The roadmap: ccNSO & DNS Abuse

TABLE OF CONTENTS

Introduction

This document refers to the topic of the ccNSO & DNS Abuse. It lists the role and actions of the Ad Hoc Group, and details their proposed roadmap for the ccNSO and DNS Abuse.

About the Ad Hoc Group

As a follow-up of the 18 November 2021 ccNSO & DNS Abuse workshop, the Council convened an Ad Hoc group of Councilors and community members to propose the next steps and decision-making process in this area.

The Ad Hoc Group will undertake the following tasks:

1. Summarize the 18 November 2021 ccNSO & DNS Abuse workshop (completed. See here)
2. Present the summary to the Council and seek feedback (completed. See here)
3. Prepare and detail a roadmap to solidify the envisioned role of the ccNSO in DNS Abuse. The roadmap navigates through the various actions and proposals from the Council and community, as well as their sequence. The roadmap should build on the results of ICANN72 and the 18 November 2021 Workshop. The Ad Hoc group also looks at various methods to understand the potential impact of its various components (i.e. influence mapping and a pro-con-fix analysis).

4. Present the first iteration of the roadmap to the ccNSO Council at their January meeting and seek their feed-back. Update the roadmap where needed, following that consultation.
5. Introduce the Roadmap to the community at the ICANN73 meeting with the goal to seek community buy-in to implement the roadmap.

Council expects to adopt the Roadmap and underlying actions, including a draft of the Terms of Reference for the ccNSO DNS Abuse Committee, at their ICANN73 meeting. It is the intention of the Ad Hoc group to conclude its work by ICANN73, after adoption of the roadmap by Council.

The roadmap: Key components

Following the ccNSO & DNS Abuse workshop, the ad hoc group identified four major components or activities of the envisaged roadmap:

1. **Sharing of Information**

Strengthen the platform function of the ccNSO to continuously share information, for instance via dedicated sessions and/or other channels. Build a repository and point of reference for ccTLDs to access relevant, reliable, and actionable information on DNS Abuse.

In strengthening the platform function, it should be ensured that:

- Not all efforts are focused on defining what is DNS Abuse. What is considered DNS Abuse is context dependent and differs per stakeholder. Demonstrate that the “one size does not fit all” principle also applies in DNS Abuse.
- Information is shared with ccTLDs, and awareness is built.
- voluntary DNS Abuse frameworks developed by the (broader) community are discussed.
- Information is shared with other parts of ICANN.

2. **Messaging**

Identify channels for messaging to be used by the ccNSO and ccTLD community. Develop narratives and a message repository. Messages targeted at various stakeholders: GAC/Governments, GNSO, Other stakeholders (including ICANN org and ALAC) and ccTLD community at large.

The Messaging should focus on:

- Promote that "one size does not fit all".
- Remind all stakeholders that ccTLDs are not gTLDs.
- Manage expectations about the role of ccTLDs & registrars.
- Share information with other parts of ICANN.
- Share information with ccTLDs and build awareness.

3. **DNS Abuse committee**

The TLD-Ops committee is a model to be used to build a (cc)TLD DNS ABUSE Oversight committee. The model would include an email list, with voluntary subscription of ccTLD reps to exchange information/incidents (alerts) and/or background information. The model also foresees the creation of a steering committee, with liaisons from ICANN and other relevant groups (CPH DNS Abuse WG? SSAC? Others?). Additional functions could be the consolidation of the metrics and information sharing, capacity building and assisting in developing (best) practices, monitoring, and addressing DNS abuse incidents. The Steering group could also be tasked to oversee and ensure regular updates to the community.

4. **Metrics**

Create an overview of existing metrics. Invite ccTLDs to share metrics (directly, through DAAR or in any other way). Inform the ccTLD community about DAAR. Possibly commission a study.

The Roadmap: 4 phases

Building on the Impact-Effort assessment conducted during the November '21 ccNSO & DNS Abuse Workshop, the following 4 phases are proposed:

First Phase (Now up and until ICANN74, June 2022)

This phase has the highest priority. Three activities are foreseen during this phase:

1. Create the ccNSO DNS Abuse committee.
    a. Complete Draft the terms of reference by the February Council meeting, to seek feed-back from Council
    b. Propose terms of Reference and explain the role of the DNS Abuse committee to the community (ICANN73)
    c. Approve Terms of Reference (ICANN73)
    d. Call for volunteers Oversight Committee (March 2022, appointment Council)
    e. Invite liaisons after Committee has been established
    f. Create email list: ask community to subscribe (Starting March 2022 -> open)
    g. Expand repository of presentations and practices
2. Prepare Messaging: includes building relations with other groups (starting March 2022)
3. Strengthen the ccNSO platform through MPC, Tech WG, DNS Abuse committee (Starting March 2022, in preparation of future meetings)

Second Phase (post ICANN74, June 2022- September 2022)

Once created and established, the DNS Abuse group is advised to focus on metrics, and other activities, including:

- Building Metrics
- Start listing practices
- Share information and messaging resulting from metrics, listing of practices
- Involve ccTLD community in DNS Abuse Operations
- Build links with other existing groups

Third phase (post ICANN75, September 2022)

Develop and/or document Best Practices

Fourth phase (after one year)

- Review the effectiveness: does the group meet its purpose? Does it meet the expectations of the community?
- Develop play-books to mitigate DNS Abuse and its impact on ccTLDs.

