

---

JOHANNESBURG – ccNSO TLD OPS Standing Committee

Monday, June 26, 2017 – 08:00 to 09:00 JNB

ICANN59 | Johannesburg, South Africa

JACQUES LATOUR: Good morning. Welcome to the TLD-OPS Standing Committee meeting in ICANN59. Who is missing?

[CRISTIAN HESSELMAN]: We are missing Fred and Jay.

JACQUES LATOUR: Anybody calling in to the bridge?

UNIDENTIFIED MALE: There's no [one in the bridge].

JACQUES LATOUR: No? Good. All right, so today, I'm chairing the meeting, and Cristian is going to co-chair for today. It's his last TLD-OPS meeting as the Chair?

CRISTIAN HESSELMAN: Yes.

---

*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:            You going to cry?

CRISTIAN HESSELMAN:      No, I won't.

UNIDENTIFIED MALE:        No, but we might.

JACQUES LATOUR:            Not a whole lot. No? So I'll chair the meeting. Today, we have a long agenda, but there are items that are merged together. We'll do a quick introduction of what TLD-OPS is.

We'll go through our action points. We have an ongoing list of action items that we work on a couple of times. We meet on a regular basis every month and a half or two months, and then we have a list of action items that we work on.

We'll cover some TLD-OPS status on operational issues. That's our mailing list, so we have things we need to work on that.

One thing we need to do is look at the charter for TLD-OPS. We need to look to see if the work we're doing in DDoS mitigation framework, the work we're doing with DDoS mitigation workshop are part of the charter and if we need to change the charter to support that kind of work to see if we need to do that.

---

There has been a request from the LAC region to do a DDoS workshop, and we need to see if TLD-OPS is going to participate in that or not. So we need to have a discussion around that.

Once we've done all that, then we need to look at the objective for the next ICANN meeting, what we want to achieve there. There were talks of doing another workshop [by] DDoS mitigation workshop, so we need to see if we want to do that or not.

Then at the end, we'll write a summary of this meeting. At the end of the workshop, I wanted to have a quick discussion on the framework, but there is the Ethos Awards. So we'll try to wrap this meeting up by 8:30 and then go over there.

What did I do?

UNIDENTIFIED MALE: [inaudible]

JACQUES LATOUR: But I can't get the mouse there. Yeah, but then it scrolls. All right, so what is TLD-OPS? It's a global mailing list. It's a list of all the security contacts for all the ccTLDs. That was put together to create a community and a medium for us to reach everybody through a mailing list.

---

It's meant to have all ccTLDs on the list, so those that are part of this ccNSO, part of ICANN or not, our goal is to bring everybody on the list together. We have about 240 people on the list, so that means twice a month we e-mail everybody in the community with the list of 240 contacts – their name, their phone number, e-mail address, and all that. So if we need to reach somebody in a different ccTLD, then we have access to all the contacts around the planet that are part of this mailing list. We have 189 ccTLDs on the list so far. Our goal is to have every ccTLD on this list, so we're trying to work on that.

The goal here is that if there is a security issue and we need to raise awareness in the global ccTLD community that this might happen to your ccTLD, then the objective is to send an e-mail on the mailing list so that everybody is aware of security issues that might impact them. So it's a collaboration. We're still trying to work on getting more and more people to use the list for that purpose, but we're making a little bit of traction so far.

The idea is to build some process to have this mailing list as part of the ccTLD incident response process so that if there's an incident impacting your ccTLD, then you can use TLD-OPS to notify other people. So try to make the use of TLD-OPS as part of the incident response process for your ccTLD. That's one of the main objectives of TLD-OPS.

---

That's the e-mail. That's what it looks like. Twice a month, we send this e-mail to the list. It contains the details of all the TLD-OPS members – the name, the phone number, the e-mail address, and all that. The idea is that you have access to this list offline through your e-mail so that you can reach anybody.

