ICANN78 | AGM – ccNSO TLD Ops Standing Committee
Wednesday, October 25, 2023 – 4:00 to 5:30 HAM

SUSIE JOHNSON: Hello and welcome to the TLD Ops Standing Committee Session at ICANN78. My name is Susie, and along with Kim, 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 for comments will be taken at the time set by the chair or moderator of this session. To ensure transparency of participation in ICANN's stakeholder model, we ask that you sign in to Zoom sessions using your full name. With that, I will hand the floor over to Jacques Latour.

JACQUES LATOUR: Thank you. All right. So, today, there's two meetings, one after the other. The first one is the TLD Ops workshop planning meeting. And then after that, we have our standing committee meeting and hopefully, it shouldn't take too long to do all of the two meetings. So, All right. So, at the last couple of ICANN meeting, the ccNSO internal role has expressed a positive feedback on TLD Ops doing more workshops at ICANN meetings like the one we did in the past.

So, the goal of today is to review the workshop that we've done, do a quick lesson learned and then figure out next step. How do we go forward in building new workshop? So, we need to put the committee

together. The main objective of all this is the last workshop, the standing committee ended up doing a lot of work ourselves. And the goal is to delegate that work to volunteers, supervised by the standing committee and try to make this something that is more sustainable. So, that's the main objective here.

So, the standing committee we have, it's here. We have three new members in the last little bit. Angela, Nicholas, and Josh. Angela couldn't make it. So, raise a hand. Well, good standing committee new members. And then Régis, Fred, Erwin. Erwin is not here. Eli is in the room. So, that's the standing committee. And then we have Warren, who is our SSAC Liaison. And then, Kimberly, John Crain, and Kim. So, anyway.

So, what I wanted to do is give a quick overview for those that have not seen what the TLD Ops is. So, you've definitively not seen what this is all about. So, I'll try to give a quick overview, so you know what we're all about. I want to go through collateral that we put together for the last workshop. So, you get a feeling of what we've done, and then we brainstorm the path forward. So, the TLD Ops, we're standing committee, and our job is to manage a contact repository of all the ccTLD. So, we got about 290 people from 200 different ccTLD on the mailing list. And every two weeks, we email everybody the list of contacts to each other. So, we have a person's name, corporate email address, their personal email address, mobile phone number and their role, what ccTLD they're part of.

So, if something is happening with dot ca, security-wise, you can go in that repository. The people on the TLD Ops mailing list can find out who

at dot ca are the security contact. And if it's super serious, they even have the cell phone number that they can call in the middle of the night. So, that's the whole purpose of this is if something really bad is happening large DDoS and somebody needs to call somebody else, or to prevent an attack from happening, that's a point of the contact repository. Unfortunately, the biggest challenge we have is we don't know who's using the list to contact other ccTLD because normally they don't tell us. So, we've heard that sometime the list works, sometimes it doesn't work because the contacts are not up to date.

So, those are internal challenge. We need to address, and we're dealing with those. But the purpose of the TLD Ops is we got 500 peep 400 people in the mailing list, and we should be able to reach or find any ccTLD on the planet. And you don't have to be a ccNSO member to be on the list. This is all ccTLD and around the planet. So, any question so far on the purpose of the TLD Ops?

So, like I said, the purpose is to review the material that we have. So, I'll go through that quickly. I'll show where it is. And then we need to figure out is this useful? Was it used as a bring value? Should we do more of it? Should we do less or in terms of documentation? And then same thing for the workshop themselves. So, this is an example of a slide we did in ICANN65. I can't remember where that is. 65? Doesn't matter.

That was before, Montreal. Right? It's under what? Where? Not there. I mean, is it Toronto, New York, Chicago, Milwaukee? Yeah. Probably. The point here so in ICANN62, we had a presentation to say, you know what, we're going to plan to do a DR/BCP workshop. And then it took four more ICANN meetings for the standing committee and volunteers

to put together a workshop. So, the point is, it was a lot of work to build a workshop. I think it was a success to some extent, but the committee did a lot of the work here, and we need to distribute the load.

