ICANN76 | CF – ccNSO: DNS Abuse Standing Committee Update
Wednesday, March 15, 2023 – 15:00 to 16:00 CUN

DAVID MCAULEY: Hello, my name is David McAuley and I will be speaking during the session today. I am testing my audio to confirm that the technical service providers can hear me clearly.

CLAUDIA RUIZ: Thank you, David. The interpreters confirm your audio is good.

UNIDENTIFIED FEMALE: Andrea, I think you're very feint. Or Claudia, sorry.

CLAUDIA RUIZ: Fernando, you're next.

FERNANDO ESPANA: Hello, my name is Fernando Espana and I will be speaking during the session today. I'm testing my audio to confirm that the technical service providers can hear me clearly.

CLAUDIA RUIZ: Okay, Fernando. This works. Nick?

NICK WENBAN-SMITH: Just testing, testing. Hello, my name is Nick Wenban-Smith and I will be speaking during the session today. I am testing my audio to confirm that the technical service providers can hear me clearly.

CLAUDIA RUIZ: Okay, that was good, Nick. Tatiana?

TATIANA TROPINA: Hello, my name is Tatiana Tropina and I will be speaking during the session today. I am testing my audio to confirm that the technical service providers can hear me clearly.

BRUCE TONKIN: Hello, this is Bruce. I'm just testing my Australian accent.

BRENDA BREWER: One moment, please. This session will now begin. Please start the recording.

Hello and welcome to DNS Abuse Session. My name is Brenda. Along with Devan, Claudia, and Andrea, we are the remote participation managers for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior.

During this session, questions or comments submitted in chat will only be read aloud if put in the proper form, as I've noted in the chat. I will read questions and comments aloud during the time set by the moderator of this session.

Interpretation for this session will include English, Spanish, French, and Arabic. Click on the interpretation icon in Zoom and select the language you will listen to during this session. If you wish to speak, please raise your hand in Zoom and once the session facilitator calls upon your name, kindly unmute your microphone and take the floor.

Before speaking, ensure you have selected the language you will speak from the interpretation menu. Please state your name for the record and the language you will speak if speaking a language other than English.

When speaking, be sure to mute all other devices and notifications. Please speak clearly and at a reasonable pace to allow for accurate interpretation. This session includes automated real-time transcription. Please note this transcript is not official nor authoritative. To view the real-time transcription, click on the closed caption button in the Zoom toolbar.

To ensure transparency of participation in ICANN's multi-stakeholder model, we ask that you sign into Zoom sessions using your full name. For example, first name and last name or surname. You may be removed from the session if you do not sign in using your full name.

And with that, I will hand the floor over to Nick Wenban-Smith, our session moderator.

NICK WENBAN-SMITH: Thank you very much, everybody, and welcome to this session of the ccNSO DNS Abuse Standing Committee. My name is Nick Wenban-Smith and I represent the DotUK registry. This committee is a

subcommittee formed by the ccNSO Council not even a year ago, so back in April 2022, and I'm very pleased that we have some substantive progress and some tangible outcomes to present to you all today and I'm really hoping for a very constructive and engaging dialogue on this important topic. I think it's very important that the ccNSO has its own thought leadership and a distinctive voice in this area.

Just a little bit of background from the terms of reference for this committee. I think it's very important to be crystal clear about what is not within our scope and what we are here for.

According to our terms of reference, we are here to provide a dedicated forum to discuss the topic of DNS abuse. It is a wide cross-community concern and I would like to say, because of the very small amount of abuse that most of the ccTLDs have, it's not really been a pressing issue for us. But we were finding that people were perceiving that it wasn't a high interest area for us and the space that we were vacating by not talking about it publicly and taking a proactive stance, other people started to talk to us actually incorrectly around what ccTLDs do in abuse. So that's part of the purpose of this, to remedy that problem

Having said that, we are not here like the GNSO to formulate policy. It's explicitly not a policy formulation project. It is about raising understanding and awareness between all of us across our wonderful community and that includes a lot of messaging and metrics and I'm very keen to get objective data so that we can have an adult conversation on it.

I'll pass on in a moment but I want to say one final thing in my introduction and that is according to our terms of reference, we are here

also to have open and constructive dialogue because I don't like silence. I would encourage everybody here to take the opportunity to speak early in the meeting because otherwise I'm probably going to pick on you with topics later on in the meeting when the questions might be more difficult. So my advice is to engage early and get some good points in soon. So please do log into the Zoom room because that's obviously the easiest way for us to keep track of the questions and answers and to make sure that we cover everything. And I will do my very best to keep to the agreed timing in the agenda.

