ICANN77 | PF – ccNSO: DNS Abuse Standing Committee Survey & Repository
Wednesday, June 14 2023 – 13:45 to 15:00 DCA

ANGELA MATLAPENG: Hello. My name is Angela 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.

UNIDENTIFIED FEMALE: Angela, all good.

NICK WENBAN-SMITH: Hello. My name is Nick Wenban-Smith 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.

UNIDENTIFIED FEMALE: Nick, all good. Thank you. Nick, we're at start time to get going.

NICK WENBAN-SMITH: Yes, let's do that.

UNIDENTIFIED FEMALE: Claudia, can you kick us off, please?

CLAUDIA RUIZ: Yes. Please start the recording. Hello, and welcome to the ccNSO DNS Abuse Standing Committee session. My name is Claudia Ruiz, and I along with my colleagues, Bart Boswinkel and Kimberly Carlson, 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 chair or moderator of this session. Interpretation for this session will include 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 the Zoom Room. 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 in 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 that this transcript is not official or 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 multistakeholder model, we ask that you sign in to Zoom sessions using your full name,

for example, a first name and a last name or surname. You may be removed from the session if you do not sign in using your full name.

Thank you. And with that, I will hand the floor over to Nick Wenban-Smith. Thank you.

NICK WENBAN-SMITH: Thank you, Claudia. Welcome, everybody, to our next session meeting of the DNS Abuse Standing Committee of the ccNSO. For the record, I'm Nick Wenban-Smith and I'm chair of this Standing Committee. By way of introduction, I have my colleagues, starting with David, Bruce, Tania, and Angela. So we're all going to be speaking today. This follows on from a number of actions and findings and discussions from the previous meetings.

There's two things I suppose I wanted to just sort of put on the table at the front of this meeting to give everybody time to think about it. Firstly, we want concrete outputs from this meeting. So I actually want people to start to think about next steps, because one of the outputs that I'm seeking for as chair of the group is to get from the community some sort of agreement about how they would like the next six to 12 months of activities of this group to look like. We have some ideas about that but we want to make sure by checking in with you that our views are in alignment with the wider community views, and it is going to be useful and meaningful sessions for everybody. Otherwise, we will end up doing things which are not in alignment with your wishes. And things are moving quite quickly in this area so it's important that they are relevant and topical.

Secondly, you heard the reminder about the Zoom Room. We will be doing some polling, not because as a British person I dislike referenda, but this is not a decision-making process. This is just to get a temperature of the room around some of the sort of further questions and things that we'll be looking into going forward. So if you could take a moment to log into the Zoom Room, then you'll be able to participate in the polling when that point in the meeting comes just to warm you up for it to make the session flow nicely.

So I think the agenda here is set up for the slide, I won't read it out. But I'll pan over initially to David who's going to take us through the Repository Subgroup activities and next steps, because that is a very interesting and useful set of resources, I think, for the community to deal with DNS abuse and we want to progress that quickly. Over to you, David.

DAVID MCAULEY: Thank you very much, Nick. Hello, everybody. My name is David McAuley, I'm employed by Verisign and participate in the ccNSO by virtue of our management of the .cc country code top-level domain. Can we have the next slide, please? Oh, I'm sorry, back to the agenda. What I'll do is go through some of the work of the Repository group on both creating a repository of information and also creating an e-mail list. So let's go to the milestones. Next slide.

When the DASC was created last year, not much more than a year ago, we pretty quickly decided to move into subgroup operations. There's a subgroup that Bruce will talk about that is conducted and will conduct surveys. And there's a group called the Repository Subgroup that I am

the chair of. The work of that group is two-fold. One is to create a repository of useful information—basically, links, PDFs, things of that nature—that would be helpful to ccTLD managers in addressing, even understanding, DNS abuse as it changes over time, and also to create a mailing list. But the Repository Subgroup, while it has both of those operations under its tutelage, we turned first to the creation of the repository itself. We had our first meeting in August of last year.

By September, we had come up with some ideas on the e-mail list. We had a presentation including from Brett Carr of the TLD Ops group that was quite helpful to us and coming up with thoughts on the e-mail list, which I'll talk about in a little while. And then continuing work on the repository itself, we came up with Terms of Reference that we'll use in managing the repository. By February of this year, we had those done and dusted through the full DNS Abuse Standing Committee and sent it to Council.

The Terms of Reference are basically how is this group managing the repository? How are we going to do it? What are we going to look for? What kind of information will we have? Will we have an archive? How will we consider things to be put on the list where we seek positive input, etc., etc.? So all of those Terms of Reference were done and dusted in February. And we intend to launch the repository, basically, at this meeting and address the e-mail list between now and ICANN78. Next slide, please.

So, as I mentioned, DASC, the full committee, tasked us with creating a resource for information. So we, in our Terms of Reference in the repository, created what we call an editorial board or the concept of

an editorial board. I better slow down before I get my first warning on speed. That is the group that will manage the repository and will accept submissions after they've been vetted by staff and sort of managed the input process. And then we will consider whether they're appropriate for the repository and at what point will things that have been posted there be appropriate to remove for archival purposes.

So the editorial board itself will probably meet monthly, maybe twice a month, depending on the pace and the amount of input that we get. We will brief the community periodically on what we're doing and how we're doing it. And we recommended to the DASC that the initial editorial board be the Repository Subgroup itself because we're familiar with what we're putting together here and moving it forward. Next slide, please. Can I get the next slide, please?