One of the main issues here is that if you're under attack or if you're under a DDoS attack or something happens to your ccTLD, typically you won't be able to reach out to anybody through e-mail or something like that. So the idea is that you can find easily the phone number of a trusted contact and text them or e-mail them and be able to reach out to them to let them know that you're under an attack or something. They can reach out to the mailing list and let them know that you might need help to resolve an incident. Just a little bit of an additional layer of information to help mitigate attacks or security incidents in your registry.

I think this is the longest list of alerts and queries we've had on TLD-OPS since it has been in use for about a year now, a year and a half, two years? TLD-OPS, the mailing list running?

CRISTIAN HESSELMAN: We started back in 2015 somewhere, so two years.

---

JACQUES LATOUR:

On this list, this is a summary of all the e-mails or issues that were exchanged on the mailing list. I won't go through all of them in detail, but the main one is we had a DDoS attack on a registry and they shared the details of that and heads up for other ccTLDs about what the attack was. So that was a good notification.

Another registry had a frontend day zero vulnerability, and that was notified to the list with the details of the day zero attack. It's kind of important to share that kind of information. Day zero is something that there is no software patches for, so letting everybody know that if you're running this piece of software on your registry, you might be vulnerable to attack, that's a good thing.

We had a bunch of alerts about DNS traffic spikes or traffic pattern happening, latency issues. There was more and more information shared on the list, and that's a good thing. We need to make sure that we get this kind of traffic going, and we need to find a way to get people not to be afraid to share on the mailing list. I think that's one issue we need to figure out over time.

Stats. I went through Cristian's spreadsheet to look at how we calculate all of this. It's pretty cool. We have right now 189 members. We're missing 102, so we're at 65% penetration

---

overall on ccTLDs. If we look at the different regions, there are some gaps we need to work on. There are a lot of small ccTLDs that we need to reach out to through personal connection or through some mailing lists to reach out to them. Over time, we have been trying to get more and more ccTLDs to join. The tail end is more on the smaller ones, and they're the ones that are difficult to reach. We'll keep trying to get them on the list.

We need to work on Latin America, Africa. We need to have more focus there. We tried some things last time. We sent postcards. It's a nice postcard. I think we showed it at the last ccTLD.

CRISTIAN HESSELMAN: We did.

JACQUES LATOUR: That didn't work out too well, so I'm not sure what the next strategy is going to be on getting more people to join.

So it's a global incident response. We're building a community of security contacts for and by ccTLDs. The idea is that every registration is individual. It's people registering to the mailing list their security contacts, their names and people and face. It's not meant to be a generic e-mail address like security@nic.whatever as a generic mailing list. The idea is that

---

people are on the list, and you can reach out to an individual by ccTLD and have a real community around this.

Right now, it's just a mailing list. It's a Mailman, and it seems to work out pretty well for our purpose. It's easy to join. We have a well-defined procedure on how to connect to and how to join the mailing list.

All right, now we're at Agenda Item 3. We have an action list. Do we show it?

UNIDENTIFIED MALE: No because we don't have it.

JACQUES LATOUR: So we have Action Item 66, which is when to reach out to Greenland and try to get them to join the mailing list.

CRISTIAN HESSELMAN: That reads [Patrick], but he's on vacation. I'll follow up with him when he gets back next month.

JACQUES LATOUR: Okay.



---

CRISTIAN HESSELMAN: We had an old contact, so I'm not sure if it still works but [inaudible] contact.

JACQUES LATOUR: Okay. Action Item 68 is to add singular e-mail address to the name field. That's from Fred. That's his action item. He did send an e-mail about this, and he said that he needs to fix the formatting on the Mailman. He wrote a script to fix that, and it's possible to add singular e-mail address for all contacts. The reason for the singular e-mail address is to have a generic, non-ccTLD e-mail address or a different ccTLD. So if you're ccTLD is down, then you can reach the same contact through a Gmail address or something. That's the reason. So we'll leave that one open.

Action item [7E] is for me to arrange an informal launch meeting at ICANN59, and I didn't do that. So I'll try that for ICANN60.

UNIDENTIFIED MALE: Okay.

