ccNSO & DNS Abuse

Summary of October ICANN72 Session, November Workshop

&

Next Steps

Table of contents

1. Introduction

The topic of the ccnNSO's role with respect to DNS Abuse was addressed during 2 sessions during the October-November 2021 timeframe. This document summarizes the discussions to date.

The Council has established an Ad-Hoc DNS Abuse group, which is looking into various methods to develop and propose the roadmap and related schedule for the next phase of ccNSO & DNS Abuse process. After the group has completed an in depth analysis of the results of the ICANN72 and workshop sessions, it will propose first to Council a ccNSO roadmap and after feed-back from Council present it to the ccTLD community.

It is the intention of the group to close the discussion on the roadmap by ICANN73 and that Council uses that meeting to present the Roadmap to the ccTLD community early 2022. The goal is that the ccNSO will launch its activities related to mitigating DNS abuse by ICANN73.

2. October 2021: ICANN72 session

The ccNSO has organized various sessions on Domain Name System (DNS) abuse in recent ICANN Public Meetings. Country code top-level domain (ccTLD) managers and others shared their experiences with respect to mitigating DNS abuse, focusing on what ccTLDs do nationally and regionally. During ICANN72 (27 October 2021, 21:30-00:30 UTC), the conversation shifted to focus on exploring the potential role of the ccNSO itself. Both ccTLDs and other stakeholders suggested activities the ccNSO could undertake to complement existing work being done by the community.

2.1. Focus of the presentations: suggestions

Each of the presenters was asked to use the following 3 questions to guide their presentations:
1. What is your perspective on DNS Abuse?
2. What are the major issues at stake?
3. What are the do's and don'ts for the ccNSO, regarding DNS Abuse (maximum 3 suggestions)?

2.2. Conversion of the suggestions into statements

The suggestions the presenters provided were combined into short statements. During part two of the session, the statements were polled, to assess the level of support by the community. Note that this session was open to all interested to attend. Therefore, the polling results do not reflect the view by the ccTLD community only.

	ICANN72 ccNSO DNS Abuse Session (part 2)	Polling Results		
	Statements with respect to ccNSO & DNS Abuse	Agree	Disagree	No opinion
1	Share information with ccTLDs and build awareness (suggested by John, Kristof, Byron)	100%		
2	Share information with other parts of ICANN (suggested by John, Jim, Byron)	87%	2%	11%
3	Consider a best-practice, educational role (suggested by John, Gabriel, Kristof, Jim)	96%	2%	2%
4	Consider a role for TLD-OPS or similar group (suggested by John and Kristof)	61%	12%	27%
5	Encourage ccTLDs to participate in DAAR (suggested by Gabriel, Anil, Byron)	71%	13%	16%
6	Support community developed voluntary frameworks (suggested by Gabriel)	65%	15%	20%
7	Manage expectations about the role of ccTLDs & registrars (suggested by Kristof, John, Jim)	65%	7%	28%
8	Create a global database of abused domain names (suggested by Anil)	33%	61%	6%
9	Create co-operations for regular audit mechanisms (suggested by Anil)	20%	43%	37%
10	Remind all stakeholders that ccTLDs are not gTLDs (suggested by Byron)	86%	8%	6%
11	Promote that "one size does not fit all" (suggested by Byron, Kristof)	89%	2%	9%
12	Create a DNS Abuse Mitigation Working Group (suggested by Byron)	65%	17%	19%
13	Do NOT focus all efforts on defining DNS Abuse (suggested by John, Jim)	78%	11%	11%
14	Promote DNS Abuse mitigation initiatives with care (suggested by Kristof)	86%	2%	12%
15	Develop a voluntary code of conduct for ccTLDs (suggested by Byron)	62%	25%	13%

More color and depth to the various statements is provided in Annex A, which includes:

- on a per suggestion-basis, relevant extracts from the session transcript
- Relevant extracts from the session transcript, grouped under nine headings.
- Links

For ease of reference, here are the 9 headings, under which the session transcript extracts were grouped:

1. What is the problem space?
2. Scope of DNS Abuse
3. Need to measure
4. Public safety perspective
5. Why is domain name abuse successful and persistent?
6. Role of (cc)TLDs
7. Scope of ccNSO role
8. Share Experience/Cooperate
9. Potential measures to mitigate DNS Abuse

3. November 2021: Council & ccTLD community Workshop

The ccNSO Council decided not to meet in November 2021, but to instead organise a workshop on DNS Abuse, as a follow-up of the October ccNSO ICANN72 DNS Abuse Session. Both Councillors and ccTLD community representatives were invited to the workshop (18 November 2021 (12:00-13:30 UTC).
The goal of the Workshop was twofold: firstly, to explore both the benefit of the various actions proposed during the ccNSO & DNS Abuse session compared to the effort needed to achieve the envisioned result, and secondly to explore how the purpose and value of the ccNSO fits with the proposed actions from the discussion at ICANN72.

