ICANN72 | Virtual Annual General Meeting – ccNSO: DNS Abuse - What's the role of the ccNSO? (1 of 2)
Wednesday, October 27, 2021 – 14:30 to 16:00 PDT

KIMBERLY CARLSON: Hi, everyone. And welcome to the ccNSO DNS abuse session. My name is Kim and, along with Claudia, we are your remote participation managers for this session.

Please note that this session is being recorded and follows 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 noted in the chat. We will read the questions and comments and aloud during the time set by the chair or moderator of this session. If you would like to ask your question or make your comment verbally, please raise your hand. When called upon, kindly unmute your microphone and take the floor. Please state your name for the record and speak at a clear and reasonable pace. Mute your microphones when you are done speaking.

Additionally, this session includes automated real-time transcription. Please note that this transcript is not official or authoritative. To view the real-time transcript, click on the closed caption button in the Zoom toolbar.

And with that, I'd like to hand the floor over to our session chair, Alejandra Reynoso.

ALEJANDRA REYNOSO: Thank you very much, Kim. And good time of the day, everyone. Thank you so much for joining. My name is Alejandra Reynoso, and I am the Chair of the ccNSO Council.

Today, we want to see if the ccNSO should become more involved in the discussion regarding DNS abuse. DNS abuse is a problem that will not go away anytime soon, if at all. It is complex and impacts stakeholder groups differently. This topic has been discussed at a various occasions in and outside of ICANN over the past years. ccTLDs are addressing this topic in their respective countries and regions. And the ccNSO as a platform for information sharing has organized various sessions on this topic, such as members meetings, ccTLD news, and Tech Day.

Recently, some of the members of the ccTLD and broader ICANN community suggested that the ccNSO could play a more active role with respect to DNS abuse and to have a more prominent voice on behalf of the ccTLD community in the ICANN environment. Participating and shaping global discussions in this area might be an opportunity to leverage the local and regional activities and influence them. Also, a more active ccNSO may assist those ccTLDs who are not yet involved in their national and regional discussions.

The goal of today's sessions is to understand what the community expects the ccNSO with respect to DNS abuse. Based on the guidance of the ccTLD community, the ccNSO Council will plan and if and how the ccNSO should get more involved in DNS abuse discussions and related activities that could assist ccTLDs in this matter. Such a plan, if

any, will be shared and discussed with the community at ICANN73 or during an intercessional webinar, depending on what is most appropriate.

It is important for everyone participating in this session to keep in mind that the remit of the ccNSO is very limited and does not include telling ccTLDs how to operate or conduct their business.

So to this, today's session is divided in two parts. In the first part, we will hear from various presenters, their view on DNS abuse, and their suggestions regarding what the ccNSO could do or should not do in terms of DNS abuse. For this part, Nick Wenban-Smith will be our moderator. And I will be introducing the presenters one by one when we get to the panel. After the 30-minute break, the second part will be a moderated discussion with the audience, and we will do some polling to see how to assess the various recommendations that we will be collecting on this first part.

And to start the panel discussion, I will give the microphone to Jim Galvin, who is participating in the DNS Working Group of the Contracted Parties House at the GNSO. Jim, you may start.

JIM GALVIN: Thank you, Alejandra. May I have the next slide, please? So as Alejandra said, I am one of the Co-Chairs of a DNS abuse working group that the contracted parties have. I have two that [are chair] from the registrars and, of course, another co-chair from the registries.

And I thought I would begin here first by just describing the problem space in which we're working in this discussion here to kick us off. I think it is fair to say and to acknowledge that abuse in general is certainly on the increase at an astonishing rate on the Internet. And this really is just abuse in all of its forms—on the Internet, with the Internet, over it, through it, in all manner of things. This is not just the DNS as a protocol. There are other mechanisms, other kinds of things going on. It really is a global problem and it affects everybody.

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

Common sources of these things of things: physical infrastructure; your ISP, your local network access. They have a role to play in recognizing when there are abused or taken-over machines or activities going on in their networks and things like that. And let's not forget service providers such as ourselves—registries, registrars, the whole domain registration system.

And we all have a role to play in mitigation of some abuse, but the question is, what is that role? And that's what we're here today to talk about: a potential role for the ccNSO. What could you or might you consider doing in this space to help contribute to the mitigation of DNS abuse?

Next slide, please. So I thought a good place to start would be on behalf of contracted parties, the registries and registrars—the Registry Stakeholder Group, the Registrar Stakeholder Group, in the GNSO. Let's talk a little bit about what we have that's working that might be an interesting resource for you or something to think about.

So the first thing that comes up—and it has already been a question in the chat room—is, what about a common definition of DNS abuse? Well, gTLD registries and registrars do share a common definition with ICANN. It's a technical definition. You've heard it many times. Malware, botnets, phishing, pharming, and, of course, spam when it's used as a distribution mechanisms of those things. And there are links in this slide that point you at that definition and its existence and its endorsement by both registries and registrars, the stakeholder groups.

It also turns out that we have a framework for DNS abuse that is shared by many of the contracted parties. This framework actually has three important key parts to keep in mind. One of course is a baseline of that shared definition of DNS abuse. So that's recognized as those who share and voluntarily sign up for this abuse framework. They acknowledge that that's the set of abuse that they promise they're going to address and they're going to take care of.

But the framework also has two other important features. It has an opportunity for a number of other common things that many registries and registrars deal with. Child sexual abuse is a common element of those things. So it provides an opportunity for people via local policy,

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

And then there is a third option for really just individualized additions. There are some registries and registrars that have their own requirements and their own set of common use policies, terms of use policies—that kind of thing—and they want to address those things. And the framework allows for all of that. So it's not prescriptive. It has a starting point and then people can do whatever seems to work for them.

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

So we actually had both a joint and separate working groups where we share our guidance, and we're producing work products. In fact, you'll see here in the slides there's two links which point you at some of those resources. It's just guidance [for] those of us who are actively doing something in this space. It's a recognition of acknowledgement of what we do that is working. And you will find those work products in both of those areas respectively. And you might find some of that useful for you.

I'm going to highlight one last thing there about working in collaboration with other parts of the community. We very actively do

outreach to other elements of the ICANN community, listening to pain points and stories, and take on those activities to address those things with work product. And we have quite a lot of success about that. Maybe you went to the session on Monday and you saw the latest update of our activities.

Next slide, please. So the last thing that I want to focus on that I was asked to suggest is, what are the kinds of things that are key takeaways in the "Do" and "Don't" category for ccTLDs, lessons learned on behalf of contracted parties, that we think would be very applicable to think about?

