ICANN | GAC
Governmental Advisory Committee

ICANN 65
POLICY FORUM
MARRAKECH
24–27 June 2019

DNS Abuse Mitigation

Session 5.1

Contents

Session Objectives

- Review recent developments and discussions regarding the definition, detection and mitigation of DNS Abuse as well as the impact of WHOIS compliance with GDPR efforts.
- Discuss positions and possible next steps for the GAC's Public Safety Working Group (PSWG) and the GAC.

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 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) asssed their effectiveness in preparation for the bylaw-mandated Review (CCT Review).

- Prior to the creation of the GAC's Public Safety Working Group (PSWG), **representatives of Law Enforcement Agencies (LEA)** took 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) negotiated between **ICANN Org, Registries and the 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)** issuing 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 led the Domain Abuse Activity Reporting (DAAR) project which 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

The 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), which 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.

In this context, ICANN's Advisory Committees, in particular the GAC, SSAC and ALAC, and various affected third parties have called upon ICANN org and the ICANN Community, to take further action[6].

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 if 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] 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 so that progress can be made towards more effective abuse prevention and mitigation.

Leadership Proposal for GAC Action

During the ICANN65 meeting in Marrakech, the GAC may wish to:

1. **Call for a process to clarify what constitutes DNS Abuse** in relation to ICANN's mission, and establish its own position on the issue. This would be helpful to advance ongoing discussions in the ICANN Community regarding the existence of such a definition, the CCT Review Team's recommendations on DNS Abuse, their consideration by the ICANN Board, as well as ongoing initiatives of ICANN's Consumer Safeguards function**.**

2. **Consider the need and opportunity for policy development**, in connection with recent discussion of such a possibility during the GDD Summit[7], and noting prior positions taken by the GAC on this matter[8].

3. **Review actions taken on CCT Review Recommendations** related to DNS Abuse (Recommendations 14 to 19), including their consideration by the ICANN Board and the work it directed to the ICANN Org, as well as further consideration by relevant ICANN constituencies and processes.

4. **Consider showcasing industry best practices in the ccTLD namespace,** such as that of .DK presented during ICANN64[9], and their application to the gTLD industry.

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

[8] In particular, in its comment (19 September 2017) on the Final Report of the Statistical Analysis of DNS Abuse in gTLDs, the GAC noted that

- *"The DNS Abuse Study briefly references a finding that certain URLs are used more extensively to distribute child abuse material [...] It would be helpful if the report could more clearly explain, elaborate, and/or quantify this statement so that stakeholders can understand to what extent the study examined this issue as well as to inform any potential future policy considerations"*
- *"The correlations drawn between stricter registration policies and fewer abuse counts suggest potential areas for future policy development."*
- *"the use of statistical analysis should inform future policies on DNS abuse and further analysis should be done to consider how this information could bolster the efforts by ICANN and its contract compliance and security teams to effectively respond to DNS abuse and better prevent future and repeat abuses."*

[9] See Session Lessons Learned: How .DK successfully reduced abusive domains (13 March 2019) and subsequent discussion by the PSWG (17 April 2019)

Relevant Developments

Definition of DNS Abuse: Consensus on Infrastructure 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.[10]

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."* [11]

Recently, **the ICANN Contractual Compliance Department has referred to 'Abuse of DNS Infrastructure'** in its communications about audits of Registries and Registrars regarding their implementation of contractual provisions in the New gTLD Registry Agreement (Specification 11 3b) - which refers to "*security threats such as pharming, phishing, malware, and botnets*"[12] - 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 exact 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."*[13], and building activities of the Consumer Safeguards function of ICANN org, **further discussions on the definition of abuse are expected by the ICANN66 meeting** in Montreal (2-7 Nov. 2019).

[10] 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.

[11] See p.88 of the CCT Review Final Report (8 September 2018)

[12] 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.*"

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

Definition of DNS Abuse: Consumer Safeguards Dialogue

Since the extension of ICANN's Contractual Compliance function to include Consumer Safeguards in 2017,[14] the GAC engaged in several related developments:

- An introduction of ICANN's Consumer Safeguards Director (27 June 2017) which discussed the establishment of an informal community-wide discussion to build awareness and community understanding, and identify ways for the ICANN organization to strengthen its performance of the Contractual Compliance and Consumer Safeguards functions.

- A webinar discussion on Contractual Compliance and Consumer Safeguards (25 September 2017), attended by nearly 100 community members, including the discussion of a Summary of Safeguards under ICANN's remit (11 September 2017) and followed by the submission of questions for Community input in a subsequent blog (11 October 2017):
  - What should ICANN's role be in addressing DNS abuse?
  - Are there gaps between DNS abuse and ICANN's authority to address that abuse?
  - What additional tools or data would be helpful in assessing DNS abuse?
  - Are there areas where voluntary measures could be helpful?
  - How should ICANN collaborate with other stakeholders addressing abuse?
  - Is there a threat of governmental intervention if the ICANN community cannot satisfactorily address DNS abuse?