Annex B contains some relevant links regarding this workshop, such as the jamboard used for the discussion, the informal meeting notes and the links to the zoom recordings.

3.1. Brainstorming Method

All attending the workshop were randomly divided into 3 groups. Each group met for 30 minutes in a breakout room. Each group addressed a different topic cluster. The percentages next to each item express the level of support, as a result of the polling with the participants at ICANN72. Note that the session was open to all interested, therefore the polling results do not reflect the opinion of ccTLDs only, but of a wider sample from the community.

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)

The final cluster was not separately addressed during the workshop, as those proposed actions should be further considered, following the conclusion of the workshop.

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%)

The groups all discussed the following elements, for each of the discussions:

- 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)

Each group had 10 minutes to report back. After each group, a "temperature of the room" was conducted via zoom polling, to gauge support for the group's findings and assessment.

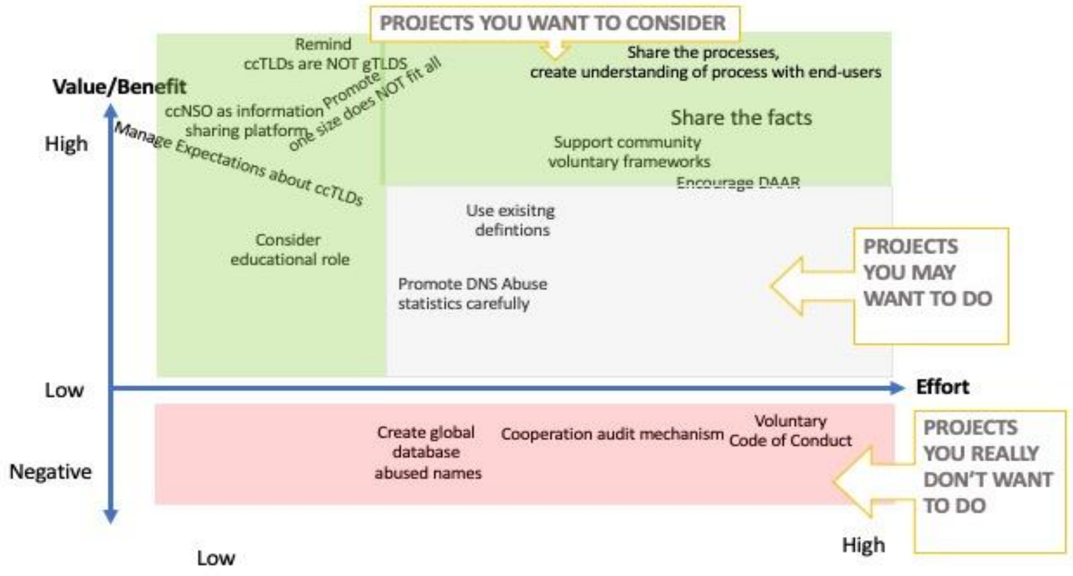
3.2. Consolidation of the results

In order to be able to make the right decisions and prioritize correctly, after the conclusion of the workshop, the results were mapped in 2 ways:

1. Firstly, to assess the value/benefit and effort
2. Secondly, to determine the impact and the effort

On 23 November, the proposed distribution was reviewed by the small group of Councillors that assisted with the planning of the workshop.