So, in Montreal, at the end of all the planning and everything, in Montreal, we held the workshop. It was a disaster recovery business continuity workshop. So, that was a full afternoon session. I think it went well. And then COVID happened and then we didn't really do a lesson learned after. And then when we came back in The Hague, the feedback was we want, the ccNSO basically we want more workshops. We like it. So, I wanted to review the slide deck that we did quickly for the workshop, the collateral, and then have a discussion on should we do more of this, less, and whatever.

So, if you go to the ICANN community Wiki, we have a TLD Ops space in there. And then we have our own space in TLD Ops. And in here, we have the documentation for all the work that we've done. So, we got the DR/BCP playbook. And it provides a good description of the work here. I think the two main architect between this was Doug and-- Yeah. In designing and the structure. So, he did a lot of work as a volunteer to TLD Ops to build this, the DR/BCP session.

So, we add DR. So, the BCP table exercise template. So, this slide deck is meant for ccTLD to use as a template to execute their own disaster recovery internally. We know for a fact, couple of ccTLDs have actually used this template and they've done exercise inside their own organization. At the bottom, you'll see there is cards. So, what we did, Doug came up with the idea of using cards to run the workshop. Who

was at that workshop? You were there? You. That's it. wo? Camille, you were there, right?

An so, we had the cards, and I think that brought interesting discussion around the simulation. It was a little bit fun. And that I think it was interesting. So, there was some feedback, was you should redo the same workshop as is. And just get people engaged and then do something different after. So, maybe if there's a lot of new people in the community, it might be a good option forward because all of our collateral would be ready. Yes.

BARBARA POVSE: Yeah, we attend a three with my colleague, she's a lawyer, and that was her first ICANN meeting, and she was completely scared. I won't sit with these techies. I don't know anything, it was actually very good, and she enjoyed it. And we used these forms and we created our own. And I'm sure that many ccTLDs would benefit from exactly the same. That means that TLD standing committee would not have so much work, but I'm sure it would be well attended and it's really useful. We started doing this table top exercises regularly because we learned how to do it.

JACQUES LATOUR: Ah, good. Okay. So, if you look at the slide, the documentation, so we have a PowerPoint template. We have a DR/BCP playbook, and we have a deck of card. But if we look at the playbook itself. New time. What happened? So, this was actually the bulk of the work that the working

group. I'm not sharing the right thing here. Wait. Sharing. So, this is the DR/BCP playbook.

So, that's a template for tune for a ccTLD. It includes the best practice of the ISO standard around BCP and DR. So, we decided to simplify this. We got the DR and BCP in the same structure. So, it's one series of one document instead of multiple. And if you look at this, we spent a lot of time on this. We took the best template from all of our DR/BCP plans individually, the CCs and the committee and we put this document together. And it's quite extensive. We have 50 pages of text, but we also have an example on how to run the work shop, the time, the very specific instruction for ccTLDs on how to run the work shop, how to use the form, how to use a card, what is that the RBCP plan all about? And so, this we don't need to update this.

So, this is a template that you could use pretty much on your own to meet the very basic DR business continuity requirement. So, I'll just scroll because we have supply chain. You need to document what your supply chain is. You need to define the scope, planning, you need to build a risk adjuster, and then you document for your ccTLD, what risk, what's the likelihood of things impacting you. If you have a volcano activity, is it not likely can end up.

It's very low likelihood. Other people have higher likelihood, so you should have DR/BCP Plan around that, very specific. So, are you worried about a hacker, ransomware, DDoS, and then for each one of these things, the one that are high likelihood, you need to have detailed plans for executing when they do happen so that you're ready instead

of being not there. So, this is the standard, the DR/BCP plan. The few CCs like you said, used it.