One is to actually not create another definition of DNS abuse. If you're going to have a common definition, find alignment with an existing definition. I did mention one. The contracted parties have a shared definition. There are a couple of others out there. But rather than trying to invent something new and completely different in this community and thus confuse all of that, try to find one that you can find alignment with for your baseline if you're going to do that. And then work collaboratively with the rest of the community as it considers this problem space and considers what is or is not within the ICANN arena's remit for DNS abuse. And I think that's important. We should work collaboratively together. Let's figure out what that collaborative environment looks like.

The next thing is I highlighted the framework on the previous slide. I want to encourage you to think about a framework. I know that ccTLDs,

just like gTLDs, all have different business models. We all have ways of doing things. With any luck, you can find a baseline that you can start from so that those who sign up to be part of this community of those who address DNS abuse … But then, if you have a framework, you can allow for different local policies so that individual ccTLDs can of course honor and respect their own jurisdictions or whatever jurisdiction of choice they might have. You can also define your own roles. Not all ccTLDs have registrars, for example, [and] other kinds of mechanisms. So, if you have a framework, then you have a baseline and you allow options for ways in which to build it out. So at least you're all talking about a common language and you're representing the party together.

And then, lastly, do work with the ICANN community with all of us in the large. I know that we all like to have our own models of the world. Even gTLDs do. We like to have our way of doing things. And ccTLDs do, too. But we can always work together, at least talk together, as issue evolve and seek to improve on an ongoing basis, whatever our baseline is. So rather than moving off in a direction in a star-like pattern, let's try to keep a holistic view of how this is going in the community and where we can go.

And that's it from me. Thanks.

ALEJANDRA REYNOSO: Thank you very much, Jim. And thank you for such great suggestions.

I wonder, Nick, if you would like to ask anything from Jim right now, or shall we wait until the end of the panel?

NICK WENBAN-SMITH: I think that was really clear. Thank you, Jim. I see there's one question already from Volker Greimann around how does the ccNSO define abuse. And I suppose it's worth saying upfront that the ccNSO doesn't set policy. So we haven't got a definition of abuse, but I see that one of your suggestions is to look at that, maybe, and, certainly, if we do look at it, not create a separate definition because that is not going to be helpful to the community to have parallel definitions which are different. The purpose of this session is not to solve all of the problems. The purpose of this session is us as the ccNSO to listen to everybody in the community about what we should take back to the ccNSO Council and look at what recommendations we want to put forward to the broader ccNSO total community as to what might be appropriate things [to do]. So we're very much in listening mode. But thank you.

ALEJANDRA REYNOSO: Thank you very much. So, with that, I think we should move on to our next panelist, which is John Crain, who currently is the Interim Chief Technology Officer at ICANN. So, John, the microphone is yours.

JOHN CRAIN: Okay. I'm not going to use slides. No death by PowerPoint from me. Firstly, thank you for inviting me. It is always good to be with my friends from the ccTLDs. As has been mentioned, the ccNSO is not really a policymaking forum, although when there are global policies, they do get involved. But in general, they don't make policies. And really the

policies they make are really for the IANA/ICANN, not, per se, for the ccTLDs.

So we were asked three questions in preparation for this. One was, what is my perspective on DNS abuse? It's a term that gets used a lot. We also use the term, within ICANN, within one of the groups that I run, which is the Security, Stability, and Resiliency Group, "security threats." In many ways, the labels don't really matter.

So if you are going to go down the route of finding a definition—I fully agree with Jim that making up yet another definition or a different definition would not be particularly useful—think about what elements of something make it DNS abuse rather than thinking in the [inaudible]. What makes something DNA abuse and something not be DNS abuse. And that's probably not something you're going to do in the ccNSO yourself. It's probably something that indeed you would work with other areas of the community on. There's a lot of work in this area. And I do recommend that your members, the ccTLDs, get involved in those discussions. That's very important. Clearly, there are problems online. There is harm caused. This is problematic for everybody, including the cc's.

And the second question was, what is at stake? Well, we all know harm to the user, the victim, of some of these harms. There's also the trust in the ecosystem and the reputational risks that came if you have a lot of abusive behavior happening within a particular TLD, be that cc or not. It's the same problem everywhere.

So you have a lot of commonality in the risks and the issues that are at stake with your colleagues and peers in the gTLD space. So talk to them about that.

And then the other question really was, what are the do's and don'ts? So the first one we talked about is don't go off and start your own definition of what is DNS abuse. Try and work with other groups that are already doing this. Don't do it on your own.

The other thing I would talk about is something that the ccNSO is very good at, and that is knowledge sharing. So there are lots of ccTLDs that have a lot of expertise in this area. I see our AFNIC friends here were doing a lot of work in this area and scientific work on recognizing various abuse types. Learn from each other. Maybe something the group could is have some form of knowledge sharing group. The ccNSO does this in the broader area of DNS security. Many of your members are on something called TLD-OPS. I have sat through many fascinating work sessions.

If anybody remembers the time when we used to get in room together, when that was still not forbidden and we actually used to be able to sit within six feet of each other, we sat in rooms with not just ccTLDs but others from the community and we discussed things like, how do we deal with incidence response, how do we deal with building sustainable systems? Well, maybe DNS abuse is another area for a forum like that, where the role the ccNSO could bring to that is actually bringing people together. We do this on Tech Day. Others are involved, but it really did

come from the ccNSO originally. That's another forum. And then of course there's TLD-OPS. Maybe there's a different one or the same one for the abuse problem.

So I really see the role of the ccNSO as this ability to bring together the ccTLD operators and share knowledge and experience. I'm going to do an advertisement because I kind of have to. When you're dealing with abuse, you've got to be able to recognize it, you've got to be able to action it, and you've also got to be able to measure it. We measure reputational data through our DAAR system. So if any of your members want to participate, they should feel free to look at that.

So I think that is a really good role for the ccNSO: bring people together, make them aware, and learn from all the skills from all the ccTLDs are quite vast. Thank you.

ALEJANDRA REYNOSO: Thank you very much, John.

Nick, any immediate question/reaction now?

NICK WENBAN-SMITH: Well, first of all, I'd like to thank John on a number of different fronts, really. I think, firstly, I want to thank him for not having any further PowerPoint slides because I think there's the curse of ICANN and curse of Zoom meetings: another presentation of PowerPoint. So it is helpful sometimes to see it summarized, but it's also refreshing just to not have it summarized.