3.2.1. Results Benefit-Effort analysis



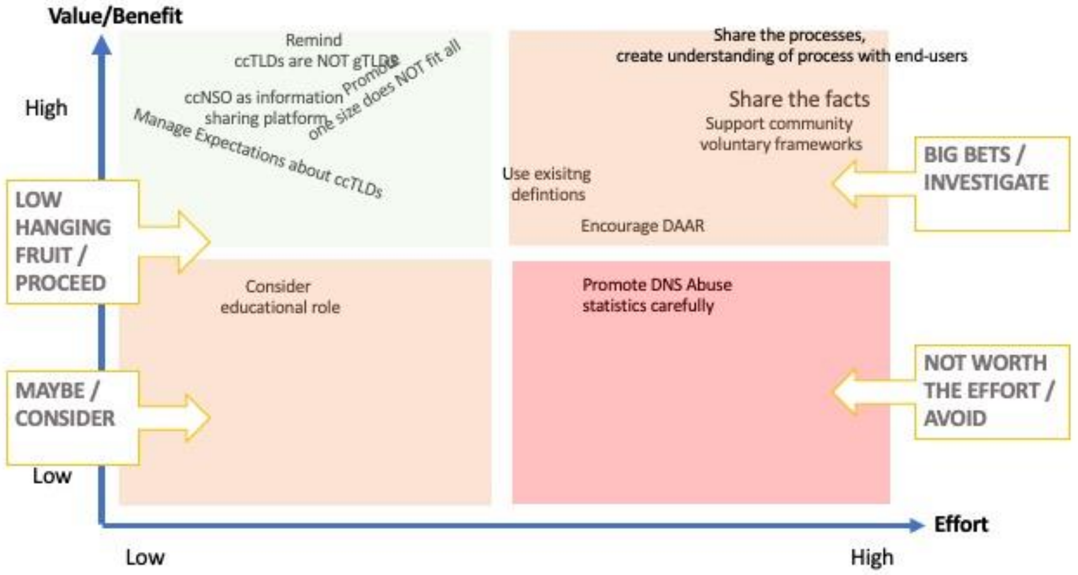
Note that the value/benefit could also be rated as being negative, meaning that the benefit or added value for the ccNSO and ccTLD community is considered detrimental i.e as being a “high risk” on the goal of the ccNSO with respect to DNS Abuse.

The statement to “Develop a voluntary code of conduct for ccTLDs” was considered to be most controversial. Although voluntary for ccTLDs the group identified a high risk that external parties would impose a (perceived) requirement to adhere to a code. Further, the development and maintenance of such a code as well as managing the subscription, implementation and monitoring of breaches of the code would be very impactful and change the role of the ccNSO. The benefit was therefore considered negative.

3.2.2. impact-effort analysis

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

Note that the suggestions with a NEGATIVE BENEFIT are NOT included.



3.2.3. Prioritization assessment

Proceed high(er) impact, low(er) effort	Investigate high(er) impact, high(er) effort
1. Remind all stakeholders that ccTLDs are not gTLDs 2. Consider a best-practice, educational role 3. Share information with ccTLDs and build awareness 4. Manage expectations about the role of ccTLDs & (ccTLD) registrars 5. Promote "one size does not fit all”	1. Share information with other parts of ICANN 2. Share the facts 3. Use existing definitions of DNS Abuse 4. Support community developed voluntary framework 5. Encourage ccTLDs to participate in DAAR
Consider low(er) impact, low(er) effort	**Avoid** low(er) impact, high(er) effort
1. Consider a best-practice, educational role	1. Promote DNS Abuse statistics carefully

3.2.3. Discussion highlights and remarks

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.

4. Next steps: What will be the Biggest Bang for the Buck?

The Ad-hoc DNS Abuse group is looking into various methods to develop and propose a roadmap and related schedule for the next phase of ccNSO & DSN Abuse process. Following a more in depth analysis the group will propose first to Council a ccNSO roadmap and after feed-back present it to the ccTLD community. It is the intention of the group to close the discussion on the roadmap by ICANN73 and use that meeting to start acting.

Based on an initial and non-conclusive analyses of both the current situation and results from the ICANN 72 session and the workshop, the following key-elements should be enhanced i.e are missing:

Missing elements

- **Enhance and Ensure continuous sharing of Information.** Strengthen the platform function to share information (dedicated sessions?) and use it to create reliable and accessible information on DNS Abuse & messages

- **Messaging.** Develop narratives and messages and build a repository and identify channels for messaging to be used by the ccNSO and ccTLD community to disseminate information and messages to GAC/Governments, GNSO, Other stakeholders (including ICANN org and ALAC) and ccTLD community at large.

- **TLD DNS ABUSE OPS group.** The TLD-Ops model to build a (cc)TLD DNS ABUSE mitigation group. Its functions could be to consolidate the metrics and share information, Assist in capacity building and best practices, monitor and address incidents. Interact with gTLD DNS Abuse and other (global) initiatives

- **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.

What to do next?

In order to close the GAP identified above tentatively the small group will consider the following steps and phasing:

First Phase

- **Create TLD-DNS Abuse Ops group**
- **Develop and Prepare Messaging**. (OISC?) includes building relations with other groups

Strengthen the ccNSO platform. Ensure MPC, Tech WG, TLD-Abuse committee are involved and in addition to other topics focus on DNS Abuse mitigation in general and ccTLDs specifically.

Second Phase

- **Maintain Platform function**

- **The TLD-DNS Abuse Ops group** is advised to focus on:
  Metrics. Build a repository and list practices. Share information and messaging resulting from metrics. Involve ccTLD community in TLD Abuse-Ops (populate the email list).
  Build links with existing groups.

