

BARCELONA – ccNSO: TLD Ops Standing Committee - Meeting
Sunday, October 21, 2018 – 10:30 to 12:00 CEST
ICANN63 | Barcelona, Spain

KIMBERLY CARLSON. Hello. October 21st, 2018, ccNSO TLD Standing Committee meeting, 10:30 to 12:00, room 131-132.

RÉGIS MASSÉ: [inaudible] It's not easy to go there.

JACQUES LATOUR: Only one missing is Erwin, so I guess we'll start. Good morning. Welcome to our open closed TLD Ops Standing Committee meeting. So, this meeting is – we do this at every ICANN meeting, and then this is where the standing committee meet. And we discuss the work that we need to do for this meeting and the next one, so you're welcome to join and participate, and I guess ask some questions.

I'm Jacques Latour, I'm with .ca, and Régis is our vice chair for the TLD Ops Standing Committee, and we have the members – some members of TLD ops here. We have Fred Neves, distinguished committee member. We have Erwin. Is he here? No?

UNIDENTIFIED MALE: No.

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.

JACQUES LATOUR: Sleeping? Erwin? Ali, here? Yeah?

UNIDENTIFIED MALE: Yeah.

KIMBERLY CARLSON. No.

JACQUES LATOUR: No? Abibu? Right there. And Brett Carr from UK. So these are the standing committee members, and then we have Warren Kumari, John Crain, Kim Davies, and Kim, staff, helping us with this working group.

This is the agenda we have for today. So we'll do a brief introduction of what TLD Ops is. We normally do that for your benefit, at least to get some feedback or information on what we're talking and what we're doing. We have a list of action point to address that we build with the things we need to address. We have operational status on our TLD ops mailing list. We'll talk about – we have a workshop this afternoon that's closed, and then we'll talk about internally on how we're going to address that, and then discuss a few objectives for this ICANN meeting, the next one, for TLD Ops.

So, what is TLD Ops? So, over the last few years, it was determined by ICANN and the ccNSO that we need to have a global mailing list, a global community of security contacts across all ccTLD so that if there was something big happening and we need to communicate with all ccTLDs

on the planet, that we would have one mailing list that we can reach everybody in here.

So that was the goal of TLD Ops, was – the original chair is Chris [inaudible] over there at the end. He started the group, he set up TLD Ops, and now we're a standing committee and we keep that infrastructure, that mailing, that community together and running.

We have about 380 people on the mailing list so far, in our contact repository, from 201 ccTLDs. So those include ASCII and IDN. The purpose of this mailing list is that it can be used as a trusted media for ccTLD to share information to report incident and all that. So we're not going to talk about anything that happens on the list in this group, because that's closed and confidential to those user, but that's what it is. And if you're a ccTLD in the room and you're not part of TLD Ops, you should be. Anybody not part of TLD Ops and is a ccTLD here? Because we're not going out unless you sign. You're stuck here.

So, did you raise your hand there?

BASUKI SUHARDIMAN: Yes.

BRETT CARR: [Wins a prize.]

JACQUES LATOUR: So –

BASUKI SUHARDIMAN: I think we will be trapped here with you.

JACQUES LATOUR: Your name?

BASUKI SUHARDIMAN: I'm [inaudible] I'm from ID registry.

JACQUES LATOUR: From where?

BASUKI SUHARDIMAN: From .id, Indonesia.

JACQUES LATOUR: Okay.

BASUKI SUHARDIMAN: Indonesia, .id registry.

JACQUES LATOUR: Good. So you're staying here.

BRETT CARR: Wins a prize.

JACQUES LATOUR: Wins a prize. We have a sticker. Yeah, give him a sticker. We have a nice sticker. Yeah.

RAED ALFAYEZ: This is Raed from SaudiNIC. We are part of the TLD Ops, but I want to know, how many contacts can we add there in this list? Is it only limited for two seats, or we can add as number as we can?

JACQUES LATOUR: We have a three – I think it's three now, yeah?

UNIDENTIFIED MALE: Yeah, three.

JACQUES LATOUR: Three contacts?

KIMBERLY CARLSON: Three contacts.

JACQUES LATOUR: Yeah, it's three contacts per CC.

RAED ALFAYEZ: So we can add up to three contacts?

