ICANN74 | Policy Forum – ccNSO: ccTLD Role in DNS Abuse Policies
Thursday, June 16, 2022 – 10:30 to 12:00 AMS

CLAUDIA RUIZ: Hello and welcome to the ccNSO: ccTLD Role in DNS Abuse Policies session. My name is Claudia Ruiz and I along with Bart Boswinkel 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 be read aloud if put in the proper form as noted in the chat.

If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will unmute in Zoom. Onsite participants will use a physical microphone to speak and should leave their Zoom microphones disconnected. Those not seated at a microphone may use the aisle microphone to speak.

For the benefit of other participants, please state your name for the record and speak at a reasonable pace. You may access all available features for this session in the Zoom toolbar.

Thank you all very much. I will now hand the floor over to Alejandra Reynoso. Thank you.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

ALEJANDRA REYNOSO: Thank you very much, Claudia. And welcome, everyone, to our ccNSO and DNS abuse session. Today we are going to have a little bit of a world tour regarding what ccTLDs are doing to mitigate DNS abuse. What are their priorities? And if we can go to the next slide, please. Here.

So this is an overview we are going to have today. We will have presenters from the African region, Asia-Pacific, Europe, Latin America and the Caribbean, and North America. We will also have two moderators. We will have Nick Wenban-Smith and we will have Tatiana Tropina who will lead the conversation regarding the questions and discussions that may arise from these presentations.

We will have each presenter show you what they are doing in their own ccTLD. And afterwards, there will be some time for questions for clarification regarding their presentation. And after all the presenters have done their presentation, we will have a general discussion.

With this, I would like to go to our first presenter which is Angela Matlapeng from .bw. Angela, the floor is yours.

ANGELA MATLAPENG: Thank you, Alejandra. And a very good morning to everyone who is joining in onsite as well as online. It's always a pleasure to share experiences as well as knowledge from the different communities here. My name is Angela, and I am the technical administration for the .bw ccTLD based in the cybersecurity unit and actively dealing with DNS abuse as well as other cyber related issues. I am also the vice president of AfTLD and the liaison person of the AfTLD to the Africa [inaudible] working group.

I will just share what we do in terms of DNS abuse, and my presentation will follow the agenda that you see on the screen. We will focus on a distinguishment between abuse of the DNS and abuse via the DNS itself. And we will also look at the types of DNS abuse that we record at the .bw ccTLD. And then we will conclude on prevention and mitigation tools and procedures that we have in place.

So why are we interested in DNS abuse? This is because as part of our value proposition we sell safety and stability as well as the security of the DNS, right? So in everything else that we package in our marketing message we let our consumers or registrars know that the domains that they are purchasing are indeed safe, stable, and secure as we invest in tools and procedures around that aspect.

Now from the .bw perspective we like to think of abuse of the infrastructure itself which could be malicious activities that intend to disrupt or even cripple the infrastructure. Or we can look at it from a perspective of abuse via the DNS infrastructure where you've got the DNS resolving and serving names as it should, but this is operated in an unintended manner. So for this presentation we're going to focus on the latter where the domain name itself is harmful.

What type of abuse do we record from the .bw ccTLD? To your left of my table would be abuse of the DNS. And this is where you typically find your DDoS, spoofing of the DNS, and poisoning, hijacks, man in the middle. The list goes on and on. And I would say from the useful tips or actions that I'd share, the main one would be to have a business continuity and disaster recovery playbook in place just to prepare in case you might experience something of that nature as well as perform cyber drills or incident drills pertaining to abuse.

But when it comes to abuse via the DNS itself, this is where you find your botnets and command and control, malware distribution via the domain itself, phishing and scamming which is focused on email domains, typo-squatting and homoglyphs, as well as defacements and web shells.

The picture that you see down below is a screenshot taken from one of the domains that we had, if I may put it that way. And this content was inserted in the website itself. So maybe you might wonder why I'm talking about defacements because it's content related. So I will go to the mitigations and we'll get to understand why this is also classified as abuse.

So, yes, prevention and mitigation. First of all, we've got policies in place to try to prevent DNS abuse at registration, to try to prevent DNS to the infrastructure itself. Things like deception, data theft, hacking and cracking and the like. So we've got your registrar accreditation agreement, acceptable use policies which is the main policy which speaks to a lot of abuse including content and IP related abuse.

We've also got your agreement which is just mainly focusing on accuracy of the registration data itself and gives us authority to take down domains that are malicious or with information that is not valid or accurate. It also gives us the right to conduct random compliance checks to see whether domains that are registered are using the correct information.

So the main reason that we look at IP and content related abuse is because the overarching mandate of our [CRA] communications regulatory authority act is consumer protection. So in every policy that speaks to DNS abuse the main umbrella here is consumer protection, and that's why we look at infringement to IP as well as content.

So some of the tools that we use for domain would be your typical Netcraft which is a commercial tool. We also have open source [intelligence] tools. They are listed there for further reference beyond this presentation.

But I'd like to highlight that we have visibility into the Deep and Dark Web where we get insights in [inaudible] domain name mentions such as when there's ransomware attacks. We also view credential leakages, BIN numbers associated with credit cards, and stuff like that. So we also use Netcraft for takedowns and active monitoring. Even after the domain is repaired then we still get to monitor that it won't behave the same way and the like.

In summary of the steps that we take [inaudible] say that we would prevent domain abuse and we should use tools to identify and notify the relevant parties using the information that I spoke about, registration information. And then we remediate and mitigate. This is because the .bw ccTLD is housed under the same roof with the cybersecurity unit where I'm attached.

And remediation is one of the big steps where we get to help security teams or administrators of different DNS infrastructure to look at steps into how to mitigate stuff like phishing in case maybe your website has inappropriate misconfigured headers, things like that. We give you a step-by-step of what to do with it.

And then most important part is to learn from the experience. To say, how is this attack coming up? Is it changing? And now to crown everything we exercise capacity building as well as carry out awareness. We realize that although it's a well-known saying to say that people are the weakest link in security, but we realize that people are actually the solution to security.

When everything is put in place in terms of security in systems and machines, we still get stuff being delivered through social engineering and other tactics that tend to trick the human being. So we focus that we participate in October cybersecurity month of cyber awareness as well as the stop, think, connect campaign which is just aimed at safety online and awareness.

So this is in a nutshell what we do at .bw, really focusing on the human aspect which is the advice I'd like to give other ccTLDs to say that it just doesn't end on that note of protecting the systems themselves. You should include the humans because they're really the solution.