Third phase

- **Inform broader community of Practices**
- **Capacity building**. Develop play-books

ANNEX A: Background ICANN72 session

1. Links

- Briefing Paper

https://docs.google.com/document/d/1DCiibYqrXb2b6T8z4sSBJdzq7qRR_4wU/edit?usp=sharing&ouid=108932396147626517991&rtpof=true&sd=true

- Recordings & session transcript

https://72.schedule.icann.org/meetings/GDebBq5NbTCHRBvCq

2. Mapping presentations and suggestions to statements

Statement 1: Share information with ccTLDs and build awareness

(John, Kristof, Byron)
The statement combines the following suggestions:

a. Be informative both to the ccTLD community but also to other parts of the ICANN community.
b. Knowledge sharing
c. Share information on DNS Abuse

Transcript:

> *The other thing I would talk about is something that the ccNSO is very good at, and that is knowledge sharing. So there are lots of ccTLDs that have a lot of expertise in this area. Maybe something the group could is have some form of knowledge sharing group.*
>
> *Awareness building and knowledge sharing to reach a certain maturity level in the industry. And I'm sure we can do that.*
>
> *I think that's important is really around Tech Day and member meetings and our community's ability to share best practices in a really constructive and collegial way, which I think is one of the great strengths of the ccNSO community specifically and probably also the ccTLD community in general.*

Statement 2: Share information with other parts of ICANN

(Gabriel, John, Jim, Byron)
The statement combines the following suggestions:

a. Be informative both to the ccTLD community but also to other parts of the ICANN community.
b. Work with the ICANN community to consider evolving issues and seek to improve, on an ongoing basis, whatever you decide to do
c. Share information on DNS Abuse

Transcript:

> *Do work with the ICANN community with all of us in the large. I know that we all like to have our own models of the world. Even gTLDs do. We like to have our way of doing things. And ccTLDs do, too. But we can always work together*
>
> *There's a lot of work in this area. And I do recommend that your members, the ccTLDs, get involved in those discussions. That's very important. Clearly, there are problems online. There is harm caused. This is problematic for everybody, including the cc's.*
>
> *Encouraging folks to share best practices, what's working in security, what's working in addressing abuse, and what's not working. when you share you best practices, I encourage you to make them available not just to other ccTLD operators but to folks in the greater community like us in the PSWG and the GAC and others that might be interested in hearing your learning points*

Statement 3: Consider a best-practice, educational role

(John, Gabriel, Kristof, Jim)
The statement combines the following suggestions:

a. Consider whether there is a "best practices" educational role, along the lines of what the TLD-OPS program does.
b. Share what works (e.g. .dk presentation)
c. Knowledge sharing
d. Create a framework within which each ccTLD can do what is best for it

Transcript:

> *Encouraging folks to share best practices, what's working in security, what's working in addressing abuse, and what's not working. when you share you best practices, I encourage you to make them available not just to other ccTLD operators but to folks in the greater community like us in the PSWG and the GAC and others that might be interested in hearing your learning points*
>
> *Awareness building and knowledge sharing to reach a certain maturity level in the industry. And I'm sure we can do that.*

Statement 4: Consider a role for TLD-OPS or similar group

(John, Kristof, Byron)
The statement combines the following suggestions:

a. Consider whether there is a “best practices” educational role, along the lines of what the TLD-OPS program does.
b. Awareness building, Knowledge sharing

Transcript:

> *Some form of knowledge sharing group. The ccNSO does this in the broader area of DNS security. Many of your members are on something called TLD-OPS. I have sat through many fascinating work sessions. So I really see the role of the ccNSO as this ability to bring together the ccTLD operators and share knowledge and experience.*
>
> *Also mentioned the TLD-OPS. have the business continuity and disaster recovery playbook developed. There’s also the DDoS mitigation playbook. So I think we can create another one that concerns domain name abuse. for this propo[sal], for this meeting, I’m not going to talk about DNS abuse but specially about the misuse or the abuse of domain names because that’s not the same name as the abuse of the domain name service itself. So that’s more like a nuance that I want to put there.*
>
> *There’s a real opportunity to create some kind of DNS abuse group within the ccNSO community. And I know this has been touched on before and there are other groups in other parts of the ICANN world that deal with this. TLD-OPs as model. And, fundamentally, it’s a very robust and up to date contact list of the right people in each of our ccNSO member registries—the ones who potentially could actually be dealing with DNS abuse. So like the TLD-OPS, it’s a very specific list. I think there’s an opportunity potentially for us to do the same kind of things for DNS abuse*

Statement 5: Encourage ccTLDs to participate in DAAR

(John, Gabriel, Anil, Byron)
The statement combines the following suggestions:

a. Contribute to DAAR (measure what is happening)
b. Encourage ccTLDs to join DAAR
c. Encourage ccTLDs to join DAAR

Transcript:

> *When you’re dealing with abuse, you’ve got to be able to recognize it, you’ve got to be able to action it, and you’ve also got to be able to measure it. We measure reputational data through our DAAR system*
>
> *Contribute to a shared understanding facts. So DAAR, in this case, is ICANN’s Domain Activity Abuse Reporting, and it’s something that I think that is, to my understanding*

voluntary for ccTLDs to contribute to, but it really helps us to understand what's actually occurring out there.