JACQUES LATOUR: Yeah.

RAED ALFAYEZ: Okay, thank you.

JACQUES LATOUR: Individuals, not internal mailing lists, and yeah, that's it.

RAED ALFAYEZ: [inaudible]. Thank you.

JACQUES LATOUR: So, the idea behind TLD Ops is that we have large ccTLDs and smaller ones, and if a smaller ccTLD gets DDoS or the registry gets compromised or whatever, then they can reach out to the – send an e-mail to the mailing list to say, hey, this happened, I need help. And then there will be a lot of people there to help mitigate the incident. That's the goal.

And this works for large and small ccTLDs, but it's meant to reach the security people in other ccTLDs to help with operation. But it's not meant to replace – we don't have an SLA, it's not meant to replace your security team. It's there to enhance or to be of assistance. And we have a standing committee and we make sure that we keep the mailing list running.

So what we do is twice a month, we send an e-mail to all the members with the list of all the contacts. So it's an e-mail with 380 lines in it, and it's all the contacts, the e-mail address, the personal e-mail address of the contact, their phone number, and that's what TLD Ops is all about so that once every two weeks, you get a detailed list of all the contacts, and then if something goes bad, you can go on your phone, should be stored there, and you can access the list, or individual people in case you see something happening on another TLD. So that's the purpose of this, the TLD Ops.

RÉGIS MASSÉ:

Just an important thing, as the contact, you can define two e-mail address. Especially if you've got a DDoS attack on your company, you can use the second e-mail address registered in your contact list to communicate with the list and ask for help or things like that. It's important.

JACQUES LATOUR:

And it's also – yeah, it's important if we get an address from somebody on Gmail saying “I need help,” at least we can validate who they are. And we have a cellphone also to validate.

Example of alerts that we've seen on TLD Ops, they vary from registry compromise notification due to a day zero attack that was broadcasted all the way to DDoS attack happening on TLDs name servers, so it depends on the list. So here are just a couple of example that we could make public.

So, we send a regular e-mail to the TLD ops contact, the mailing list is used to share information or request information, and TLD Ops, we also do workshops. That's something we started with – so we had DDoS mitigation workshops way back a couple of years ago, and then out of that, we built DDoS mitigation playbook documentation.

This afternoon, we're having a disaster recovery workshop, and the goal of this is to build a playbook that is specific for ccTLD to mitigate DDoS attack. So it's not going to be ISO or standard-based to mitigate –

UNIDENTIFIED MALE: [inaudible]

JACQUES LATOUR: Disaster recovery, yeah, and BCP. Sorry. [inaudible]. So, for disaster recovery, and then to make sure that – I think the goal is to see if we can build a playbook that is specific for ccTLD. So, it's another experiment. We'll see how that goes.

So, it's an open – it's a closed open community. That means that we control the access to it, we vet all the members that come in, but it's open to all ccTLD, but we're very specific on what kind of member we accept. It's a mailing list, so if you have any questions, we have e-mail addresses, we have a webpage on the ICANN website, and so that's what TLD Ops is all about.

RÉGIS MASSÉ: Yes, as a ccTLD, you don't have to be part of the ccNSO to join the TLD Ops group. So, it's really very open to all ccTLDs all over the world.

JACQUES LATOUR: Yeah, so I think we have more members in TLD ops – we have more ccTLDs in TLD Ops than there are ccTLDs in ccNSO today.

BRETT CARR: Perhaps I can ask an obvious question on behalf of all the people. Are TLD operators who are only gTLD operators able to join?

JACQUES LATOUR: No, it's only for ccTLDs. Just in case you wonder. But thank you. So, action point [inaudible] can't read that. So we have a list of action points. Alright, so like I said, this is a standing committee meeting, so we have action points.

So action 89, so you can guess that we actually addressed 88 action points since the beginning. So we were – I think we can close this one. This is the TLD Ops member discrepancy. Oh, no, we can't close. So we need to make sure that the website, the spreadsheet that [Christian] invented, multi-tab thing with all the ccTLD joining.

We're out of sync by one, so we've got to consolidate that. So we still need some work to do that. So you – I think Régis started to do something on this also.

BRETT CARR: I think we said we're going to have a meeting, but we've not had a meeting yet. We will.