I will take questions and comments as well as in the chat. Thank you.

NICK WENBAN-SMITH: Brilliant. Thank you very much, Angela. That was a very clear and thorough, comprehensive presentation. So the structure of this session is we will have five presenters. So the main Q&A will be a discussion after all of them have spoken. But if there are any clarification questions from anybody whether in the room or in the chat, then you can raise your hand or come up to the speaker asking any clarification questions. I've got one from Olusegun. Happy to unmute yourself and ask your question, please.

OLUSEGUN AKINWUNMI: Okay, good day, everyone. My name is Olusegun. I would like to thank Angela for the presentation and ask three questions. Number one, you talk about policy. I want to ask what are the measures that you take if the policy that you guys have in place has been breached either by a registrar or a registrant. That's one.

Number two, you listed a lot of things that you guys use for cybersecurity to mitigate or to monitor what is going on. I want to ask how often do you normally experience DNS abuse?

And from the experience of the ones that you have had in times past as the vice president of the AfTLD have you ever attempted to notify the community? Thank you.

ANGELA MATLAPENG: Thank you for the questions. Yes, so the first one is what happens if policy is not fulfilled. As the regulator, we have the compliance and legal department which would take care of that. But first of all, yes, you try to resolve that from a nonformal perspective. Try to figure out why whatever stuff that's happened did happen. Was it out of ignorance or was it out of lack of knowledge? So always try to come from that perspective to say, "Listen, this is what you've done. We are giving you a period of maybe one week to change your information if it's not proper."

If it goes to a point where there's infringement and we can't handle it from an informal manner, then we'd have to take it to legal and compliance and the whole procedure would be followed from that department.

The second one was how often we experience abuse. On a daily basis, I'd say we receive thousands of notifications, especially around botnets and phishing. So that's the whole reason why we had to focus our awareness on educating people because we are receiving thousands of those [inaudible]. But when you trace it, you'll see that it's from human behavior. You know, people are clicking links they're not supposed to click. Downloading stuff from unsolicited websites and the like.

The third one, yes, I'm aware of the DAAR or a project by ICANN. And as the AfTLD, we promote that. We work with African ICANN to have those webinars around that. We've also worked with TLD-OPS to have a webinar around your business continuity and things like that. And we also work with Africa [inaudible] when it comes to DNS abuse as well as capacity building around that. So, yes, the community has been engaged, and we plan to do more work with AFRALO as well. Thank you.

NICK WENBAN-SMITH: Brilliant. Thanks very much. That's good to answer all three questions in one go. That was impressive. There's a question in the chat from Javier, fellow ccNSO Council member: "Angela, you mentioned CRA in your presentation. Is that a local legal mandate in your country?"

ANGELA MATLAPENG: Yes. So this is the communications regulatory authority at which is an act that gives the communications regulatory authority powers to take down domains, do anything related to Internet and ICT governance as well as other areas. So, yes, this is a local mandate. And like I did say, it cascades down to everything that's housed under [inaudible].

NICK WENBAN-SMITH: Brilliant. Yeah, I think you find this a lot in ccTLDs. There are lots of local jurisdictional mandates and statues. There are two more questions and then I think we'll move on to the next presentation. It's great to see a lot of African engagement here. So Lerato from ZADNA, can you unmute yourself and ask your question, please? Can you hear me, Lerato?

UNIDENTIFIED FEMALE: Coming to the mic.

LERATO SEEMA: Okay, thank you. I'm Lerato. I'm from the .za domain name authority in South Africa. This is quite interesting from a regional perspective, but I think my questions are around the issue of the policy framework in Botswana. With the bulk of the reactive reactions we get from the reports I'd like to know the effectiveness of the policy framework that is administered at registration level. And secondly, how does .bw ensure the credibility of the information provided and the mechanisms for updating such? Lastly is the issue of the transparent reports emanating from [inaudible] present in .bw but also serving a foreign market. Thank you.

NICK WENBAN-SMITH: I think that was…we haven't got that much time for questions, but I can see maybe this is going to be a more general point for the full discussion. But I think many countries get the feeds and reports. I know that the quality and the volume of those makes it difficult in terms of actionable. But the questions about transparency and credibility I think are going to be a common theme. Do you want to just quickly address them? Do you report? How many things do you do in terms of transparency? And you must presumably check the information you receive from your intelligence feeds.

ANGELA MATLAPENG: Thank you for that question. I think I would say generally a lot of ccTLDs struggle with accuracy of data. And now that we've recently had our data protection act come into place and one of its requirements is accuracy, I foresee that we're going to do more work in having that information accurate. But as I had mentioned in the presentation, we do have regular checks, very random, and would select some of the domains and check if they are up to date.

But I forgot to mention that we operate on a 3R model where we are the registry, we've got registrars we accredit, and the registrars take care of the registrants. So anything we take down or we think is not in the proper manner would go through the communication of the registrars.

So they have more answering to what's [inaudible] as the regulator to say, why is this information not accurate? How are you collecting the information? But the policies themselves will stipulate what makes [inaudible] registration information and say that it needs to be updated. So, yeah, we try in that regard.

NICK WENBAN-SMITH: Okay, just one further question and then we need to move on. So from .mw, Malawi, how do you work with your local CIRT? I understood that you're part of that cybersecurity. That's right, correct?

ANGELA MATLAPENG: Yes. So luckily we've got the ccTLD and the [CIRT] and the regulators. So we don't even have to be writing letters or anything. It's just a matter of just emails or [walking to the unit]. So what we do is everything relating to the security and stability of the DNS is monitored under the [CIRT] unit. And so advisories are given through CIRT unit to the ccTLD. The ccTLD's main focus would be on policies as well as administration and takedowns. Anything that has to do with zone data and anything like that is left to the ccTLD. So mainly the CIRT unit is for monitoring and advisories.

NICK WENBAN-SMITH: Okay, thank you. I'm sure there will be lots of questions at the end, and there are more opportunities there. So we need to move on to the next presentation. This is Ben Lee from .hk. If you're ready, then off we go.

BEN LEE: Yes, let me set up the screen. Is the screen working?

JOKE BRAEKEN: Hi, Ben. If you could put it in the full screen, that would be great.

BEN LEE: Okay, thank you. Thank you, ICANN. And thank you ccNSO for having me here.

JOKE BRAEKEN: Ben, apologies for the interruption. This is Joke. Could you please put your slide deck in full screen mode.