DAAR is very important, which has said. It's a project of ICANN and I think most of us should adopt it. And there should be an improvement of the DAAR also, that more information should come and more analyzation should come.

Joining ICANN's DAAR Programme, I think, is a good and easy first step. Of course, as we've seen in some of the chat, people have questions about some of the elements of it. It continues to be a work in progress. But I think we can all agree that it's a reasonable first step that registry operators can take to get an understanding of both absolute numbers but also a relative perspective in terms of their zone. provides an independent verification or validation of what we believe to be true in our registry. Lead our organizations and are responsible and accountable for the performance of our organization, including DNS abuse. And I think one of the things that we want to do is benchmark so we know where we stand. Are we keeping up with the community? Are we doing what we need to protect our corner of the Internet?

Statement 6: Support community developed voluntary frameworks

(Gabriel, Jim)
The statement combines the following suggestions:

a. Support community developed voluntary frameworks where available (e.g. framework on DGA linked to botnets and malware)

Transcript:

Encourage you to think about a framework. I know that ccTLDs, just like gTLDs, all have different business models. We all have ways of doing things. if you have a framework, you can allow for different local policies so that individual ccTLDs can of course honor and respect their own jurisdictions or whatever jurisdiction of choice they might have.

Make better the voluntary frameworks that we're trying to stand up. So, again, the framework on domain-generation algorithms associated with malware and botnets is something you might have reason to come across as if a cop brings it to your attention in the future.

Statement 7: Manage expectations about the role of ccTLDs & registrars

(Kristof, John)
The statement combines the following suggestions:

a. Manage expectations
b. Focus on what ccTLD registries, and their registrars can actually do

Transcript:

> *Expectation management. Abuse is of all times. It will remain forever. There is no silver bullet. And it's not because people, others, ask us to hunt the crooks instead of the police that e-crime with evaporate*
>
> *When you're dealing with abuse, you've got to be able to recognize it, you've got to be able to action it, and you've also got to be able to measure it.*

Statement 8: Create a global database of abused domain names
(Anil)
The statement combines the following suggestions:

a. Create Global Data base of abused domains & share with all ccTLDs

Transcript:

> *Create a global database of abusing domains—and not only creating a global database but we should also share this global database with all because there are no boundaries of domains, whether they are ccTLD domains or gTLD domains.*

Statement 9: Create co-operations for regular audit mechanisms
(Anil)
The statement combines the following suggestions:

a. Create Co-operations and associations for regular and sustainable audit mechanism

Transcript:

> *Create the cooperations and associations. For what? For a regular and sustainable audit mechanism. Again, the audit may not be mandatory, but it can be voluntary. But an audit helps in understanding, with the operators, with everybody, how and what effectiveness is there and how we have to mitigate this*

Statement 10: Remind all stakeholders that ccTLDs are not gTLDs
(Byron)

Transcript:

> *Don't forget that ccTLDs are very different than gTLDs. And while many of you here may know that—it's literally in your DNA; you know that innately—that's not always the case. When we're talking to the broader ICANN audience, such as we are today—we need to*

continue to reinforce that point that there's significant difference between the cc and g space on a number of fronts, not the least of which is contractual obligations to ICANN.

Statement 11: Promote that "one size does not fit all"
(Byron, Kristof)

The statement combines the following suggestions:

a. Do NOT act as if one size fits all

Transcript:

> *Remember that ccTLDs within the ccNSO and more broadly very widely are very, very different across the spectrum of our TLD community. You can think of .uk or .de for Germany have 11 and 17 million names respectively. But there are many ccTLDs who would count their domains under management in the tens of thousands or, quite frankly, even less. Issue on resourcing. Going to ask this community to do new things or think about being responsible for new things—we really have to take into account the variation within our registry community, the size of the registries, the scarcity of resources that some of those registries experience.*

Statement 12: Create an Abuse Mitigation Working Group -> TLD-Ops kind of Group
(Byron)

The statement combines the following suggestions:

a. Consider Creating a DNS Abuse Mitigation Working Group and Wiki

Transcript:

