting registry operators, requiring demonstrated plan for DNSSEC deployment, prohibiting wildcarding, removing orphan glue records when a name server entry is removed from the zone, requiring the maintenance of thick WHOIS records, centralization of zone-file access, requiring documented registry level abuse contacts and procedures

Issues - Awareness and Transparency: Domain Abuse Activity Reporting (DAAR)

ICANN org's Domain Abuse Activity Reporting Project emerged as a research project concurrently to the GAC and PSWG engagement of the ICANN Board and Community on the effectiveness of DNS Abuse mitigation, between the ICANN57 (Nov. 2016) and ICANN60 meetings (Nov. 2017).[14]

The stated purpose of DAAR is to "*report security threat activity to the ICANN community, which can then use the data to facilitate informed policy decisions*". This is achieved since January 2018 by the publication of monthly reports, based on the compilation of TLD registration data with information from a large set of high-confidence reputation and security threat data feeds.[15]

As such, DAAR is contributing to the requirement identified by the GAC for publication of "*reliable and detailed data on DNS Abuse*" in the GAC Abu Dhabi Communiqué (1 November 2017). However, as highlighted in a letter from the M3AAWG[16] to ICANN org (5 April 2019), by not including security threat information on a per registrar per TLD basis, DAAR is still falling short of expectation from the GAC PSWG Members and their cybersecurity partners that it provides actionable information.

Recently, registries reported in an Open Letter (19 August 2019) interacting with ICANN's Office of the CTO "*to analyze DAAR with a view to recommending enhancements to OCTO to ensure DAAR better serves its intended purpose and provides the ICANN community with a valuable resource*". While registries recognized that "*some members of the community may rely on data provided in ICANN's Domain Abuse Activity Reporting - or DAAR - to support claims of systemic or widespread DNS Abuse*" they believe that "*the tool has significant limitations, cannot be relied upon to accurately and reliably report evidence of security threats, and does not yet achieve its objectives*".

Issues - Effectiveness: Current DNS Abuse Safeguards in Registries and Registrars Contracts

Building on the Law Enforcement Due Diligence Recommendations (October 2009), the GAC sought the **inclusion of DNS Abuse Mitigation Safeguards in ICANN's contracts** with Registries and Registrars:

- The 2013 Registrar Accreditation Agreement (17 September 2013) was approved by the ICANN Board (27 June 2013) after the inclusion of provisions addressing the 12 Law Enforcement recommendations (1 March 2012)
- The New gTLD Registry Agreement was approved by the ICANN Board (2 July 2013) after the inclusion of provisions in line with the GAC Safeguards Advice in the Beijing Communiqué (11 April 2013), consistent with the ICANN Board Proposal for Implementation of GAC Safeguards Applicable to All New gTLDs (19 June 2013)

[14] See cross-community sessions led by the GAC PSWG during ICANN57 (Nov. 2016), ICANN58 (March 2017) and ICANN60 (October 2017), as well as questions to the ICANN Board regarding the effectiveness of DNS Abuse Safeguards in Hyderabad Communiqué (8 November 2016), follow-up questions in the GAC Copenhagen Communiqué (15 March 2017) and a set of draft responses (30 May 2017) by ICANN org.

[15] For more information, see https://www.icann.org/octo-ssr/daar-faqs

[16] Messaging, Malware and Mobile Anti-Abuse Working Group

After the first few years of operations of New gTLDs, during the ICANN57 meeting, **the GAC identified a number of provisions and related safeguards for which it could not assess effectiveness**. As a consequence, in its Hyderabad Communiqué (8 November 2016) the GAC sought clarifications on their implementation from the ICANN Board. This led to a dialogue between the GAC and the ICANN org, follow-up questions in the GAC Copenhagen Communiqué (15 March 2017) and a set of draft responses (30 May 2017) which were discussed in a conference call between the GAC and the ICANN CEO (15 June 2017). A number of questions remained open and new questions were identified as reflected in a subsequent working document (17 July 2017).