Work items identified from the ICANN72 and ccTLD consultation workshop

Results 18 November 2021 ccNSO & DNS Abuse workshop

Building on the results of the ICANN72 session ccNSO & DNS Abuse, the ccNSO Councillors and community members held a workshop to further explore and map:

1. Whether the proposed actions from the discussion at ICANN72 are within the purpose and value of the ccNSO, and
2. The benefit of the various actions proposed during the ICANN72 ccNSO & DNS Abuse session compared to the effort needed to achieve the envisioned result.

All attending the workshop were randomly divided into 3 groups to discuss the items included in the clusters 1-3 below. Cluster 4 was not dealt with during the workshop as it was considered a manner to organize activities, if any. The percentages next to each item express the level of support, as a result of the polling with the participants at ICANN72. Note that as the session was open to all interested stakeholders the results of the polling do not reflect the opinion of ccTLDs.

Cluster 1 – Information Sharing – Best practices

- Share information with ccTLDs and build awareness (100%)
- Consider a best-practice, educational role (96%)
- Do NOT focus all efforts on defining DNS Abuse (78%)
- Develop a voluntary code of conduct for ccTLDs (62%)
- Do NOT try to solve all the problems of the world (not polled)

Cluster 2 – ccTLD outreach and promotion

- Encourage ccTLDs to participate in DAAR (71%)
- Promote DNS Abuse mitigation initiatives with care (65%)
- Create a global database of abused domain names (33%)
- Create co-operations for regular audit mechanisms (20%)
- ccTLDs should not be complacent about the extent of DNS Abuse in their ccTLDs (not polled)

Cluster 3 – External, non-ccTLD outreach and promotion

- Promote "one size does not fit all" (89%)
- Share information with other parts of ICANN (87%)
- Manage expectations about the role of ccTLDs & (ccTLD) registrars (65%)
- Support community developed voluntary frameworks (65%)
- Remind all stakeholders that ccTLDs are not gTLDs (65%)
- Do NOT ignore the relationship between ccTLDs and national governments (not polled)

Cluster 4 - How to organise these efforts?

- Create a DNS Abuse Mitigation Working Group (65%)
- Consider a role for TLD-OPS or similar group (61%)

Each of the the groups were asked to rank each of the items according to the following criteria:

- What is the envisioned benefit for ccTLDs?

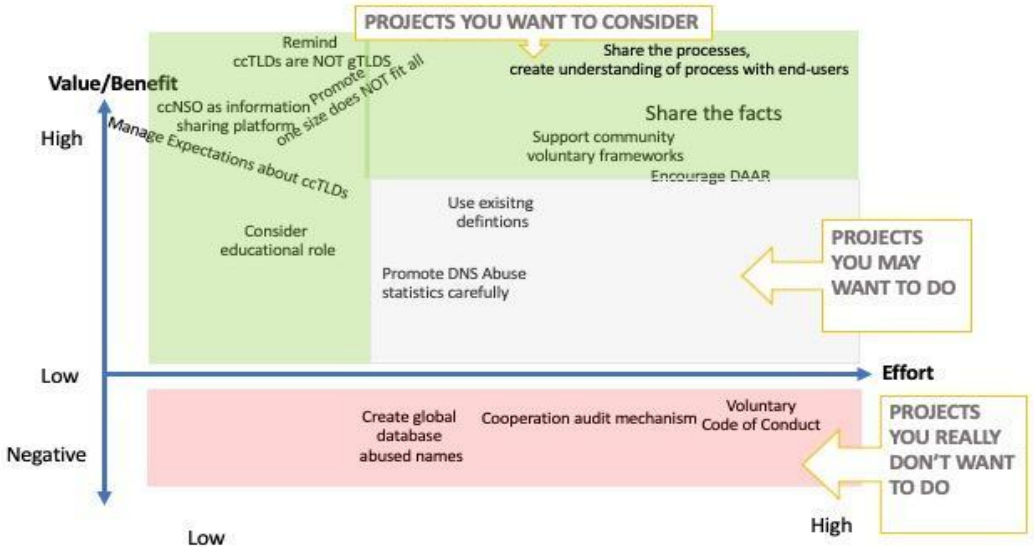
- What is the level of impact? (H, M, L)
- What is needed to achieve the result?
- What is the level of effort required? (H, M, L)