JACQUES LATOUR: Sounds good. ICANN60. That's it for the open action items. Agenda Item 4, TLD-OPS status and operating issues. Kim?

---

KIMBERLY CARLSON: I don't have anything new since the last time we met.

JACQUES LATOUR: Thank you. Agenda Item 5 is to talk about the TLD-OPS charter and figure out where the DDoS mitigation framework is. A little bit of a background on this. At the last ICANN meeting, Copenhagen, we had a DDoS mitigation workshop. We had about 60 people in a room, and we spent about half a day going through a real workshop and going through how to mitigate frameworks. Out of that, we had a bunch of action items for the mailing list for TLD-OPS to look at and to work on with the community to create a better environment for a ccTLD to mitigate DDoS.

The issue is that the charter for TLD-OPS is to run the mailing list and to maintain and operate that list and building... So the first one is hosting or having TLD-OPS run DDoS mitigation framework. We need to see if that's part of the charter or if we need to change the charter. We need to look at the TLD-OPS charter to see if it supports the framework. We need to look at the charter to see if it supports the TLD-OPS doing workshop, and we want the charter to support us building a framework for DDoS attacks. It's pretty easy to change the framework, but we need to figure out if this is something we actually want the group to do.

---

CRISTIAN HESSELMAN: I think that in general it would be smart to have a look at the charter anyway because it has been out there for two years and we've done a lot of work. So it might be a good thing to revise what's in there. For example, it doesn't mention at all that we're also sharing security alerts on the mailing list, and it purely focuses on the contact repository function. So we actually broadened a little bit already.

JACQUES LATOUR: Just taking some notes here. So how do we go about revising the charter? Do we create a small group and then we create an action item to revise and propose a new charter for TLD-OPS, and then we get next ICANN meeting to review and approve?

UNIDENTIFIED MALE: [inaudible]

JACQUES LATOUR: Yeah?

CRISTIAN HESSELMAN: Yep, it needs to go through [inaudible].

---

JACQUES LATOUR: But that would be the procedure? So who wants to volunteer in reviewing the charter and create the next version of this for the next ICANN meeting?

UNIDENTIFIED MALE: I can do that. Just need to find out what to put in there, what do we want to do exactly. To me, we already started moving out into different areas of security and cooperation between TLDs. I think that would be a more broad definition of what we want to do, simply because the mailing list is now running so we have a bunch of really active people so [inaudible] more stuff. So I think that's [inaudible] to give them more work, and anything in security and cooperation between TLDs sounds like a good idea for us to do.

JACQUES LATOUR: Okay. Kim?

KIMBERLY CARLSON: Bret is on the Adobe Connect room, and he has volunteered as well.

JACQUES LATOUR: Who?

---

KIMBERLY CARLSON: Bret.

JACQUES LATOUR: Oh, Bret. Perfect.

UNIDENTIFIED MALE: I could use a co-Chair.

JACQUES LATOUR: Well, I'll be –

UNIDENTIFIED MALE: [inaudible]

JACQUES LATOUR: Yeah, but you just volunteered to be the Chair of that, right?

UNIDENTIFIED MALE: Of the sub-subcommittee.

JACQUES LATOUR: The prime of the sub-subcommittee? Perfect.

I guess the main components we'd look at integrating into the charter would be to share security events on the mailing list, to have security-related workshop – it doesn't need to be DDoS

---

specific, but it can be anything – and to look at building a framework or to build process and procedure that could be used by all ccTLDs to improve their security posture. So generally that would be the three main areas. Okay? So we'll create a new action item with that, and then we'll propose our charter at the next ICANN meeting. Good.

So we have eight minutes left. Number 6 is we had a request from LAC region and NIC.CR for the TLD-OPS group to participate in a DDoS workshop at their next LACNIC or LACTLD meeting in Costa Rica at the end of August. So we had a bit of clarification around that and the ideas. Initially, we thought they wanted a TLD-OPS workshop only. That means only members of TLD-OPS would participate in that workshop. But they want to have a DDoS workshop that's open to everybody, and they want the expertise of somebody from TLD-OPS to participate at the workshop.