So, that brings me on to the first update, which is from one of our two subgroups and this is an important subgroup around we call the DASC repository and I will hand that over to David for a little overview of their activities, and then after that there will ben an opportunity for some questions and answers. So, David, over to you.

DAVID MCAULEY: Thank you, Nick, and hello again, colleagues. My name is David McAuley. I am an employee of Verisign and participate in the ccNSO and this committee by virtue of our management of the DotCC country code top-level domain. I am here today as the lead of the repository subgroup of the Domain Name Abuse Standing Committee of the ccNSO and we are here today to talk about what we do which is basically informational help for ccTLD managers. So, for the first slide I'm going to turn to my colleague in the subgroup, Fernando Espana. Fernando, over to you.

FERNANDO ESPANA: Thank you, David. And I will be speaking Spanish, so if you need to use a headset, please do so.

Good afternoon, I am Fernando Espana from GoDaddy. I am here presenting DotUS. Today we are going to focus on the subgroup of the DASC repository. This subgroup has two projects on which we are working.

The first one is setting up a repository with information links that can be useful for all DNS abuse and other resources and tools for ccTLD managers. This project is the one which we are carrying out right now.

The second one is to create an email list, a dedicated one for the ccNSO, so that it is used by ccTLD managers for exchanging information related to DNS abuse. This project will start once project number one has been completed.

And now I give the floor again to my colleague, David, who will give you additional information about other topics.

DAVID MCAULEY: Thank you, Fernando. Thank you for the next slide. So, you can see the information on the slide in front of you, but basically what we're doing in this group is creating a repository of information that should be helpful to ccTLD managers to ccNSO members, and we're going to start lightweight. We're going to get the information out to those people I just spoke about, the ccTLD manager, the ccNSO member. The group may go beyond that in the future, but we want to get our legs under us. We want to get started and well grounded. So this will all be done under the auspices of a group that we will establish which is basically a repository

editorial board and I'll talk about that in just a moment. Next slide, please.

So, the DASC. All of this will be controlled, by the way, to the DASC to which we will be reporting. But the DASC will be an appointing an editorial board whose job it is, is going to be to manage what we do to make sure that we're coming up with the correct information.

Now, I'd like to speak to the bottom bullet point first which has four sub-bullet points and this is the information categories. This is what we're looking to put out to our CCD colleagues. And it will be things such as presentations and reports. Just a couple of examples. There was an Interisle report on DNS abuse. There was an EU study on DNS abuse. There's any number of these kinds of things that appear and what we intend to do is get links to those, briefly describe them, and give the ccTLD managers access to these links.

Next we want to have a category of tools and the tools are just, as the name implies, things that will be helpful to ccTLD managers when it comes to dealing with, to understanding DNS abuse and the issues that DNS abuse presents. Our colleagues in the DNS Abuse Institute have come up with some tools I'll use as an example. One is their netbeacon.org tool for reporting instances of DNS abuse. Another is their DNS Abuse Compass project which is a tool that measures DNS abuse, phishing and malware. So it's tools like that that have become more and more prevalent, perhaps. We'll give access to those and pointers.

Third, we'll point to various iterations of definitions and policies. Many of you I'm sure have watched this discussion unfold in the overall ICANN

community and understand that there are more than one definitions or approaches to understanding DNS abuse. So we will give you access to those we see and we think are relevant to see and to see what the perspective of these definitions are coming from.

Then, fourthly, we will have pointers to articles and commentaries which of course are also numerous and you'll see those in publications like CircleID where there's oftentimes very interesting commentary but you can also see it in newspapers and things of general interest. We will look those and this board that I spoke about will be considering them and doing its best to point to our members, those that are most useful, most relevant. So the board will work under the direction of the DASC overall. Next slide, please.

This board will also do the administrative work to vet the information, to make sure it's reliable. We will be doing work to promote knowledge of this website that we will have and usefulness of it and to increase access to it. We will be moving things to an archive when we think that their timeliness, the immediacy of their timeliness has passed and things of that nature. And we will stay in touch with the DASC. We will report to them and keep them apprised of just what's going on. It's very lightweight. So, next slide, please.