JACQUES LATOUR: So I'll update this. You, Régis, will meet and figure out your plan to –

UNIDENTIFIED MALE: Yeah.

JACQUES LATOUR: Do I take my name out? And put Régis. Alright. Action item 90, Erwin, [ping.] Alright. So, Erwin was supposed to update our new member onboarding procedure so that the IANA tech contact could validate the TLD Ops. Remember, Kim? Do you have any updates on that?

KIMBERLY CARLSON: [inaudible].

JACQUES LATOUR: Sorry, this is the IANA tech contact to create – to [inaudible] procedures to allow not the admin contact but the tech contact to add TLD Ops members.

KIMBERLY CARLSON: Okay.

JACQUES LATOUR: So we haven't done anything.

KIMBERLY CARLSON: We haven't done anything.

JACQUES LATOUR: Okay. So this is still work in progress.

KIMBERLY CARLSON: That's just a procedural thing.

JACQUES LATOUR: Yeah. But we need to make sure that it's legit everywhere. Alright. So Erwin was – action item to look at GDPR impact on our mailing list and all that, so I guess there was some work on that, but he's not here, so we don't know what happened. So we'll leave it open.

Action item 93, ccNSO status update presentation rebuild. So, as you can tell, we have a new look and feel, we have a new logo, we have new slides, we have a brand-new image. The only thing we don't have are new stickers. So that, we can close the item, so new logo, new slide, new collateral. So that was one of our action items closed.

Régis, we did the APTLD outreach presentation, so that's closed.

RÉGIS MASSÉ: Yes, it's closed. I made a presentation at the last APTLD session, a remote one, in Uzbekistan, and now you can say it's closed, can close this slide.

JACQUES LATOUR: Okay. And action 95 was to do all the stuff required for the workshop, so that, we can close, because it's happening today. Alright. Save. Step by step, right?

UNIDENTIFIED MALE: Yeah.

JACQUES LATOUR: This is going to be the most exciting meeting you'll ever be part of. So, action points are done. So, operational status since the last meeting. On the mailing list, there was one notification that was sent to all. It's not unusual that we don't have – to have no notification between ICANN meetings.

We actually met our objective of adding new ccTLDs to the list. So – this is small. So we added Peru, Guam, Mexico, San Salvador/El Salvador, Mauritania, and Cote d'Ivoire. So, in the last TLD Ops or the second to last TLD Ops meeting, we had a campaign that the standing committee members, we set up a goal to add a couple of members each, and it actually worked because we added six since our last one. So, we'll give it a shot again to try to do more outreach. So, that was good.

Probably six is our biggest, I think, that we've done in a while, so the outreach is working good. We added – there were five TLD Ops changes on the mailing list, and Régis did the presentation like he said at APTLD74 in Tashkent in Uzbekistan.

So like I said before, if you're not part of TLD Ops, now is the time to join. Super simple. You send an e-mail – the procedure is on TLD Ops website. You send an e-mail, we verify that you're a trusted contact. We require the admin, the ccTLD admin contact to send an e-mail to Kim, a specific ICANN address with a template to fill in, and that's how we add new members to the list. So, onboarding, super easy. [inaudible]. We need to make the numbers bigger. Do you want to cover that? [inaudible].

RÉGIS MASSÉ:

So, as you see on the map, it's a little bit small to read, but we're going to make a campaign to make the ccTLDs of the African region and Asia Pacific region to join the list. There are more than half of them joined the list for the moment, so that's a good point.

As we made some local campaign in Africa and for APTLD this year, some ccTLDs joined us, and it's a good thing. So now we are more than 200 on the mailing list. It's important to – going on that, if you have contact with ccTLDs that are not on the list, I think it's important to join this list, because it's made to help. As Jacques said, it's made to help the CCs when you've got issues, when you've got the attack, the DDoS attack or things like that.

I don't know if this room – who read the first playbook we produced. Yeah? Was it useful for you? Okay. We're happy to have a lot of comments on the first draft before writing the final versions, and the goal of the workshop this afternoon is to create another – I hope another useful playbook to help not on DDoS attack but on disaster recovery, and to share, because I think this topic is very different from one region to another. So I hope it will be helpful for you.

So, okay, the number grows. There are still some ccTLDs that didn't join for the moment, so let's [go on] to try to get them on the list, because I think that we can help them and they can help us.