BEN LEE: Yeah. It’s not yet?

JOKE BRAEKEN: Not yet.

BEN LEE: Let me try this. How about this?

JOKE BRAEKEN: Thank you. That looks good.

BEN LEE: Thank you. Thank you for having me here. I am Ben Lee from .hk. We are the registry from Hong Kong administering the .hk top-level domain name. I’m the head of IT of .hk [inaudible]. And I also have the [inaudible] officers role of this company. We share the same objectives with I think most of the TLDs that the domain name registry is one of the important or critical infrastructure of the Internet, and we play an important role to help make the Internet safer by handling the DNS abuse situation. So my presentation will be in four parts, and without further ado I will go through one-by-one.

First of all is this overview about how we handle the case. The first thing is about the preventive measures or preventive setup. It’s about our policy, how we prepare it and how we require the registrant to provide documentation to prove their identity before passing their registration.

The second part is about our detection way. We have two parts. First is how we proactively check the domain names, and the second is how we collaborate with the local authorities or regulators.

And the third part is in the case that there is confirmable or verified case, what procedure we will take to take down the domain name.

So first thing first, this is about our registration policy. On the screen you have extracted how we put up our policy. So in short, it gives us the right to handle the domain name registration or take down or suspend an active domain name. We also give the rights to registrants as well. So in case that they have enough information or proof, then they can take action even faster before Commission with us.

The main point is that the registrant should have to agree and accept our acceptable use policy. And of course, they have to be legal and work according to the Hong Kong law. So anything related to that is breached, then we will have the rights to take down the domain name.

The next point is about the registration. During any new registration they will have to provide documentation proof of their identities. We have different types and different categories of domain names. They are targeting different applicants and different eligibility. And no matter which they are they will have to provide the respective documentation.

For instance, for the company/commercial they will use the .com.hk domain names. And they will have to present a copy of their business registration that is issued by Hong Kong company registry.

Okay, the third part is about our detection and what we do due to our proactive checking against the registered active domain names. First off, that is about the checking. There are online tools to check the domain name, any reputational problems or issues. That is such as phishing or malware hosted by a certain domain name. We will use that to check on our active registrations, and we will take out some suspicious cases and we will take follow-up actions.

Another thing is about the documentation. Some domain names may have been used for quite some time and the initial documentation provided may have already expired. So we will recheck those. We'll have to ask them to resubmit their active documentation and to refresh their identity information.

The second part is about the collaboration. We work with our local authorities to obtain security information. For example, we work closely with police force. So they will communicate with us if any domain names are related to any law enforcement case and we may be asked to take action.

And the second is our custom and excise of our government. They will handle any case related to intellectual property infringement or counterfeit website or counterfeit point of sale or website.

And the third one is we work with local community emergency response teams, the CERT teams. They will have their intelligence with other international CERT teams and related to malicious websites or malware or phishing that might be using .hk for that [inaudible].

With this effort we can keep our cases limited. Recently we only had less than 10 cases per year.

And the final part is about how we handle a case. Since they different case by case and different source of information, we will take a verification step by ourselves to make sure that the information is complete and is trustworthy before persisting.

All the domains are registered with registrars. So in the third step we will communicate with the registrar to understand the registrant and contact the registrant. This is important because it is very common that the domain name holder may not be the one, the bad guy [inaudible] bad guy. He may be only the victim. For example, the website may be hijacked or hacked by other hackers and used that website to do illegal things. The domain name holder may not know.

So in this stage we will through the registrar communicate with the registrant to make sure that they know what is happening and they may have a chance to communicate and fix the problem before the domain name is taken down.

In case there's no response from the registrant, we will proceed and we will take down the domain name. And we will remain active and hear any objections from the domain name holders in case they have other reasons and they take their action late and did not respond quickly.

So case by case the steps it takes maybe takes different times, but on average we would expect that this will take one week to handle completely a case.

Thank you. I hope this is an overview of how we handle DNS abuse in Hong Kong. Thank you.

TATIANA TROPINA: Thank you very much, Ben, for such a comprehensive and detailed and great presentation. So I would encourage anybody who is in the room and has questions just come to the microphone. We have a few minutes for clarifying questions if you have them to Ben. Or we can discuss in general later. I do not see any hands in the Zoom room. I see no queue to the microphone yet. Well, I will give it a few seconds in case you are still straightening your mind.

But I would say that to me as a moderator being here it's already interesting to see how already after two of these presentations we see that the ccTLD managers are part of a bigger picture or bigger community like CERTS, like police, like other authorities, and also like Angela mentioned users which are fighting DNS abuse and tackling this problem.

I see the question in the chat from Javier: "Then is HKIRC your local authority?"

BEN LEE: Yes. Actually, I am from HKIRC, and we are the registry for the .hk. And we have the endorsement from the Hong Kong government to take the role of the administration of the .hk. So as the registry we will be the policy setters, and so registrars will follow how they handle our .hk registrations.

TATIANA TROPINA: Thank you very much, Ben. More questions? You have three seconds to raise your hand or walk to the microphone. If not, we're moving from Asia region…oh, sorry. We're not moving from Asia region to Europe yet. Gopal, please go ahead. You can unmute yourself and ask your question.

GOPAL TADEPALLI: Thank you very much. What is the impact disproportionate verification obligations on the people who seek the domain names and the registrars across the globe on DNS abuse? CcTLD, the verification obligations are very, very varied across the globe.

TATIANA TROPINA: Well, I believe this is an interesting question. Ben, I don't know if you want to address it from your perspective. Perhaps this is something for us to discuss in more general discussion. But, Ben, go ahead if you want to answer it from your region perspective.

BEN LEE: Thank you for the question. From our end, I think it is, for instance, I think we have quite some…from the early days we already required the documentation requirements. And that has set up for how we verify the identity of the registrant. And we think this is an effective preventive measure because I don't think it is easy to obtain a false or fake documentation and to do the registrations. And this also has traceability so in case a domain name has any related issues, we can always trace back to the identity.

TATIANA TROPINA: Thank you very much, Ben. Thank you. So I see that this is also a part of prevention process in this regard and mitigation process. Any more questions? I'm seeing none, so we are moving to the European region. And I would like to give to Masa Drofenik to showcase us what is happening with the DNS abuse and how register.si from Slovenia is dealing with this issue. Masa, the floor is yours.