So here on this screen—obviously, there's no way that you can read this—but this is a screen that is setting forth the Repository and the Information Library and how to submit information. We will be sending this out in our announcement of the repository but it will have a QR code. Basically, the information that will be available will be information along the lines of what is this resource that we're talking about? What are the topics, the categories of information it might have? How can one submit something to be considered for this group and those kinds of steps? So I don't expect anybody to be able to read this here, but it will be submitted to the community. Next slide, please.

This is a similar slide but this one is pointing to the actual repository itself, which will have categories along the lines of presentations and reports, DNS abuse mitigation, addressing DNS abuse tools,

commentaries, articles, and things of that nature. We have four categories that we will use and we will also have a QR code that will give you access to this resource as well. And again, that'll be in our formal announcement. Next slide, please.

So I'd like to, in a moment, come up with a poll to ask you these questions. But I want to sum up what the repository is simply by saying what we're going to try and do is put together things that people can look at, click on, and get immediate information with a heading saying to them, "This is about…" it might be phishing. This is about malware. This is about X, Y, or Z. And by the way, this is a tool that can help you or this is an article that can inform you, things along those lines. That's what we intend to put together and to keep current.

So I would like to start the poll. So the first question is how likely would you be to visit the repository for such information? I guess we will leave that open for a reasonable period of time. In reply, there's a great percentage that is either very likely or likely to use such a tool, 6% unlikely, so little bit less than 10%. Roughly 10% that would be unlikely to use the tool. So that's useful information for us that tells us that there is a space for this tool. Obviously, once we launch it, we're going to be watching what the reaction is to it and the participation is in it. We will tweak it accordingly, and if need be at some point in the future, end it if it's not a useful tool.

I have another question here. Would you be interested in providing content to this repository? We will make the content submission process very easy. I spoke about it briefly, but it will be quite easy. I'll wait for a reasonable period of time on this as well. So providing

content, almost 60%, another 30%, possibly. I would guess that makes sense as people see how this shakes out, how it—not unravel—but unrolls in practice. And no, roughly 10%. So I appreciate that information. Again, that will inform us as we manage this resource going forward. So can I have the next slide, please?

Repository scope and community feedback. What I'd like to do here is—and there will be a polling question related to this—I want to address the scope. The scope of this is to provide useful tools to the community, as we mentioned just before. There are a couple of things the DASC does not do is create policy or codes of conduct, as we've mentioned a number of times, and that's important to us. The other thing we want to do is make sure that the resource is appropriate for the ccNSO community. It's not a resource to point fingers or to make criticisms.

So this particular article that I have here—and I'll explain what it is in just a moment—is possibly a good test for is this appropriate for us to put in the repository? We in the subgroup would like to have this kind of feedback. It's too bad we only have time for one example but we only have time for one example. This is a brief article from CircleID. It's not a blog. It's from a CircleID reporter. It was posted at the end of May. It basically, as you can see from the headline, says that "Meta Lawsuit has Led to Significant Decline in Phishing Domains Tied to Freenom." Now, there was a very specific article about Freenom in another publication, not this one, that called out five particular ccTLDs. In our view, in the editorial board group view, that would not be appropriate for posting. That's not what we want to do here. This article, on the other hand, simply points to this and says that as a

consequence of this lawsuit, phishing in five ccTLDs has gone down significantly. We think that's useful because it pertains to the ccTLD community and it has information about DNS abuse. But we're going to poll about whether even this is appropriate or is it to the word I used is attenuated? Is it too far out? Is it something we don't want? So as I said, the editorial board, while we're ready to launch this, we're still getting our legs under us on what is appropriate content. We thought we would create a test here for this particular group. So can I go to the next slide, please? Oops, there should be a polling question, I thought. If I'm wrong, I apologize. Okay. I don't see the polling question. So my apologies.

UNIDENTIFIED FEMALE: There's indeed a third polling. One moment, I will bring it up. Thank you.

DAVID MCAULEY: I'm sorry?

UNIDENTIFIED FEMALE: I will bring the polling up. Thank you.

DAVID MCAULEY: Okay. So apologies for that. But any feedback that anybody would like to give us on this would certainly be welcome. By the way, we're going to show a picture in just a minute of the members of that group. We're open. We want feedback on this, please. Please do see us.

So do you think this article that I just spoke about is appropriate for the response for the repository? Or do you consider it too attenuated or are you unsure? I'll leave that open for a moment. This information will be quite useful for us.

Appropriate is almost 70%, too attenuated is 5% unsure. Thank you. So that helps us. We may do a poll on this at the next meeting just because we will have some practice under our belts. Next slide, please.

Here are the people. Here are the six of us that are on this committee. Please seek us out, give us your feedback, your comments, your reactions, good, bad, whatever, we want to hear them. Next slide, please.

So I want to talk briefly about the dedicated e-mail list and I'm going to truncate this a bit. I'm looking at the clock and I want to keep this within the time scope that I have. So pardon me if I don't go through every bullet item. But our job in this subgroup is also to create a dedicated e-mail list along the lines of ccNSO list. It's specifically looking to TLD Ops as a possible model. And that is a list that's supposed to be a useful contact list for people to get information about a certain topic in TLD Ops security. In ours, it's going to be about DNS abuse.