JACQUES LATOUR:

So, that is a good question. I created a new action item, which is playbook distribution. So there's a bunch of new people that joined the list since we last published it, so we need to find a way either make the document public or on a regular basis e-mail all the playbook to everybody. So that's something we need to share.

RÉGIS MASSÉ:

Perhaps we could imagine a closed or secure storage somewhere to get the files from what was produced from the TLD Ops group since the beginning and not just sending the document by e-mail.

JACQUES LATOUR:

I need to figure that out. Okay. Thanks, Régis. Alright, next agenda item, disaster recovery workshop. See, I didn't see DDoS mitigation. Making

progress. So this afternoon, we have about 50 registered attendees for the workshop, so that's pretty good numbers.

We have the agenda that we prepared so far. So the idea that we have is that we'll do a quick introduction on disaster recovery, BCP, the strategy for TLD Ops that we have so far for this. We have a couple of presentations. They're limited to five minutes. I think we'll have a timer, except for Japan, we agreed to have up to a ten-minute presentation on the disaster they had. I think it's their first time presenting this, so we give them.

The idea also is that we'll ask the audience to quickly – the opportunity to go and talk about things they want to share, and so we'll limit – so we have about half an hour of presentation, five-minute chunks, and then we'll make sure that we control the timing tight. So that's important. So that gives – we have two that are lined up, and then we'll be looking for three or four five-minute presenters then.

I think there's value in having CCs, not prepared to talk about it, just to go in and share information in an open manner. Like I said, this is a closed session. What happens in that room stays in that room, there's no Tweeting or picture taking and stuff. So it's – there's no recording, and it's Chatham rule or something like that. Whatever happens stays there.

So we want to do breakout session, so we'll have two different breakout session. The first breakout is about an hour, and it's to look at disaster recovery, business continuity for the registry and DNS, so both together. And then we break out in two groups. So one – originally, we

thought about breaking out in four groups, but 50 people, if, what, 30 is going to show up, two group is 15 per.

BRETT CARR:

I think if 50 show up, it's not unreasonable to split into four groups. If 30, it seems more likely to do two. We need to like just decide on the fly [a little bit during this afternoon one.]

JACQUES LATOUR:

Yeah. So we can break out potentially in four groups, or two, and we came up with four areas, which is we're going to look at detection, analysis, and then the other one is activation and communication plan.

So, specific for the registry and the DNS, get people in a group and talk about information that is specific for the registry and DNS in detection. And then put some bullets of what we need to do. And then analysis of a disaster on the DNS, put some bullets and then do the same thing with the action plan and communication.

So about 45 minutes of that, we'll have flipcharts, and then at the end, each group will present a summary of what they did for their action item. And then the second workshop is to look at the corporate IT infrastructure that runs the ccTLD and the people business continuity.

And then the idea there is that group two is going to look at detection and analysis, so they're going to switch so that everybody has a chance of looking at the four different components, and then group one will do activation and communication.

So I think if we have two groups, everybody gets to think about everything. If we have four groups, then we have less crossover. So, ideally, two groups is better. And corporate IT is the IT infrastructure, e-mail, all of the stuff you need to run the business and the people. So if you lose your corporate office, you need to activate the disaster recovery.

And then the key challenge, the steering committee, that we need to make sure is that we keep the full [inaudible] to the registry [inaudible] some stuff that is specific for ccTLDs and not get into – and then also try to get out of – not go in the weeds.

So if there's a discussion that's getting too focused or too deep at this level, so the steering committee, we need to take that discussion and make sure that it stays at the appropriate level so that we cover a lot of ground instead of spending 20 minutes talking about DNS, DDoS mitigation or whatever.

So like I said in the beginning, this is an experiment. We're going to try to see if there's real interesting stuff that comes out from the workshop. And that'll be the conclusion and the summary, is that we'll look at this – we also – the challenge that we have with this workshop is on the Wednesday.

The ccNSO meeting, Wednesday at 9:00 AM. We have a 30-minute timeslot to present the outcome of the workshop. So that's pretty quick, so we need to summarize the workshop, build some slides and then come up with a story on how the workshop went. And then from there, we'll know pretty quick if we need to do more work on this or not.