> *There's a real opportunity to create some kind of DNS abuse group within the ccNSO community. And I know this has been touched on before and there are other groups in other parts of the ICANN world that deal with this. TLD-OPs as model. And, fundamentally, it's a very robust and up to date contact list of the right people in each of our ccNSO member registries—the ones who potentially could actually be dealing with DNS abuse. So like the TLD-OPS, it's a very specific list. I think there's an opportunity potentially for us to do the same kind of things for DNS abuse*

Statement 13: Do NOT focus all efforts on defining DNS Abuse
(John, Jim, Byron)

The statement combines the following suggestions:

a. Do not create another definition of DNS Abuse
b. Do not get into the weeds in joining the discussion on definitions
c. Do NOT re-invent the Wheel - Acknowledge that there is a lot of excellent work going on in other fora on this subject

Transcript:

> *One is to actually not create another definition of DNS abuse. If you're going to have a common definition, find alignment with an existing definition. The contracted parties have a shared definition. There are a couple of others out there. But rather than trying to invent something new and completely different in this community and thus confuse all of that, try to find one that you can find alignment with for your baseline if you're going to do that.*
>
> *Don't go off and start your own definition of what is DNS abuse. Try and work with other groups that are already doing this. Don't do it on your own.*
>
> *if you are going to go down the route of finding a definition. Think about what elements of something make it DNS abuse. What makes something DNA abuse and something not be DNS abuse. And that's probably not something you're going to do in the ccNSO yourself. It's probably something that indeed you would work with other areas of the community on. There's a lot of work in this area. And I do recommend that your members, the ccTLDs, get involved in those discussions. That's very important. Clearly, there are problems online. There is harm caused. This is problematic for everybody, including the cc's.*

Statement 14: Promote DNS Abuse mitigation initiatives with care
(Kristof)

The statement combines the following suggestions:

a. Do NOT promote the "wrong" initiatives (be aware of methodologies, objectives etc.)

Transcript

> *Don't promote projects, studies, or data sources that lack transparency about your region, that lack of transparency about the methodology that we use, about the reliability of the information, or, even worse, try to commercialize DNS abuse mitigation.*

Statement 15: Develop a voluntary code of conduct for ccTLDs
(Byron)

The statement combines the following suggestions:

a. Develop a voluntary code of conduct for ccTLDs

Transcript:

> *Establishing a voluntary code of conduct for ccNSO members in terms of dealing with DNS abuse. it would have to be voluntary, given the nature of our community. And I see it, quite*

> *frankly, as being a best-practices list issue. What is actually in that code would be something for the ccNSO to decide over time*
>
> *Lead our organizations and are responsible and accountable for the performance of our organization, including DNS abuse. And I think one of the things that we want to do is benchmark so we know where we stand. Are we keeping up with the community? Are we doing what we need to protect our corner of the Internet?*

Additional Statement: Relation with Government
(Byron)

Transcript:

> *Don't ignore the relationship between ccTLDs within the ccNSO membership and national governments and other elements of national governments if any ccNSO member wants to strengthen their cybersecurity posture in general and work to address DNS abuse specifically, building a good relationship with your national CERT is certainly an important step. So don't let those relationships with government or government entities wither or not be developed. GAC that, if they're concerned about their ccNSO's TLD rule in addressing DNS abuse, I think, as the saying goes, "Physician, heal thyself." Reach out to your ccTLD directly.*

3. The combined story of the presenters

Each of the presenters was asked to use the following 3 questions to guide their presentations:
1. What is your perspective on DNS Abuse?
2. What are the major issues at stake?
3. What are the do's and don'ts for the ccNSO, regarding DNS Abuse (maximum 3 suggestions)?

Via questions one and two, the presenters were able to introduce and provide context, including colour and depth, to their suggestions. Grouped under nine headings, please find included below relevant extracts from the session transcript.

1. What is the problem space ?

Transcript:

> *DNS abuse? It's a term that gets used a lot. We also use the term, within ICANN, within one of the groups that I run, which is the Security, Stability, and Resiliency Group, "security threats." In many ways, the labels don't really matter.*

So DNS abuse is, without a doubt, a plague, and it's a plague that's actually getting worse. And I think the first step for any registry operator is to really find out the extent of that plague in their zone, in their registry.

Fair to say and to acknowledge that abuse in general is certainly on the increase at an astonishing rate on the Internet. And this really is just abuse in all of its forms—on the Internet, with the Internet, over it, through it, in all manner of things. This is not just the DNS as a protocol. There are other mechanisms, other kinds of things going on. It really is a global problem and it affects everybody

"Everybody" in this sentence, I really do mean all of us as individuals, all Internet users. You're either a victim or maybe you're an unintentional co-conspirator because your home laptop has been taken over or something else along those lines. Countries have issues in terms of being a source or even being a victim.