- A meeting of Community representatives in Washington DC (11 January 2019) was organized to further discuss these matters towards future possible community-wide engagement at ICANN meetings

More recently, during the GDD Summit (9 May 2019), the Contractual Compliance and Consumer Safeguards department led a session to continue the ongoing dialogue:

- **Some contracted parties consider their voluntary anti-abuse practices appropriate and oppose their becoming obligations**, in part due to the limitation on ICANN's remit as well as the burden that unactionable reports of abuse represent (often submitted by parties uninformed on the limited scope of mitigations available to Registries[15] and Registrars).
- Other representatives suggested **ICANN has a duty to set rules and appropriate incentives** to discourage bad actors while not harming responsible actors (**'polluter-payer' principle**) and that **parties responsible for abuse should be named** in relevant ICANN reports.
- **ICANN org introduced the idea of a GNSO Policy Development Process** to align contracts with expectations of Advisory Committees and third parties, as well as to prevent the impact of future heterogeneous legislations that could be put in place in lieu of ICANN policy.

[14] with the hiring of ICANN's Consumer Safeguards Director (23 May 2017) tasked to "*raising awareness of ICANN's current safeguards, facilitate discussion across stakeholders concerning additional ways ICANN could potentially improve its safeguard mechanisms*"

[15] See for instance the *Categories of Actions by Registries in Response to Security Threats* in the voluntary Framework for Registry Operator to Respond to Security Threats

- This suggestion was met with **strong opposition and calls for alternative ways to tackle the problem**, including reconciling existing definitions in relevant parts of the community or entering into Registry Agreement negotiations similarly to what was done for the 2013 RAA.
- **Contracted parties** requested that **ICANN org facilitates efforts to educate the ICANN Community** on their behalf during ICANN66 in Montreal, including a presentation of best practices and providing data showing the prevalence of non-actionable complaints.

Awareness and Transparency: GAC-led Community Engagement

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**, most notably:

- 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[16].

Awareness and Transparency: DNS Abuse Studies

A number of DNS Abuse safeguards were built into the New gTLD Program through new requirements[17] 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.

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

[16] 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)

[17] 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

DNS Abuse mitigation, between the ICANN57 (Nov. 2016) and ICANN60 meetings (Nov. 2017).[18]

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.[19]

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 recent letter from the M3AAWG[20] 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.

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)

After the first few years of operations of New gTLDs, during the ICANN57 meeting (November 2016) **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

[18] 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.

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

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

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.*"[21]
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*". As reported during the GDD Summit (9 May 2019), ICANN Org is due to release the final report of this Audit (originally planned for May 2019) and is currently planning to initiate a similar audit of Registrars starting in July 2019.

Contacted parties have taken issue with these audits as exceeding the scope of their contractual obligations.[22] Registry and Registrar Stakeholder Groups are **understood to be working with ICANN org's Contractual Compliance department** to ensure that the final report of the Registries DNS Infrastructure Audit does not lack clarity in terms of ICANN's remit (out of concerns that it may lead to community calls for the initiation of a Policy Development Process), and that concerns of Registrars are taken into account before the start of their audit.

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

[21] 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

[22] 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*"

credible origin such as a government 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[23] 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,[24] 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."*[25]

Current Positions

- GAC Nairobi Communiqué (10 March 2010) section VI. Law Enforcement Due Diligence Recommendations
- GAC Dakar Communiqué (27 Octobre 2011) section III. Law Enforcement (LEA) Recommendations
- GAC Beijing Communiqué (11 April 2013), in particular the 'Security Checks' Safeguards Applicable to all NewgTLDs (p.7)
- 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)

[23] 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*

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

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

- 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 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 Comment on SADAG Initial Report (21 May 2016)
- GAC Comment on the Statistical Analysis of DNS Abuse in gTLDs (19 September 2017)
- GAC Comment on the CCT Review Final Report and Recommendations (11 December 2018)

Key Reference Documents

- Law Enforcement Due Diligence Recommendations (Oct. 2019)
- LEA Recommendations Regarding Amendments to the Registrar Agreement (1 March 2012)
- 'Security Checks' GAC Safeguard Advice applicable to All New gTLDs (p.7) in Beijing Communiqué (11 April 2013)
- 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)
- Statistical Analysis of DNS Abuse in gTLDs (9 August 2017)
- GAC Comment on the Statistical Analysis of DNS Abuse in gTLDs (19 September 2017)
- GAC Comment (16 January 2018) on New Sections of the CCT Review Team Draft Report (27 November 2017)
- CCT Review Final Report and Recommendations (8 September 2018), in particular Section 9 on Safeguards (p.88)
- GAC Comment on the CCT Review Final Report and Recommendations (11 December 2018)
- ICANN Board Scorecard of Action on the Final CCT Recommendations (1 March 2019)

Related Information

- ICANN65 GAC Session 11.1 on ICANN Reviews (including relevant briefing on the status of Implementation of the CCT Review Recommendations)
- ICANN65 GAC Session 8.1 on WHOIS and Data Protection Policy
- ICANN65 GAC Session 4.1 on New gTLDs Subsequent Procedures PDP

Document Administration

Meeting	ICANN65 Marrakech, 24-27 June 2019
Title	DNS Abuse Mitigation

Distribution	GAC Members and Public (after meeting)
Distribution Date	Version 2: 17 June 2019