ICANN72 | Virtual Annual General Meeting – ccNSO: TLD Ops Standing Committee Session
Thursday, October 28, 2021 – 12:30 to 14:00 PDT

KIMBERLY CARLSON: Hi, everyone. Welcome to the ccNSO TLD Ops Public Session at ICANN72.

Please note that this session is being recorded and follows the ICANN Expected Standards of Behavior.

If you would like to ask a question during the session, you may write a message in chat or you may raise your hand and you will be called upon. Kindly unmute your microphone and take the floor. And with that, I'll turn the call back over to you, Jacques. Thanks.

JACQUES LATOUR: Thank you. Welcome to our first TLD Ops meeting in the last two years, I guess. I can't remember when and where our last meeting together was. But this time, we put in a request with ICANN to have a session dedicated for TLD Ops like we used to in the past, and then here we are.

So today we'll do a quick intro like we used to on what TLD Ops is. Now we'll talk about operational status issues. That should be short. I know we have an action point review discussion so we have an Excel spreadsheet that tracks all the action items for the committee members. The reason we're having this meeting is we're going to

establish a Security Committee, and Brett is going to do the introduction around that, and then we'll go from there.

So TLD Ops was put in six years ago, I think, by the ccNSO to create a repository of other security contacts within the ccTLD. That was the goal. So all ccTLDs, there was a requirement to connect people together and that's what TLD Ops is all about. So we have around 300 or 400 contacts in the contact repository from over 200 different ccTLDs.

The goal is for ccTLD is to work together when there is operational or security issues that impact the stability of ccTLDs. So in the past, we focused mostly on building the community and putting some best practice together. But today with Brett and the Security Committee, we're going to take it one step further and trying to have the mailing list more collaborative with security incident or security alerts or events or vulnerabilities that we need to address.

So the goal of TLD Ops—we need to repeat this—it's not to extend a ccTLD security team but it's there as a resource to help a security team address bigger issue. And then our goal—so the TLD Ops Standing Committee, you'll see on the last slide, all the members were there to put this mailing list together, this community together. We also have liaisons from SSAC, IANA, and ICANN security.

So the outcome of this is once every two weeks, we send an e-mail to all the members with the list of all the contact repository. So if you're a member of TLD Ops, you'll get an e-mail with 400 lines with everybody's name, phone number, their e-mail address at work, their

personal e-mail address. And the reason for personal is there's an issue with your TLD, most likely your work address won't work so we need the means of reaching out. And the mobile phone number is in case you get a text message from somebody, you can vet that it's coming from a person and TLD Ops.

So we have detailed procedures on how to join the TLD Ops. That's documented on the Community ICANN webpage. But in essence, the ccTLD tech or admin contact need to put a request with ICANN with the ccNSO secretariat to do any add or change to the contact repository. So that's the procedure.

So that's the main focus of TLD Ops is the contact repository. But over the last couple of years, we did two workshops. One is on the DDoS Mitigation Playbook. And that's published in our wiki pages. We spend a whole lot of time and effort to put a Mitigation Playbook together. I think our biggest success was putting the DR BCP Playbook together. And we did a workshop in Montreal where we did a tabletop simulation using this documentation, and it turned out to be a successful event.

Régis will talk about AfTLD. I thought you wanted to say a couple of words around that.

RÉGIS MASSÉ: Yes. Thank you, Jacques. To go through with this DR BCP Playbook and the Mitigation Playbook on the game we did in Montreal, AfTLD asked us to help them to appropriate the tool, and we will try to plan

two webinars. It's very difficult to play the game in virtual by Zoom, it makes no sense. But we will try before the end of the year to have two webinars, one in French and one in English, for African ccTLDs who has joined the AfTLD to explain the playbook and how to use it. So now we are trying to find a place in our planning because the planning is very full since the end of the year. But we will try to do our best to show and to explain how to use the playbook and how they can appropriate the playbook in their own ccTLDs.

JACQUES LATOUR: Thank you, Régis. I know that .dk Denmark, they did a tabletop simulation using the DR BCP Playbook, and it was an interesting event. Dirk said in the chat that he's done three virtual DR tabletop exercises. I'll take that as note, Dirk, then we can talk about it later.