So, these are the members of the group. So, for all of our colleagues here, feel free to contact us as a group or individually. You know us, see us in the halls. Give us your reactions if you wish. I want to thank my colleagues on this team. We are moving forward, and as Fernando said, once we're done with the repository—and that's very close—we will be moving on to the dedicated email list to help in this messaging effort.

And with that, Nick, I am done. I'm happy to take questions.

NICK WENBAN-SMITH: Thank you very much, David. And muchas gracias, Fernando. Questions if anybody has [inaudible]. I think we're trying to [inaudible] through the Zoom room but … There's no questions in the Zoom room at the moment.

A question here from John McCormick. Have you considered adding details of which TLDs are running [descanting] offers as there is a correlation between [descanted] registrations and DNS abuse in the gTLDs?

David, is that something that is [covered] within the subgroup? This is a really interesting question and I don't know if it's pertaining specifically to the subgroup update. I think we can address it. It's a question I've been asked before a few times, so I've got some answers for that. What do you think, David? It's not really a subgroup question, I don't think.

DAVID MCAULEY: Well, that is not on our radar screen to this point. We can certainly take that under consideration and run it past the DASC to see if there's an interest in it. There may or may not be, John. But I want to reiterate what our goal is right now is to do this lightweight start so that we do get started, get things underway. A more sophisticated question like that, Nick, I think will wait for the future and we will report back to you if we have any thoughts on it. Thank you.

NICK WENBAN-SMITH: Thank you. And John, I have made a note of your question because it's going to come up in the next agenda item, so I don't want to cover it twice. Are there any further questions? Just put them in the Zoom. I get told off if we follow different rules.

Okay, seeing no further questions, we move on to the next agenda item which is covering the second of the two subgroups. That subgroup has been looking at a survey and it was a great pleasure, really, that I'm introducing these sets of topics. I've had a fantastic group of colleagues on the survey subgroup and we're really pleased with the richness of the data that has been obtained and we're very pleased with the engagement and participation from our community, you folks here.

If you can see the … Can we go on to the next slide, please? Okay. So, this is about the survey. The raw data is that 57 ccTLDs provided unique responses representing approximately 100 ccTLDs out of the total of 316 delegated. So, obviously, there's no compulsion to take part in this. We're pretty pleased at the response rate. We understand also that some ccTLDs are unable to participate in this sort of survey work for various reasons, largely around their own internal processes and structures and governance mechanisms. So we were never going to get 100%.

We have given survey respondents the option to remain anonymous or to have a public statement that their data is for public consumption and we respect that and I think it helped get engagement and to get participation in the survey itself. Go on to the next slide.

Okay. So, the demographics section I would like to hand over to one of my remote participants and a very engaged member of the subgroup. Angela from the DotBW, the Botswana ccTLD.

ANGELA: Thank you, Nick. Are you able to hear me loud and clear?

NICK WENBAN-SMITH: We hear you loud and clear. Perfect, thank you. And continue.

ANGELA: Awesome. All right. Good time of the day to all participants that are joining remotely and buenos tardes to everyone who is physically present in Cancun.

So, going into the demographics, what I'm about to present is really just a retelling of a story about what makes the ccTLDs different. It's basically reiterating the notion that the ccTLDs are indeed not one size fits all. So, this is what we're going to see through the presentation. But what I'd like to bring to your attention is one thing that's interesting about the survey is that we were looking into DNS abuse as a subject that rather doesn't respect borders. So, DNS abuse or cybercrime in general does have the … It has a way to strike anywhere or with anyone who is connected to the Internet. So, with what we're trying to indicate here or what the survey showed as [inaudible], nonetheless what is within each and everyone's country where its ccTLD is housed could hugely determine the methods of mitigation when it comes to DNS abuse.

So, with that in mind, we have the first [makeup in] the region, so most of the responses came from the Europe region followed by APAC, Latin America, Africa, and North America as shown on the screen. We also took a survey on the governance models and originally we used the study that was conducted by the former ccNSO chair, Katrina, to give other options. But we later discovered that there's two more right at the bottom there. You find company limited by guarantee as well as member-driven statutory organizations. But for most of the survey respondents, the not-for-profit organizations stood out the most.

Then of course we had the registry model as well and we see that the highest respondents came from the 3R model which is the registry, registrar, and registrant. But we also had a couple coming from the combination of the [three RNs], the direct registrations. Next slide, please.

