NETBEACON INSTITUTE

GAC Communiqués and Community Activity on DNS Abuse

June 2024

Contents

Background

This report is published by the NetBeacon Institute ("The Institute").[1] Established in 2021 by Public Interest Registry, the registry operator for the .ORG top-level domain, the institute was founded to advance PIR's non-profit mission. Initially launched as the DNS Abuse Institute, it was rebranded as the NetBeacon Institute in May 2024, continuing its mission to combat DNS Abuse..

The institute works to reduce DNS Abuse by fostering collaboration, establishing best practices, and developing open, industry-wide solutions offered at no cost. DNS Abuse encompasses five key 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 other forms of DNS Abuse). This definition, adopted from the work of the Internet and Jurisdiction Policy Network (I&JPN), a multistakeholder organization that addresses the challenges between the cross-border Internet and national jurisdictions, and is also used in ICANN's contracts with accredited registries and registrars.

The Institute's work is closely aligned with the efforts of the Internet Corporation for Assigned Names and Numbers (ICANN), whose mission is to help ensure a stable, secure, and unified global Internet. ICANN operates a multistakeholder model and creates community-developed policies to facilitate the use of the Internet's systems unique identifiers, which includes domain names. As part of this process, exists the Governmental Advisory Committee ("GAC").[2]

The GAC, an Advisory Committee within ICANN, consists of representatives from governments of Member States and Territories, along with Observer Organizations, as established under the ICANN ByLaws. It advises ICANN on public policy matters related to the Internet Domain Name System (DNS). The typical format for this input is in a GAC Communiqués, these are produced following each numbered ICANN meeting and include formal advice to the ICANN Board as well as the identification of important issues. While the ICANN Board is obligated to respond to formal advice, it is not obligated to respond to issues of importance. Most of the references to DNS Abuse contained in GAC Communiqués are issues of importance rather than formal advice and as such they did not require a formal response from the ICANN Board. The response of the ICANN Board to formal advice is tracked by ICANN, and GAC advice is itemized on the GAC website.

GAC membership is composed of national governments and distinct economies recognized in international fora. Multinational governmental and treaty organizations, as well as public

[1] https://netbeacon.org/
[2] https://gac.icann.org/

authorities (including all the UN agencies with a direct interest in global Internet governance such as the ITU, UNESCO, and WIPO) are usually permitted participation in an observational capacity.[3]

This report aims to map out references to DNS Abuse, particularly points of interest and action statements, made in GAC Communiqués from 2016 to June 2024 to relevant DNS community initiatives, including those undertaken by the Institute.

This report is designed for use by the ICANN community, and interested parties, to improve their understanding of the active steps the DNS community is taking to combat DNS Abuse, the progress on GAC's recommendations, and where further work is needed. To illustrate this, we are presenting "issues of importance" identified by the GAC, then relating them to relevant community initiatives. We also identify current gaps, where the Institute believes additional attention is needed.

These issues have been categorized into four main themes: (1) implementing new DNS Abuse obligations, (2) enhanced reporting, (3) work on compromised and malicious registrations, and (4) measurement and clarification of standards. These issues are frequently raised in other ICANN forums, including The Security and Stability Advisory Committee (SSAC) and The Generic Names Supporting Organization (GNSO). The report includes an appendix that summarizes the references to identified DNS Abuse.

The Institute is committed to continuing its work and looks forward to continuing work to combat DNS Abuse alongside members of the DNS community, including GAC members. We welcome feedback on this report and encourage the community to share with us any additional DNS Abuse initiatives.

GAC on DNS Abuse and Community Responses

1. Implementation of new DNS Abuse Obligations

GAC Communiqués

> "The creation of effective and enforceable requirements for registrars and registries to disrupt or mitigate DNS abuse will represent a positive and concrete first step in addressing [DNS Abuse] at ICANN" (ICANN76, 2023).[4]

[3] https://gac.icann.org/work-products/public/fact-sheets-igf-ist.pdf
[4] https://gac.icann.org/contentMigrated/icann76-cancun-communique?language_id=1