So this is an overview of TLD Ops. Basically, it's a repository of contacts, a directory, the phone book, and we e-mail the phone book to every member every two weeks. We have very specific process to onboard and offboard people on the mailing list. The expertise that we have in the Steering Committee and the community both enables us to do workshop and do more, but we need to be careful and strategic on what we do. So that's the overview of TLD Ops.

In terms of operation, we used to be better at this. We used to do a status update incremental between the ICANN meetings. But over the last two years, there's been not a whole lot of security notification in the mailing list, and that's what we're going to address with the Security Committee. There were actually a couple of requests on the

mailing list for trying to find critical contacts, contacts for ccTLDs because they had operational issues that need to be addressed, and that was useful for that.

Zero joined. What update? I'm not sure that … So one thing we need as a committee—we're trying to figure out how to keep the TLD Ops contact up to date. So that's an internal thing with the Standing Committee on how do we ensure ccTLDs maintain their contact up to date. We know that it's not 100% accurate and what do we need to do to get there.

This is our very exciting action list. We have seven open action item on our list. A couple of them are work in progress. One is for the IANA tech contact to validate the TLD Ops. So that's a change in our process. We're halfway to implementing this change. We're doing a review of the charter. It used to be Brett on that action item. We changed it to all. We're making progress. So that's since Montreal. We should review the charter and make sure it's accurate. So we might not address it this meeting but hopefully we can look at it by the next one.

We need to update the website. So we have an issue today with the counts or the number of ccTLDs that are part of TLD Ops, the number on the website, the numbers we have in the mailing list and that we keep. They're not all syncing together. So we need to find a way to align our numbers correctly.

Security Committee. So we decided in December to create a Security Committee to add some more value to the mailing list with action item 106, and that's what Brett is going to talk about today.

Then the other one is we wanted to have a discussion to see if ICANN or somebody can operate our mailman servers. So that's the discussion we need to have with ICANN.

The CardDev proof of concept, I think this is something that you need to do at our next Standing Committee with Warren. You build a use case that we need to look at. So we'll take this offline.

Then the last action item we had was TLD Ops contact validation. That's finding a way to validate the contacts on the e-mail. So having every member on a monthly or quarterly basis do something to say I'm active, and that way we know our database is accurate.

So this is all a list of action items. The one we're going to address today is 106 Security Committee. And that's the next slide. So, Brett?

BRETT CARR: Thank you, Jacques. Thank you. Can you go back? Yeah. As Jacques already mentioned, we've been discussing ways that we can stimulate more useful activity on the mailing list to create more useful updates and the idea we came up with back in July was to form a separate Security Committee. The idea of this is to have a more focused set of individuals who are looking for security events and vulnerabilities that might be of interest or impact TLD operating. They don't necessarily have to be specifically—there could be things related to DNS, there could be related to EPP, etc. Also, there could be more generic things that might impact TLD operators' business systems. Anything goes in this area that might impact TLD operator in operating their systems.

As Jacques already mentioned, one of the reasons that TLD Ops was brought together to start off with was to create that database of contacts, but also to create an environment where we could send vulnerabilities and incidents in a trusted, closed environment to assist each other. I think it's fair to say that that part of the TLD hasn't been entirely successful over the last few years. And so this is really is an effort to try and get a smaller group of individuals to really look for things that really could be of interest to TLD operators. And that's not to say that anybody can't post to the list because we're certainly not saying that only the Security Committee can do this. It's just that it's a more targeted set of individuals that will seek out security events, be aware of vulnerabilities, and post details to the list, and then also stimulate and respond to discussion on those events as well.

The intention is that the Security Committee will meet periodically. But I would envision that'd be two or maybe three times a year at most. The point isn't of the Security Committee meeting and discussing. The point is of them actually finding things and posting to the list. But obviously, we want the Security Committee to be brought in to this concept and discuss ways to improve the content and look back at what we've done over the last few months and see how we can improve it going forward. So we will meet periodically to discuss the effectiveness. The Security Committee [inaudible] we're running a survey to see how effective this has been, and then we'll be analyzing and responding to that survey at ICANN74. We put out a call for volunteers in July and we've had a few responders. Can you go to the next slide?