BART BOSWINKEL: David, this is Bart. Excuse me. Just a question. We have a question online regarding the repository. Do you want to take it at the end of your presentation or now before you go into the e-mail list?

DAVID MCAULEY: Can I take it at the end? But thank you. Thank you. So we want to create this e-mail list along the lines of TLD Ops, and it's to help ccTLD managers with DNS abuse issues. It is going to be a closed list. In other words, it will be moderated as to who joins, but no e-mail list is confidential. People can forward e-mails. So we will have that kind of disclaimer. This is meant to be for certain ccTLD managers but it's not guaranteed as confidential. But we will create a list that will be able to inform people of new things that are cropping up that are DNS abuse so that they're aware of it. And we will importantly have on this a contact list so that people can take offline and e-mail colleagues who have experience in certain areas and get information if they're addressing that kind of issue for the first time themselves. That's the intent of the e-mail list. We will be, between now and ICANN78, filling in the Terms of Reference for that, getting our particulars together, and we hope to launch that at ICANN78, but that's the intent of the list.

We have a polling question. Would you be interested in subscribing to such a list? As you answer that, one of the things we'll do between now and 78 is decide who we target this to—will it be executive people, policy people, legal people, operations people? We haven't decided fully yet but we will be addressing those kinds of issues. Should it be everybody at a ccTLD manager? Okay. I see there's a fair amount of interest in that. Thank you. Including the maybes.

The next question is would you be interested in a dedicated contact list as a part of that e-mail list? In other words, knowing contacts, relevant contacts in other ccTLDs? Okay. That's very helpful. Between the yes and the maybes, it's a high number. No I see is just under 10%. Thank you. Next slide, please.

So we're going to invite people to submit comments or information to the repository and we're going to promote it. We're going to ask the community to please promote it, get used to it, see what it looks like. And then we will convene probably in a couple of weeks to start our work on the dedicated e-mail list that I mentioned to you. You can see what's on our plate with respect to that.

So I'm bumping up against my time limit. I would like to stop now, Bart, and I'm happy to take that question.

BART BOSWINKEL: It's not so much a question, it's a comment, and maybe you want to respond to the comment. This goes back to the example you used from CircleID. The comment is—and it's from John McCormack from Hosterstats—"You need all the information that is available from open sources when fighting DNS abuse. It isn't about hurting feelings, it is about stopping abuse." So that was his comment, and there is a second one from somebody else. I don't know if of the panel wants to comment on this comment.

DAVID MCAULEY: I'll take an initial stab at it. But first of all, thank you for the comment, John. We will take that under advisement as we roll this out. We want to get experience under our belt. I think going into it, it's a fair point. Obviously, in fighting DNS abuse, we want as much information as we can get. One of the things that we'll be paying attention to, especially with respect to initial reports, is, are these accurate? Especially when ccTLDs are mentioned, they may be, we'll have to have some finesse in

doing this. It's a fair point. We'll take it under advisement. But we want to make sure that what we are at heart is an information source and information repository, and not so much a group here to critique or point fingers at other members. So we need to think that went through. It's a very fair comment. Thank you.

BART BOSWINKEL: The second comment is from Luc Seufer from Namespace, "As a registrar, we would value getting access to the repository." I don't know if you want to respond to that.

DAVID MCAULEY: I didn't quite hear, Bart. Sorry,

BART BOSWINKEL: "As a registrar, we would value getting access to the repository."

DAVID MCAULEY: Thank you. Thank you for that comment. That's important to us, we will consider that. But as I said, we need to get our legs under us, get this thing out as we've described it. That too was a fair comment. If the resource turns out to be as good as we hope that it does, we'll do what we can to make sure it's as useful as possible and spread it out. Thank you. And, Nick, I'm done. Thank you.

NICK WENBAN-SMITH: Thank you very much, David. Almost on time. So there's no other comment I can see about the launch of the repository. I suppose

there's opportunity to put more questions in the Zoom chat if there are any more questions for David. But I suppose I have one question. David, I have spoken about this. It's a friendly question, I hope. There's a significant amount of community resources going into the repository and the editorial board and the curating of content to keep it current and useful. I think that's quite a significant resource effort. One of the things that I always talk about is that the resources of volunteers in this community is a finite resource. So my question for you, David, is really in terms of evaluating whether the sort of the mailing list and the repository is fulfilling a useful function. How will you decide that and how long does it need to go? I recall that the TLD Ops list, for example, had quite a sort of slow burn. It did take a number of years before getting significant traction is now considered a very valuable part of the community resources. But I'd rather not wait years to have this up and running and going successfully, so how are we going to ensure that it does have a take up and how do we know that it's been successful? Thanks.

DAVID MCAULEY: Thank you, Nick. It's very good question. I think it's fair to say that we haven't thought this through all that much so far. But our initial thoughts are things along the lines of seeking community feedback as best we can on how this thing is playing, whether it's useful and informational. Two, asking you for maybe five and a few minutes at the next succeeding ICANN meetings to create reminders. We might also create printed reminders in the nature of postcards and hand those out in order to encourage early adoption, and online to seek feedback on usefulness.

Then the question of continued vibrancy and relevance will not be for our subgroup but will be for the full DASC, of course. We will report to the full DASC, give our recommendations. But I expect we would hope that this would run for at least a couple of ICANN meetings. Thank you.