So, we also categorized the responders, or the ccTLDs rather, according to size, being the number of domains registered. So, from the respondents, again, we see that over a million domains have been registered, but on average we had responders having over 10,000 domains. We also looked at the size in terms of how many employees each ccTLD had, and for the most diversity, we saw that they have more than 50 employees. But as you see the graph does a lot of combinations here and there, so it's a good representation to say that, despite the size, different ccTLDs are still able to register or monitor DNS abuse as well as you can see that at least two respondents indicated that there's one employee within the ccTLD.

Moving on, we also looked at whether the ccTLDs have an abuse officer. I think this also comes quite important when it comes to looking at mitigation to see if you've got the skills within the ccTLD to look into DNS abuse or if whether ccTLD just uses its normal employees being the ccTLD engineers or the administrators. So, over 75% of the respondents indicated that they actually do not have a dedicated DNS abuse officer. Next slide, please.

So, we also looked into data protection legislation and its possibility to affect the different ccTLDs when it comes to DNS abuse and over 60% of the respondents did state that they are indeed affected by data protection legislation, and of course in the [free] text section, we did allow the respondents to type down what those legislations are.

ccTLDs also indicated that they participate, rather, in some form of collaboration. So, over 80% of the respondents indicated some form of collaboration with either CSET, law enforcement agencies, or trusted notifiers. Some even indicated a combination of those three.

We also finally looked at the percentage of DNS abuse that the different ccTLDs are exposes to, and most of their answers indicated a percentage less than 0.05%, and when you look at this number, it's quite relating to the size itself. So we did have some ccTLDs indicating a 0.5 percentage, yet they have over a million or they have less than a million or they have maybe 5,000 domains. So I just wanted to bring that out, that even though this percentage is a little bit low, it could be coming from ccTLDs that either have more domains or less domains, and so the survey really showed a distributed number.

Also, from the survey results, we see that a lot of respondents indicated that they were not sure of the kind of abuse that the registering or the percentage rather.

So, I think this is about it when it comes to demographics. I'll hand back over to Nick.

NICK WENBAN-SMITH: Thank you very much, Angela. If we could move on to the next slide. So, now I'd like to hand it over to Bruce to take us through the next section on abuse types.

BRUCE TONKIN: Thank you, Nick. I'll use English because my Spanish is even harder to understand than my English.

In terms of types of DNS abuse, bare in mind you'll see on this slide, you'll see numbers. So, as Nick mentioned, at the beginning it was 57 responses to the survey, so a score over 29 indicates that it was a majority of respondents. So, in this case, you'll see in terms of the types of DNS abuse that country code respondents to the survey take action on, the majority are pretty much aligned with what we're seeing with the gTLD community. So that's phishing, malware, botnets, and farming.

With respect to the respondents of the survey, about a third also take action on spam and I think that would be fairly high compared to the gTLD community. So this shows that the ccTLD community is a bit more proactive on spam than some of the other TLDs.

In terms of content abuse, you'll see much the same as what you'd see in the gTLD world but more than half of the respondents take action on child sexual abuse materials or CSAM.

One thing to be careful of when you look at this statistic is it doesn't mean that the other 20 or so that responded don't care, it generally means that the other 20 or so don't actually see this sort of material in their ccTLD. So you've got to be a little bit careful how you read some of these results.

You'll see that in terms of some of the other types of content abuse related to some terrorism content or drugs or cyber bullying, that type of thing, the percentage is much lower, so generally these numbers are coming in at below 25% of the respondents.

When we correlate that against the types of ccTLD data, you see that it's more likely that organizations that are fairly vertically integrated—in fact, they may well be government organizations that actually look after content abuse under their legal framework as well as providing domain name services, whereas in other countries, they're quite separate. So the domain registry operator has a very narrow remit and has no remit for content abuse, but there are other organizations within that country that have that responsibility and the country code operator takes action in response to those other government entities that have responsibility for content. So quite often this links a little bit with trust and notifiers as well and I'll come to that in a further slide.

Then, the graph to the right, which is talking about respondents that take action on trademark matters—and again you might look at those numbers and think, well, they're less than the majority of country code

operators taking action, but most of the country code operators, when you look at the written responses to these questions, have some form of independent dispute resolution service. Often they're based on something similar to the UDRP model from the gTLD world, so the country code operator doesn't take direct action on trademark matters as an independent dispute process and implements the decisions of that dispute provider. Next slide.