This goal and its related actions aim to address a common complaint that ICANN lacked a comprehensive enforcement mechanism, as the Registrar Accreditation Agreement (RAA) and the Registry Agreement (RA) did not include clear requirements to mitigate DNS Abuse. The GAC specifically emphasized the need for more detailed contract provisions: “Improved contract provisions could focus on the reporting and handling of DNS Abuse and enforcement of related contract requirements" (ICANN74, 2022).[5] The GAC further noted that “[t]he following would assist in developing such contract provisions: abuse reporting at the registrar and registry level; more detailed breakdowns of the types of DNS Abuse measured; and availability of raw aggregated data” (ICANN74, 2022). This builds on the GAC’s 2016 Advice to the ICANN Board, which requested details on various issues, including ICANN’s diligence regarding , Section 3.18 pertaining to ‘Registrar's Abuse Contact and Duty to Investigate Reports of Abuse’ in the 2013 Registrar Accreditation Agreement (ICANN57, 2016).[6] ICANN responded to this request.[7]

In 2023, the GAC expressed its support for contract negotiations between ICANN and the Contracted Parties, which aimed to strengthen existing DNS Abuse obligations and promote further progress (ICANN76, 2023).[8] These contract negotiations were expected to mandate that Contracted Parties address DNS Abuse. The increased clarity and depth of ICANN compliance obligations would allow ICANN the ability to facilitate negotiations and discussions with Contracted Parties to address concerns of not adequately mitigating and disrupting abuses. “The GAC. . . encourages the Contracted Parties and ICANN to further consider, inter alia, proactive measures as well as positive incentives for registries and registrars in future work on DNS abuse mitigation or disruption” (ICANN76, 2023). The GAC welcomed the clarification that ICANN Compliance would be able to “suspend or revoke the agreement with the contracted party” in case of non-compliance (ICANN77, 2023).[9]

After negotiations concluded, the GAC actively encouraged Contracted Parties to adopt the DNS Abuse amendments and expressed its intention to engage with the community on the implementation of the amendments (ICANN78, 2023).[10] In 2024, the GAC received updates from ICANN Compliance regarding enforcement of the amendments and expects the assessment of their impact to be resolved before the next round of gTLD applications (ICANN79, 2024).[11] The

[5] https://gac.icann.org/contentMigrated/icann74-the-hague-communique?language_id=1
[6] https://gac.icann.org/contentMigrated/icann57-hyderabad-communique?language_id=1
[7] https://gac.icann.org/advice/correspondence/incoming/Marby-to-Schneider-with-Enclosure-8Feb2017.pdf
[8] https://gac.icann.org/contentMigrated/icann76-cancun-communique
[9] https://gac.icann.org/contentMigrated/icann77-washington-d-c-communique?language_id=1
[10] https://gac.icann.org/contentMigrated/icann78-hamburg-communique?language_id=1
[11] https://gac.icann.org/contentMigrated/icann78-hamburg-communique?language_id=1

GAC expects to receive further updates from ICANN Compliance on their efforts to implement the contract amendments at ICANN81 (ICANN80, 2024).[12]

Community Activity

The community first made significant strides through voluntary mechanisms, most notably with the creation of the Framework to Address Abuse (the "Abuse Framework") in 2019. The Abuse Framework is based on the principle that registrars and registries must act when faced with DNS Abuse. The Abuse Framework also has sections relating to certain limited categories of website content abuses. The Abuse Framework launched with only eleven signatory registrars and registries, but has since grown to over fifty signatory registrars and registries (to include both gTLD and ccTLD registries). The definition of DNS Abuse set forth in the Abuse Framework has since been formally adopted as the definition of DNS Abuse by the Contracted Parties House and included in ICANN contracts with registries and registrars.

From 2022 to 2023, ICANN and the Contracted Parties began contract negotiations resulting in amendments to enhance obligations to require registrars and registry operators to promptly take reasonable and appropriate action to stop or otherwise disrupt DNS Abuse. The GAC submitted a public comment on this proposal, expressing general support and identifying specific issues for consideration. The GAC welcomed the amendments, noting they were a 'significant achievement' stating "[t]he proposed amendments are timely and relevant and, when adopted, will represent an important first step forward to combat DNS Abuse."[13] The ICANN Board adopted these amendments in January 2024, marking a significant step toward strengthening DNS Abuse obligations. The amendments entered into force on 5th April 2024.