So we now have some founding members of the committee. We decided that all of the Steering Committee should become members of the Security Committee. But also we've had five other people volunteer as well. Now listed on the slide is Daniel from Switzerland, Anthony from France, Raft from Madagascar, Misak from Armenia, and Dmitry from Ukraine. I think, at least some of those people are on the call now. So thanks to all of you for volunteering. We're intending to organize the first Security Committee meeting sometime in November. Kim is going to send out a Doodle poll for suitable dates in the next week or two when she's recovered from ICANN72. This is a call to other people as well. If you got a particular focus on security in your organization and you think you can help us, and you're a member of TLD Ops already, then please consider volunteering. We'd love to hear from you. We'd love to have you involved. I think that's it from me, Jacques, unless you think I've missed anything.

JACQUES LATOUR: No. One of the major observations from the community on TLD Ops was the lack of security notifications. So in the beginning, just putting the repository together was a big enough job. But now we're mature enough to put this in place. If we do this right, it's going to provide really good value to the community. So people ask for it, we're going to do it, and hopefully it's not work that goes unnoticed. So the survey is going to ensure that it provides value to people, and then we can tune it to meet the requirement. Any question from the attendees? We have a question button on.

KIMBERLY CARLSON: Just a chat pod.

JACQUES LATOUR: So no questions.

KIMBERLY CARLSON: No questions and no hands.

JACQUES LATOUR: ISO 27001. So this is not in scope for the Security Committee helping people pass their ISO certification, Right, Brett?

BRETT CARR: It's not in scope, but we like to see successes like that. So if our work on the playbooks, we've done things like that, it leads to people successes really nicely.

JACQUES LATOUR: So people can ask the newbie question on ISO 27001. I think we can respond to those, I guess.

KIMBERLY CARLSON: Jacques, we do have one hand from Anthony Hubbard.

JACQUES LATOUR: You can unmute.

ANTHONY HUBBARD: Hello, everyone. Well, I have no question for the moment. However, I just wanted to tell you that I'm glad to have joined the new Security Committee of the TLD Ops. We often say that the attackers, they are always one step ahead of the victims. But while I am convinced that the pooling of information that we all in charge of security are about to produce with this mailing list. I hope and I am sure that in some case, that should provide an advantage over the attackers. I hope that with all the other founding members, we will provide the list with useful information about vulnerabilities and threats coming from daily monitoring.

JACQUES LATOUR: Thank you, Anthony. It's great to have you on Board. One other thing I wanted to quickly mention is a shout out to Daniel. Daniel actually posted to the list this afternoon with a pointer to some malware that had been posted to the list. It was really good to see as well.

ANTHONY HUBBARD: Yeah. I saw that this afternoon. I must have the same kind of reflex to post to the list. I am going to have this.

JACQUES LATOUR: I think it's a habit that we'll need to get into. That's what we'll talk about in the first meeting.

ANTHONY HUBBARD: Exactly. It's a habit that I will have to have.

JACQUES LATOUR: Yeah. Thank you. Okay. So that covers it for the Security Committee. So Brett will set up a starter meeting and define the operating mode for the team, I guess. And then it's going to start generating some input to the mailing list.

This is a fairly quick meeting. In terms of AOB, so we just talked about already the webinar for AfTLD on DR BCP, so we need to talk about that with Dirk to see how we can actually do virtual webinars. I thought it would be difficult to do this in a large room context with a whole lot of people. We think to do a DR BCP with 10 people, a small team is one thing, virtual, I think that's achievable. But if there's 5200 People like we did in Montreal, I don't know how feasible that is. You can unmute, Dirk, if you want to comment … or not.