NICK WENBAN-SMITH: Thanks very much. Can I have the next slide, please? So just to summarize the survey group. So there's two working groups within the DASC. We just heard from the Repository, the second group is the Survey group. So I'm just going to quickly recap what we did. We had a survey the last quarter of calendar year 2022. There were a good number of responses, I think. We had a mixture of geographic and linguistic responses, which were excellent. You can look at the headline numbers, but you need to understand what's behind some of the numbers. So as we know, some ccTLD managers have multiple ccTLDs but respond for one. So you need to put a little bit of knowledge and thought when you're evaluating the response and the success of the survey. So we presented the initial report at ICANN76. Next slide. And the next slide.

I think this is quite a nice slide illustrating if I had a pound or dollar of every time ccTLD say how different they are from gTLDs and from each other, then I wouldn't be here now. But you can see that there's a lot of interesting variation within the ccTLDs. I think that's why when you're looking at survey outcomes and data, there are some of these things intrinsic to the model of the registry. Some ccTLD registries have got a very restrictive registration policy. Some of the European ones I know have mandated eID verification for registrants, and that

comes down to national ID models and things. Some essentially follow a gTLD model. So there's a lot of different things. So, when you're looking at the data, you need to have a little bit of a thought about what you're looking at, and that's always something to take into mind. Next slide.

We had a look in the ICANN76. There are recordings online. We've specifically looked at a large number of questions focusing I think largely on where registries take proactive steps to combat abuse, looking at trends and trusted notifiers with a long set of discussion around one of the questions on the sorts of tools and feeds that ccTLDs use. I think we're all in this room aware that depending on the definition of abuse, you get a lot of false negatives in the feeds you get from reputation block lists, and that makes the ccTLDs life quite difficult where you're trying to do things at scale and quickly. So any shared intelligence about what actually is very good for ccTLDs to use and provides meaningful actionable data without too many false positives is something that I think the community is very interested. I think we're all very interested in doing that. And maybe our combined efforts will have a feedback loop into some of these feed notifiers so that they make the feeds more appropriate for us. So that's something I'm very interested in. And yes, of course, looking at regional variations and registry models, size of registry. Obviously, there's a huge diversity in terms of size. Just one or two individuals and others have hundreds. So very interesting findings. So if we go to the next slide. So I'll now hand over to Tania.

TATIANA TROPINA: Thank you very much, Nick, and hello, everybody. We are extremely pleased to share the results of the next portion of our work of our deep dive into data, especially data related to virus checks and verifications, that the ccTLD managers perform during the life cycle of a domain name to tackle DNS abuse. This data is very rich. And we could look at various practices of performing these verifications from pre-registration to the renewal of domain name. So basically, through the entire life cycle.

There is a word of caution here because it's not an experimental research, it's an explorative survey. So we cannot claim causation between the checks performed and the level of DNS abuse in a particular ccTLD. Sometimes we cannot even claim correlation. But what this data shows to us is the wealth of practices and tools and techniques that ccTLDs use to maintain healthy DNS. And as Nick said, proactively tackle and prevent DNS abuse. While you will see that approaches differ, we very much encourage the ccTLD managers to use this information and to share the best practices. Next slide, please.

I started during the ICANN76 but I understand that not everybody was there in that session. That sometimes when we look at statistics is one thing, and we will look at it a bit later in a few minutes. But before we go to statistics, I want to say that one of the most interesting things to look at when you look at the results of the survey is not only deep dive into data, but also deep dive into the free text comments, because it shows us that first of all there is no one-size-fits-all-solution approach. And it also shows to us how much the practices differ and how rich they are. So they can be performance of the regular Know Your Customer technique exercises, random compliance checks. Different

times when checks are performed, sometimes it is like combination of different checks like you can see within 24 hours after registration. In case of complaints or sometimes it's monthly and in case of complaints, when something arises, random checks, randomly regardless time of registration. And also there is a combination of manual and automatic verifications. The ccTLD managers shared with us that sometimes they even invite students to manually look through data. And some of the ccTLDs run automated checks, but then the secondary manual checks to verify yet again when it relates to high risk registrations. Some ccTLDs shared with us that in addition to other checks, they use registrant agreement requirements only or relationship between registries and registrars. Some of them have the triple I policy—incomplete, incorrect, and inaccurate policy. With this, I will wrap this up. I think we will go to Angela next.

ANGELA MATLAPENG: Thank you, Tatiana. Good afternoon to everyone and good time of the day to our remote participants. My name is Angela Matlapeng from .bw ccTLD. I work as a CSIRT analyst but previously managed the .bw namespace.

I guess what we'll be seeing here is just some of the highlights that came from the rich data that Tatiana referred to. We have in front of us here just some of the information that is collected at registration. When you look at the variations between the collected data versus the validated data, you'll see that there's quite a margin of what is collected. Not most of the respondents indicated that they would validate the information. So what stands out right now is the contact

name, the e-mail address, and the phone number. These are at least the three that showed that when information is being collected at registration, this is at least what we're looking out for.

Interestingly, not quite a lot of registrars would collect the abuse contact, and we don't even see that being validated. I guess the different approaches to this, and there have been talks around having the abuse contract being clearly out there in case you're dealing with cases of that being redacted and you still have to look into the abuse. So sometimes the abuse contract sits with the registrar, but in cases where abuse is much on the content side of the domain, like maybe a malicious code injection, then you'd need to have the abuse contract of whoever the domain belongs to so they could deal with stuff like that. Next slide, please.