BRETT CARR: Yeah, I think we can only come up with a very brief summary though for Wednesday. We're going to need more time, maybe tell the ccNSO on Wednesday that we're going to give them a more in-depth overview at the next ICANN meeting.

JACQUES LATOUR: Yes. So it's a pretty short timeline. So, any questions for the workshop?

RÉGIS MASSÉ: Yeah, just one thing. If you look at the agenda. If you look at the agenda, you'll see that the session will end at 5:00 PM. If you look at the general agenda of ICANN, the session is going until 5:30. The last hour, the last 90 minutes is for us to summarize all the things for the ccNSO meeting for Wednesday, [especially.] So I think the slots will end for the people who joined the workshop at 5:00.

JACQUES LATOUR: And the timing is also ballpark, so it could be plus or minus. It could be a lot quicker depending – because if we keep the scope only to the registry, DNS and very focus high-level on the things we need to look at, there's a good chance we're going to be requiring less time than this. But the idea is to get all the good scenario or feedback or topics on the chart so that we fully document this.

So I guess for each of the –the group will get somebody that has good handwriting to write the notes so that we can decipher them after. That’s a requirement. So that excludes me from writing in the thing.

UNIDENTIFIED MALE: [inaudible].

JACQUES LATOUR: So we need to find good notetakers so that we can actually use them. So the plan that we have for the workshop is to do the workshop at this meeting, and then at ICANN 64, to have a draft playbook delivery if we have the time or if we have the content.

There's a possibility that at the end of the workshop, that we determine there's no need to do a playbook, if there's nothing very specific for ccTLD. So maybe the thing is you just follow the procedure in ISO whatever for disaster recovery, business continuity, and maybe that’s all we need to do. So it’s an experiment and we need to determine.

RÉGIS MASSÉ: Perhaps as we've got time in the room, what would be your expected for this kind of playbook? Do you have some ideas about that that can help us this afternoon to drive the workshop?

JACQUES LATOUR: Yeah. So you've got to remember the reason we're doing this is because the ccNSO asked us to look at this, because there was a need. So we're actually doing it, but the outcome is still unknown.

BRETT CARR: I guess to phrase Régis' question more directly, what disasters do you worry about?

JACQUES LATOUR: Yeah.

BRETT CARR: Or do you not worry about disaster? I do.

STEVEN BARRY: Steve Barry from .ca. Jacques knows us, because of course, we work together very closely on it. But recently, we've had weather-based natural disasters. We're from Ottawa, Canada. There was a tornado that touched down actually about a kilometer from Jacques' house, and it caused us to invoke our disaster recovery and continuity plan.

It required us to access our disaster recovery plan. So weather-based interruptions or natural disaster interruptions is something that we're keen on investigating. It's not something we've really contemplated before.

BRETT CARR: Yeah. I think for us, the thing that we probably worry about more than anything else is even though we're not really a bad weather country in the UK, we do sometimes suffer from snow during the winter months that we are woefully unprepared for as a country because most of the time, we don't suffer from it.

Last year, we had quite a lot of snow and we had at least four days I think it was when nobody could get in the office. So that's probably the thing that gets the most attention.

STEVEN BARRY: We can help you with that.

JACQUES LATOUR: So we'll have an action item with winter tires. Alright, so that's the kind of stuff that we need to talk about, and with the weather changing, we need to better – we'll see how the workshop goes. So hopefully, we'll have an interesting playbook, and then it's going to be useful, that's specific for ccTLDs.

Every ICANN meeting, we review the objective that we've set for this meeting and we try to define the one for the next meeting. For this meeting, we wanted to host a workshop, and we are. And then the other objective that we set was to increase the membership by three to 198, but we didn't have a steering committee at the last ICANN meeting. Is that right? We didn't. The one before.

Yeah, so the goal was to go to 198 at the last steering committee, and we're now at 201, so we exceeded our objectives. So I think the objectives that we want for the next meeting, by ICANN 64, is by then to have a draft playbook put together, hopefully with volunteers from the community, and hopefully not returned by the steering committee.

So the DDoS mitigation playbook was written by the steering committee, and the goal was to have members of the community to help us write it. And there was good feedback from the community to review the document, but the core was written by the committee. so here, it'd be nice to have volunteers that work with us to make this work.