The efforts of the SSAC and the gNSO Council DNS Abuse Small Team provided significant momentum towards the contractual negotiations. The findings of SSAC115 made reference to the possibility of "universal expectations for all ICANN contracted registries and registrars to adhere to when it comes to the types of abuses they should address."[14] The gNSO Council DNS Abuse Small Team also highlighted limitations in the current contracts, particularly in terms of interpretation and enforcement. In particular, this work highlighted that ICANN Compliance believed the current (at the time) RAA "does not require registrars to take any specific action on

[12] https://gac.icann.org/contentMigrated/icann80-kigali-communique?language_id=1

[13] https://www.icann.org/en/public-comment/proceeding/amendments-base-gtld-ra-raa-modify-dns-abuse-contract-obligations-29-05-2023/submissions/governmental-advisory-committee-gac-18-07-2023

[14] https://www.icann.org/en/system/files/files/sac-115-en.pdf A Report from the ICANN Security and Stability Advisory Committee (SSAC), 19 March 2021

the domain names that are subject to abuse reports."[15] The DNS Abuse Small Team noted its concern that this "may allow DNS abuse to remain unmitigated, depending upon the registrar's specific domain name use and abuse policies" and recommended that future work take place to confirm the gaps and possibly introduce minimum requirements.[16] ICANN Compliance has provided a dashboard forContracted Parties can track enforcement actions related to the amendments. It shows the number of violations reported each month for each type of DNS Abuse, and whether the reports are deemed actionable.[17] ICANN has issued several compliance notices in relation to these amendments which are visible on their website.

For implementation, the Institute provides several initiatives that can help the Contracted Parties as they consider the new contractual requirements. **NetBeacon Reporter** [18] is a centralized tool designed to simplify and standardize the process of reporting online abuse to registrars and registries. Previously known as NetBeacon before the Institute's rebrand, this tool supports Contracted Parties by helping meet the improved contract provisions requiring higher standards for reporting and handling DNS Abuse. NetBeacon is one option to help Contract Parties comply with more rigorous reporting requirements. Reporting from **NetBeacon Measurement and Analytics Platform** ("MAP"),[19] explained in further detail below in Measurement, provides contracted parties with an objective, external independent measure to benchmark their DNS Abuse levels against peers, and over time. Formerly known as DNSAI Compass, MAP continues to serve as an effective tool for registrars and registries to receive analyzed data on DNS Abuse.

It should be noted that **NetBeacon Reporter** only accepts reports of DNS Abuse, not infringements of the new contractual amendments. ICANN Compliance has provided a guide on how to report registrars or registries that fail to meet their obligations in responding to reported cases of DNS Abuse.[20]

Current Gaps

Promoting tools that help Contracted Parties comply with contract provisions is essential. As Contracted Parties work to meet more rigorous requirements, there is an increasing need for support tools and mechanisms to manage DNS Abuse reports and take prompt mitigation

[15] DNS Abuse Small Team Report. 7 October 2022 https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf#page=16&zoom=100,557,181
[16] DNS Abuse Small Team Report. 7 October 2022 https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf#page=16&zoom=100,557,181
[17] https://compliance-reports.icann.org/dnsabuse/dashboard/trends-list.html
[18] https://netbeacon.org/reporting/
[19] https://netbeacon.org/map-analytics/
[20] https://www.icann.org/compliance/complaint

actions. Although several tools and resources exist to improve process efficiency, it's crucial to connect Contracted Parties to these tools as they work toward compliance. Measuring the impact of these amendments on DNS Abuse[21] and the implementation effectiveness is crucial going forward. The NetBeacon Institute is currently working on data to publish on measuring the impact of the amendments. It is also important to ensure that the Industry responsibly uses reporting mechanisms for cases of failure to adhere to the obligations set out in the RAA and RA.

2. Enhanced DNS Abuse Reporting

GAC Communiqués

The GAC highlights the importance of DNS Abuse mitigation and prevention, emphasizing its growing relevance with the upcoming new round of gTLDs. In light of this, it acknowledges the need for measurement and reporting initiatives. “Mitigating DNS Abuse continues to be an issue of concern and the GAC emphasizes the importance of building on the current work which includes effectively preventing, reporting and responding to DNS Abuse” (ICANN75, 2022).[22] In the ICANN76 Communiqué, the GAC welcomes information about the Abuse Contact IDentifier tool from the Registrar Stakeholder Group, which helps identify the appropriate parties for addressing DNS Abuse.[23] Additionally, the GAC acknowledges the “importance of quality of the abuse reports and that good reporting practices need to be further developed and widely shared” (ICANN79, 2024).[24]

The GAC acknowledges the need for efficient abuse reporting mechanisms, along with further encouragement, facilitation, and education on this reporting process. It notes that “[e]nhanced Abuse Reporting would enable more focused dialogue within the ICANN community and provide the basis for targeted contractual improvements” (ICANN74, 2022).[25] The GAC stressed the need for improved abuse reporting systems in light of the “inevitable evolution of DNS Abuse…” (ICANN78, 2023).[26] Additionally, it noted that “[t]he GAC welcomes the launch of a free, centralized abuse reporting tool by the community in response to recommendations made in both SAC115 and the SSR2 Review Final Report.” (ICANN74, 2022).[27]