MASA DROFENIK: Thank you, Tatiana. Hello, everyone. Good day. My name is Masa Drofenik. And today I am representing register.si from Slovenia, a European ccTLD. During this short presentation I will try to explain why and how we are dealing with DNS abuse within our registry and what we can do or what we cannot do regarding the topic. Next slide, please.

Here is just a short introduction. Our registry operates within public institution and as part of the public institution or public benefit is really essential to us. We see keeping abuse low on the Internet as an important element to safeguarding end user trust and safety within our zone. We aim to provide a stable, secure, reliable DNS. This is our mission which hasn't changed over the years.

As may be deduced from the registration numbers, we are not a large registry. But of course, we are not immune to DNS abuse.

We have suspended 223 domains since 2020 and all of them due to inaccurate registration data. Next slide, please.

Here you can see a title of one of our articles published on our webpage which can give you a hint what we are trying to do when dealing with DNS abuse. We try to prevent everything. Prevention is better than mitigation. And secondly, we always, always keep in mind that according to our national legislation monitoring and assessing the legality of online content is not our responsibility. And we try to be concerned about these two factors. In this article we introduce some of our internal procedures and measures taken regarding DNS abuse. Next slide, please.

How are we preventing DNS abuse under .si? Here are top five measures. I would say not all of them but top five. First one is keeping accurate registration data. We put a lot of time and effort to maintain our database. Being a smaller registry, it is possible for us to do manual checks, to do manual verification of randomly selected domain names or newly registered domain names.

But apart from that, we also do machine-based verification by keywords. For instance, domain names that were related to the words COVID or mask, this was the topic from the past two years.

Then sometimes the registry is informed about a domain name that is being used for malicious or illegal activity. Again, we try to be proactive. We are not the one who will decide if this is true or not, but we will contact the registrant to verify the data because as Ben already explained sometimes they domain name holder doesn't even know that his domain name is being used for malicious activity. Or we contact the competent authority.

We also have a very close cooperation with our national CERT which is a part of the same public institution as we are. We also have very close cooperation with our registrars. This cooperation goes really smooth for us, and I think this is important because we waste no time in cases like phishing or malware or even fake web shops.

Throughout the practice of dealing with DNS abuse we have also learned that raising awareness and establishing good relations with lawmakers and national authorities [the less] [inaudible] especially from consumer protection authority Market Inspectorate in Slovenia. We learned that it is important that they understand what a registry does. We try to explain to them how can we help them in cases of illegal content. But we are also make it very clear that we are not the one who can remove the content from the Internet.

And also, we use our communication channels like Twitter and Facebook to warn end users. To warn them against illegal activity. Again, this is an action taken together with national CERT and their program of safety on the Internet.

And that's it. These are the measures that work for our registry. I think that European ccTLDs are very different. Maybe something that works for us wouldn't work for another registry. What we have in common is that we have always been aware of our responsibilities and taken care of a stable, secure, and safe DNS. But we are all committed to different national framework, and this is why I think that others like ICANN for instance is not the one with the mandate to regulate ccTLDs. But because this is a matter of, like I said, national legislation.

And that's it for now from me. If there are some questions, I will be happy to take them.

NICK WENBAN-SMITH: Brilliant. Thank you so much, Masa. I didn't see any questions in the chat so far. If there are any questions in the room, please feel free to come up to the mic and introduce yourself. I can't see into the room 100% clearly, but if there's anyone there.

JAVIER RUA-JOVET: Yes. Thanks to all. Thank you, Masa. Question, Masa. You mentioned of course you don't have a mandate to deal with content. But is in your jurisdiction in your country, is there an authority that deals with content or that's completely banned, dealing with content regulation? Thank you.

MASA DROFENIK: Thank you for the question. No, there is no authority, but there are certain authorities for the certain specific parts. Like for instance, I mentioned consumer protection authority Market Inspectorate. They check whether this activity is legal or not. Whether the taxes are being paid or not and like this.

JAVIER RUA-JOVET: Thank you.

NICK WENBAN-SMITH: I think it's a really interesting area of discussion. And I think we've seen in contrast to the gTLDs where the gTLD policies explicitly exclude content, I think pretty much all the ccTLDs don't really draw that sort of artificial distinction in the sense that there are certain types of content which all ccTLDs would consider [inaudible] in their abuse prevention policies. I think this is an interesting one for maybe discussion at the end in the full plenary session.

There's a question here from [Anne and Rafik] in terms of the accuracy data. I was impressed actually that you only had 223 inaccurate records in your registry because that's a pretty good strike rate in terms of percentage inaccuracy. But he's asking about, how do you ensure that it's accurate? Particularly, obviously, there's the point of registration, but then there's postregistration transfers or changes made. Do you then redo the accuracy?

Then after that there's a question from Pablo.

MASA DROFENIK: Yeah, a lot of work also [do] our registrars. They know their customers, and they also check this data. And like I said, for us as a registry it's not that much of a problem to do it manually for now because there are not many registrations. So we can check newly registered domain names or randomly, but randomly picked up domains.

NICK WENBAN-SMITH: So there's a proportionality. You don't check everything? There's sort of a threshold.

MASA DROFENIK: Yeah.

NICK WENBAN-SMITH: I see. Perfect. Pablo, you're next.

PABLO RODRIGUEZ: Thank you very much, Nick. And thank you all for sharing this information with us. Masa, I have a quick question for you. Once you identify or you have been told that there is an incident of DNS abuse, how do you exchange information with the appropriate local authorities? Do you wait for them to reach out to you? Do you reach out to them? Do you have a pre-convened agreement with them? Can you expand on that please? Thank you.

MASA DROFENIK: No. Thank you for the question. We always try to be proactive with every measure. So we try to contact the proper, the competent authority. But in most cases this is our national CERT team which is, like I said, part of the same public institution. So this is not difficult to exchange information with them.

PABLO RODRIGUEZ: Thank you so much.

NICK WENBAN-SMITH: Fantastic. And then final question here from [Anna] and then we move on to the next presentation. [Anna]?

UNIDENTIFIED FEMALE: Yes. Hi. Masa, I want to ask you, if you received in registry the abusive message, do you explain them that you do nothing with content? Or you suggest or pass this abuse to appropriate [inaudible]?

MASA DROFENIK: Yes, thank you for the question. We do exactly this. We explain them that unfortunately we are not the ones that we can remove the webpage, for instance. But we tell them which authority would be appropriate that they go to, or even we contact the authority so the process is quicker. We do both.