All right. So, that's available. So, the DR/BCP workshop was around doing this. Maybe we can share this. Oh, yeah. So, those are the example of the cards we have for the workshop. We have shut down the authoritative name server. So, you play rounds in the disaster. You play, it's like playing a game. You put the card down to say this is what I'd like to do at this time based on the cards you have in your deck, because when you have a DR/BCP, you don't always have the right tools at the right place to make decisions. So, I kind of force the people to think about what should I do? The last card is the best card. If you have a disaster, blame TLD Ops, that's us. Woo-hoo.

We're here to help. So, DR/BCP is the playbook. It's well documented. The workshop ran well. We translated the book that we have in many languages. We haven't updated anything since. So, the other stuff we've done is we actually put a DDoS mitigation playbook together and you can look at it. It tells you basically what to do to mitigate the DDoS attack and, how to be ready, how to prevent them, and how to respond to them when you're under attack and blame TLD Ops when it doesn't go well. So, that's an example of a document that we wrote. We don't know. We used it again, but our goal, what we don't want to do is TLD ops, people write stuff that nobody uses.

So, you could probably ask today. You can ask chat GPT to write you a DDoS Mitigation book in two minutes. So, yes. Do you want to try it? Try that compared to this because it's probably going to be based on this. Yeah. This is now open source and it's inside that monster

machine tool. And then we have other stuff like TLD Ops monitoring tool. So, back to the agenda.

Feedback. So, the workshop. So, we've reviewed the workshop. So, you saw what it was about. We have about the gazillion pictures that we took during the day. I don't know where they are. We reviewed the documentation here. Next step. So, we heard loud and clear people want more workshop. So, let's see if we do the exactly the same workshop as is, that's one path. But if we decide to do something different than its worth and if it's worth, we need to plan all the development of the material and collateral to do because then the other example that came up is somebody wanted to do a ransomware specific workshop. Like, what do you do when you get ransomware?

The question, do you pay for the ransomware you don't pay? What's the policy? What's the government policy? You need to build a plan. There's a lot of work around that and a DR/BCP is if it includes ransomware, but ransomware is a very specific plan in this. So, I'm done talking. Let's talk about what we want to do as a standing committee, you guys are a committee, what should we do, and then we'll do whatever we do. Josh. What do you think?

JOSH SIMPSON: I think as a newcomer, first time at ICANN, for the newcomers, if there is a significant portion of people that the existing one is a good idea, but I'm definitely interested to see if there's other opportunities as well. ransomware and I guess identifying and accessing resources is a crucial point as well.

WARREN KUMARI: I mumbled myself and through Jacques's attention. Mean, it feels like there could also be other types of workshops which some TLDs might benefit from, which more sort of basic how do you run a name server? How do you do DNSSEC? How do you configure one of the registry services back ends? etcetera. Like, instead of focusing necessarily on the security and stability part, whichever this is a core part of it, but more just sort of how to run stuff well so that it doesn't go boom, which I don't think was any of the ones we already covered more, just like how to do this from scratch.

JACQUES LATOUR: I'm thinking that should be something we add to the tech day program to have best practice workshop. That's a really good idea, but not the TLD Ops. But take to have the training session and stuff. We definitively need that, especially for doing algorithm rollover. Well, we could use that to sync. Okay. So, say something. That's why you're sitting at the table.

BARBARA POVSE: I saw that you also made a monitoring tools playbook, but there was no workshop. Was it planned or not really? I mean, at the beginning, was there an idea to do also a workshop on that or not necessarily. No.

RÉGIS MASSÉ: No. The word, it wasn't an idea to make a watch of that, the idea of the monitoring tools here is just to give the URL of many tools then CCs can

use to monitor their DNS infrastructure. Perhaps it could be a way to go through in the workshop of disaster recovery, simulate with some tools what people see, what tech people see during the incident could be an idea to add this to the scenario, I think just having a workshop on the tools, it's difficult because it needs more training, that's workshop.