I guess we're looking for a volunteer to participate in that workshop in ICANN at the LACNIC meeting. We'll share an e-mail with the mailing list to see if somebody is willing to participate [on] the steering committee. Since it's not 100% just TLD-OPS workshop, I guess it's just a voluntary basis to see who wants to attend or if we can participate. So we'll put a request out there to see who wants to be part of that. There's supposed to be a meeting this week that's going to get organized with NIC.CR,

---

LACTLD, and some of us, so we're still working out the details of that workshop [inaudible].

Number 7, objective for ICANN60, do you have a slide on that?

CRISTIAN HESSELMAN: No, I don't because that was the preparation work that we did.

UNIDENTIFIED MALE: Yeah.

CRISTIAN HESSELMAN: I think that one of the key objectives would be to revise the charter, of course. That was the important thing.

JACQUES LATOUR: ICANN60, revise the charter, and I guess what we could also do is, if we have time, we could go over the DDoS mitigation framework, maybe look at that as a first pass and see how that would integrate into the work group. So I guess those would be the two main objectives.

We also talked about doing – the next ICANN meeting is an A. It's a big one, and we talked about hosting another DDoS mitigation workshop. So that's something we need to think of. It's a lot of work to plan.

---

ABIBU NTAHIGIYE: I can see the request by LAC region for the workshop and from the membership records I saw on your slides, two of the regions have low membership: Africa and LACNIC. So I would suggest that if we are thinking of a workshop, then we could put the focus or our workshop or priority of the focus in Africa region as well. So we can communicate with the AfTLD for the possible workshop in Africa as well so that we can increase awareness and have more members in Africa.

JACQUES LATOUR: So would you see the workshop as part of the ICANN meeting or as part of a region specific TLD event?

ABIBU NTAHIGIYE: I think it's better if we have region specific because with a region specific probably there could be more member attenders compared to the ICANN meeting. The good thing is we have the AfTLD Chairman here. Maybe he can contribute to that.

CRISTIAN HESSELMAN: Also, we organized the workshop in Copenhagen. We have all the basic material in place to reorganize it again. The only thing we need is people to carry out the organization because everything



---

is there like invitations, agenda, and all that sort of stuff. So the templates are all there.

UNIDENTIFIED MALE: Thank you. I think that I support the idea from Abibu.

Dot nz, I'm acting as Chair of AfTLD. It could be interesting because we are trying to have some local events in Africa. One we have at the end of the month is [Africa Day], and we suppose also to have other workshop dealing with ccTLD issues. So we are very interested, and we can get in touch with you to see exactly what agenda we can set up with you.

CRISTIAN HESSELMAN: You'll need to get into contact with Jacques, but I was just saying that the entire format is already there. So it's basically organizing it and setting things up. We've already tried it once, so we know that it works. So that will reduce the amount of work on your side.

UNIDENTIFIED MALE: Makes sense.

---

JACQUES LATOUR: Okay, so we need to add that to the charter: preparation or having a kit that we can use to do a security-related workshop for ccTLDs.

UNIDENTIFIED MALE: Okay. Well, that's enough for the next meeting.

JACQUES LATOUR: So summary: we need to prepare the – that's your favorite, that's the thing you're good at – preparing the summary call, right?

CRISTIAN HESSELMAN: Are you giving me an action point? Your last one?

UNIDENTIFIED MALE: Sorry, question. Is it the objective having the revised charter by ICANN60 or considering the revision of the charter during the ICANN meeting?

JACQUES LATOUR: I think we need to propose a new charter that includes the workshop. Then if that gets approved at the next ICANN meeting or before at a Council meeting or something, depending on what the timing is, then we can actually start planning how we would

---

do this if the charter allows the group to do this kind of work.  
Yes?

UNIDENTIFIED MALE: DDoS attack is just one of our security [tracks] to the [DNS], so we don't need to be specific because it is the only [track] we have. So I think it is better to broaden the security issues like some malicious change of DNS [inaudible]. There are many [tracks] we have to consider, so it's better to have some time to specify which DNS [track] we have. After listing up, we can have some measures to take. So I think it is not just the DDoS that is the issue here. That is some of the security issues we are watching frequently but, however, I don't think that is the only security issue in this [phase]. Thank you.