UNIDENTIFIED FEMALE: And one short question about accurate registration data. In our registry, it's still manual registration so we have a chance to [inaudible] verify registration data. But can we ask, if something looks not complete, can we ask…we ask our registrant to give us more documents. We ask our registrars to give us more information about registrant. What about your registry? Thank you.

MASA DROFENIK: Thank you. No, we don't ask for any documents. We just ask them to verify the data. But mostly when we react when we suspend a domain name, these data are completely wrong, like obviously wrong. But in most cases what we've learned is that if we just ask them to verify the data, they don't verify it if it's not true. So then we give them a limited time like three to five days, it depends on the case. And if we don't get an answer, then we suspend the domain name.

UNIDENTIFIED FEMALE: And the last question, do you have rights to suspend domain names because of content? Or you can…?

MASA DROFENIK: No because of content, only because of the inaccurate data. This is according to our [inaudible].

UNIDENTIFIED FEMALE: Okay, thank you very much.

NICK WENBAN-SMITH: Super interesting. Super interesting. So let's move on to the next presentation. Now we have Jenifer Lopez from .pa, Panama. Jenifer, the floor is yours.

JENIFER LOPEZ: Thank you, Nick. And good morning, everyone. And thank you, ICANN, for having me here today. I'm going to present the .pa DNS abuse perspective. Next slide, please.

We use many tools to identify abuse or malicious resources. Like for example, suspicious contact data, phishing, or confusing us of a brand name, domain [hosted] and suspicious name server, suspicious or several hosting service changes, and [base site content] is nonexistent or suspicious or maybe bad.

So we detect DNS abuse by monitoring our DNS servers and applying security analytics to detect it and avoid it on time. We also audit our DNS zones that give us the insight we need to discover DNS related vulnerabilities. And that helps us to understand what needs to be addressed in that moment.

Also, in our policies we can suspend any domain temporarily or permanently if it has been registered for technical abuse of DNS or practices. And in that case, we have an email abuse@utp.ac.pa for reports. And in a case of evidence of DNS abuse, what we do is report to the contacts of the domain name and also to the hosting provider in case of violation of our terms and policies. And in case of incomplete or inaccurate data for the registration, we ask contacts for updates, relevant updates.

Back in 2019, we had a [DDoS] problem, a nonexistent domain name causing troubles. We were very lucky that the .cr technical team was there to support us and help us. And they collaborated to solve the problem with us quickly. We also had help from Carlos Alvarez, the SSR engagement from ICANN. What we did or our tech team did was commented on the [inaudible] policy so it did not request queries from other secondary servers when the domain did not exist on .pa. And it was QSnatch malware that infects QNAP [inaudible] devices, so that was the case in this time.

We also use dnstop on some DNS servers who see a lot of queries and in ns.pa in case of a massive queries event of the sink holing type. Next slide, please.

Since we have renovated our servers [inaudible] as a more dynamic version of security tools and also improvements on the [inaudible] at the time of [hardening] our security [rules] and [inaudible] [firewall]. And the configuration of other applications such as [inaudible] or security enhanced Linux and depending on the chosen operating system.

As far as our training teams, we also participate in illegal content forum, [inaudible] initiative aimed to strengthening knowledge and sharing and networking where the ccTLD managers, local authorities, and law enforcement are trained and collaborate to effectively address and respond to DNS abuse.

And also and finally, as part of our responsibility to end DNS abuse problems our next steps will be deploy DNSSEC to the .pa [inaudible]. And that will allow delegation to end users to increase the security level. And because we provide the DNS like comes from the correct source.

And also, we are going to implement our new web app that will be improved in security level also. And want to use this new web app, the client must log in with a unique user and password. We call that user a [co-manager].

So that's what we have to share with you. Thank you so much.

TATIANA TROPINA: Thank you very much, Jenifer. A fantastic presentation, very detailed. We already have comments and questions in the chat, so we have a bit of a queue forming here. So first of all a comment from Brett Carr, Nominet U.K., "Just a reminder all, the ccNSO TLD-OPS is a great option for tech collaboration. A lot of expertise across many ccTLDs which are happy to help." So a note to ccTLDs on this.

Then we have a question from [inaudible]: "Jenifer, how do you identify the confusing use of a brand name? Do you use any artificial intelligence based tools, software, or do you do it manually?"

JENIFER LOPEZ: Thank you for the question. Our system right now is [inaudible] automatically, so we have the help of humans. So they collaborate to the final [inaudible] of domains. So when we get a domain registration, we call first, see if the domain is correct, if the information is correct and [inaudible] have accuracy. So that's the way we are working in it right now.

TATIANA TROPINA: Thank you very much, Jenifer. Are there any more questions? Because I actually want to follow up a question from your presentation exactly about this. Because you mentioned suspicious contact details. Is it also checked by humans, or do you have any sort of tools to predict that contact details are suspicious?

JENIFER LOPEZ: We use [inaudible] based systems and also the human beings to fulfill that extra level. Because you know until human eyes you can [inaudible], so that's the way.

TATIANA TROPINA: Thank you very much. And my vision is not quite well but, Javier, is it you? Please go ahead.

JAVIER RUA-JOVET: Explain a little bit more or expand on LACTLD's project, what they do and how they help. And then if possible, a question to all participants, to all panelists. Do any of you somehow use ICANN's DAAR initiative or DAAR project, or is that being relevant? Is that being useful? The domain name, I think, abuse reporting project. So thank you.

JENIFER LOPEZ: Okay, the initiative of LACTLD is a very good initiative. I think all the LACTLD region are using it. And it is an annual forum, if I don't mistake. And it's a [meet with] law enforcement, local authorities, ccTLD managers are engaging to know how to deal with DNS abuse. So it's a good way to address that kind of problems.

TATIANA TROPINA: Thank you very much, Jenifier. And, Javier, if I may, let's ask questions about DAAR in more general discussion. I took a note. Any more questions here? Because I see that Angela was already replying on the chat, but let's really discuss it a bit later. Any more questions? I'm trying to see. In the Zoom room, I see no hands. I think I see nothing on the chat yet. So we are moving from Latin America up to the North America and almost finishing our around the globe trip in terms of looking at the ccTLDs. And our last presentation, last speaker is Crystal Peterson from .us. Crystal, the floor is yours.

CRYSTAL PETERSON: Thank you, Tatiana. Hello, everybody. My name is Crystal Peterson. I work with the .us registry operator. I handle operations and account management with them.