Among the outstanding topics of interest to the GAC, an Advisory, New gTLD Registry Agreement Specification 11 (3)(b) was published on 8 June 2017 in response to questions from some registry operators seeking guidance on how to ensure compliance with Section 3b of Specification 11 of the New gTLD Registry Agreement. **The Advisory offers one voluntary approach registry operators may adopt** to perform technical analyses to assess security threats and produce statistical reports as required by Specification 11 3(b).

As part of regular **audits conducted by the ICANN Contractual Department**, a targeted audit of 20 gTLDs on their "*process, procedures, and handling of DNS infrastructure*", between March and September 2018, revealed that "*there were incomplete analyses and security reports for 13 top-level domains (TLDs), as well as a lack of standardized or documented abuse handling procedures and no action being taken on identified threats.*"[17] Shortly thereafter, in November 2018, a DNS Infrastructure Abuse Audit of nearly all gTLDs was launched to "*ensure that the contracted parties uphold their contractual obligations with respect to DNS infrastructure abuse and security threats*". In its report of the latest audit (17 September 2019), ICANN concluded that:

- the vast majority of registry operators are committed to addressing DNS security threats.
- The prevalence of DNS security threats is concentrated in a relatively small number of registry operators.
- Some Registry Operators interpret the contractual language of Specification 11 3(b) in a way that makes it difficult to form a judgment as to whether their efforts to mitigate DNS security threats are compliant and effective.

Contacted parties have taken issue with these audits as exceeding the scope of their contractual obligations.[18] ICANN org indicated that it will initiate an audit of registrars focusing on DNS security threats.

[17] As reported in the blog post of 8 November 2018, Contractual Compliance: Addressing DNS Infrastructure Abuse: https://www.icann.org/news/blog/contractual-compliance-addressing-domain-name-system-dns-infrastructure-abuse

[18] See correspondence from the RySG (2 November 2019) to which ICANN org responded (8 November), and in comments posted on the announcement page (15 November): registries have taken issues with the audit questions as threatening enforcement action exceeding the scope of their contractual obligations [in particular underSpecification 11 3b] and indicated their reluctance to "*share with ICANN org and the community relevant information regarding our ongoing efforts to combat DNS Abuse […] as part of an ICANN Compliance effort that goes beyond what is allowed under the Registry Agreement*"

Effectiveness: Non-Binding Framework for Registries to Respond to Security Threats

As part of the New gTLD Program, the ICANN Board resolved (25 June 2013) to include the so-called "security checks" (Beijing Communiqué GAC Safeguards Advice) into Specification 11 of the New gTLD Registry Agreement. However, because it determined that these provisions lacked implementation details, it decided to solicit community participation to develop a framework for "*Registry Operators to respond to identified security risks that pose an actual risk of harm (…)"*. In July 2015, ICANN formed a Drafting Team composed of volunteers from Registries, Registrars and the GAC (including members of the PSWG) who developed the Framework for Registry Operator to Respond to Security Threats published on 20 October 2017, after undergoing public comment.

This framework is a voluntary and non-binding instrument designed to articulate guidance as to the ways registries may respond to identified security threats, including reports from Law Enforcement. It introduces a 24h maximum window for responding to High Priority requests (imminent threat to human life, critical infrastructure or child exploitation) from "*legitimate and credible origin*" such as a "*national law enforcement authority or public safety agency of suitable jurisdiction"*.

Per its recommendation 19, the CCT Review Team deferred the task of conducting an assessment of the effectiveness of the Framework to a subsequent review[19] as the Framework had not been in existence for a long enough period of time to assess its effectiveness.