JACQUES LATOUR: And to be really, really honest, I don't remember off and the DDoS mitigation workshop we had. Christian was the previous chair for TLD Ops or secure Yeah.

CRISTIAN HESSELMAN: This was in Denmark. Right? No?

JACQUES LATOUR: Yeah.

CRISTIAN HESSELMAN: Yeah. That was a long time ago. Yeah. I remember we were doing flip charts and all that, but I forgot what the real workshop, what the gist of the workshop was, to be honest.

JACQUES LATOUR: Yeah. So, the outcome of the workshop is afterward, we put this document together to document, the DDoS mitigation playbook. So, that work. I just can't remember the session at all.

CRISTIAN HESSELMAN: But the question as well might be, what does the community want in terms of what kind of workshop would they would like to have? I mean, perhaps DDoS is no longer an issue for most of the community members. I don't know. So, perhaps a survey to ask what the topics should be of the workshop that might get you some buy in.

BARBARA POVSE: I'm afraid that you guys in TLD Ops are those who really know what's going on. And unfortunately, not many registries. I mean, they well, we all face some frights, of course, but I don't know whether the survey will give you right results. Maybe, due amongst on the list with TLD Ops list, where there are people who know who are they, what are they talking about when it gets to security, I think that here, you are the experts and you're not aware. That's why I'm here to let you know that people are not. So, ccTLDs are not all of them so advanced and even the basic stuff on security would be very helpful. I am aware that lots of work is required and therefore, we are all just volunteers in ICANN. so maybe, if some registries would be called to help with that, that we know that they have experts in different fields. I'm sure that TLD Ops can organize or could organize some workshops.

JACQUES LATOUR: Yeah. So, the I guess the challenge is exactly defining what the input are. So, if it's security training, then that, I think that's an ICANN capacity building thing. They should do more of that. I don't know. I know they do CCs region by region training, but there's no training session the day before or something specific.

WARREN KUMARI: There's this MRC training, ICANN was doing security training, but I don't know if they're doing it.

JACQUES LATOUR: But not part of the ICANN meeting. Right?

WARREN KUMARI: I think they did it a few times.

ABRAHAM SELBY: I think we can, because we try adjust it to share a survey in the last time, but I think we didn't get more response from their CCs. I'm not sure that if today we ask the members. I don't know, but how we can make sure that we will have feedback from the members, I'm not sure. But that, I want just to propose that we can set up in a version now that the different workshop we've done, maybe can be the first one, the version 1, and we can set up another version just to make sure that we have more information about our workshop, our first one.

Second one, I think we can organize a workshop region by region because we don't have the same issues in the Africa. If we have a specific workshop, they're not same issues when we are in Europe or in America, etcetera. This, I just want to propose.

RÉGIS MASSÉ: Yes. Régis, for the record. I understood what you say. I think, okay. Because we when we created these documents, they were high level to

be adaptable to each region because of course, disaster recovery plan. I would just remember at the beginning of this topic, we were after the Puerto Rico Disaster and we will be in Puerto Rico next year, everything's fine now. But when we decided, in Kobe, to create the workshop. It was just after the disaster of Puerto Rico. And, yes, we know that in Japan, in Puerto Rico, in Africa. It's not the same cases about natural disaster.

And we wanted just not having natural disaster, we wanted to have a disaster recovery plan more and with templates and with things that every CCs can adapt to use. But yes, I think it's a good idea to have regions specific exercise, but what we are trying to do with Jacque is finding a way to making a workshop when we are in the ICANN meeting. And if we are in an ICANN meeting and we just focus on one region, it's difficult because there are people everywhere from everywhere in the world when we come to ICANN meeting. So, we if you want to make a regional exercise, we must delegate some more resources to go the place to play these kinds of things.