A little bit about the situation and where we sit with .us: .us is run by GoDaddy registry who has a unique position of being a ccTLD registry operator as well as a gTLD registry operator. So we do have the opportunity to see across a spectrum from our ccTLD portfolio and gTLDs, and we believe that that helps in a lot of the abuse mitigation that we have put together over the past few years.

One of the things from a .us perspective that we look at is the policies and procedures that we have in place. Along with a lot of the other ccTLDs that have shared here today, we do have an acceptable use policy that is put in place along with registration policies. The acceptable use policy does have certain prohibitions in it that are stated.

One being the sale and distribution of illegal pharmaceuticals. We also have the prohibition of spam noted directly in our acceptable use policy. In addition we do state that we have the implementation of abuse mitigation services for certain types of DNS abuse including phishing, botnets, malware, things of the like.

In addition, .us does have a nexus policy and a WHOIS accuracy policy that is employed and does allow for the review of domain names from that perspective as well. And our policies do then define the mitigation efforts that we will take which includes the review, potential suspension and/or deletion of domain names based on the policy and/or the abuse measure.

I wanted to share three separate types of abuse mitigation that we do employ within .us. The first is our registry threat mitigation service or RTMS for short. We use this across both .us, our ccTLDs and our gTLDs. And this is a service that does employ feeds and helps to monitor for the certain types of DNS abuse. For our gTLDs as a side note, this does help to meet the requirements of Specification 11 of the registry agreement. But for .us this is a powerful tool that we have developed in order to be able to monitor and investigate different types of DNS abuse.

We do have the feeds that come in and alerts that come through, and we are able to investigate and then able to communicate with our registrar partners and/or registrants in certain circumstances to be able to mitigate. The most that we do employ is through those communications. We look to have a relationship with our registrar partners in order to be able to as a community mitigate against abuse. However, we do have policies in place that do allow for us to take down domains if that is needed.

From a perspective of looking at certain threats, we took a view from January to May of 2021 and January to May of this year. From an actual alert perspective we had a 43% decrease in alerts, but we found that the percentages from there were rather stable. About 5% of the domains that are alerted to our registrars are cleaned and therefore left open. Ten percent are generally actioned by the registrar themselves and put on client hold. About 1% come back to the registry where nothing is done and we do need to put domains on server holds. And then the remainder of the alerts are generally cleared as either false positives. We do have some dead links in there, things of that nature.

In addition to our RTMS service we also have two trusted notifier relationships that I wanted to share today as well. The first is with the Internet Watch Foundation which does review for CSAM or child exploitation. And we have certain alerts that are received from the Internet Watch Foundation.

We also have a relationship and have developed a close relationship with the National Center for Missing and Exploited Children or NCMEC for short in the United States and look to take down any domains that are alerted from that relationship within a 72-hour timeframe. So we do have communications with our registrar partners for those certain URLs and/or domains. But if they do not come down, then the registry will take action and will take them down.

In addition to our relationship with IWF, one of the other trusted notifier relationships that I did want to share was with the U.S. Food and Drug Administration or the FDA. This relationship started with collaboration in a pilot program back in 2020 between the FDA, the NTIA in the United States, Verisign, ourselves, and PIR, the registry operator for .org.

And we put a pilot program together for six months where the FDA would notify registry operators of any illegal sale or distribution of pharmaceuticals and that then we would also give the same

72-hour window we have with the IWF. We would give that 72-hour window to registrars. FDA would also notify registrars as well. And if no action was taken, then according to our policies and the fact that this was for .us against U.S. law we would then be able to take action.

This was a pilot program that was a successful pilot program, and so we have continue that relationship voluntary and look to be able to also any complaints that come in be able to have a two-way relationship. So it's not just FDA notifying us but if we do have anything come in, we are able to send to the FDA as well.

I know I went very quickly through this. One of the things that I wanted to follow up and finalize with is just a kind of spectrum of where .us is, .us sits just under 2 million domain names under management at this time. We have about 225 registrar partners. In addition, we have a U.S. locality space that has another 440 delegated managers which is a different type of registrar. So abuse mitigation is something that we take very seriously to keep all of our registrants and end users safe online throughout their time on the Internet and definitely their time on .us domains. Thank you very much.

NICK WENBAN-SMITH: Brilliant. Thanks so much, Crystal. There's been [a bit] of questions in the chat around the difference between ccTLDs and gTLDs in terms of abuses and reporting. I guess, obviously, you operate both. Do you see much difference between your ccTLD and your gTLDs in terms of trends or anything? I guess the question is directed, right? This is a ccNSO presentation and obviously we want to say that it's not a competition but we're better than everybody else in our own different ways. Do you think there's a difference in what you see in the ccTLD? Obviously, .us has got a jurisdictional nexus to the U.S. so there are some differences in recognition policy too.

CRYSTAL PETERSON: Yes. Thanks, Nick. I think that's a very good question, and that is probably one of the biggest differences is within some of our policies. The fact that we do have a nexus policy for .us where our gTLDs do not. Most of our gTLDs do not. For example, .nyc does have its own nexus policy as well. But that's where I would see the difference. The types of alerts that come in, our RTMS service pulls in feeds and it pulls in for many different TLDs. The types of alerts that come in are the same for phishing, botnets, malware, all of that.

And how we deal with them is to each of our registry operator policies for [inaudible] registry, our policies don't exactly mirror each other but they do have a strong resemblance to each other from that perspective, .us having the nexus policy would be probably the biggest difference between our CC and our gTLDs. I hope that helped answer the question.

NICK WENBAN-SMITH: [I'm sorry.] The question is, is .us safer or better than the gTLDs you run because of the national nexus and policies and is it different between the other ccTLDs or is it impossible to tell? Is it not possible to make that general conclusion?

CRYSTAL PETERSON: Gotcha. I wouldn't want to make that conclusion. We like to believe all of our domain name spaces are safe to be on and good to be on and we want people in all of them. And so I wouldn't say that .us is safer than .biz or .co which we also help to manage as well. So I wouldn't necessarily put that correlation. There are differences in how we manage. But at the end of the day, we want all of our namespaces to be just as safe as any other.

NICK WENBAN-SMITH: Thanks. I see [inaudible] has put a comment about nexus doesn't really help if it's a compromised site in terms of abuse, and that affects quite a lot of them. So it's [a curious] position. I'm moderating but I can see one of my persons in the queue is my co-moderator, Tatiana. So, Tatiana, if you want to ask your question, please. And then, Pablo, get ready.