So the first graph shows a relation between pre-registration and renewal. So most of the respondents will indicate that they don't necessarily do the verifications, right? But that kind of stands out really much on the renewal side. One of the comments that we got was some of the registries just treat registration once, so you can't verify the information when it comes to renewal. So once you register a domain once, you do that check, and that's about it.

On the right side, we see the different ways of how the verification is carried out. What stood out was manual checks. I think, just following what Tatiana spoke to, a lot of exercises do speak to manual checks. Some respondents that indicated having tools that would help with automation, there was also combination of having both manual and automated. I think it was about 25% of the respondents. And also a

very significant number of the respondents did indicate that they don't do the checks at all. Next slide, please.

The type of action that the ccTLDs would take post registration, it's quite very clear that most of them follow approach that's more investigative, so they wouldn't immediately take action, such as maybe deleting a domain immediately or maybe suspending it. So, most of them say that they would rather have an approach that depends on the risk assessment and the results that come there. Of course, we do have some of the ccTLDs that take no action. Going back to the previous ICANN meeting, I think there was information that stood out about most ccTLDs not having the proper tools to monitor or measure DNS abuse. So it didn't come as quite a surprise when we got some of the responders saying, "Well, we don't take any action because we probably don't even know the kind of abuse that we're faced with to begin with."

The other question went to what would the ccTLDs do in case of maybe government request or maybe law enforcement. A little bit slightly different from the previous question, so they both also carry out due diligence, but they can also just execute the request without further verification.

Just to wrap up, maybe a little summary on also what we found out from the slides, you will realize that some of the questions spoke to whether the ccTLD is affected by data protection legislation. Even though most of the respondents answered yes, verification is still—they're so high when it comes to whether the people conduct the verification. So most answered no, but they did say they're affected by

legislation. So you might maybe wonder what happens when it comes to obligations that speak to perhaps the WHOIS accuracy and stuff like that. But otherwise, I think I'm going to hand over to Bruce.

BRUCE TONKIN: Thank you. If you can just jump to the next slide. When we presented the results last time, we asked ccTLDs, "What level of abuse do you think you're seeing in your ccTLD?" We asked, we got 57 responses to the survey. And out of those, more than 20 on the left side said that they thought the level of abuse was less than 0.05%. But we also had 20 of the 57 that said they weren't sure. So the question opened, "In that not sure category, is there much higher levels of abuse than as being reported?"

So we went and approached the DNS Abuse Institute which has aggregated feeds from a number of different reporting organizations that report phishing and malware and botnets, etc. So they've aggregated many feeds together and then broken that down by country code. We mapped that data against those parties that submitted responses, so the 57 responses. So the graph on the right is then showing what the DNS Abuse Institute was seeing. You can see that of the 57, nearly all of them had less than 0.05% of abuse of their TLD.

Now, one of the reasons why you might see some people self-reporting high levels of abuse is they may consider a wider set of problems to be DNS abuse. So they might be reporting fake web shops or they might be reporting trademark infringement or some other form of complaint, they get a better domain name. But the graph on

the right is at least using a common definition across those ccTLDs. What they're showing is really, for the vast majority of ccTLDs, the level of abuse really is low, it's rare. And it only really becomes noticeable in absolute numbers when a ccTLD has millions of registrations. So most of those that responded to the survey in the DNS abuse data, there was less than 20 names that had some form of DNS abuse. So it's very low. Then to actually have levels of abuse in the hundreds basically means the country code needs to be in the millions. What we've seen is that most of the large country codes do have a feel for the level of abuse because they are taking some action to get DNS abuse feeds and take some action against them. If we move to the next topic.

So another topic that we heard last time was—we had questions from several audiences, I think, both the GAC audience and the ccTLD audience—does price make a difference? Essentially, TLDs that are priced low, they're the sources of a lot of abuse, and TLDs that are priced higher, they're basically completely safe. So the first thing we did is we took the 57 responses that we received and then went to their websites, and as best we could determined what the wholesale or retail pricing was for that TLD, and just roughly mapped it against that sort of TLDs. The majority of ccTLDs here in the $20 to $100 price point, there's a significant number of TLDs that are priced less than $20, and there's a few ccTLDs that are priced less than $5.

We then looked at which of those ccTLDs had higher levels of abuse. This was just looking at April data, I want to stress, so there may have been some months where they were for any particular ccTLD could be a high level of abuse. But using the April data, there wasn't really a

correlation on the level of abuse with pricing. And if anything, some of the TLDs that had higher levels of abuse were actually in the medium category. So what it's tending to look at really as a hypothesis is that it's perhaps more to do not so much with pricing, but what tools and techniques ccTLD uses to combat abuse. Some of those that have very low prices have a lot of automation. So they could take in a DNS abuse feed and just automatically suspend or delete a domain name, for example, which will keep their level of abuse low. Whereas a ccTLD that might have a higher price might use manual process to check whether a name has a level of abuse on it, and maybe that means is at any point in time, a higher level number of names that are presumed to have some form of abuse in them. So the conclusion was that we couldn't see any correlation between price and level of abuse.

So back to you, Nick.