So just coming back to a couple of points that you made, I appreciate that you recognize ccTLDs and ccNSO is a broader coalition, as it were. It's not as if we don't talk about things. We talk about things in great detail. And I don't want anybody to come to this session thinking the ccTLDs are starting from a standing start on any questions of abuse, whether it's DNS abuse or wider abuse or anything reputational, because we talk about these things whether it's in our regional organizations or within smaller groups or in groups of likeminded communities sometimes within the ccNSO, sometimes without the ccNSO. So there's a huge amount of work.

And I should also point out that some of us are also signatories to the framework and to the common definitions. So there's a broad [traction] there. And I think I do appreciate your acceptance and recognitions. I want to put that on the record: that we just do a huge amount already. The question is, should it be more broadly coordinated by the actual ccNSO formally as a thing as opposed to having lots of informal structures and ad hoc, given our specific remit as Alejandra stated up front: that we do not, apart from some very specialist areas, actually set policies for ccTLDs?

And I wanted to thank also Pierre for highlighting some of the work that's done by individual registries or consortiums of registries already in this area. There's a huge amount of work done. For myself, I know more about the EU region, and there's a massive amount of stuff we coordinate nationally and internationally to a great degree of knowledge.

I suppose what I took from your suggestion, apart from the DAAR suggestion—I know you have to upsell it there—is the fact that there are some examples of things that we already do. And I think Tech Day is a great example. I think the TLD-OPS is also a great example. I know there are people—I'll just maybe put a pin it for now because we've got time for Q&A later on—who participate actively in those communities. So I want to get them involved at some point.

But let's a pin in it for now and move on to the next presentation. Thanks.

ALEJANDRA REYNOSO: Thank you very much, Nick. And for our next presenter, we have Gabriel Andrews. He comes from the Public Safety Working Group of the GAC. Gabriel, the microphone is yours.

GABRIEL ANDREWS: Hi, folks. So I guess let's go the next slide, just to start this. There's the adage that you speak to what you know, and I have to come into this then confessing and recognizing that, as a member of the Public Safety Working Group, I'm a career law enforcement officer. I am not an engineer. I don't really know the ins and outs of ICANN and its policy setting, much less ccNSO-specific rules and responsibilities. So I want to approach this with a level of humility that I'm not going to be the true expert on what is or is not "DNS abuse," nor your respective roles within it.

But—and there is a "but" to this statement—I feel that perhaps I can add some value here in the sense that I can speak to some of the major trends that are occurring in cybercrime over the last several years, I guess, the broader context of this conversation is happening, and why these trends should be allowed some of your consideration as you each are playing your own role in this DNS abuse conversation.

When you see this slide here, I threw this up because this is the closest thing that I ever get to creating my own website when we seize other sites from others. But I do want to give credit to the Dutch national police. This is their seizure of the double VPN criminal service. And our colleagues in the Dutch national police do great work.

Next slide, please. So I wanted to talk about the big trends that we're seeing in 2021. And these are actually a continuation of crime trends that have been plaguing the world for literally years. And the two big trends that I just want to special attention to—they're not the only types of crime and abuse out there, but they're most worrisome and ongoing—is ransomware, on one hand, and what we call business e-mail compromise on the other.

So ransomware—I think everyone knows at this point—is when malware encrypts victim data and then the bad guys ransom that data back to the victim. It's been in the news a lot lately. Business e-mail compromise, on the other hand, is a subcategory of phishing attack. And I think, in Europe, for a while it was called CEO fraud. You might recognize it by that name. but it's where the bad guys are seeking to use

a phishing e-mail to elicit a wire transfer from a victim. It's very low tech but super effective, super abundant, and rampant in the world. And neither these, again, are new. They just keep getting worse.

Let's flip to the next slide, please. So the FBI does its best to track reporting on cybercrime through a site that we have called IC3.gov. It's the Internet Crime and Complaint Center. It puts all of the reports that we get into a centralized database and tries to aggregate all that victims reported so we know what's worthy of our limited investigative resources.

They also put out, at the end of every calendar year, statistics on what we're seeing—what's being reported to us, in other words—so we're able … We try to track more than just U.S. losses. For example, I know that the business e-mail compromise scheme I mentioned we started tracking in 2013. And as of the 2019 close of calendar year, it reached more than 26 billion dollars in global loss exposure. In 2020, in the U.S. alone, it was two billion. So it's not small potatoes.

When we try to track ransomware, however, I am going to suggest that our data is nowhere near the whole picture. I suspect that most ransomware victims don't tell us that they were victims. And so we often turn to private [central] reporting to supplement our understanding of what's actually occurring.

And I'll ask for the next slide here. We can see that folks in the private sector in position to pay attention to such are tracking such ransom payments being made. And pretty interesting stats. Like, in 2021,

ransoms are now in the tens of millions of dollars in the most extreme cases, with the highest ever publicly confirmed ransom reaching 40 million dollars.

And next. There is a company named Coveware that actually is engaged in ransomware negotiation as a core business model. So they'd be in a position to have very good insight into payments being made. They estimate that the REvil Group—that's one of the groups out there involved in ransomware—have received approximately $100 million in ransom payments in the first six months of 2021 alone.

Next slide. I recognize, having said this and having talked about these big schemes, that not all of the incidents of these criminal ongoing schemes are actually directly relevant to DNS abuse. That said, we can turn again to Coveware and see that, for the top three categories of ransomware that are being used out there, a significant amount of it is directly linked to e-mail phishing as the initial intrusion vector. There are other categories. If someone is using a remote desktop protocol vulnerability, that might completely bypass DNS. But a non-trivial amount is directly linked to phishing. And BEC, of course, is a subcategory of phishing. So a full 100% of that is directly relevant.

Next slide, please. So all of this is to say that, outside of the ivory tower of ICANN—sorry for calling it such, but it feels like it can be that sometimes—there is now more tension than literally ever before being placed on cybercrime. I know that COVID has warped time and space for us, but it was this year, if we recall, when a newly elected president

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

Let's go to the next slide. So when we talk about what can be done at the DNS level, with this unprecedented level of attention that's being directed towards cybercrime, it shouldn't be a surprise that many of those same eyes are looking at the multi-stakeholder constituency groups like ICANN and asking about what's being done here, what's happening, trying to learn more about what is actually being done to move the ball forward on these issues. And so it might be unrealistic to expect that ICANN can solve these huge, thorny, crazy issues, but nonetheless, we have to recognize that the decisions we're making here do have direct impact on the schemes I've just discussed.