---

[21] https://netbeacon.org/measuring-icann-dnsabuse-amendments/
[22] https://gac.icann.org/contentMigrated/icann75-kuala-lumpur-communique?language_id=1
[23] https://gac.icann.org/contentMigrated/icann76-cancun-communique
[24] https://gac.icann.org/contentMigrated/icann79-san-juan-communique?language_id=1
[25] https://gac.icann.org/advice/communiques/ICANN74%20The%20Hague%20Communique.pdf
[26] https://gac.icann.org/contentMigrated/icann78-hamburg-communique?language_id=1
[27] https://gac.icann.org/advice/communiques/ICANN74%20The%20Hague%20Communique.pdf

The SSAC called for centralized abuse reporting mechanisms in 2021 with SSAC115 which "proposes a general framework of best practices and processes to streamline reporting DNS abuse and abuse on the Internet in general" and called for the ICANN community to continue this work.[28] It outlined the following elements and recommended next steps, including: "1. encourage standard definitions of abuse (see Section 2); 2. encourage 'notifier programs' that will expedite and make more efficient abuse handling in certain parts of the ecosystem; 3. determine the appropriate primary point of responsibility for abuse resolution; 4. identify best practices for deployment of evidentiary standards; 5. establish standardized escalation paths for abuse resolution; 6. determine reasonable timeframes for action on abuse reports; and 7. create a single point of contact determination whereby a reporter can identify the type of abuse and get directed to appropriate parties."[29] The Second Security, Stability, and Resiliency (SSR2) Review Team Final Report also recommended establishing and maintaining a "central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties."[30]

Community Activity

NetBeacon Reporter,[31] The Institute's centralized abuse reporting system, aims to address the challenges of complexity and quality DNS Abuse reporting. NetBeacon Reporter seeks to remove barriers to reporting DNS Abuse, such as a lack of technical knowledge, confusion on how to report abuse, and difficulties navigating the DNS ecosystem. NetBeacon Reporter streamlines the reporting process by standardizing and enhancing reporter registrars and registries. Additionally, NetBeacon Reporter empowers individuals and organizations by simplifying the reporting process through automated emails or API connectivity for all gTLD registrars. The Institute also published a blog post outlining best practices for submitting reports on phishing that provides what information Contracted Parties need to take appropriate action and why it is necessary.[32]

The **Abuse Contact IDentifier tool (ACID Tool)**[33] provided by the Registrar Stakeholder Group (RrSG) facilitates DNS Abuse reporting by helping users identify the relevant parties, such as the hosting provider and email service provider. The ACID Tool also provides registrar and registrant details for the entered domain name . This tool clarifies which party the reporter should contact

[28] https://www.icann.org/en/system/files/files/sac-115-en.pdf A Report from the ICANN Security and Stability Advisory Committee (SSAC), 19 March 2021
[29] https://www.icann.org/en/system/files/files/sac-115-en.pdf A Report from the ICANN Security and Stability Advisory Committee (SSAC), 19 March 2021
[30] https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf
[31] https://netbeacon.org/reporting/
[32] https://netbeacon.org/making-phishing-reports-useful/
[33] https://acidtool.com/

based on the typeof abuse or issues are suspected. By giving reporters confidence in whom to report to and the correct contact information, abuse reporting becomes more accessible and straightforward. The RrSG also published a guide on best practices for reporting DNS Abuse to registrars and registries.[34]

The multistakeholder network **Internet & Jurisdictions Network** developed two key documents. The first is a **Due Diligence Guide For Notifiers**,[35] which lists questions notifiers should ask themselves to determine if issuing notices to operators is appropriate. The second document, **Minimum Notice Components for Technical Abuse**[36] includes a table listing components that support actionable notices for reporting technical abuse. To clarify the concept of a "trusted notifier" for DNS Abuse reporting, the Internet & Jurisdiction Policy Network developed **Trusted Notifiers: Typology and Framework Components**.[37]

Current Gaps

A lack of knowledge and awareness about reporting tools persists. Although community initiatives aim to streamline and improve the reporting process, many potential reporters are unfamiliar with how, where, and with what evidence to provide when reporting suspected DNS Abuse.