NICK WENBAN-SMITH: Thank you very much. So we've now had two sessions on the survey, sort of a high level introduction and top-level findings in the last ICANN meeting, and a couple of in-depth analysis sections on registration data. And the price point, I think the price point is quite interesting because I think for those of us who have a desire to keep our prices as low as possible in terms of consumers, the anecdotal evidence that low prices equals high levels of abuse didn't seem to hold true. So I think that was a very interesting finding. Bart, you're waving. Is there a question?

BART BOSWINKEL: Yeah, there is a question and comments. I think before you go into the next item, it will be useful. So one of the questions from Raitme Citterio was, "Has it been considered good practice for ccTLDs to join forces with local ISPs in order to identify potential DNS abuse patterns?" Thanks.

NICK WENBAN-SMITH: I think the short answer to that is no. But if you just hold that thought, because in terms of next steps and other topics to look at, I think that's one of the things that has been suggested and it's one of the questions that we've got about future sessions and workshops. So I will try to highlight that point when we get to that point in the presentation later.

BART BOSWINKEL: There is one comment on the pricing. There is also another common coming in. So first, on the pricing. "On pricing, ccTLDs seldom do USD 1 promotions, so they are not able to detect correlation between prices and abuse." That's more on the method of comparison, I think. It's more for Bruce, maybe you have a comment.

BRUCE TONKIN: The pricing I used in this graph is what I call the standard rate that they have on their website, rather than any promotional pricing. I know that different times TLDs, whether they're country codes or gTLDs, sometimes run promotions like free promotions. But we haven't done an assessment. I did a particular free promotion generate a higher level of abuse, we haven't got that data.

NICK WENBAN-SMITH: I think that's an interesting comment. I suppose maybe we should be cautious in drawing firm conclusions from the correlation between the registry retail price, because we know quite frequently it's at the registrar level. So the registrar will, as a loss leader, have a promotion. So they will sell under the price that the registry sells out to the registrar because the margin or the business model is on selling other services, not the domain name. So they look at a longer whole of life value to the domain name registration in connection with other services that they offer.

So I think perhaps maybe at the registry's level that might be the case. But if there's a specific very low price promotion, free domains, $1 domains, as the comment goes, that we need to be careful that that's not a conclusion that we draw, I suppose, from ccTLD perspective. I don't know there's very much that we could do about registrar level pricing. And if they want to offer good promotions, then I think a registry would be treading on dangerous ground to say that that's not appropriate. But yeah, it's an interesting comment.

There's another comment from John McCormack I can see around ccTLD abuse is often trending towards phishing and SEO compromised sites. The SEO compromised sites are more content abuse than DNS abuse.

BART BOSWINKEL: Nick, Mike Chattan has his hand up.

NICK WENBAN-SMITH: Mike?

MICHAEL CHATTAN: Thank you. Michael Chattan, Newfold Digital. I also wanted to throw out there that the registries also work with registrars on growth incentive programs. So generally, that's when we see the price increases, or at sign-up, price decreasing at the registrar level, that definitely does drive abuse. So it's a good and bad.

NICK WENBAN-SMITH: I think we can all agree that if there were no registrations, the amount of abuse would be a lot less. But it's a trade off, isn't it, between providing a public utility and resource to industry, SMEs, consumers as broadly and as accessible as possible yet safely mitigating abuse. And this is why it's such a fascinating topic, I think. So if we just go on to the next section, which I think I'm speaking to.

So we have some ongoing work as you've just heard, both from the Repository who's launching their e-mail list and expanding that. So I think that's going to be ongoing over the next 6 to 12 months. So look out for the formal launch of that. Speaking from the survey, I think the Survey subgroup found a very interesting exercise to do, and I think we would like to do another survey. But we're also mindful about sort of leaning too heavily on the community and survey fatigue.

So what I'm proposing is that we will do another survey in the final quarter of 2024. But we don't want to do that if the community thinks it's too annoying and not useful. So there's a couple of questions here in the Zoom poll around do you want to see any more of the survey

results and when do you think we should do the next survey? Do we mean 2025? I thought we were going to do in 2024 because 2025 would be a three-year gap. For the record, this should say November 2025. 2024. I confuse myself. I'm trying to speak and read at the same time. Okay, so 80%. Okay, so I think we will take that away.

We will look at some areas of the survey where the respondents gave us sort of inconsistent results or seem a bit confused by the questions, to see if we can make the questions a bit better and clearer for the second time around. So we will try and learn from that experience. And I think there are a couple of areas where we wished in hindsight that we'd ask some questions which we hadn't asked at the time. So we will obviously evolve the survey. But the idea will be to have the main cohort of questions the same as the last time so that we can therefore try to extrapolate around whether this whole initiative within not just the ccNSO but the whole community, whether we are actually achieving something useful in terms of reducing the amount of DNS abuse by better understanding it and sharing best practices in this sort of way.

So there's another question here around "Do you want even more in-depth analysis of the survey that we did in quarter four of calendar year 2022?" Wow, you guys, I don't know whether this is a sort of self-selecting audience that the people who are interested in more DNS survey discussion are the people who come along to the DNS Survey Discussion group. So there's probably a self-selecting sample. So maybe we could have predicted the answer to that question. Thank you.

I want to emphasize that this is supposed to be a two-way process, which is why we're trying to get some of this feedback. I don't want to just sort of deluge of different interesting looks [inaudible] and samples, but it does sound like there's an appetite to continue exploring some of these interesting questions and correlations.