As an example here, I call out as a public safety official that we benefit tremendously from having swift access to accurate domain registrant information. So the decisions made in constituencies like ICANN can and do impact whether or not public safety officials can successfully notify victims of ransomware in emergency situations like when—and this has happened and I've been involved in this—we discover that ransomware is about to be executed on a victim network and we may only have—let's throw out—24 hours before that victim network is going to be encrypted. And we need to convert the known victim domain to a working telephone number or office address to make that victim notification. There may be other use cases where we're trying to identify subjects or even just the sheer component of dissuading the

abusive activity before it occurs if there are actual authentication measures put into place.

I'm going to go ahead and move to the next slide. So, having discussed what I view as some of the largest trends that exist out there and the most worrisome trends that do sometimes—not always—touch on DNS and policy therein, I do also want to call out that there is a very high-impact but low-frequency touchpoint where law enforcement does speak to ccTLD operators along with other TLD operators, registries. And that is when we talk about addressing the criminal use of botnets and domain generation algorithms that are sometimes employed by botnets. I mention this because there's been some really promising dialogue and conversation and collaboration between the Public Safety Working Group and the Registry Stakeholder Group to address domain-generation algorithms where they are employed by malware and botnets. It's something that's actually a lot of work for registries and law enforcement alike to deal with, but we feel that there's been a lot of progress made in discussing this issue and trying to minimize the amount of administrative burden and overhead associated with law enforcement's activity in trying to take down these criminal pieces of infrastructure.

And so if you are a ccTLD operator and you haven't heard about this particular framework, it's worthy of at least a cursory read so that, perhaps the next time a law enforcement agency reaches out to you about domains on your ccTLD, it's not the first time that you've seen it.

And I will now ask for the final slide with my limited dues. It's my understanding that the ccNSO is already engaged in encouraging folks to share best practices, what's working in security, what's working in addressing abuse, and what's not working. And so I want to encourage … That's awesome. My very first ICANN in person was at Kobe, and I remember seeing a phenomenal presentation by .dk folks, where they talked about categorization of their registrants into different risk buckets and how they might employ different levels of identity verification based on the risk they assigned each of those buckets. I found it super interesting, as someone that never touches ccTLDs, and super educational. And so when you share you best practices, I encourage you to make them available not just to other ccTLD operators but to folks in the greater community like us in the PSWG and the GAC and others that might be interested in hearing your learnings points.

The second point—I'm going to reiterate what John already said—is I encourage folks to contribute to a shared understanding facts. So DAAR, in this case, is ICANN's Domain Activity Abuse Reporting, and it's something that I think that is, to my understanding voluntary for ccTLDs to contribute to, but it really helps us to understand what's actually occurring out there. And it helps us to avoid what so often happens in ICANN circles of us talking past each other because we approach issues with a different understanding of what's actually the ground reality.

And finally, I want to throw out again to read, be aware of, and throw tomatoes at and criticize and help us make better the voluntary

frameworks that we're trying to stand up. So, again, the framework on domain-generation algorithms associated with malware and botnets is something you might have reason to come across as if a cop brings it to your attention in the future. But feel to ask questions of it and fix it if there's issues that you see now that might not be relevant to your particular ccTLD or if there's other room for contribution to voluntary frameworks. I think this is something where we see a lot of progress being made, and we encourage more dialogue on that.

And that will wrap it up for my portion of this. I thank you for your attention and hope my slides didn't bang you in the head too hard.

ALEJANDRA REYNOSO: Thank you very much, Gabriel, for such a complete presentation.

I will now suggest that we move from one presented to the next so we can have at the end the Q&A. Otherwise, we might get shortened time. So with that, I will give the floor to Kristof Tuyteleers—sorry if mispronounced it—from .be, .brussels. Kristof?

KRISTOF TUYTELEERS: Thank you very much. Yeah, it's a very hard name to pronounce or forget. So good evening, everyone. It's midnight over here.

I want to start by clarifying the scope within which I think the ccNSO can have real added value and—who knows?—maybe even be a differentiator.

Next slide, please. So to kick off, I've put some code from an ICANN report from 2019 on this slide. Pierre also mentioned another study which I could have used for the same propo[sal]. So I think it's important to keep in mind that most ccTLD registry operators are concerned about cybersecurity and about the amount of abuse in their zones. I'm also convinced that they try to do what is within their power and means. So although we all face cases of abuse, the problem is mostly concentrated at the small number of players. Those are not my words. We can read that in this ICANN report.

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

Next slide, please. So to put things in perspective, there are a couple of reasons why domain name abuse is so popular and so successful. And like Jim already mentioned, I have a couple of concrete examples put

on this slide. Sorry that its such a mess and ugly slide. So, first of all, e-mail short message service security is fundamentally broken. We tried to create security extensions to fix it, but there is slow adoption, poor implementation. There's so much misconfiguration. So it's still insecure.

We have OS and software vendors that want to make us or keep us unaware. I have a concrete example. We had the discussion about hiding URLs in browsers. And also I specifically want to mention this on this slide with the discussion with the [green locks] where security experts and software developers thought that the way certificate authorities implemented "know your customer" was not the way forward, that it was causing more insecurity than security. I want to mention that because, as most of you, certainly in Europe there is, again, a vivid discussion going on about whether or not registries should implement a kind of "know your customer."

Next to that, there are so much exploitable resources on the Internet: hacked DNS servers, mail servers, vulnerable [inaudible] systems, compromised web hosting, etc., etc. Too much to mention. We have the IT security that's still poor, where devices are connected to the Internet with known vulnerabilities on board and we're unable to patch it, etc., etc.

And the last one—and I think that's the one that we should really aim at—are the security issues in the domain name sales channel—so the channel, the chain between the registrant and the registry. There can

be a reseller or multiple resellers between them—and also registrars, but that's not always the case of course. And since the [Seater] Campaign, this is also a hot topic in Europe for policymakers. And we also see that reflected in the EU cybersecurity [pact]. So there are a lot of legal initiatives now getting their way to new directives and new laws in Europe. And if we're honest to ourselves, we know we can step our effort in [inaudible] domain. It's also there, I think, as a community, that we can make the difference.

Next slide, please. And what I certainly want to say is to please keep in mind that we're all part of the blue team. So we're the good ones. And sometimes we may nag at each other because we disagree with the way we implement things or we approach security, as I just did with the OS and the browser vendors. But we all have a role to play—that was also mentioned before—in securing our digital world. And for me, if we do nothing, there is a risk of market disruption and then risk that we end up—and "we" means the ccTLD registry operators—doing business on an unequal playing field, meaning that cc's will be overregulated and others not so that we have a much bigger burden than others and less flexibility to run our businesses.