This is looking at the type of abuse mitigation trends. So here to mitigate against DNS abuse, complaints, procedures. So the majority of CCs have some form of complaints procedure that won't take into account DNS abuse.

A lot of ccTLDs use consumer awareness to raise the understanding and the community of the types of abuse and how to take action. [inaudible] are typically DNS abuse feeds or DNS intelligence feeds of some form or another. Procedures are either checks at either the beginning before the domain is registered or checks immediately after the domain is registered. So quite a few of the respondents in their written comments talk about checks that they provide after registration and they're looking for patterns, and based on those patterns they might take action. Then a majority of country code respondents have some form of registration policy that deals with DNS abuse. In other words, if a phishing site is found or reported by a member of the public, under their registrations policies they can take action.

The next one here about relationships with trusted notifiers. In many cases, you will see towards the bottom of the graph, the trusted notifiers tend to be local. So they have the local national computer

security incident response team or local national law enforcement or a local national body that specializes in some form of content abuse are likely to be trusted notifiers. That's work that we can understand a little bit more, what trusted notifiers do people use that are outside of the country and that have more global acceptance in the community.

And the last graph here talking about outreach. I think this is part of getting more yeses than nos. I think those that are doing DNS abuse don't necessarily talk about it that much and don't do a lot of broad education. So we've got less than half are doing focused outreach and I think these sort of events that we've had this week and talking to other stakeholders as part of the ccNSO's activities at least to broaden the outreach. Next slide.

So, this one, interestingly, the number I've mentioned in the previous slide you can see that quite a lot of the respondents to the survey do have some sort of local trusted notifier, but not very many of them have a formal agreement and that's probably because some of those trusted notifiers are actually specified by law. But the number of people that have a formal agreement is less than a quarter, so they're generally informal country code operators choosing to take into account the information from some local notifier.

Then if a ccTLD detects abuse, you'll see a range of action but really most … So 31 respondents said that they do a risk assessment, and what that really means is that very few of us will actually take action just because we're notified of the matter, whether it's from the public or even from a trusted notifier. Most of us will actually do our own risk assessment to see whether we can verify that there's phishing or verify

that there's malware before we would take action, and hence that bar graph there saying the approach depends on the results of the analysis that the country code does.

Then the last table here has basically as you'd expect, most of us have some form of ability for the public to report an incident of DNS abuse. Next slide.

TATIANA TROPINA: Thank you. Tatiana Tropina here, ccNSO Council, NomCom appointee. So, up to now, what you saw on the slides, you saw what the numbers say. But sometimes to actually see the fuller and more interesting picture, we look beyond these numbers, beyond these statistics and look at the free text comments. For example, Bruce ended with his slide on the existence of reporting mechanisms. But just the sheer existence of reporting mechanisms does not show us the full diversity.

So, when we look at the free text comments, we will see that ccTLDs utilize a variety of mechanisms. It can be reported by email, reported by [inaudible], reported by special forms on the website, a whole combination thereof. And interestingly, we can look also of the role the appropriate agencies or first responders like computer emergency response teams. So some of the ccTLDs rely on these institutions as a reporting mechanism, and at the same time some of the ccTLDs indicated that once DNS abuse is reported, they try to direct public—general public—to appropriate law enforcement agencies or again to computer emergency response teams. So there is like sort of two-way road. Next slide, please.

I'm going to come back to what Bruce was already talking about. I'm trying to see the next slide. Yeah. So, what I was going to talk about until the next slide appears is the actions the ccTLDs take upon receiving a request from the law enforcement agencies to take down a domain name. You probably know this yourself, right? There are a few ways to go. You can perform your own due diligence. You can rely on this request. But most of the respondents indicated that they do perform their own due diligence as Bruce said. What is going on at this domain name? is there really any abuse? I'm still waiting for the slide. Sorry about that, shall I just continue? Next slide, please.

The next slide was supposed to be free text comments. What do you think about due diligence? Even if ccTLDs say, okay, we do not perform … So we have to forward two slides. So, one after that, the next one. So, again, we are coming through to free text comments to see the picture in more granular, nuanced details.

So, even if ccTLDs do not perform their own due diligence, there are always some checks involved. Even if you as ccTLD exercise, so grant this request without performing checks on what is going on, you still have to do some checks. Do they spell the domain name correctly? Does this request actually come from the law enforcement agencies? So, performing no due diligence does not mean that there are no checks performed at all. And we will go the next slide and I will briefly hand it back to Bruce to talk about tools.