Individuals attempting to report abuse often lack technical expertise, leading to unclear or unactionable reports. Everyone should be able to report abuse in a way that provides recipients with sufficient evidence to address suspected DNS Abuse, but this is not yet the case. For registrars and registries to decide on an appropriate course of action, they need sufficient evidence from reporters. One way to close this gap is by improving technical skills in the reporting community, such as enhancing knowledge of how to extract email headers and message bodies.[38]

---

[34] https://rrsg.org/wp-content/uploads/2022/01/CPH-Guide-to-Abuse-Reporting-v1.0.pdf

[35] https://www.internetjurisdiction.net/outcome/dns-level-action-to-address-technical-abuses-due-diligence-guide-for-notifiers-ref-20-113

[36] https://www.internetjurisdiction.net/outcome/i-j-outcome-minimum-notice-components-for-technical-abuse-ref-20-109

[37] https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-22-101-Trusted-Notifiers-Typology-and-Framework-2022.pdf

[38] https://netbeacon.org/making-phishing-reports-useful/

3. Distinguishing between Malicious and Compromised Domains

GAC Communiqués

The GAC recognizes the importance of distinguishing between observed registration types, specifically maliciously registered and compromised domains.“The GAC notes the ICANN73 community plenary session on ‘Evolving the DNS Abuse Conversation,’ which focused on malicious versus compromised domain names. It was universally agreed that the distinction is important, and the GAC supports the community exploring the opportunities highlighted in the session for further work to disrupt DNS Abuse” (ICANN73, 2022).[39]

“The GAC welcomed the many activities taking place across the ICANN community to address DNS Abuse, including . . . a forthcoming discussion paper from the Contracted Parties House on ‘malicious vs. compromised’ domains” (ICANN75, 2022).[40]

Community Activity

Distinguishing between malicious and compromised domains is essential because benign but compromised domains require different mitigation strategies than malicious domains. Maliciously registered domains are typically more appropriate for mitigation action at the DNS level. The **COMAR (Classification of Compromised versus Maliciously Registered domains)**[41] study made significant advances in distinguishing between maliciously registered and benign but compromised domains. Developed by SIDN Labs, AFNIC Labs, and Grenoble Alpes University ,COMAR can automatically distinguish between compromised and malicious domains with 97% accuracy.[42] COMAR uses 38 indicators or features studied by collaborators to determine whether a domain is benign but compromised (typically at the website level) or maliciously registered. For instance, benign domains that have been compromised often use a wider range of technologies to build the website, whereas malicious websites typically use fewer.

The Institute offers free articles likes **“Compromised Sites and Malicious Registrations: Best Practices for the Identification and Mitigation of DNS Abuse”,** [43] which educate readers on the technical definitions of the compromised websites and malicious registrations, how to distinguish between them, and the best mitigation practices for each. These educational tools highlight the

[39] https://gac.icann.org/contentMigrated/icann73-gac-communique?language_id=1
[40] https://gac.icann.org/contentMigrated/icann75-kuala-lumpur-communique?language_id=1
[41] https://comar-project.univ-grenoble-alpes.fr/
[42] https://www.sidnlabs.nl/en/news-and-blogs/distinguishing-exploited-from-malicious-domain-names-using-comar
[43] https://netbeacon.org/best-practices-identification-mitigation-of-dns-abuse/

importance of distinguishing registration types while providing tangible and actionable mitigation advice.

NetBeacon MAP publishes charts illustrating registration types (malicious, compromised, and uncategorized) and how they change over time in cases of phishing and malware. The data visualization separate phishing and malware, helping readers understand the registration type composition of DNS Abuse. Individualized dashboards are available, free of charge, helping domain registrars and registries better understand and combat DNS Abuse.[44]

The **Internet & Jurisdictions Network's Operational Approaches: Norms Criteria and Mechanisms** document also highlights the importance of distinguishing between compromised and malicious registered domains. It notes that additional measures may be necessary "to assist the registrant if the domain is obviously compromised by third parties without his/her knowledge."[45]

Current Gaps

Community discussions on DNS Abuse now include the distinction between malicious and compromised domains, but more work is needed to ensure compromised domains are effectively mitigated. Recognizing that a significant portion of phishing and malware cases involve benign but compromised domains highlight the need for more nuanced approaches to DNS Abuse mitigation strategies to prevent undue restrictions and collateral damage. Mitigating compromised domains requires engaging with a broader segment of the internet ecosystem, including hosting providers. [46] Addressing compromised domain name registrations also requires a broader public policy approach to improve cyber security hygiene among the general public, businesses, charities, and other internet users. It is essential that GAC members understand this distinction and its potential impact on national and regional public policy making. One issue explored by the gNSO Small Team on DNS Abuse is the potential request for Preliminary Issue Report to potentially inform a narrowly defined Policy Development Process on DNS Abuse, focusing on malicious registrations.[47] The difference in mitigating compromised and malicious domains should continue to be studied, and collaboration with the broader Internet ecosystem will be essential for effective mitigation.

