NCSG DRAFT AGENDA FOR DNS ABUSE

- NCSG Discussion on DNS Abuse
- Mapping NCSG thought on DNS Abuse
- Assessment of DNS Abuse
- What are the issues noncommercial registrants faced with DNS abuse?
- How effective are the mechanism to address DNS abuse

OUTCOME:

- Defining NCSG DNS abuse Objectives
- Draft NCSG statement on DNS abuse.

NB: Kathy noted:

- Fairness and due process, especially where the suspension and revocation of domain names is concerned since the beginning of ICANN.
- Are these principles preserved in this paper and its proposal?

—---

NCSG Draft DNS Abuse Position

The Non-Commercial Stakeholder Group (NCSG) is a constituency of the Generic Name Supporting Organisation (GNSO). The NCSG represents the interests of non-commercial users in the formulation of Domain Name System policy within the auspices of the Generic Names Supporting Organization (GNSO). Since our inception, we have facilitated global academic and civil society engagement in support of ICANN's mission, stimulating an informed citizenry and building their understanding of relevant DNS policy issues while raising awareness of the need for ICANN to comply with applicable privacy and data protection legislation.

Draft position on Definitions

NCSG is of the opinion that there is no clear definition of what the limits of DNS Abuse are. We highlight that the term originates from the standard registry agreement made between ICANN and registry operators. The agreement outlines a series of 'public

interest commitments' to which registry operators are required to adhere. Specifically, Specification 11 (3)(b) mandates an obligatory responsibility on registry operators to proactively conduct technical analyses to assess whether domain names are being used to perpetrate security threats. This is despite the fact that the document does not definitively or exhaustively define what constitutes such a threat.

There are three documents which attempt to elaborate Specification 11 (3) (b) and clarify the limits within which DNS Abuse falls:

1) The 2020 Contracted Party House (CPH) Definition of DNS Abuse, which states that

"*...DNS Abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam when it serves as a delivery mechanism for the other forms of DNS Abuse… .*"

2) The 2019 Framework on DNS Abuse, which similarly states that

"*...DNS Abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for the other forms of DNS Abuse) ....*"

However, we note that the Framework also includes the term "Website Content Abuse" and states the following:

> "*Despite the fact that registrars and registries have only one blunt and disproportionate tool to address Website Content Abuse, we believe there are certain forms of Website Content Abuse that are so egregious that a registry or registrar should act when provided with specific and credible notice. Specifically, even without a court order, we believe a registry or registrar should act to disrupt the following forms of Website Content Abuse: (1) child sexual abuse materials ("CSAM"); (2) illegal distribution of opioids online; (3) human trafficking; and (4) specific and credible incitements to violence. Underlying these Website Content Abuses is the physical and often irreversible threat to human life. Additionally, each registrar and registry has its own acceptable use policies or terms of use that set forth provisions that may cover these and additional forms of Website Content Abuses.*"

3) The 2020 ICANN Guide to Registrar Abuse Reporting Practices, which defines DNS Abuse as "... *a range of activities collectively identified as abuse, including, phishing, spam, malware, and trademark and copyright infringement…..*"

ICANN's guide goes beyond the definition provided in the first two definitions and includes issues such as trademark and copyright infringement. However, we note that these issues already have a mechanism to resolve them: the ICANN Uniform Domain Name Dispute Resolution Policy. The UDRP was created in 1999 with the goal of dealing with challenges at the intersection of domain names and intellectual property rights, with specification of "trademarks" and "service marks".

The nuances of how DNS Abuse is defined will have implications for the liability on registries and registrars to participate in content moderation without appropriate transparency and accountability mechanisms.

Human Rights Concerns on DNS Abuse

a) Lack of clear definitions

There is a uniform requirement specified in all three documents that registries and registrars must reject the registration for a domain name, suspend a domain name, or block a domain name for being potentially "abusive" in the case of DNS Abuse. However, as demonstrated above, there is no uniform definition of what DNS Abuse is.

This lack of a consensus definition creates ambiguity in compliance, as registries and registrars may not be certain of when they are compelled to reject, suspend, or block a domain name under this framework. Therefore, to ensure that they are not held liable, registries and registrars will resort to an overly cautious approach, which will almost certainly impinge on the availability of legitimate content. We specifically note that, under the definition provided in the 2019 Framework on DNS Abuse, "Website Content Abuse" includes "...*specific and credible incitements to violence…"* Without appropriate judicial oversight, this kind of wording is overly broad and may be abused by authorities to limit legitimate forms of expression, such as online protests, as we have seen occur in offline contexts.

b) The use of proactive monitoring systems

As currently drafted, Specification 11 (3)(b) of the standard registry agreement made between ICANN and registry operators requires proactive monitoring, rather than responding only after activity or material that violates the specification has been flagged by users or complainants.