So I think we have some questions here. Bart, can you help me sift through the comments and questions? Because there's quite a lot.

BART BOSWINKEL: These were more to questions on the ongoing work. Now you go into we have a few more questions, can you go back a slide, please? We have now reached the point where you want it to go is, what are the work items for the DASC going forward? We got the survey done, we got the repository and the e-mail list, you got four topics.

NICK WENBAN-SMITH: Thank you. So if we're not going to look at the Zoom comments and questions now, that's good from my perspective. When I was presenting the first cut of the data, I had a lot of questions around—this is all very interesting—but why don't you consider this specific topic or that specific topic? I have to admit, I've applied some purely subjective judgment as to pulling the comments and questions that came in to me and suggestions for future work into these four topics here. So we have here four suggestions, if there are any more, please feel free to include them for our consideration. But four areas came through for further sort of investigation or workshop or discussion topics.

I'll go back to the Terms of Reference of the Standing Committee, which is to share best practices and to educate and to provide resources to the community. So firstly, there's one around—we've already looked at this because it's a fairly obvious point around the data validation registration policies and how that intersects with the levels of abuse observed. So we could have sort of a longer, deeper dive into that. So that was the first thing. I guess a lot of people already know. But if you didn't already know, as a ccTLD, a lot of us are very cautious about any sort of content-related issue. But we do get a lot of content-related complaints. But the avenue for dealing with a content-related complaint will frequently be through, okay, we don't have a content policy, but we do have data accuracy and completeness provisions. And if you're a threat actor or other malicious actor, you don't tend to put in genuine detail. So we effectively deal with a lot of complaints through sort of a dog-like mechanism of looking at the data quality underneath it. So we can explore that in a bit more. So that's the first topic.

The second topic, I think, it touches on actually the question around pricing and promotions that registries maybe—we go off into our ivory towers without really taking into account the factors that the marketing mechanism and the relationship with the customers is with registrars. So maybe we should be smarter about working with our registrars maybe across different ccTLDs and across different registrars, to be smarter about combating some of the threat actors that we see. So I think a little workshop between registries and registrars and some examples of how that can be very, very successful

would be something that would be useful to share with the community. I think that's quite a nice, a nice topic.

Third one and it comes down a little bit more to benchmarking. As you could see from the first survey, we had a significant number, more than 30% of the survey respondents were unsure about the levels of abuse in their own ccTLD. It's been interesting to think, well, maybe they're unsure because there isn't any. So they don't know what they don't know. But actually, there wasn't any abuse or no realistic levels of abuse. It's in sort of smaller ccTLDs, you don't have the numbers of abuse in absolute terms to sort of like anything. So providing a bit more benchmarking tools and measurements. So we've had obviously the DNS Abuse Institute yardsticks for benchmarking, but I know there's also the ICANN DAAR project. I know some ccTLDs have signed up to DAAR, some haven't, some thinks it's great. So we could have a bit more of explorers to those sorts of tools and measurements and socializing a bit more. I think shining a light on areas where previously we didn't really have a good understanding of what was going on and trying to, in a friendly way, get good comparators about what's successful and not what's not successful for the benefit of the whole community could be a very useful way to do that next step.

The fourth topic is around—it's easier to go more slowly when you're not so excited about governance and regulatory models. But in the ccNSO, over the years, we have looked at governance models as a comparison. But we have never looked, I believe, at the intersection between types of legal frameworks and governance models, which ones are more successful or seem to be more successful in terms of

abuse, measurement, mitigation, and management. So that was also suggested as a fourth area.

I believe we have a poll time. So please give us a steer. I'll give people are reasonable amount of time. We're doing okay for time on the deck. Okay. Thank you.

In terms of the prioritization, is there a particular topic which people would want us to deal with first? So, with this question, we're trying to prioritize one or two items to deal with before others. So in terms of, just as you answer the question, don't tick all the boxes, just tick the ones that you want us to prioritize. This is sort of a plan as we get what we deserve, I suppose, and the result is no overall winner. Well, I mean, in a sense, that's helpful because I can just decide. Thank you. I'll exercise chair's discretion when I'm formulating the work plan through.

So that's actually a good segue because we're looking forward to the Hamburg meeting now. I think I am going to try to have a deep dive into one of those topics at the Hamburg meeting. We will talk about this within the whole Standing Committee and come to some sort of agreement. I think it's very tempting to be quite internally focused around what we all do within the ccTLDs. So what I'm aiming for is a sort of a more of a cross-community type thing, either with registrars or with the ICANN Technical team and Org staff around either DAAR or measurement and working with the registrars and the other contracted parties. I think there's some very interesting things going on there. So if we're not giving you what you want, then you know where we all are.

BRUCE TONKIN: Just one comment on—maybe if we go back a couple of slides on those topics. One thing I'm seeing on the first one in particular but starting to emerge a bit is the difference between domain names that are maliciously registered. In other words, the domain name has been registered for the purpose of setting up a phishing site or setting up malware. The other category is domain names that are registered legitimately by a person or an organization, but their websites have been hacked, and in fact, are then being used for phishing and malware. So the first category, validation and registration policies can deal with, if you like, the malicious behavior. But it doesn't stop the hacking of websites and other things, which is probably where the tools of measurements come in a bit. So you can't solve the whole problem with any one solution, really.