It could be a way, but first, I think the first question here is to find, if you want to make something in one year, it won't be in Puerto Rico, but in Puerto Rico, we have to think about the topic and define what we want to do. The goal, I think, the aim here is to have a workshop in one year, in October next year. So, we have to find a way to get the most CCs we can in this kind of exercise.

JACQUES LATOUR: So, if we decide to create something new, it looks like that. It's going to be a year, two years, at the speed of volunteers on committee to

develop collateral and to do the planning and all that. And finding the volunteers is probably going to be hard to do, I think. I didn't think about that, but to do a replay as is of the workshop, that would be interesting because if we do that, obviously people are going to like it.

It's going to be a replay for some people, but it would bring the ambiance back for people to do more. And then if we say we need to do ransomware and they know it went well and we can do ransomware, maybe we can shorten the time, get a good enough documentation, and maybe energize a group or the volunteers that way. So, I think that's what I'd like to propose is we replay

RÉGIS MASSÉ: Yes. Régis, for the record. I just follow the record. Yes, Jack. I think we can replay the exercise, but changing the parts of the scenario. Changing thing, for example, within somewhere or something else, having new ideas for even the people who came playing the first time in Montreal can make the… it's another scenario, when we work for these ideas, we are making some exercise regularly. It's not the same exercise, but if we help people in the CCs to make some exercises. And we are just for this idea, finding a new scenario, perhaps using the cards or making some additional cards to address this scenario. But we don't have many works, it's not creating from scratch a new workshop.

JACQUES LATOUR: So, part of the work. Yeah. Exactly. So, part of now-- It's all coming back. So, this is good. Well,

JOSH SIMPSON: 66 was Maracas.

JACQUES LATOUR: Maracas. Okay. So, when we did the session in Montreal, the first step was we had forms to fill in and it was to build the DR/BCP plan quickly for a scenario, and it wasn't set. So, people didn't know what scenario they had to do. So, based on what you're saying, we had roundtables with maybe fifteen people around each. So, maybe one table should have a volcano. One table should have earthquake. Another one as different type of scenario.

And then the people at that table, they build the DR/BCP plan, the response plan together for that scenario. And then maybe switch people around and then, play the cards on other people's scenario on using that plan and see if it's usable, something like that. I think that would be recycle, reuse, and make it different. Any? sounds good? Is that a plan? Because that meeting can be super quick. If that's a plan, raise your hand, and then we're done. That's the general direction. Like that? Any?

VADIM MIKHAYLOV: Yes.

JACQUES LATOUR: Okay. You know, you raised your hand just before, so you're good.

VADIM MIKHAYLOV: No. Just, to play a little bit the role of divested, I'd want to break it, but just thinking that was when I saw the details mitigation playbook. Apparently, nobody here recalls what was the previous workshop, whether it should maybe make sense to try repeat this one, rather than disaster recovery workshop because it seems to me like the details mitigations in the current situation of the war in Europe and the much more real scenario than disaster recovery. So, like, have to have the workshop about the ways because I think that the last work last workshop for the DDoS mitigation was mainly focused on DNS. So, but mostly, the attacks now go to the to the websites and to the to the web and this wasn't probably covered.

So, there are definitely some, ways how we can learn from each other how to stop these DDoS attacks by implementing the IP blocking or fail to ban or these tools, how to fight against the DDoS. So, I'm not saying, like, it's probably not being the same. It will not be the same fun as the disaster clear workshop was that was in Montreal, but maybe if this is not the, like, little bit more interesting for the registries. Actually, I don't know but, just making suggestions.

JACQUES LATOUR: So, we play with the existing, then DDoS is existing. So, maybe that's a table. Maybe we can have a group that will do DDoS mitigation as part of the workshop and they get cards. Cards is shut down the name server. You know, that's not a good idea, maybe, but just, Okay.

VADIM MIKHAYLOV: Noted.

JACQUES LATOUR: Noted.

VADIM MIKHAYLOV: Noted. Yeah. Yes.