BRUCE TONKIN: Thank you. The tool slide up. One thing we found is there are a lot of tools being used in the country code community and we just divided

them on this slide, which is coming up now, broadly. There's some that are essentially free or opensource tools and those that are commercial.

Of the opensource tools, a lot of them is just literally a raw list of domains that have been reported to that provider. Some of the more commercial services, they're by and large, or many of these commercial services are not-for-profit organizations but they do charge for access to the data to basically cover their costs of operation.

What you get more with the commercial tools is you won't just get a list of domains but they'll actually provide you information on what abuse was detected at that particular domain. So, for example, if it's a phishing attack, the free service might just give you a name and say, "This has been involved in phishing," and that's used by ISPs and others to block the domain.

But where we're interested in actually doing due diligence on a domain, we need to see what was the full URL that was associated with phishing and that's the type of thing that you tend to get with the commercial services.

And some of the commercial services are again literally just a list of names with the corresponding URL. Others of these commercial services actually do take-downs on behalf of the country code operator. So some of them are really providing a service. They're not just providing a list of data. So essentially you can choose to outsource the management of the takedown with that provider and they will do the contact with the registrar or the hosting company or the registrant to try and address that abuse rather than you having to take action yourself.

And others are these aggregate fees. So, the one at the bottom, IQ Global effectively aggregates a whole range of fees rather than you having to independently go to each individual group and then they provide case management tools. They're tool sets that allow you to open a case, write case notes. So effectively a ticketing system that goes along with the management of the DNS abuse.

Some of these areas we think that what we might do as future work is some more deep dives into these topics that we've talked about like the tools and get feedback from the ccNSO community on what tools are the most useful. Over to you, Tatiana.

TATIANA TROPINA: Thank you very much. Next slide, please. One of the points that was interesting about the tools, this choice between open tools and feeds and commercial instruments—waiting for the next slide. But it's a free text comment so you can rely on me fully in delivering you the message.

So, the choice between commercial and opensource really relates to their functionality. So, as ccTLDs indicated, some of the opensource tools can be extremely helpful but you need to set up a central place. The choice for commercial tools usually is driven by their functionality by the type of data you can get by additional services that you can get, but basically we also saw that many of the ccTLDs are utilizing both commercial tools and opensource tools indicating that diversity is the key. Next slide, please.

And I'm going to move to one rather interesting finding, rather general finding that almost as a threat going through many, many—next slide,

please—through many responses. And this finding is last but not least explains why do we have to look beyond the numbers. Why do we have to look beyond the sheer answers we get, just choose an option.

We have to understand—and this came across to us when we were reading through many of the answers that the way that ccTLD managers deal with the DNS abuse doesn't boil down only to their internal procedures. It's not only what you set up, how you scope DNS abuse, what kind of tools you choose and how you react. Actually, it is very much also in many jurisdictions dependent on the external factors and many of these depends on the legal context. Sometimes the law of course very strictly establishes what you can and what you cannot do and it relates both to the scope of the DNS abuse, like some ccTLDs indicate that anything that is criminal and relates to domain name, well this will be DNS abuse.

UNIDENTIFIED FEMALE: Excuse me, Tatiana.

TATIANA TROPINA: Yeah.

UNIDENTIFIED FEMALE: May I kindly ask that you slow down for the interpreters? Thank you.

TATIANA TROPINA: Thank you so much and apologies to interpreters. So, some of the ccTLDs indicated that anything that is criminal and related to the use of

a domain name would fall under the scope of DNS abuse. In some other cases, we see that ccTLDs cannot take any action proactively or not unless they have a request from the law enforcement agencies or competent authorities.

And to us, it very much highlights this idea that there is no and can be no one size fits all solution. And handing it over to Angela, I think.

ANGELA: Next slide, please. I think that's the last slide on the deck.

NICK WENBAN-SMITH: Just give us a couple of moments.

ANGELA: No problem.

NICK WENBAN-SMITH: Just while we've got a couple of minutes. We have a couple of questions in the chat around ICANN and what is ICANN going to do about a ccTLD where the suggestion is the ccTLD has gone rogue, as it were. That's not within the scope of the terms of reference from this work and it's a very longstanding point that ICANN does not set policies for country codes which are considered sovereign assets and govern their own rules and laws and jurisdictions.