NICK WENBAN-SMITH: I think that's a good observation. I think when I've been listening to other sort of talks on DNS abuse, and particularly with the new gTLDs, for them maliciously registered domains are more of an issue. For a lot of us ccTLDs, we've been around now for 30 plus years, so we are very much in the sort of the mature plateau of large existing registrations, high levels of renewal. Growth isn't so much the thing now because we are in a very mature stage. Therefore, the amount of abuse for a mature ccTLD is going to be much more focused on compromised domains rather than newly minted ones. So I think that's a very interesting area. I know some registries will take action even if the registrant is innocent. They will still suspend a domain name if it's

spewing out malware. But I think that's not very common, and certainly we wouldn't do that without a lot of careful thoughts in the .uk. But the point is well made that the data validation only tackles one aspect of maliciously registered domains. And when we're talking about abusive registration or abusive use of a domain name, it's not necessarily the registrant who's the guilty party. The registrant could themselves be a victim of DNS abuse. Okay. Thank you.

I'm trying to follow the various comments and questions.

BART BOSWINKEL: There's a lady up front has a question, and there are questions there as well.

NICK WENBAN-SMITH: Go ahead.

MAHUM KHAWAJA: Hello. My name is Mahum. I'm a NextGen from Toronto, Canada. My question was on the repository, actually, and I think I should have asked this earlier. But as new joiners, we would just want clarification on how the repository was different from ICANN wiki, which is also supposed to be neutral and you're not pointing fingers, and this has a database of information. Thank you.

NICK WENBAN-SMITH: Thank you. That's an excellent question. Thank you, and welcome. David, over to you.

DAVID MCAULEY: Thank you. Just to make sure I heard is how is it different from the ICANN wiki? Thank you for the question. The repository, as we get it up and running, is going to be focused on information useful to ccTLD managers. Oftentimes, it may be useful to others equally, but we're going to be focused primarily on serving this community, and so it'd be different in that respect. Then it'll probably be a bit more focused than some of the information you could see on the wiki. I will say maybe it will become a lot alike. But at the outset, we're going to be focused on that manner. Thank you.

NICK WENBAN-SMITH: Okay. Are there any more questions in the room or on the Zoom?

BART BOSWINKEL: Nick, there is one question from Raitme and I've waited until the end because it is again around ISPs. I'll read it out. "Is it considered a good practice to join the efforts of the ccTLDs with the local ISPs in order to identify potential DNS abuse patterns?"

NICK WENBAN-SMITH: Okay. Thank you for the question. And thank you for reminding me. So I think when I talk about acting in combination or collaboration with registrars, I think it could be an interesting thing to expand that cooperation not just to registrars, but also other internet infrastructure within jurisdiction. So I think if the ISPs and things are spotting things at a level, then if that intelligence is useful to the

ccTLD, then I think that could be quite an interesting area. Just anecdotally, I don't know myself of that many ccTLDs who work very closely with ISPs, but of course, some of the registrars themselves will be ISPs. So I think within that discussion point on working collaboratively with registrars, I would hope to include some of the registrars who also provide ISP type services.

BRUCE TONKIN: I can comment, Nick, that one observation I have about ISPs is they're often using the same DNS abuse feeds as the registries are. But they use those DNS abuse feeds basically just to automatically block the website. And one of the challenges that we find with compromised names as opposed to maliciously registered is when the compromise is corrected so that the phishing content is removed or the malware content is removed, they often find it hard to actually get off the DNS abuse feeds and therefore not get blocked by the ISP.

NICK WENBAN-SMITH: That's why I think we were all a bit cautious on this topic about block lists. I'm not trying to be critical about the block list providers who provide valuable service but they do seem to market themselves on the number of names which are blocked. So there's very little commercial incentive for them to remove something which had been compromised in sending out malware and was accurately reported. But you do find that name on that list for years, if not decades, afterwards, even if the domain name sometimes has been cancelled and then re-registered, you'll still find the name on it. This comes back to the false positives in the block lists and the sort of the high degree

of caution and skepticism that the registry staff needs to have. It was back I think in one of Angela's slides, you could still see that actually handling DNS abuse when people are trying to automate it. But because of the high error rate, the majority of us still are forced to go down, so the manual processes and doing it at scale is certainly a real challenge for anybody who's operating a large registry. That's an interesting point.

So we've actually got three minutes left and I'd like to say it's because of my skill for chairing. But actually, if that's luck, I'd like to thank all of my panelists. There's an opportunity for another couple of questions, if anybody's got any last minute ones. Otherwise, thank you all for attending and look out for next steps. We will take your balanced feedback about what we should prioritize. We will come back with a work plan. As you know, I think I said in the Cancún meeting, I really wanted to have a forward looking program which built up with the community input so that people could see, okay, in six months time we're doing this. In a year's time, we're going to look at registries and registrars working collaboratively, we're going to have something about better data. And we will also be able to obviously follow the launch of the repository.

So, thank you very much. There's now, I think, a short break for 15 minutes before the ccTLD new session. I'd like to thank very much my co-panelists. It's been an amazing work. It's incredibly unstressful when you work with such competent and diligent and organized colleagues. I don't think they could say the same about me. But it's been a real pleasure. Thank you.

BART BOSWINKEL: You can stop the recording. Thank you.

[END OF TRANSCRIPTION]