DIRK JUMPERTZ: Yes, yes. I'm here, I'm here. I was trying to find the right buttons. Indeed, I've done the tabletop exercise a couple of times virtual but with smaller teams. So the clue there is to actually have smaller teams going on, which we actually also did in Montreal. In Montreal there were also smaller teams. At every table was a smaller team of roughly 10 people. So if you can handle 10 people, if you can have breakout rooms where there are like 10 people and you have sufficient people that can guide the different participants, then I think it's feasible.

What we do, we use a combination of Zoom or any other video conference too, combined with Miro. I don't know if you know Miro.com, which is a virtual whiteboard. And what we do there is we represent those cards as different types of—yeah, as visual characters, I suppose, it notes. And then we allow people to have like three choices where they have to make three different choices from the different scenarios. It actually works. It's doable. With a relatively small team, it's doable. The original idea is not mine. It was actually Kristof from DNS Belgium who used that in a rather large setup, and then I just copied it and used it internally with [inaudible].

JACQUES LATOUR: Okay. So that's something we should figure out. Because if we break up in groups, then we need to have many of us TLD Ops present at that session to schedule that. It's possible but it's a lot of work.

DIRK JUMPERTZ: It's more work. There's definitely more work involved. Yes.

JACQUES LATOUR: Okay. So we'll take that offline to our next Standing Committee meeting, and then figure out what the next step is. And the other one, the other AOB that came out was for somebody—so today our mailing list is based on mailman and it's operated by OARC and we have limited control over the list, the server. So I'm not sure it makes any sense. We wanted to see if ICANN could operate the mailman. I don't know if John Crane is here? I don't think so. But we can pass a request

to them. Other than this, are there other business for TLD Ops? Comments? Are we doing good job, bad job?

RÉGIS MASSÉ: Jacques, I will just want to share something with you. It's not on the slide because it's fresh news. It's about the ccNSO DNS Abuse session last night. We were talking about—one of the question was if it's the goal of TLD Ops to address the topic of DNS abuse, and a lot of conversation of the good work TLD Ops group is doing so I wanted today to share it with the other members of the group, of course. But after discussion and after seeing that we are not really on the same thing from TLD Ops and DNS Abuse, we have decided during the ccNSO session last night to create specific working group to work on DNS abuse based on the model, on the way TLD Ops group is working. So I think in the next month, helping the new group to organize themselves to communicate each other to perhaps to help us working on this topic, it won't be TLD Ops group will address DNS abuse. But I think there will be a new working group in the ccNSO and I can repeat today what I said yesterday evening. I'm sure that all the Steering Committee members will be happy to help the community on this new group with this new topic to address.

I don't know if, Alejandra, if you want to add something about that. You were there yesterday or other people were there this night, if you want to add something about this?

ALEJANDRA REYNOSO: Hello, everyone. What I can tell you is that the summary of this session was shared just about an hour ago with the Council. So the next steps are to review what was proposed and to seek a plan on what to follow up. And afterwards when the plans develop, then it will be consulted back with the community to see if we're going the right way. And, of course, to gather more ccTLD oriented feedback now because we did a very broad consultation yesterday, as in anyone who was in the session, but we want to narrow it down to see if ccTLDs agree with the way forward. So it looks like such a group might be on the future but not yet there. So stay tuned and we will be posting you about that. Thank you.

RÉGIS MASSÉ: We will be ready and please do help when the group will be created.

ALEJANDRA REYNOSO: Thank you very much. I appreciate it. Jacques?

JACQUES LATOUR: Thank you. That was it for TLD Ops. So we're going to try something new, the Security Committee. So, that'll be the focus for TLD Ops for the next little bit. And we're going to try to enhance how we operate internally within TLD Ops. And that's it. Any questions? Now is the time. That's the members of our TLD Ops Standing Committee. That's it. No questions? Next time, hopefully we'll do this meeting in person.

RÉGIS MASSÉ: It will be nice, yeah.

BRETT CARR: Yeah.

JACQUES LATOUR: All right. Then this meeting is adjourned, whatever that word is.

KIMBERLY CARLSON: Thank you, everyone. Bye. Please stop the recording.

RÉGIS MASSÉ: Thanks a lot and goodbye to everyone.

[END OF TRANSCRIPTION]