Having said that, what I would like to do as part of this work is to shine a light on what behaviors and practices are there and to have a conversation about those and I think the way that we tend to do these

things in the ccNSO is to highlight good practices and to encourage good behaviors and to help people raise the bar and raise the standards where they can, where there seem to be issues. The best way to do that is to have dialogue and to do things like have data-driven conversations like we're having today. So, very much welcome those questions but we need to keep in mind our scope and terms of reference and the fairly limited powers around policy making that the ccNSO has as a fundamental point that I thought I'd just [state].

ANGELA: Should we go ahead, Nick?

NICK WENBAN-SMITH: Yes, please, Angela. Sorry.

ANGELA: Okay, lovely. All right. Next slide. Okay, thank you, there we go. I think with everything that has been said this afternoon concerning the survey, Tatiana already put it that really the numbers that we got from [inaudible] aren't necessarily indicative of what's going on within each ccTLD. There could be even additional methods of mitigation but here it's just a snippet of some insights that we got from the response to show that indeed different ccTLDs from different regions do engage in the different methods in registry policies or tools awareness and the like. So I think this really shows that despite the region, all ccTLDs in effect have the capability to exercise the different methodologies when it comes to DNS mitigation.

So that's about it from the slide and do look forward to more insight as we will be compiling it in more detail [inaudible]. Thank you. Back to you, Nick.

NICK WENBAN-SMITH: Brilliant. Thank you very much, Angela. A few questions in the chat. People are very welcome to add further questions. If we can move on to the next slide, hopefully there's a few more.

So, we've got the [raw data] and as I said at the beginning, many of the respondents didn't want to have their data made public. But I think we as a working group have identified further topics for deep dive and further work over the next six to twelve months. I think we understand that we will repeat a survey and then try to see whether the evolution of different policies and practices as we start to focus on this work and start to highlight different things.

One of the questions in the chat I saw was around the relationship between low cost of a domain name and high levels of abuse and I think that's one of the things that I've heard anecdotally that there is a relationship between, say, a particular promotion run by a registrar and gTLD that has been an observed correlation between a price promotion and a spike in, say, phishing domain registrations.

So I think that topic is a very interesting one and I think it's one of the areas that we have identified for a specific session on. As part of this survey, we did not collect price information. I only have a small number of data points for myself, but I know within the European region, there were a couple of us registries who are [inaudible] and my friend from

Germany, it's very well known that the United Kingdom and Germany are large registries with very competitive markets and very good prices I would say for domain name registration. But we have fantastic levels of low numbers of abuse. So it's clearly not as simple as cheap equals high abuse. It's much more nuanced than that and I think it's an interesting area to try to explain why it is that there are some not just TLDs or not just gTLDs but there are some ccTLDs which are definite outliers to the general rule that there are very, very low levels of abuse within the ccTLDs and I think it's interesting to understand that and to have a conversation about what are the drivers for those sorts of outcomes and I don't think it would be responsible for us to shy away from some of those difficult conversations. So I'm happy to do that. And certainly the relationship between price and abuse I think is an interesting topic and it deserves a fuller talk within ourselves and our communities.

And to my final point on this topic, I think those of us here are acutely aware of our responsibilities to the public that we serve and that includes end users who are going to be the victims of abuse and phishing scams and other criminality. We are acutely aware of the importance of high standards and higher reputation for business contacts in our own communities or [international] communities, obviously. And I think that is our overall focus. It's such an important area because business relies on a good reputation and I think where we want to show what good looks like in order to raise standards where there are observed problems, then I think what can we do is try to have that conversation and try to move things in the right direction for the whole of the CC community, and my extension the whole of the global

community as well and that's something that I would like to try to move the dial on a bit.

In terms of other work, I think we all understand the relationship between the registry and its registrar channel is a really important piece of working in a team to work collaboratively and in a coordinated manner with the registrars and I think we all know that certain types of abuse—maybe the vast majority in some areas—is much better for the registrar to be the party taking action in the sense that what they can do is more effective rather than what the registry can do. As we know, registry tools are quite, by their nature, blunt and it's a metaphor—it's sort of the sledgehammer, not a scalpel. It is one piece of abusive content in a website. There's not much the registry is in a position to do about.