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

Next slide, please. So for the “do’s,” I always keep in mind that threat actors prefer the path of least resistance. And the image of the community will be partly determined by its weakest link, like I said in the first slide or wanted to show in the first slide with the ICANN quotes. So the “do’s” are awareness building and knowledge sharing to reach a certain maturity level in the industry. And I’m sure we can do that. And we also mentioned the TLD-OPS. And we have a good track record.

And you know that, Alejandra, because you were the person, I think, that requested to have the business continuity and disaster recovery playbook developed. There’s also the DDoS mitigation playbook. So I think we can create another one that concerns domain name abuse. And I specifically mention or I phrase it like that with domain name abuse. I know we’re not going to have a discussion today about what’s the definition of abuse, but for me in this session, for this propo[sal], for this meeting, I’m not going to talk about DNS abuse but specially about the misuse or the abuse of domain names because that’s not the same name as the abuse of the domain name service itself. So that’s more like a nuance that I want to put there.

So the second thing that we should do is expectation management. Abuse is of all times. It will remain forever. There is no silver bullet. And it’s not because people, others, ask us to hunt the crooks instead of the police that e-crime with evaporate. That’s just not the case. It’s not going to happen.

Next slide, please. And then for the "don'ts," also I already I mentioned, I guess, to not make obstruction of the singularity of the ccTLDs and their relationship with local, national, and international authorities. The example there is: don't make it look like ccTLDs, for example, can always ask as content police because that's also just not the case. And then I've cheated a little bit because there is a fourth one due to my personal frustration. Don't promote projects, studies, or data sources that lack transparency about your region, that lack of transparency about the methodology that we use, about the reliability of the information, or, even worse, try to commercialize DNS abuse mitigation.

And with that, I would like to give it to the next speaker.

ALEJANDRA REYNOSO: Thank you so much, Kristof, for your presentation. And indeed, when the community builds things that can help others, it's always a good idea to share it.

With that, let's move to our next presenter, which is Anil Kumar Jain from .in. Please, Anil.

ANIL JAIN: Thank you, Alejandra. Good morning, good afternoon, good evening to all of you. These days, there are two groups of people, who are getting affected. One is the big people who say, "We lost $600 million and we have to pay for this." Then $30 million of the customer data has been

stolen—those kind of things. Then there are small, small customers, citizens, who are impacted by daily abuse. For example, somebody says, "Somebody has stolen my $100." Somebody says, "Somebody has stolen my entire Facebook information." These small, small, small [accumulations accumulate] and make a bigger part of this. So basically these cyber threats or DNS abuse is a big problem—and a problem, a challenge, which cannot be ignored.

Next slide. So let us see whether the DNS has any definition. That is what the previous speakers were also saying. We are evolving. It is very hard to define and has a broad scope. It cannot be narrowed down. Industry players like us, the users, have come together with a working definition. It is a good starting point, but what is next? But the reliable and consistent metrics of definitions are absent. Currently, metrics are based on incident-based measurement. Let us look at that different people have different perspectives.

Next slide, please. Now, if you come to the government, the government has a different set of definitions about this kind of abuse: establishing a distributed command and control, spam and phishing activities, malware attack on countries' critical information infrastructure, which impacts the nation as a whole, and espionage. And in fact, the discussion which is happening at the top level whether the military attacks in the future are going to be cyberattacks rather than physical attacks. So the problem is much, much bigger than what we are discussing today. DDoS attack and also the attack which attracts

society at large is spreading the fake news. So this is perspective from the government.

Next slide, please. So what we are saying is DNS abuse is there. It is a relatively very studied definition, as we have learned. ICANN, ccNSO, and different units are studying them, and talking to them. And this particular session is also to initiate that discussion, to know that the community feels about it. Combating it is in the public interest. There is no doubt because we are losing both money as well as the data. And less discussions at different forums are going on. But are we coming to the mitigation level. Focus on awareness raising seems to yield a benefit. That is what the speakers have said: awareness is a very, very important aspect which is required in all the policymakers, the organizations, registrars, registries, and all those things, including the public. I think there is a great push for coordinated efforts. That is what we are talking about today. And ccTLDs are at the forefront of the dialogue because we are one of the unique [inaudible].

Next slide. Let us look at how .in looks at it. We are part of the DAAR, and this is the report of August, where we can see that we can only see what is the percentage of a particular abuse, which can be collected and which can be demonstrated. For example, in this particular [inaudible] that .in has 55.7% spam, 27% phishing, and other aspects as small. So does it make sense or help us to go for the mitigation level?

Next slide, please. Now let us see, looking at this [vote, what] we have done. First of all, we designed an algorithm for blocking the key words

which are impacting DNS abuse majorly. For example, we blocked "gov" to be given to the public. "Gov" is the government. .gov.in. And then mil.in. "Mil" is military. So if we are able to do that, then we are able to get good results. Separate the domain for government and academia and distribute that very carefully. Registry participation in global coordination in spam takedown requests along with CERT-In. So this is an internationally global coordination which we are able to do and we are able to achieve it.

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

Another thing we've done is that … Whenever there was a cold case or there is a LEA request to block a domain name, that block of domains was for a limited time—for three months or so. But those bad guys again pick up again after that particular time and start doing the same abuse. We have decided to permanently block those reported abuse domains, and this has improved.

Let us see what is the result. Next slide, please. We have compared the domains reported over the last three years, and you must have seen that the domains have reduced subsequently. And in 2021, the remains have reduced significantly.

Next slide, please. We see the phishing has subsequently come down in 2021.

Next slide, please. The pharming has also come down with the efforts which we are able to do.

Next slide, please. And let us see the other abuse. The total other aggregated abuse has also come down.

Now let us look at that, looking at what we have done and what has been reported. What is the way forward? Next slide, please. First is, I think, that DAAR is very important, which has said. It's a project of ICANN and I think most of us should adopt it. And there should be an improvement of the DAAR also, that more information should come and more analyzation should come.

Then second is to create a global database of abusing domains—and not only creating a global database but we should also share this global database with all because there are no boundaries of domains, whether they are ccTLD domains or gTLD domains. If a bad guy is working in one part of the globe, he will start doing the same thing in other parts of the globe. So I think it is very, very important to have a global database.

Then we should also try to draw, maybe best on the best practices, model terms and conditions for the ccTLD registrars. And again, as it is an advisory, we can send it to other ccTLDs. Other people can look at it, and a good number of us can definitely reroute it. Then we have to explore the role of technical solutions in mitigating DNS abuse. We have seen in the last few years that a lot of new technologies have come up. Whether they are impacting for us, whether they're helpful to us, that is what we have to see. And we have to explore [inaudible] spaces.