2. Scope of DNS Abuse

Transcript:

So if you are going to go down the route of finding a definition. Think about what elements of something make it DNS abuse. What makes something DNA abuse and something not be DNS abuse. And that's probably not something you're going to do in the ccNSO yourself. It's probably something that indeed you would work with other areas of the community on. There's a lot of work in this area. And I do recommend that your members, the ccTLDs, get involved in those discussions. That's very important. Clearly, there are problems online. There is harm caused. This is problematic for everybody, including the cc's.

Scope of the issue: keep in mind that most ccTLD registry operators are concerned about cybersecurity and about the amount of abuse in their zones. I'm also convinced that they try to do what is within their power and means. So although we all face cases of abuse, the problem is mostly concentrated at the small number of players.

Well, we all know harm to the user, the victim, of some of these harms. There's also the trust in the ecosystem and the reputational risks that came if you have a lot of abusive behavior happening within a particular TLD, be that cc or not. It's the same problem everywhere. have a lot of commonality in the risks and the issues that are at stake with your colleagues and peers in the gTLD space. So talk to them about that.

Big trends that we're seeing in 2021. And these are actually a continuation of crime trends that have been plaguing the world for literally years. Most worrisome and ongoing—is ransomware, on one hand, and what we call business e-mail compromise on the other.

Not all of the incidents of these criminal ongoing schemes are actually directly relevant to DNS abuse. The top three categories of ransomware that are being used out there, a significant amount of it is directly linked to e-mail phishing as the initial intrusion vector.

So DNS abuse is, without a doubt, a plague, and it's a plague that's actually getting worse. And I think the first step for any registry operator is to really find out the extent of that plague in their zone, in their registry.

3. Need to measure

Transcript:

And I think there's an age-old management maxim that we probably all heard before, but it is effectively that what gets measured gets managed.

Reliable and consistent metrics of definitions are absent.

Currently, metrics are based on incident-based measurement. Government has a different set of definitions about this kind of abuse: establishing a distributed command and control, spam and phishing activities, malware attack on countries' critical information infrastructure, which impacts the nation as a whole, and espionage.

The lack of availability of healthy collaborations. And with that, I mean—and I put it on the screen—that, too often, it comes down to a third party, another party, saying to us, "Give us your data and we will tell you whether you're doing your job well enough." And I think that's not really a good example of good cooperation.

4. Public safety perspective

Transcript:

Not all of the incidents of these criminal ongoing schemes are actually directly relevant to DNS abuse. The top three categories of ransomware that are being used out there, a significant amount of it is directly linked to e-mail phishing as the initial intrusion vector

Newly elected president made ransomware a top priority for international dialogue on the global stage. And that, to my eyes, was unprecedented. Really eye-opening to folks in my line of work.

It might be unrealistic to expect that ICANN can solve these huge, thorny, crazy issues, but nonetheless, we have to recognize that the decisions we're making here do have direct impact on the schemes I've just discussed.

From a public safety official side benefit is tremendous from having ***swift*** *access to accurate domain registrant information. Most worrisome trends that do sometimes—not always—touch on DNS and policy therein, I do also want to call out that there is a very high-impact but low-frequency touchpoint where law enforcement does speak to ccTLD operators along with other TLD operators, registries.*

Combating it is in the public interest. There is no doubt because we are losing both money as well as the data. Coming to the mitigation level.

5. Why is domain name abuse successful and persistent?

Transcript:

These days, there are two groups of people, who are getting affected. One is the big people who say, "We lost $600 million and we have to pay for this. Then there are small, small customers, citizens, who are impacted by daily abuse.

Couple of reasons why domain name abuse is so popular and so successful.

1. *e-mail short message service security is fundamentally broken. We tried to create security extensions to fix it, but there is slow adoption, poor implementation. There's so much misconfiguration. So it's still insecure.*
2. *We have OS and software vendors that want to make us or keep us unaware. I have a concrete example. We had the discussion about hiding URLs in browsers. security experts and software developers thought that the way certificate authorities implemented "know your customer" was not the way forward, that it was causing more insecurity than security*
3. *Many exploitable resources on the Internet: hacked DNS servers, mail servers, vulnerable [inaudible] systems, compromised web hosting, etc*
4. *Security issues in the domain name sales channel—so the channel, the chain between the registrant and the registry. And since the [Seater] Campaign, this is also a hot topic in Europe for policymakers. And we also see that reflected in the EU cybersecurity [pact]. So there are a lot of legal initiatives now getting their way to new directives and new laws in Europe. And if we're honest to ourselves, we know we can step our effort in [inaudible] domain. It's also there, I think, as a community, that we can make the difference.*