Effectiveness: Proactive Measures and Prevention of Systemic Abuse

Based on its analysis of the DNS Abuse landscape,[20] including consideration of ICANN's Report on New gTLD Program Safeguards (15 March 2016) and the independent Statistical Analysis of DNS Abuse (9 August 2017), the CCT Review Team recommended, in relation to DNS Abuse:

- The inclusion of **provisions in Registry Agreements to incentivize the adoption of proactive anti-abuse measures** (Recommendation 14)
- The inclusion of contractual provisions aimed at **preventing systemic use of specific registrars or registries** for DNS Security Abuse, including thresholds of abuse at which compliance inquiries are automatically triggered and consider a possible DNS Abuse Dispute Resolution Policy (DADRP) if the community determines that ICANN org itself is ill-suited or unable to enforce such provisions (Recommendation 15)

The ICANN Board resolved (1 March 2019) to place these recommendations in "Pending" Status, as it directed ICANN org to "*facilitat[e] community efforts to develop a definition of 'abuse' to inform further action on this recommendation.*"[21]

---

[19] CCT Review recommendation 19: *The next CCT should review the "Framework for Registry Operator to Respond to Security Threats" and assess whether the framework is a sufficiently clear and effective mechanism to mitigate abuse by providing for systemic and specified actions in response to security threats*

[20] See Section 9 on Safeguards (p.88) in the CCT REview Final Report (8 September 2018)

[21] See p.5 of scorecard of Board Action on the Final CCT Recommendations

Current Positions

The current positions of the GAC are listed below in reverse chronological order:

- GAC Comment (3 April 2020) on the SSR2 Review Team Draft Report
- GAC Comment (23 December 2019) on the RDS-WHOIS2 Review Final Recommendations
- GAC Statement on DNS Abuse (18 September 2019)
- GAC Comment (11 December 2018) on the CCT Review Final Recommendations
- GAC Comment (16 January 2018) on New Sections of the CCT Review Team Draft Report (27 November 2017)
- GAC Comment on the Statistical Analysis of DNS Abuse in gTLDs (19 September 2017)
- GAC Comment on SADAG Initial Report (21 May 2016)
- GAC Barcelona Communiqué (25 October 2018) in particular sections III.2 GAC Public Safety Working Group (p.3) and IV.2 WHOIS and Data Protection Legislation (p.5)
- GAC Copenhagen Communiqué (15 March 2017) including Abuse Mitigation Advice requesting responses to the GAC Follow-up Scorecard to Annex 1 of GAC Hyderabad Communiqué (pp. 11-32)
- GAC Hyderabad Communiqué (8 November 2016) including Abuse Mitigation Advice requesting responses to Annex 1 - Questions to the ICANN Board on DNS Abuse Mitigation by ICANN and Contracted Parties (pp.14-17)
- GAC Beijing Communiqué (11 April 2013), in particular the 'Security Checks' Safeguards Applicable to all NewgTLDs (p.7)
- GAC Dakar Communiqué (27 Octobre 2011) section III. Law Enforcement (LEA) Recommendations
- GAC Nairobi Communiqué (10 March 2010) section VI. Law Enforcement Due Diligence Recommendations
- LEA Recommendations Regarding Amendments to the Registrar Agreement (1 March 2012)
- Law Enforcement Due Diligence Recommendations (Oct. 2009)

Key Reference Documents

- Scorecard of ICANN Board Action on the Final RDS-WHOIS2 Review Recommendations (25 February 2020)
- Scorecard of ICANN Board Action on the Final CCT Recommendations (1 March 2019)
- CCT Review Final Report and Recommendations (8 September 2018), in particular Section 9 on Safeguards (p.88)
- Statistical Analysis of DNS Abuse in gTLDs (9 August 2017)

- GAC Questions on Abuse Mitigation and ICANN Draft Answers (30 May 2017) per Advice in the GAC Hyderabad Communiqué (8 November 2016) and Follow-up in GAC Copenhagen Communiqué (15 March 2017)

Document Administration

Meeting	ICANN68 Virtual Policy Forum, 22-25 June 2020
Title	DNS Abuse Mitigation
Distribution	GAC Members (before meeting) and Public (after meeting)

Distribution Date	Version 2: 18 June 2020 (edits highlighted)