---

[44] https://netbeacon.org/new-compass-dashboards/

[45] https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf

[46] https://netbeacon.org/secure-your-website-save-the-internet/

[47] DNS Abuse Small Team Report. 7 October 2022 https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf#page=16&zoom=100,557,181

4. DNS Abuse Measurement and Clarification of Metrics

GAC Communiqués

The GAC values the progress made in measuring DBS Abuse. “Improvements to the measurement, attribution, and reporting of abuse are also much needed, and the GAC will continue to closely follow developments within the community related to any such improvements” (ICANN71, 2021).[48] A deeper industry understanding of DNS Abuse concentration, types, and other metrics can lead to more effective mitigation practices. The GAC seeks to focus on regional experiences with DNS Abuse and “would welcome such learning opportunities from [different] regions on good practices to prevent and mitigate DNS Abuse at future ICANN meetings” (ICANN80, 2024).[49] Quantitative data on mitigation response times and analysis of abuse trends can illuminate weaknesses in DNS Abuse responses. “The GAC welcomed the many activities taking place across the ICANN community to address DNS Abuse, including. . . voluntary initiatives on measurement and reporting” (ICANN75).[50] Making DNS Abuse trend information publicly available enables more strategic discussions that improve mitigation practices. The Second Security, Stability, and Resiliency (SSR2) Review Team Final Report also called for identifying “registries and registrars whose domains most contribute to abuse.”[51]

ClarifyingDNS Abuse standards, especially regarding terms introduced in the contractual amendments, is closely tied to efforts to measure DNS Abuse. The GAC has stated its intention “to engage the community in discussions on policy efforts around….other key themes linked to effective implementation of the amendments, such as clarification of key terms from the amendments (ie., ‘reasonable’, ‘actionable’, ‘prompt’), and further actions to mitigate DNS Abuse, such as capacity building efforts” (ICANN78, 2023).[52] After the amendments were adopted, the GAC acknowledged the need for “minimum evidential thresholds and standards for ‘actionable evidence’ [that] should be consistently applied.” The GAC also referenced the 96-hour minimum standard for “prompt action” outlined by SSAC15. The GAC recommended that Contracted Parties Establish a context-sensitive understanding of the term “stop and/or otherwise disrupt,” which includes the action taken and the considerations leading to those actions in the enforcement information provided (ICANN79, 2024).[53]

[48] https://gac.icann.org/contentMigrated/icann71-gac-communique?language_id=1
[49] https://gac.icann.org/contentMigrated/icann80-kigali-communique?language_id=1
[50] https://gac.icann.org/contentMigrated/icann75-kuala-lumpur-communique?language_id=1
[51] https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf
[52] https://gac.icann.org/contentMigrated/icann78-hamburg-communique?language_id=1
[53] https://gac.icann.org/contentMigrated/icann79-san-juan-communique?language_id=1

Community Activity

ICANN's **Domain Abuse Activity Reporting (DAAR) project**, designed to study and report domain name registration and security threats across top-level domain registries, enhances the community understanding of DNS Abuse. DAAR's goal is to help guide policy decisions in the ICANN community by providing a "robust, reliable, and reproducible methodology for analyzing security threat activity."[54] DAAR accomplishes this through collecting TLD zone data and Reputation Block List security threat data feeds. The compilation of statistics and data enables the analysis of abuse activity at the registry level. DAAR's monthly reports identify general trends, break down individual security threats, and provide metrics such as the percentage of security threat domains in a TLD per domain within a TLD zone.[55] DAAR's reports, methodology papers, and contextual documents inform stakeholders about the concentration of security threats within the TLD space and how it changes over time. ICANN is now evolving their measurement efforts by creating **ICANN Domain Metrica: A Measurement Platform.**

MAP builds on the high-level abuse trends introduced by DAAR by producing monthly DNS Abuse reports on phishing and malware, broken down by registrar and TLD.[56] MAP measures phishing and malware and categorizes unique domain names as either compromised or malicious. It also measures whether the harm has been mitigated and how quickly. Interactive charts accompanying the full-length reports provide timely and detailed quantitative data. NetBeacon MAP also offers individual dashboards to registrars and registries, containing specific information on their zone. Additionally, the breakdowns of high and low volumes of observed maliciously registered domains by registrar in the June 2024 Report[57] provide more insight into DNS Abuse on the registrar and registry level. In March 2024, the Institute published a report outlining the considerations and challenges of different DNS Abuse measurements.[58]

The new ICANN funded project, **Inferential Analysis of Maliciously Registered Domains (INFERMAL)**,[59] marks an important next step measurement. INFERMAL systematically analyzes cyberattackers' preferences, including domain name, security practices, and payment method. The findings from this project can expand knowledge on which mitigation measures and proactive actions are most effective in preventing DNS Abuse.