6. Role of (cc)TLDs

Transcript:

We all have a role to play—that was also mentioned before—in securing our digital world. And for me, if we do nothing, there is a risk of market disruption and then risk that we end up—and "we" means the ccTLD registry operators—doing business on an *unequal playing field, meaning that cc's will be overregulated and others not so that we have a much bigger burden than others and less flexibility to run our businesses.*

We all have a role to play in mitigation of some abuse, but the question is, what is that role? And that's what we're here today to talk about: a potential role for the ccNSO

7. Scope of ccNSO role

Transcript:

Clarifying the scope within which I think the ccNSO can have real added value and—who knows?—maybe even be a differentiator.

Focus on awareness raising seems to yield a benefit. Awareness is a very, very important aspect which is required in all the policymakers, the organizations, registrars, registries, and all those things, including the public. I think there is a great push for coordinated efforts

Scope of the issue: keep in mind that most ccTLD registry operators are concerned about cybersecurity and about the amount of abuse in their zones. I'm also convinced that they try to do what is within their power and means. So although we all face cases of abuse, the problem is mostly concentrated at the small number of players.

The lack of availability of healthy collaborations. And with that, I mean—and I put it on the screen—that, too often, it comes down to a third party, another party, saying to us, "Give us your data and we will tell you whether you're doing your job well enough." And I think that's not really a good example of good cooperation.

8. Share Experience/Cooperate

Transcript:

Focus on awareness raising seems to yield a benefit. Awareness is a very, very important aspect which is required in all the policymakers, the organizations, registrars, registries, and all those things, including the public. I think there is a great push for coordinated efforts

A framework for DNS abuse that is shared by many of the contracted parties. This framework actually has three important key parts to keep in mind.

- *One of course is a baseline of that shared definition of DNS abuse. Those who share and voluntarily sign up for this abuse framework.*
- *It has an opportunity for a number of other common things that many registries and registrars deal with. Child sexual abuse is a common element of those things. So it provides an opportunity for people via local policy, local considerations, to*

agree they're going to deal with that. Terrorism is another common thing, among a whole set of other things. But, again, the important thing is that's local policy.

- *option for really just individualized additions. There are some registries and registrars that have their own requirements and their own set of common use policies, terms of use policies—that kind of thing—and they want to address those things*

In general, we (contracted parties) share a commitment to advancing remediation and mitigation of DNS abuse. And that's important. I think that that's what the ccNSO is considering here. What role might it play in promoting and advancing these kinds of activities among ccTLDs in general?

We very actively do outreach to other elements of the ICANN community, listening to pain points and stories, and take on those activities to address those things with work product.

9. Potential measures to mitigate DNS Abuse

Transcript:

First question to you all is, which angle do you choose? Do you go for, let's say, the narrow sight or are you going for the broader view on the problem? And with the narrow vision, I mean that it's not because domain names are used as a tool—and I really mean a tool—in the cyber kill chain that DNS infrastructure operators should also be obliged to fight abuse [with] or, even worse, they should be held responsible when abuse fighting doesn't result in a safer Internet. worrisome that, in a DNS abuse session, such an example as ransomware is used where there is a massive, very long, cyber kill chain, and a domain name is only really a tool that is used when all those different aspects go wrong, like [p]atching and lack of monitoring, etc

Explore the role of technical solutions in mitigating DNS abuse. We have seen in the last few years that a lot of new technologies have come up. Whether they are impacting for us, whether they're helpful to us, that is what we have to see.

- *First of all, we designed an algorithm for blocking the key words. For example, we blocked "gov" to be given to the public.*

- *Secondly, registry participation in global coordination in spam takedown requests along with CERT-In. So this is an internationally global coordination which we are able to do and we are able to achieve it.*

- *Most important thing which I want to share with all of you is that we have implemented electronic "know your customer" verification. And this is a resulting in real reduction in DNS abuse.*

ANNEX B: Background November Workshop

1. Links

- Workshop Invite https://ccnso.icann.org/en/announcements/announcement-17nov21-en.htm

- Background material, recordings and attendance https://community.icann.org/x/FAe7Cg

- Jamboard https://jamboard.google.com/d/1GLUyZAOeMrChSo40EAwqh3cZMYswSuh9pHS4f_qMGmU/edit?usp=sharing

- Informal notes https://docs.google.com/document/d/1cJfS0wGm7rtrDa_QiqIdUGuMD6DdwWL0iGtJVXWGvMI/edit?usp=sharing