Next slide, please. Now let us look at what are the prescriptions from oversight on the “do’s.” First, I also want to be equal with all my other speakers. First of all, it’s to encourage more and more ccTLD to enjoy DAAR because if more people can join, then globally they should get more analysis. And we want that more analysis should be developed as part of the DAAR Programme so that we also come to know a ccTLD. What is the next step? What mitigation exercise are we supposed to do?

The second which we want to prescribe is to create a global database of abuse domains. You must have seen that, regarding the bad guys in [inaudible] also, there are global efforts which are there, and it has helped all the countries. And this global database should be shared with all ccTLDs.

And the last prescription is that, whatever efforts we are doing at any level, whether it is at the ccTLD level, the gTLD level, registry level, registrar level, or registrant level, we should create the cooperations and associations. For what? For a regular and sustainable audit mechanism. Again, the audit may not be mandatory, but it can be voluntary. But an audit helps in understanding, with the operators, with everybody, how and what effectiveness is there and how we have to mitigate this.

So this is all from my side. Thank you very much for giving this opportunity.

ALEJANDRA REYNOSO: Thank you very much, Anil. And with this, I will move now to our last panelist, which is Byron Holland from .ca. Byron, the mic is yours.

BYRON HOLLAND: Thanks very much, Alejandra, and thanks to my co-panelists here. Very interesting discussion so far.

One of the challenges of course of going last out of six is there probably will be a couple of things that you've heard before that I'm going to suggest. On the other hand, given the diversity of perspectives represented on this panel, the fact that there are some common threads actually hopefully is a very positive sign.

So DNS abuse is, without a doubt, a plague, and it's a plague that's actually getting worse. And I think the first step for any registry operator is to really find out the extent of that plague in their zone, in their registry. And I think there's an age-old management maxim that we probably all heard before, but it is effectively that what gets measured gets managed. And I think that DNS abuse is a classic case of that.

Joining ICANN's DAAR Programme, I think, is a good and easy first step. Of course, as we've seen in some of the chat, people have questions about some of the elements of it. It continues to be a work in progress. But I think we can all agree that it's a reasonable first step that registry operators can take to get an understanding of both absolute numbers but also a relative perspective in terms of their zone.

I know that CIRA has participated or does participate in DAAR, and the monthly reports compare your zone file to roughly 1,100 gTLDs and more than 20 ccTLDS. So you get a good relative perspective on how you're doing. And it's from that place that you can start to act or least better understand your zone and decide if you need and want to act.

The ICANN team has been reaching out to the community through the various regional organizations, and I certainly think they should continue to do that. That's a useful place to go more into the operation side of our community. And I'm going to volunteer John Crain, if anybody has further questions and details that they want clarified, both on methodology and anything else. I'm sure he's the guy to ask. So, John Crain, I'm putting some work on your shoulders potentially.

The second thing I think that's important is really around Tech Day and member meetings and our community's ability to share best practices in a really constructive and collegial way, which I think is one of the great strengths of the ccNSO community specifically and probably also the ccTLD community in general.

My organization, CIRA, has the good fortune of running a fairly clean registry, at least by the definition of all the various reporting mechanisms that we see. The DAAR reports the same thing. And for us, if nothing else, it provides an independent verification or validation of what we believe to be true in our registry.

And that's useful on a number of fronts. It certainly helps from an absolute perspective, but it also helps in providing an objective and

independent third-party perspective. And whether it's DAAR for others—I'm not a pitchman for DAAR—I encourage all of my colleagues here to look at the other potential sources of this information and consider which one works best for you.

We're fortunate in the .ca zone and at CIRA that we do run a relatively clean registry, and I think in large part that's due to the fact that we're, in the parlance of the old days, a thick registry and we valid registrant information because of our [nexus] requirements. And this provides likely a strong deterrent to malicious actors. Certainly I believe that. Either there aren't many Canadian bad guys or at least they don't want to give us their real names.

So while we have relatively few challenges on this front—again, that's a relative statement—we're nevertheless very aware of the problem because not only do we run the registry, .ca, and the DNS for it but we also sell, in a sense, a DNS abuse mitigation product ourselves, and that's DNS Firewall, which provides protection against malware and phishing attacks but, for us, gives us a really different insight into the problem not just in our own zone but more globally as well as our own zone. And that gives an interesting lens through which to view it, which of course we'd be happy to share in further Tech Days and such.

But that's my point. We have the opportunity to talk about those things in venues like Tech Day, which as we heard, started in the ccNSO but has now become something of a fixture more broadly in the ICANN environment. And I think that Tech Day and other ccNSO meetings like

this one provide great formats and forums for us to have these kinds of knowledge-sharing discussions and also intentional discussions about where to go next.

So I want to say, from a [due] perspective, let's keep these going. The question I have, really, is, do we need to go further? And that's something I'm going to come back to in a moment.

But first—next slide—if we go to some of the things that fall under the "don't" category, don't forget that ccTLDs are very different than gTLDs. And while many of you here may know that—it's literally in your DNA; you know that innately—that's not always the case. And we certainly have people in this meeting right now and, more broadly, in ccNSO meetings over time, who aren't necessarily directly in our community or a ccTLD manager.

I remember, in fact, that the last time we all got together face-to-face was in Montreal. And I remember talking to somebody from the GNSO Council. So this is somebody who has been around a while. They are a councilor. And they didn't realize that ccTLDs in general don't have contracts with ICANN. That was actually news to them.

So I need to remind myself often—and I think we in general—that, when we're talking to the broader ICANN audience, such as we are today—we need to continue to reinforce that point that there's significant difference between the cc and g space on a number of fronts, not the least of which is contractual obligations to ICANN.

I think that we also really need to remember that ccTLDs within the ccNSO and more broadly very widely are very, very different across the spectrum of our TLD community. You can think of .uk or .de for Germany have 11 and 17 million names respectively. But there are many ccTLDs who would count their domains under management in the tens of thousands or, quite frankly, even less.

So if we want to ask them—we're going to ask this community to do new things or think about being responsible for new things—we really have to take into account the variation within our registry community, the size of the registries, the scarcity of resources that some of those registries experience. And of course I would say it carries over to the ccNSO itself as an entity. We do all of this as a volunteer community. And many members of the ccNSO don't necessarily have the luxury of participating more robustly in the ccNSO. And we need to be aware of that and we need to take that into consideration. So if we want to do more in the future, we need volunteers, but we got to remember this has to be done on top of those volunteers' daily job.