---

[54] https://www.icann.org/octo-ssr/daar
[55] https://www.icann.org/en/system/files/files/daar-monthly-report-31mar23-en.pdf
[56] https://netbeacon.org/dns-abuse-if-we-cant-measure-it-does-it-exist/
[57] https://netbeacon.org/wp-content/uploads/2024/06/MAP-Report-June-2024-.pdf
[58] https://netbeacon.org/wp-content/uploads/2024/04/DNS-Abuse-Measurement-Challenges.pdf
[59] https://www.icann.org/en/blogs/details/new-icann-project-explores-the-drivers-of-malicious-domain-name-registrations-25-04-2023-en ; https://infermal.korlabs.io

The DNS Research Federation's Data Analytics Platform **DAP.LIVE**[60], is an open data platform offering metrics on malware, phishing, and abuse trends, illuminating how and where DNS Abuse occurs within the DNS ecosystem. Data on malware and phishing reports by URL are among the various sources and packages that users can utilize to generate tables, visualizations, and graphs. From quantifying phishing[61] to exploring registrant identification counts for specific domains,[62] DAP.LIVE allows users to investigate and work directly with DNS Abuse data, aiding discussions on DNS Abuse mitigation.

ICANN issued an advisory on the terms included in the new contractual amendments to establish a practical standard for their interpretation.[63]

Current Gaps

Measurement projects are currently constrained by the quality of available data, which typically comes from reputation block lists designed for network protection rather than for measuring abuse.. The next challenge for the DNS Community is to develop more detailed and accurate methods of measuring DNS Abuse and to provide analysis on specific issues, such as aging domains and the impact of various policies and processes (e.g., incentive schemes). Expanding our collective understanding of DNS Abuse will be crucial to ensuring that Contracted Parties have the information and tools needed to manage in their zones. Establishing a common understanding of relevant metrics for the RAA andRA will be essential as registrars and registries work to meet their new obligations, and as ICANN Compliance evaluates compliance.

[60] https://dnsrf.org/
[61] https://dnsrf.org/blog/dns-as-a-vector-for-phishing-attacks--different-victims--different-methodologies--different-results/index.html
[62] https://dnsrf.org/blog/brand-names-in-blockchain-domains---new-frontier-for-brand-owners/index.html
[63] https://www.icann.org/resources/pages/advisory-compliance-dns-abuse-obligations-raa-ra-2024-02-05-en

Appendix 1: Summary Table

Please note:this table is summarizing this report by issue. If a GAC Communiqué references multiple issues it is listed multiple times. Readers may find the GAC Advice itemized tracker and the ICANN Board response tracker helpful for further understanding GAC Advice and progress. Also, most of the references to DNS Abuse contained in GAC Communiqués are issues of importance rather than formal advice and therefore they did not require a response from the ICANN Board.

Issue	GAC Communique	Issues of Importance to the GAC
Implementation of new DNS Abuse Obligations	ICANN57, 2016	* **GAC Advice to the Board** Requested information from ICANN on a variety of issues, including the diligence applied by ICANN in relation to '3.18 Registrar's Abuse Contact and Duty to Investigate Reports of Abuse' in the 2013 Registrar Accreditation Agreement (ICANN57, 2016). ICANN responded to this request.
	ICANN74, 2022	"Improved contract provisions could focus on the reporting and handling of DNS Abuse and enforcement of related contract requirements" "The following would assist in developing such contract provisions: abuse reporting at the registrar and registry level; more detailed breakdowns of the types of DNS Abuse measured; and availability of raw aggregated data"
	ICANN76, 2023	"The creation of effective and enforceable requirements for registrars and registries to disrupt or mitigate DNS abuse will represent a positive and concrete first step in addressing [DNS Abuse] at ICANN" In 2023, the GAC offered their support for contract negotiations between ICANN and Contracted Parties that improve existing DNS Abuse obligations and encouraged additional work.