JACQUES LATOUR: And recorded. Yeah. Okay. So, reuse, recycle and modify a little bit. And then, so, what we'll need to figure out when the workshop can be or all that, I don't know. Puerto Rico's probably too early.

RÉGIS MASSÉ: Yes. Sorry. Are there any notes about what made those workshops successful previous times? Some lessons learned or something like that documented?

JACQUES LATOUR: We did a survey. Right?

WARREN KUMARI: Yeah. We did a service attestation.

JACQUES LATOUR: After?

WARREN KUMARI: Yes.

JACQUES LATOUR: I'm looking at Kim. You don't remember. That's the problem. COVID happened. We all forgot. It's unreal.

RÉGIS MASSÉ: Might be good to learn from this and see how can we improve from there.

JACQUES LATOUR: We didn't do a real lesson learned. And the goal of this session today was to bring people in to do a lesson learned and then we got the feedback that would've it was great, and that's it. Maybe. I know the feedback was, we tried to get feedback. It was hard, and they say, we liked it, and we want more. And that's why we're here to plan how to do the more, but maybe we should have a formal lesson learned after the next workshop and then try to do improvement.

RÉGIS MASSÉ: I mean, do a replay. Do it one more time in the same way. And learn from the other.

WARREN KUMARI: A little bit different.

RÉGIS MASSÉ: Yeah. Slightly different. If I remember well, after the workshop was on Sunday. We had at this time, an update of ccNSO. No, an update of ccTLDs in each ccNSO session. And I will find quickly the slides. And we

had, the result of the survey in the slide, I think. I thought we had the result of a survey, I think. So, it was the team. It was the people who were there. So, this is GNSO status update check. Oh, we can look after that. That's all. Not this one, not this one.

JACQUES LATOUR: I thought the date is wrong. Remember, I saw John Crain on the picture. We have record some feedbacks directly in the room. Play too far now. So, now it's coming back. Oh my god. So, we recorded people. We have videos of the feedback live after the session. And that was at the end of that deck, but I don't think it's in that one. It's probably in the Wiki in the ICANN site somewhere, but there is feedback. it was good. Internally, we had to tune it a little bit based on the flow and I don't think there's much more to do than that.

RÉGIS MASSÉ: The idea is to find back this feedback and show you, show to the community in the next ICANN visit.

SUSIE JOHNSON: Jacques, there was an engagement survey from TLD Ops on the usefulness of TLD Ops. And if anybody uses it, but there was no survey regarding the playbook.

JACQUES LATOUR: Okay. All right. So, we have a plan. We'll try that. We'll figure out when the timing and because it's still some work to plan the workshop. So, we have all the instruction, but we need the room. We need the people.

We need to have people that supervise each of the little table, the islands of the yard disaster, and then make sure they follow the program. And then we have a ceremony, somebody that reads a scenario out loud, they ring a bell. Okay. Now step 3 scenario 2. This is happening, and then people need to go, it keeps getting worse. This scenario. So, either we use the same scenario or modify it a little bit, and then all of that equals more work and time, but we'll figure it out.

RÉGIS MASSÉ: My idea about the when is Puerto Rico, it was perhaps a bit too short to organize all the things. And, for the ICANN, the next ICANN in June, it will be in Kigali, and I don't really know who will come there, will go there. So, I think the most secure to having the chance to have a lot of people joining us is to make it in 81, meeting 81, in one year.

JACQUES LATOUR: Yeah. And then Puerto Rico meeting on the Sunday, we should get a block or two, and then we do the detailed planning of the session, the workshop. We review the material, build a scenario, figure out everything we need to do to run the workshop. And then try to figure out how many people we need to recruit to do the session. And then plan that either one or two meetings after. That would make sense. But there is a lot of work in Puerto Rico to put the package together for the date. Okay. Thank you. Meeting done. We have another meeting. It's a separate. All right, we can end the recording.

[END OF TRANSCRIPTION]