I think the other thing that's important to remember is: don't ignore the relationship between ccTLDs within the ccNSO membership and national governments and other elements of national governments. It's another way that ccTLDs are quite different from the gTLD community, and the ccNSO membership is different from the broader gTLD community. And that is our typically our relationship to national governments.

Many ccTLDs are, in some way, shape, or form a part of their national governments. They could be part of their telecom regulator group, for example, or are directly related by government or have legislation governing their operations. So my organization, CIRA, is a not-for-profit private corporation. Our bylaws allow for an independent observer on our Board from government. And this is not something we fear. In fact, it's something that we actually welcome. Don't tell them I told you, but quite frankly, we exploit it for the benefit of CIRA and hopefully their benefit, too. We're pleased to have a very close working relationship with our national CERT, and I think that's a very important relationship for literally any ccTLD. In our case, it's the Canadian Center for Cybersecurity. And we make sure that we have a good relationship with them and work closely. If we do it in advance of needing it, of course that's always a better position to be in.

So I think if any ccNSO member wants to strengthen their cybersecurity posture in general and work to address DNS abuse specifically, building a good relationship with your national CERT is certainly an important step. So don't let those relationships with government or government entities wither or not be developed.

And of course, to that end, let me remind our friends in the GAC that, if they're concerned about their ccNSO's TLD rule in addressing DNS abuse, I think, as the saying goes, "Physician, heal thyself." Reach out to your ccTLD directly. ICANN has no sticks that they can wield over the ccNSO community on this issue. So it's important for our GAC colleagues. If you want to have a discussion, enter it as such, as a

conversation. You no doubt can each benefit from the expertise from the other party. So build that relationship.

Next slide, please. You've heard it before. I've said it. Others have said it. I think there's easy low-hanging fruit here. Join DAAR. As the last speaker … It gives me the opportunity to kind of reinforce a few messages that we've already heard, and that is certainly one of them. It's cheap. In fact, it's so cheap it's free. It's understood and it's evolving taking into account the feedback that our community of TLD operators provides to the folks who run the DAAR Programme.

So it gives us an understanding. It's not the be all and end all. And I certainly don't want to say that, but it gives us a good sense of where we stand as independent ccNSO TLD operators. I think, quite frankly, given the price, given the context in a sense, it's a no-brainer for our community to participate. So, in a sense, just do it. If it doesn't provide value, well, then you can act accordingly later. And, again, I'm sure John would be happy to answer any detailed questions you have about that.

This has been touched on, but I think that there's a real opportunity to create some kind of DNS abuse group within the ccNSO community. And I know this has been touched on before and there are other groups in other parts of the ICANN world that deal with this. I think that, given the nature of our community, we need something that's right-sized for us. I hesitate to even use the term "working group," as many in my community, in our community, will see this as, "Oh no. Not another working group. Not another volunteer request. Not more bureaucracy.

We already have enough of these." I see it more being potentially modeled on the way that TLD-OPS works. And, again, this was mentioned previously. But that has been a highly successful endeavor for this community—highly valuable, highly successful. And, again, it started out with some trepidation but has become, I would say, one of the key features and one of the key benefits of our community.

And, fundamentally, it's a very robust and up to date contact list of the right people in each of our ccNSO member registries—the ones who potentially could actually be dealing with DNS abuse. So like the TLD-OPS, it's a very specific list. I think there's an opportunity potentially for us to do the same kind of things for DNS abuse. And we allow our membership to be able to connect and reach out individually to the right people in each of our peer member registries.

As I said before, Tech Day has sponsored work around this subject, DNS abuse mitigation, and I would certainly hope it's going to continue to do so. And some entity within our community that is DNS-abuse-focused could even help the tech group folks with those programs and help organize, potentially, and take some of the weight off of the considerable weight that's on the Tech Day community. So I don't know since I'm not that right person in my organization, but I know who that is and I'm sure that community could figure out the right weight and measure of what this group could look like.

Now, lastly, I'm going to throw something out there that we haven't really talked about and that hasn't been raised, and that's the notion of

establishing a voluntary code of conduct for ccNSO members in terms of dealing with DNS abuse.

Now, before anybody gets too up in arms about that, there are three words there: “voluntary,” “code,” and “of conduct.” And of course, it would have to be voluntary, given the nature of our community. And I see it, quite frankly, as being a best-practices list issue. And joining DAAR could be one of those elements. But what is actually in that code would be something for the ccNSO to decide over time. And some may respond negatively to that because the ccNSO shouldn’t necessarily be doing anything prescriptive, and that’s not what I’m suggesting. But I think we should discuss it for the benefit of our community. And, of course, participation would be completely voluntary.

But many of us lead our organizations and are responsible and accountable for the performance of our organization, including DNS abuse. And I think one of the things that we want to do is benchmark so we know where we stand. Are we keeping up with the community? Are we doing what we need to protect our corner of the Internet?

So that’s my notion here: establish a voluntary code of conduct, where benchmarking could be a key part of that. When we saw gaps as individual operators and managers, we can act on that and we can work even within our own community for assistance and consultation. And I think that’s one of the great things about this collaborative community: I know that my peers around the other members of the ccNSO would absolutely be willing to do that.

So I would encourage us to have that discussion. I'd be interested in hearing what you think about this idea. And thanks for listening. Back over to you, Alejandra.

ALEJANDRA REYNOSO: Thank you very much, Byron. And now I will give the microphone to Nick for a moderated Q&A.

NICK WENBAN-SMITH: Thanks very much, Alejandra. And thank you very much to all of the presenters. I think the six of you showed a lot of thought and consideration and insight and shared a lot of good practices and experiences. So I think, for those who participate a lot in the ccNSO, this is like another normal session of the ccNSO where we talk about experiences, best practices, and good things to do and things to avoid.

I've put a question in the chat. If anybody wants to raise their hand—I see Regis is first in the queue—while other people are thinking … And if there are questions that didn't get asked, then we can deal with that.

I just wanted to talk very briefly because I've seen a lot of conversation in the chat around access to data, GDPR, and those sorts of questions. And obviously, if we wanted to solve all of the wrinkles in frameworks caused by GDPR, we'd need a different session.

But I suppose I'm just interested, Gabe. You said that access to data was one of the things that we could really do to help mitigate abuse, and I

think we'll have a huge amount of respect for folk who work on the front line to prevent criminality and to help us.

And I guess my question was, in terms of the ccNSO, what do you think we should be doing in terms of data access, given that we don't mandate policy? Is there specifically an issue with specifically ccTLDs getting access to registrant data? Because my understanding is that the ccTLDs are incredibly flexible because of the nature of their jurisdiction in their own countries. There's usually a very strong cooperation with local law enforcement. And I've heard no complaints about that, certainly from my perspective domestically nor from colleagues. So if there's a problem there, then I didn't know about it to date. And if you can elaborate on that, that'd be really helpful. Thanks.