TATIANA TROPINA: Thank you very much, Nick. I put up my hand only because we have a question on site. Actually, we have two. So please go ahead.

MICHAEL PALAGE: Thank you, Crystal. Could you give us some statistics on the takedowns with the FDA. Because it was a three-month pilot but you continued it for I guess that last two years. Do you have any statistics?

CRYSTAL PETERSON: During the time of the pilot we actually did not have any alerts directly for .us. I can't give any statistics on either PIR or Verisign from that perspective. But we did have an open relationship so they were able to discuss with us. Since that time, I don't have direct numbers for how many alerts. I do know our alerts have been low from the FDA.

But we have in addition to receiving anything from the FDA, what this pilot and relationship has done is also opened up the fact that if we have complaints that come in, we can send their way. Not that we couldn't before—but we have a more open relationship that we can send their way.

So we have had certain complaints. I can't quantify exactly how many, but we have had certain complaints that we can send to them as well for investigation. And then ultimately if certain measures need to be taken, they can respond back.

MICHAEL PALAGE: So is it possible that those numbers could be made available perhaps in the future in consultation with the U.S. policy council?

CRYSTAL PETERSON: I will look into that. I don't want to promise some of those numbers to be able to shared publicly, especially because we're talking about several different parties here. But I will definitely look into that.

MICHAEL PALAGE: Thanks.

CRYSTAL PETERSON: Of course.

MICHAEL PALAGE: The only reason I used that is I was just looking at the recent exchange between the FDA and Göran. So to me I think this would be interesting to see the level of abuse and whether this voluntary trusted notifier program actually did help and make the namespace safer. Thank you.

CRYSTAL PETERSON: Yes, absolutely. Thank you.

NICK WENBAN-SMITH: Thanks. Pablo, did you have a question? Is it a more general question or is it specifically for .us? Because I think at one point we need to have a more general Q&A applicable across all of the five presentations.

PABLO RODRIGUEZ: Sure. So my question is regarding with .us. Crystal, thank you for the presentation. I would like to know if any ccTLD within the network in GoDaddy can participate in that FDA pilot program. Also, can all other gTLDs and ccTLDs who are not part of that network participate in such a program?

CRYSTAL PETERSON: Thank you, Pablo, for the question. This pilot program with the FDA was put together through the NTIA collaboration with the FDA and the like. So this was not led by us. We were part of that group. So from your question, can any ccTLD participate? That's not necessarily our decision to make. That would be something that you would want to work with most likely the FDA. And so I don't want to answer yay or nay for that.

PABLO RODRIGUEZ: Thank you so much.

CRYSTAL PETERSON: Sure.

NICK WENBAN-SMITH: Brilliant. Thank you. So there's a question in the chat here, and I think it's a question very briefly we would like all five of the presenters to answer if they can manage it. Which is around implementation of systems to prevent malicious registrations, i.e., analyzing the registration data at the point of registration to prevent the DNS abuse. I think Masa in her presentation spoke about preventing abuse being better than curative after the event action.

And I guess in terms of systems if you can get it right, it's a lot more cost effective, right? Because to investigate something after the event takes a lot of manual time as we've all heard, and that's an expense which then has to be shared across all of the registrations and user of the TLD. So questions in turn, and I think Angela first, around prevention of malicious registrations. Do you do anything on that front or do you plan to?

ANGELA MATLAPENG: Thank you for the question. I would say that from the .bw ccTLD we did try parking domains before registration, especially during the pandemic where we had insight into other domains that were likely to abuse the DNS.

But we had a discussion from the multistakeholder engagement, and there was concern from the public that this might be disadvantaging genuine registrations, especially concerning the need to have those domains up and running to share information critical to COVID-19 response. But with now the data protection act in place we might have to look into that because of the accuracy requirements. So we might have to do that.

But just to comment on it, it's quite a difficult thing to achieve, especially with your false positives and needing human intervention to go through the domains and figure out which ones are correct and which ones are malicious and stuff like that. But I believe from previous presentations during this meeting some ccTLDs did even mention the use of AI to help them with this feature. So it's not entirely unachievable.

NICK WENBAN-SMITH: Brilliant. Thank you. Ben, how about from .hk perspective?

BEN LEE: Thank you for the question. From our side I think we do not yet have an automated system because we also share the view that managing the false positive, that is not yet a mature or easy way to handle that. I think from the data point of view for the registrant information we will try to keep it up to date with the registrant. So in case something happens from one domain name that we may relate it to other domain names registered under the same registrant. So we can follow up the case [inaudible]. And I think that's one of the ideas.

And another one is about the technical information. That part is rather quite difficult. I think with the maturity of [the cloud] and the [cloud] servers and setup, the technical information such as the name servers or the IP address for that domain name become quite [available] and then it is not easy to correlate those information. It is easy to be changed by the [inaudible] [host] to another IP address or other name servers and it's rather difficult to analyze. So that part is another challenge that we have to keep [inaudible] and see what we can do.

NICK WENBAN-SMITH: Thank you. Masa?

MASA DROFENIK: Yes, I have to say I'm a lawyer so I don't have an IT knowledge. But, yes, prevention is of course better. It would be nice to have such a system, but for us as a smaller registry it's time…we have very limited resources. In person, in time, in money, everything. So for now we haven't introduced any such a system.

NICK WENBAN-SMITH: Thanks. And Jenifer.

JENIFER LOPEZ: Yes, Nick. Well, right now we don't have a planning to implement something like that. But with our new [web] system it could be quite difficult for them commit DNS abuse because they need to use the user and the password as I mentioned on my presentation. And also, with the measures we are taking right now, so maybe that's the way we are heading with that.

NICK WENBAN-SMITH: Thank you. Crystal?

CRYSTAL PETERSON: A lot of our efforts definitely are reactive. I think one of the discussion points in prevention or at the time of registration is, is a domain name abusive at registration? It technically has had nothing done to it, and so we don't want to penalize a domain name for having nothing done to it. Which means that it is more reactive in nature. Once abuse is detected, then how do we mitigate that? But if there is no abuse, should we be taking action against a domain name that has no abuse?

One of the areas of discussion that we have internally that we have been looking at too is certain bad actors. So is a bad actor who has done abuse in the past from a registrant perspective in their next domain name that they buy are they inherently a bad actor already before they've actually acted bad on a domain?

That is a discussion that I would love to hear comment on as well because that's something that we have been battling. Not battling but discussing internally too. But right now we are more reactive because unless a domain name has abuse on it, we don't take action against clean domains.