The results of the workshop were mapped in 2 ways:

1. Value/Benefit and Effort grid
2. Impact and the Effort Matrix

Value/Benefit and effort Assessment

Figure 1: Value/Benefit and effort grid



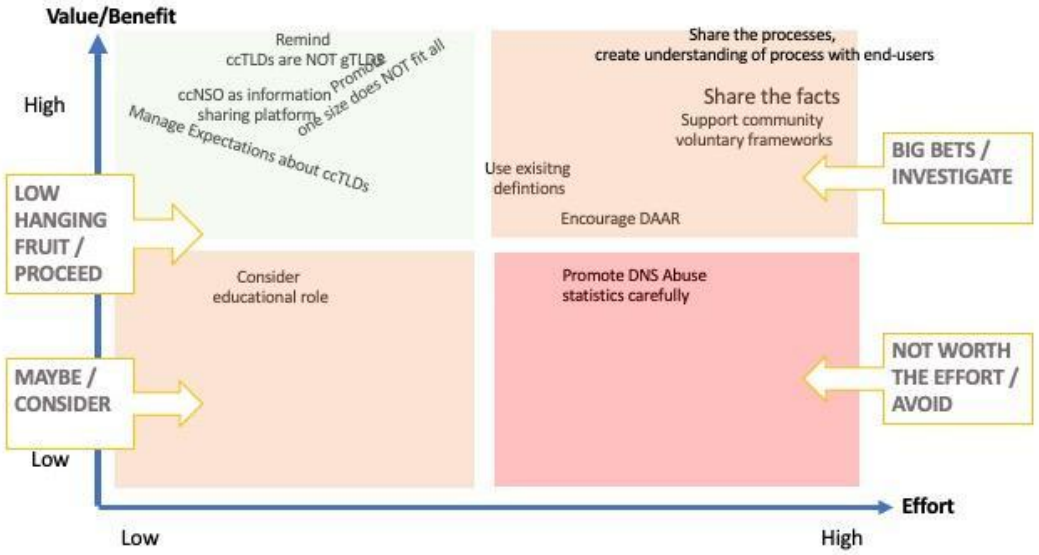
Note that the value/benefit could also be rated negative (the benefit or added value for the ccNSO and ccTLD community is considered detrimental i.e as being a "high risk") to the goal of the ccNSO with respect to DNS Abuse.

The statement to "Develop a voluntary code of conduct for ccTLDs" was considered to be most controversial. Although when presented the voluntary nature of a code of conduct was stressed, the attendees agreed with ranking it as a "high risk" effort: external parties could impose a requirement to adhere to such a code. Further, the development and maintenance of such a code would require a very high level of effort in terms of subscribing, implementing and monitoring breaches to the code. The benefit was therefore considered negative.

Impact – Effort Assessment

As a second step, the various items from the brainstorming, which at a minimum had a positive impact were mapped in a matrix. The 4 quadrants in the matrix mean: proceed, investigate, consider, and - last but not least - avoid.

Figure 2: Value/Benefit – Effort Matrix



Areas of activities identified and their sequence

Proceed

- Regarding the statement “one size does not fit all”: it is very obvious to ccTLD-insiders, but not necessarily to those not affiliated with the ccTLD community. Making this clear is all about expectation management. In order to achieve this goal, the ccNSO could consider creating a database with contacts from responsible persons at a ccTLD manager, dealing with DNS Abuse. Best practice sharing and experience sharing on such a mailing list would have a high impact on ccTLD managers and ccNSO.

Investigate

- The suggestion was raised for the ccNSO to conduct its own studies that relate to ccTLDs, and not to rely on data by third parties. This was considered to be a high effort, unless it is done externally. In that case the ccNSO should mainly focus on the scoping of the exercise.
- Regarding participating in DAAR, participants mentioned that the data is not so relevant for ccTLDs, or even not suited for ccTLDS, since the only interface available was to provide regular "zone files" copies to the system. Also, the suggestion was raised to have a ccTLD-focused session on DAAR at ICANN73.

Avoid

- Those discussing cluster number 2 had concerns regarding the statement “promote DNS Abuse mitigation initiatives with care, and suggested to rephrase the suggestion as follows: “The ccNSO should neutrally assess the various DNS Abuse mitigation initiatives”. This was considered to be a high-effort, with medium impact, to be conducted most likely by a small group of volunteers from the security-oriented side of the industry.

Additional remarks

- There is a small number of TLDs that typically do not participate in these meetings, where the problem is concentrated. It was proposed that the ccNSO should consider if and to what extent it should call out fellow community members who do not do enough to fight DNS Abuse, as they negatively impact the reputation of the ccTLDs and ccNSO.
- With respect to fighting DNS Abuse the overall impression was that ccTLDs are doing better than average and ccTLD Managers are strongly advised to share their practices.