GABRIEL ANDREWS: So let me clarify that. There isn't a systemic problem. It's rather that I just wanted to stress, I guess, for the greater community the importance of this type of data for investigations, where they touch on some of these bigger issues of criminality, whether it's the BEC scheme, whether it's ransomware, whether it's entirely unrelated types of crime that nonetheless touch upon DNS.

And full disclosure. Most cops have very little understanding as they approach this of even the difference between a registrar and a registry, much less who owns what ccTLD, or administers it on the back end as sometimes a ccTLD might be indicative of a certain country but actually is operated by folks in a different country entirely.

All this is to say is, when we engage folks in that space, the responses can be ad hoc or just—perhaps that's not the ideal way to describe it—inconsistently applied, depending on whether it's a local law enforcement agency contacting a local ccTLD operator or folks that are making requests across border, which is probably more frequently going to be the case.

And so to the extent that each member within the ccNSO—not the … Apologies, but I am speaking more in general to the community of operators than the ccNSO itself. I just want to make it clear that, to the extent that an individual ccTLD operator within your own jurisdiction and legal framework specific for your own nation is able to respect the request of folks that you understand are law enforcement officers in, perhaps, a neighboring nation, the speed with which the request can be answered sometimes can have very big impacts on perhaps subjects but perhaps victims that are within your ccTLD as well.

And so if you have, just as an example, a United States law enforcement agency reaching out because we see a potential ransomware infection on a registrant within your ccTLD, it can make a very big deal whether that is something that can be handled as an expedited matter directly or if there is blanket rule or prohibition against responding to folks outside of your jurisdiction.

And I just bring these specific use cases as examples because I feel it's better to think about them in advance before they happen. And so that's really the thrust of where I'm coming from in bringing these

examples. It's not because I've identified any systemic issues across the board but rather because we have so many unique situations in ad hoc circumstances, usually on a Friday afternoon after most people are already going to bed or our European colleagues already have. And so often it's just a matter of whether folks are willing to engage directly or whether there is, as I say, already a rule of "Oh, well, these requests must come from our local law enforcement," in which case—full disclosure—that typically means for us employment of what's called MLAT (Mutual Legal Assistance Treaty), which is, in my experience, done over a period of three to nine months, on average, and is just not serviceable as a tool for these use cases—

NICK WENBAN-SMITH: Okay. I just wanted to understand the point.

GABRIEL ANDREWS: I believe you're muted, Nick.

NICK WENBAN-SMITH: Sorry. I muted myself before I introduced the top of the queue. I've got Regis Masse from .fr and then, after him, Anil.

REGIS MASSE: As the Co-Chair of TLD-OPS, I'm very proud that some presenters this evening spoke about TLD-OPS during this session. And thanks, all, for all the presentations. It was very interesting.

I will be very quick, but I just want everyone to remember in all the communities what is the goal of TLD-OPS and how it works. At the beginning, it was mailing list [inaudible] CTOs in the ccNSO community. And the goal is to share security information about DDoS attacks, [inaudible] about the operating systems of software. And after that, we started to write two white papers and even played games when we met in a face-to-face meeting during ICANN. But it's always about security.

And we have to remember that we have more than 200 ccNSO members in the mailing list, but as Kristof says, less than 20 are very active on the list. It's not a problem, but if we want to share, if we want to raise an issue and work together on security, we have to have more than 20 people who are addressing this kind of problem.

And we didn't speak with Byron before this session, but with Jacques Latour, the Chair of the TLD-OPS Group, we don't think [TLD-OPS] is something we will address in TLD-OPS Group, first of all, because it's not in the charter for the moment and it's not the case we are addressing. In the first presentation, we talked about DNS abuse as policy issues or things to work on. And in a certain way, we already work on DNS abuse in a technical way because we are working on vulnerabilities. But what is about policies especially? We don't address that in our group. And for the moment, we are going further in the group on security. We have defined a security committee to go and seek out the security events to share and share things about security.

So I think I would be [be pleased] to be the first to say that, but Byron said it in his slides. I think having a new group based on the TLD-OPS motto would be a good thing. And finding in all the ccTLDs all the right people to work on this topic I think is a good way. We will pleased in the TLD-OPS group and Steering Committee to help the new group to give our experience of what we did and how we work and we can work with the communities on that.

But thank you, Nick, for giving me the opportunities to place in the conversation the role of the TLD-OPS and how we work. Thanks a lot.

NICK WENBAN-SMITH: No, no. Thanks, Regis. I know from my own security people how valuable they find that group in terms of best practice sharing specifically around security in the ccTLDs. So the idea that you could do something similar around DNS abuse specifically, copying the template already used quite successfully, is kind of interesting idea, right? Thanks very much.

Okay. Next up in the queue I've got Anil. Anil, the floor is yours.

ANIL JAIN: Thank you, Nick. Two comments. One, we are ccTLD managers. We were discussing the information sharing between the registrars and ccTLD manages. We are able to get WHOIS details quite good, but accuracy of WHOIS data again is questionable. That is what we are discussing.

But the issue which we are not able to get quickly is the payment detail. Sometimes the LEAs want to trace the country back to understand, but this payment detail will help them a lot, which takes a lot of time. This is one.

Second, I personally feel that unconnected ccTLDs who are not yet connected with the ccNSO community should get connected because there is a lot abuse which is happening in those countries also, those ccTLDs. If we are able to get the information from them, I think we will be able to come quite close to the mitigation of ccTLDs' DNS abuse. Thank you.

NICK WENBAN-SMITH: Brilliant. Thanks very much. And look at that. I don't think there's any more questions in the queue. Hopefully we've answered some of the questions in the chat. If not, I'm sure the session can continue in 30 minutes.

I'll hand it back over to Alejandra with time to wrap up the session. Thanks very much, everybody. Thanks very much for all the questions in the very active chat. It's been very useful for those of us who have to take it away.

ALEJANDRA REYNOSO: Thank you very much, Nick, and thank you very much for all our panelists, and especially for those who have a very tough time joining us today. As Nick said, we will reconvene here in 30 minutes. The Zoom

room will remain open for those who want to stay. Of course, we will stop the recording when we are on break.

And in the next part, we will continue our discussion and see the recommendations that have been proposed and see what the community thinks about them.

Thank you all very much. And this first part is adjourned. Thank you.

[END OF TRANSCRIPTION]