The other topic I think which came up in our preparation session is to look further at the tools because there's a lot of tools that some of us pay for and there's a lot of free opensource tools, and I think socializing within experiences of selection of tools, the criteria that we've used, which one is a good value for money, which ones … I think it's a problem that we all face is the number of false positives within the various feed providers and tools, depending on what they are designed for which quite often is not specifically for registries which is what our main focus is, but DNS type stuff. There's very few of them which are specifically limited to that and the scope of, say, the reputation block lists is much broader than how any of us would describe DNS abuse. That leads into a significant number of false positives, where we're trying to proactively take action, then that is very time consuming for us to do.

So, I'll just take a quick look at the next steps.

PABLO: [inaudible].

NICK WENBAN-SMITH: I see.

PABLO: [inaudible] had a question. I do. I was waiting to have the floor. Thank you. First and foremost, I want to congratulate the DNS Abuse Standing Committee for a tremendous amount of work that you have done and for the very informative presentation that you have given us. So, kudos to all of you.

I would like to share a comment regarding a strategy that was used by the regional organization, the local regional organization, LACTLD, in which prior to the [inaudible]—and I'm talking about days before the [inaudible]—we were here in Cancun and we had the opportunity to bring judges, public defendants, and police from our various countries and we had an opportunity to present to them what we were seeing and had the opportunity to ask them in the event that something would come across their desk if they knew who to speak to, who to approach, who to talk to. So we began a process of exchanging information and knowing each other and building bridges and that was very helpful.

I understand that, as we all know, one size doesn't fit all. But in those areas, in those regions in which it would be possible to do that, it would be very helpful. Thanks.

NICK WENBAN-SMITH: Gracias, Pablo. It's near the end of the session and I'll just end on a point which is I think you are completely right. The whole ecosystem has this task and education and helping people to find the right person to talk to, to take [action] quickly, that does include training and outreach to judicial authorities and prosecutors and members of the public. What do you do if you experience a problem and how do you make sure you don't repeat it and how do you help other people from being a victim of crime, fundamentally? I think it's everybody's responsibility and the more that we can do to give people the resources and education to help with that, that's part of our mission, absolutely.

So, with that, I would like to thank very much all of my panelists. There will be plenty more work and outreach.

UNIDENTIFIED MALE: Nick, there is still one question from Allan MacGillivray.

NICK WENBAN-SMITH: I'm sorry, I don't see it.

ALLAN MACGILLIVRAY: That's okay, Nick. I'll try and be quick. It's Allan MacGillivray from Canada. Just a couple of comments or questions. First, I'd be cautious about drawing anymore general conclusions from the survey, because obviously the sample is not random, so I'd be careful. Even though I'm very pleased with the size and I certainly want to echo Pablo's comments. It's a significant undertaking.

The other comment is just looking at slide eight of the data but we don't have to find it. Really it's the number for how many CCs do not know the rate of abuse, and depending and looking at the chart or the text, it's somewhere between 25 and 35% and I think that's a significant finding and that's something you might want to try and understand a little better as you go forward. Thank you.

NICK WENBAN-SMITH: I appreciate that, Allan, and I agree. It is not a representative sample [inaudible] selecting and probably the people who have got the best stories to tell are the quickest to come forward to tell that story and I think that's well understood and I think there's plenty of work to go and your point is well made about drawing conclusions.

And I think [inaudible] are very well made that getting a handle on what you mean by abuse and how much of it there is, is not straightforward. I have some empathy and sympathy for the position of it's easier to say we don't know the answer to that question. I can easily see how people would find it difficult to give a precise answer and work on metrics is absolutely within the scope of this subgroup.

TATIANA TROPINA: Yeah and just to add indeed we discussed the sample. We discussed the methodology at length in our group. We perfectly understand that, to some extent, the sample is not representative and for us it is important to see if we can highlight some trends to see some interesting information to build capacity, to start the dialogue, and maybe if we

identify some gaps in our methodology as well, we can always issue the second survey. We can always follow-up. We can always continue.

And just for the future, I want to say that we also talk about the further analysis and it is important for us also not to run too much or too quickly into let's say some causation like this, anecdotal price, low price and high level of abuse evidence. So, we are discussing methodology and we are trying to be careful. I hope I didn't speak to quick for interpreters.

NICK WENBAN-SMITH: It's a balance between speaking too quickly and running out of time. We have actually run out of time, so I'd like to draw the session to a close. Thank you very much for attending. Keep your eyes peeled for further work and thank you very much to my colleagues who have put a huge amount of work in over the past year and I look forward to working further. Thank you.

CLAUDIA RUIZ: Thank you very much. You can stop the recording.

[END OF TRANSCRIPTION]