		"The GAC … encourages the Contracted Parties and ICANN to further consider, inter alia, proactive measures as well as positive incentives for registries and registrars in future work on DNS abuse mitigation or disruption" (ICANN76, 2023).
	ICANN77, 2023	"The GAC welcomes the clarity provided during its DNS Abuse session that in case of non-compliance ICANN Compliance would be able to suspend or revoke the agreement with the contracted party, and it encourages ICANN org and the negotiating team to ensure this is clear in this process under the amendment." "The GAC also welcomes any further work the negotiating team can do to clarify forthcoming reporting obligations with a view to promote transparency of the contracted parties' policies and how they respond to DNS Abuse."
	ICANN78, 2023	"The GAC urges the Contracted Parties to adopt the DNS Abuse amendments so that baseline obligations for gTLD registries and registrars regarding DNS Abuse are established in ICANN's contracts. The GAC also urges ICANN org to provide the community with the ability to monitor the implementation of the amendments."
	ICANN79, 2024	"The GAC appreciated hearing from ICANN org's Compliance department about plans for auditing and enforcing the amendments" "The GAC discussed what a reasonable timeframe for assessing the impact of the obligations might be. Some suggested six months. However, there remains a general expectation that significant progress occur in advance of the next round of new gTLD applications. The GAC will track reports from ICANN Compliance on DNS Abuse enforcement."

	ICANN80, 2024	"The GAC looks forward to continuing discussions on DNS Abuse before and during ICANN81 where it expects to receive updates from ICANN Compliance on the implementation of contract amendments."
Enhanced DNS Abuse Reporting	ICANN74, 2022	"Enhanced Abuse Reporting would enable more focused dialogue within the ICANN community and provide the basis for targeted contractual improvements." In addition they noted that "The GAC welcomes the launch of a free, centralized abuse reporting tool by the community in response to recommendations made in both SAC115 and the SSR2 Review Final Report."
	ICANN75, 2022	"Mitigating DNS Abuse continues to be an issue of concern and the GAC emphasizes the importance of building on the current work which includes effectively preventing, reporting and responding to DNS Abuse."
	ICANN76, 2023	GAC welcomes information about the Abuse Contact IDentifier tool from the Registrar Stakeholder Group that works to identify to which parties it is appropriate to identify DNS Abuse.
	ICANN78, 2023	"The GAC also recalls the practical need to recognize the inevitable evolution of DNS Abuse, including how it is defined in the amendments, as well as abuse report handling, tackling systemic abuse and additional reporting and data collection requirements."
	ICANN79, 2024	"The GAC also acknowledged the importance of quality of the abuse reports and that good reporting practices need to be further developed and widely shared."
Distinguishing between Malicious and Compromised Domains	ICANN73, 2022	"The GAC notes the ICANN73 community plenary session on 'Evolving the DNS Abuse Conversation,' which focused on malicious versus compromised domain names. It was universally agreed that the distinction is important, and the GAC supports the

		community exploring the opportunities highlighted in the session for further work to disrupt DNS Abuse."
	ICANN75, 2022	"The GAC welcomed the many activities taking place across the ICANN community to address DNS Abuse, including... a forthcoming discussion paper from the Contracted Parties House on "malicious vs. compromised" domains" (ICANN75, 2022).
DNS Abuse Measurement and Clarification of Metrics	ICANN71, 2021	The GAC values advances made in DNS Abuse measurement. "Improvements to the measurement, attribution, and reporting of abuse are also much needed, and the GAC will continue to closely follow developments within the community related to any such improvements."
	ICANN75, 2022	"The GAC welcomed the many activities taking place across the ICANN community to address DNS Abuse, including ... voluntary initiatives on measurement and reporting."
	ICANN78, 2023	"Once the amendments are adopted, the GAC intends to engage with the community in discussions on policy efforts around the above mentioned topics as well as other key themes linked to effective implementation of the amendments, such as clarification of key terms from the amendments (i.e., "reasonable", "actionable", "prompt")."
	ICANN79, 2024	"The GAC acknowledged the recommendation that, to support effective enforcement, the community would need to establish minimum evidential thresholds and standards for "actionable evidence". Such standards should be consistently applied. Regarding "prompt action," reference was made to SSAC115, which outlines a 96-hour minimum standard. To develop a clear appreciation of what "stop and/or otherwise disrupt" means, it was recommended that the information Contracted Parties provide on enforcement actions taken include the action taken as well as the considerations that lead

		to it.”
	ICANN80, 2024	“Speakers in the session also urged further collaboration across the African region to address DNS Abuse, including among ccTLD operators. The GAC would welcome such learning opportunities from other regions on good practices to prevent and mitigate DNS Abuse at future ICANN meetings.”