For this reason, the .eu registry operator has already implemented the Abuse Prevention and Early Warning System (APEWS), a machine learning system that evaluates patterns of domain name registrations and predicts whether a domain name may potentially be used in an 'abusive' manner.

Additionally, the .uk registry operator implements the Domain Watch initiative, a blend of manual and automated checking processes to identify, at the point of registration, which new domains are likely to be used for phishing. As of March 2020, the registry proactively suspended over 180 domains, pending 'evidence of good intentions'.

Constant scanning of domain-related activities poses a serious problem, as the use of predictive systems can lead to the rejection, suspension, or takedown of legitimate domains based on the *likelihood* that a violation will occur, rather than in response to a violation after it has taken place. This approach results in a system where people are punished for actions they have not actually taken.

In addition, the exclusive use of machine learning to moderate content, whether in predictive monitoring systems or otherwise, should be highly discouraged. Machine learning and automated processing systems are poor evaluators of the nuanced context in which content is posted.Without human analysis and oversight, these systems may trigger the takedown of parody or comedy websites, artists' homepages, protest sites, and the domains of other Internet users who are protected under the principles of free speech and fair use, thus violating their fundamental rights.

c) Lack of transparency and due process

We note that there are several concerns regarding the lack of transparency and weak due process that must be addressed before further actions are taken as part of countering DNS Abuse:

1) Registrants are not properly involved in decisions. Of the three documents discussed above, not a single one provides a manner for involving a registrant before the suspension or termination of a domain name. Registries are not required to notify or provide justification to registrants when their domain names have been suspended because of alleged or 'potential' DNS abuse. Moreover, there are no meaningful appeals mechanisms to challenge these decisions. Registrants/ users have a right to due process under international law[1]. Within the DNS ecosystem, this would require registries or registrars to proactively disclose the policies that govern their relationships with registrants and be accountable to registrants while making any and all decisions that impact them. The right to due process at the DNS level provides a registrant with the means to understand why their registration for a name might be rejected, why their domain might be suspended, and why the domain name might be taken down by a registry or registrar. The right also allows the registrant to have an adequate

[1] The right to due process is provided under article 14 of the International Convention on Civil and Political RIghts (ICCPR) which states that, "*...All persons shall be equal before the courts and tribunals...everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law..*"

opportunity to challenge the validity of the decision and assert any privileges associated with their domain name, including the right to an appeals process and the ability to make necessary amendments to their domain names.

2) The use of "trusted notifiers". The October 2019 Framework to Address Abuse proposes the use of trusted notifiers or Domain Reputation Service Provider(s) to report instances of DNS abuse to registries as a mechanism for introducing greater community accountability. However, the use of trusted notifiers is not appropriate, as they are often not independent and may not have sufficient expertise to assess the lawfulness of content or takedown decisions. Additionally, the outsourcing of content moderation to profit-driven private actors may lead to situations where notifiers are incentivized by special interests to block legitimate speech.

Recommendations

Taken together, the above three key human rights concerns regarding the current state of the DNS Abuse framework poses serious risks to human rights. Thus, NCSG must clearly restate the following redlines as our policy position:

- The ICANN multistakeholder community must engage in a Policy Development Process that clearly outlines the definition and scope of DNS Abuse. The NCSG position is that the definition of DNS Abuse should be limited to malware, botnets, phishing, pharming, and spam and exclude actions that would make DNS operators the unilateral arbiters of what is lawful and unlawful content. It must also include an indication of clear procedures, remedies, and actions that registries may take in instances where there are legitimate cases of malware, botnets, phishing, pharming and spam at the DNS level, while giving registrants an opportunity to recover their domain name in cases where these incidents have occurred without the willful intent or knowledge of the registrant.
- The ICANN multistakeholder community must amend Specification 11 of the registry agreement and implement a notice and takedown framework with independent judicial oversight to limit the legal liability of registry operators as intermediaries and possible penalties accruing therefrom.
- The ICANN multistakeholder community must implement minimum due process guarantees for internet users when tackling DNS Abuse, including notifying users when enacting domain suspensions or takedowns and providing meaningful opportunities for appeal.
- The ICANN multistakeholder community must avoid the use of trusted notifiers to monitor and flag content in efforts to combat DNS Abuse. In the case that they are used, their decisions must not be taken as the final decision.