JACQUES LATOUR: Yeah, I agree. So the charter will talk about hosting security-related workshops, and then over time it would be the flavor of the week that we need to talk about – so DDoS or ransomware or vulnerabilities in the DNS that we need to address and stuff like that.

UNIDENTIFIED MALE: For that issue, maybe CIA – confidentiality, integrity, and availability – will be [inaudible] some criteria we can consider

---

from the security perspective. DDoS will be one of the attacks to the availability, so we can have some more time to think about that perspective.

JACQUES LATOUR: Okay. Another aspect I was thinking of also was to develop a maturity model for ccTLD to assess themselves to see where they're at on the security posture point of view. So having something that a ccTLD can use to say, "These are the main things we need to focus on by priority," and then probably have a workshop related to getting around those topics too.

All right, so summary, Number 8 – oh, we're done. So summary for the TLD-OPS meeting?

CRISTIAN HESSELMAN: I think the key thing that we talked about is the revision of the charter, and there were actually other elements associated with that: the workshop and the DDoS mitigation framework. So I think that the charter revision is the main topic of today. And perhaps you could add that we discussed the goals for ICANN60. I think those are the two key takeaways for today.

JACQUES LATOUR: Perfect. Thank you. Any other business? Yes?

---

ROLAND LAPLANTE: I'm Roland from Afilias. We do the technical support for a number of ccTLDs. One of the great opportunities I think we have at this meeting is recruiting more African ccTLDs. I can't remember from the chart earlier that you showed, Jacques, about the penetration of membership of African ccTLDs here, but when I look at the attendance list for this meeting, there are a lot of African ccTLDs here. I wonder if it might not be a goal to try and sign up half of the remaining ones or something. Every time we see somebody from an African ccTLD, we should talk about this with them and just get them on the list. Because it doesn't cost them anything, and it's all positive. So I guess I'm wondering.

JACQUES LATOUR: I agree.

ROLAND LAPLANTE: It might be a little bit of a recruiting drive here for the folks that are in to get other people to do it.

JACQUES LATOUR: All the ccTLDs you operate, are they in TLD-OPS?

---

ROLAND LAPLANTE: I don't know if they are or not. I was going to check with Kimberly to see who's in or who's out.

JACQUES LATOUR: Okay. I have the list, so that's something we can check.

ROLAND LAPLANTE: Perfect. I'll stop and check with you afterwards.

JACQUES LATOUR: All right. So Copenhagen, we had [sticker] – oh, sorry, Warren.

WARREN KUMARI: What might be useful is if we could actually just bring up the list of missing African ccTLDs so that we can just look at it now and if we see somebody wondering around – I don't know if that's easy to do or not.

JACQUES LATOUR: It's on the website. The list is live on the TLD-OPS website, so you can see the list there.

ERWIN LANSING: I just want to add for the workshops, we're talking about Costa Rica and Abu Dhabi, to have them open. The last one in

---

Copenhagen was only for TLD-OPS members. We have them open for any TLD would be a good idea, especially in those regions to recruit more members. I think we should try that. We closed it because we wanted to be able to trust [between ccTLDs] for only the ones that are on the list. I think especially for those reasons it would be good as a recruitment opportunity.

JACQUES LATOUR:

Oh, yes, definitively, having an open meeting would be. If it's not just TLD-OPS, then we've got to make sure people understand the rules when we're at the workshop.

At Copenhagen, we had something very simple. We had stickers, right? We had TLD-OPS stickers on our badge, and that's how you can tell. People are asking about how do I get a sticker because people like stickers for some reason. That was a great thing to get people actually, so maybe next meeting we should have always TLD-OPS meetings at the stickers. Then that's how we do some recruiting.

Any other? That's it? Well, I call the meeting to a close. Thank you.

**[END OF TRANSCRIPTION]**