NICK WENBAN-SMITH: Thank you. Thanks, everybody, for those perspectives. I think it's an interesting area and it's something that we're going to probably carry forward as a point for discussion in further meetings. As you know, we've got a domain abuse standing committee now for the ccNSO, and I think there's a lot of interest in this area.

I mean, I think my personal perspective I'd say that there are some registrations that you just see and you just think, well, that looks so suspicious that there can't be a legitimate justification for it. And I think registries now have access to a lot of data. I think [Jack] makes a good point in the chat around if you're using certain personal data credentials probably ID theft or fake in one ccTLD, then that would be an alarm flag to investigate further across other ccTLDs. And there are ways that we can share our information better to be more effective at this. That would be an interesting point for further discussion.

There are a few more questions. Tatiana, is there a question in the room?

TATIANA TROPINA: Yes, there is a question in the room. I know that Javier was waiting as well. But was your question…yeah, okay. So there are two people in the room. I hope that you have more general questions. Please go ahead and ask them.

UNIDENTIFIED MALE: I guess you already provided an overview, but there's a lot of GDPR issues in sharing information. But if we start small and people opt in and we start sharing information like this, like on abusive email address, there's way to protect that we can collaborate together. And then we would be able to have some statistics, measure and progress on how we fight abuse. Like you said, there are patterns. We've seen a bunch of email addresses being used in multiple registries to do mass scale phishing and spam. And if we share…sometimes we share them and other CCs will say, yeah, we've seen them. But I think it's time that we actually start thinking of building something to enable us to start sharing information and measure and report and be more proactive in fighting abuse. So we're ready to do that now.

TATIANA TROPINA: Well, I did when I saw this on the chat, I was thinking the first about GDPR and data sharing. Perhaps this is…Nick, do we still…? Nick, Alejandra, do we still have time for one more intervention I guess, right? And then back to Alejandra. Yes, please?

NICK WENBAN-SMITH: One more, yes.

BRUCE TONKIN: Thank you. I just [inaudible] agree with the last intervention. I think that's a good idea to look at ways we can share information. Also a comment that I think listening to all these presentations it seems that there's a fairly common business process. There's probably slightly different parameters. Sometimes people are given 48 hours. Some have 72 hours. Some have a week. I think it would actually be interesting for the ccNSO to collect that in a structured way just so we have a bit of a perspective that here's the common business process. Here's some different time periods people are using. Here's some different providers people are using. So sharing information that way.

Just a question for the panelists, a bit more to do with, I guess, the proactive nature of looking for patterns of bad behavior. But we've seen quite a bit of people registering previously registered names because they've got traffic or some reputation associated with them. And then when those names expire they then use them to perform various forms of abuse. But I'm just interested whether others are proactively monitoring the drop lists if you have such things to look at activity in recently registered names or recently deleted names, I guess.

TATIANA TROPINA: Thank you very much, Bruce. I guess it's an excellent question. Do we have time to give answers? So, Alejandra, shall I just pass it on to you or what's our next…?

ALEJANDRA REYNOSO: Yeah, so we have time to….

TATIANA TROPINA: Quickly. So, yeah, Crystal, do you want to go first?

CRYSTAL PETERSON: So, Bruce, thank you for your question. In monitoring drop lists and looking at any patterns or picked up of abusive domains. Actually, from some of our observations we've seen certain activity the other way. Meaning we have had domains that have been abusive, have been flagged as spam in the past and have then been reregistered and the new registrant has been flagged or that domain has still been flagged and the new registrant is doing nothing of the sort and is wondering why their domain is having abuse….

BRUCE TONKIN: Yeah, because you can inherit good reputation and you can inherit bad reputation.

CRYSTAL PETERSON: Bad reputation, yes. So it is something that we have been looking at, but to be quite honest the complaints the we have received have been from the other where it's been inheriting the bad reputation.

BRUCE TONKIN: Interesting.

TATIANA TROPINA: Thank you very much, Crystal. Anybody else from panelists? Masa, would you like to address this as well? Or Angela? First Masa. Well, I see that we are running out of time. So if anybody from the panelists wants to answer the same question, please raise your hand and I will call on you. Otherwise, we can just safely wrap it up right now. Alejandra?

ALEJANDRA REYNOSO: [inaudible]

TATIANA TROPINA: Yeah, the question on DAAR as well. But I think that we are so severely running out of time. We have three more minutes. Anybody want to address question on DAAR?

CRYSTAL PETERSON: I can.

TATIANA TROPINA: Oh, yeah? Well, Crystal, the floor is yours.

CRYSTAL PETERSON: So there was a question on being involved in the DAAR project. From our perspective we do have the .co domain that is involved in the DAAR project as well as our gTLDs are already involved, .us is not. If you look on the list, you'll notice that .us is not. One of the things we have actually been speaking with ICANN regarding this project and looking at as ICANN itself moves into Phase 2.0 of its DAAR project we do want to develop a relationship there and look to get involved.

One of the places that we found we wanted to be able to study and/or help mitigate any of the numbers that were coming and all we saw were numbers. And so as the DAAR project progresses and develops we do want to have a relationship there, but we were cautious with putting all TLDs there while we were sitting as it came and developed.

TATIANA TROPINA: Thank you very much, Crystal. And just to wrap it up and bring it home and give it back to Alejandra, I indeed remember that when we were working on the DNS abuse roadmap the DAAR issue was interesting, was important but not every ccTLD was actually ready to be a part of it due to various differences.

Thank you very much to speakers for this fantastic session. Alejandra, back to you.

ALEJANDRA REYNOSO: Thank you. Thank you very much, everyone. This has been a very productive session. It will serve very useful input to the ccNSO in DNS abuse standing committee and has started its mandate recently. And with this, I want to also thank the working groups in the ccNSO who made this session possible. It was a joint collaboration between the MPC and the IGLC and those stand for their Members Program Committee and the Internet Governance Liaison Committee.

For which I would like to give a preview of what is going to happen in the ccNSO Council meeting later today is that we will have a new chair. Currently, it's [inaudible] our chair and we thank him very much for leading all these efforts in the IGLC and hopefully the council will appoint Annaliese Williams in .au.

So please to everyone attending the session we invite you to keep collaborating with us and sharing your experiences regarding DNS abuse topics and any other topics that are very useful for the ccTLDs to know about and to get inspiration from and to cooperate with each other.

With this, I thank you all. This session has ended. Thank you very much.

[END OF TRANSCRIPTION]