So that's the objective for the ICANN 64. And then hopefully, we can increase and add another three. Three looks like the good number to add every ICANN meeting.

BRETT CARR: We've got one already.

JACQUES LATOUR: We've got one already. We need to figure out if that one counts. No, it's too late, right? So once I say the meeting is over, then we're already 33% done our objective. But we don't want to increase by four to 205, right? That makes – no, we'll stay there. So we add by three member. Any other objectives by then we should add, or that's enough?

BRETT CARR: Do we need to come up with an idea for another workshop?

JACQUES LATOUR: No.

BRETT CARR: No?

JACQUES LATOUR: Not yet. So when we did the first DNS – the DDoS mitigation workshop, we actually had two workshops in a row. So the first workshop, we had, I think, 200 bullets that were written down, and the other workshop that we did is we took those bullets and summarized it into the playbook. So there might be another workshop to do something similar depending on the amount of information we collect. So it's potential, but we'll figure that out over time.

So I'll do this after. This is – so I send an e-mail to the ccNSO community with the status update of this meeting. So I'll do that after. This is the Org chart for the standing committee. So I'm the boss on top. So I'm the chair, and then we have the standing committee members here that were introduced in the beginning. And then the liaisons, and Kim. We can't do any of this without Kim, so thank you.

Any other [inaudible]? That's French. [inaudible]

UNIDENTIFIED MALE: [inaudible]

JACQUES LATOUR: Yeah. That's correct spelling. That's good. Any other questions? Information, so this is the website, tld-ops-secure-communication.htm, that's the link. You'll go there. the procedure to join are there, and then we'll do that for Indonesia. You're not leaving the room. And my contact information and Régis' information. So, any questions? Erwin is missing in action.

UNIDENTIFIED MALE: [inaudible]

JACQUES LATOUR: Yeah. Yes. So, Abibu, how do we – so there's four of us, so we're going to split for the workshop. We're going to split two by two. Three? Five?

UNIDENTIFIED MALE: [inaudible].

JACQUES LATOUR: So, do we have –

UNIDENTIFIED MALE: So you're going with the two groups?

RÉGIS MASSÉ: [inaudible]

JACQUES LATOUR: So, do we stick to – do we follow the group, or we stick to that action analysis, the focus area, and then we do [both?] So if we follow the group, that means steering committee, we need to learn –

BRETT CARR: [I have a preference from my experience] to do detection analysis in group one, and activation, action plan and comms in group one in a second breakout. So stay with group one, basically.

JACQUES LATOUR: Stay with the group one? They switch, right?

BRETT CARR: Yeah, they do different things. So stay with group one. We'll do detection analysis in the first section and activation action in the second.

JACQUES LATOUR: So you want to stay with group one?

BRETT CARR: Yeah.

JACQUES LATOUR: And then we follow – okay. So we do get to cross the – okay. So there's six of us. One, two, three – okay. Alright, that works.

BRETT CARR: I'm also happy to give a five-minute presentation at the start of the slides, but on top for a bit about what we do about corporate data.

JACQUES LATOUR: Yeah. Alright. So we have the lunch. People know about [whoever's –] so we're full for –

KIMBERLY CARLSON. Almost full. We've got a couple spots left, but it's on the banquet hall [with its] list.

JACQUES LATOUR: Okay.

KIMBERLY CARLSON. So if you RSVP'd, you're on the list, and that's all we're going to do.

JACQUES LATOUR: That's it?

KIMBERLY CARLSON. That's it.

JACQUES LATOUR: Okay, so that's it. Questions before the meeting is closed? If there's no question, three, two, one –

RÉGIS MASSÉ: How many of you are planning to be at the workshop this afternoon?
Great.

JACQUES LATOUR: Yeah, the disaster recovery. So you're going to be there?

UNIDENTIFIED MALE: [Yeah.]

JACQUES LATOUR: Did you register? No?

UNIDENTIFIED MALE: No, not yet.

JACQUES LATOUR: Okay.

UNIDENTIFIED MALE: [inaudible].

JACQUES LATOUR: So we'll register you, and then you can be part of the workshop.

UNIDENTIFIED MALE: [inaudible].

JACQUES LATOUR: Alright. Thank you. It was a fun meeting, eh?

[END OF TRANSCRIPTION]