EN

COPENHAGEN – GAC PSWG Presentation to the GAC Plenary
Tuesday, March 14, 2017 – 13:45 to 14:30 CET
ICANN58 | Copenhagen, Denmark

CHAIR SCHNEIDER: Welcome back to the afternoon. And we're again with the PSWG, so I will right away give the floor to Cathrin. Thank you.

CATHRIN BAUER-BULST: Thank you, Thomas. And good afternoon to everyone. We have four points for you this afternoon. Next slide, please.

So we want to provide a brief update on the recent activity of the GAC Public Safety Working Group. We want to update you on what's happening on abuse mitigation and the follow-up to the GAC advice and the cross-community session we had here yesterday.

We want to briefly update you on what's happening on the security framework for registries to respond to security threats notified to them. And then we're hoping to also briefly cover the status quo on the privacy proxy services accreditation disclosure framework as time permits.

And you should have briefing materials for all these points in your briefing pack.

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.

So moving on to recent Public Safety Working Group activity, we're aware -- and this has come up several times already throughout the meeting -- of the immense workload that everybody is under and the challenges that people have in keeping up to date with all the different work streams that the GAC and GAC PSWG members are involved in. So we have tried to find different ways of, basically, handling summaries for people to catch up on the work without necessarily having to go through pages and pages of documents to understand what exactly is happening on given processes and to find a quick way back into topics that maybe you haven't followed for a month or two or longer to, basically, find your way again.

So, as part of that we have started writing an activity report to the GAC where we have a very short two to three sentences update on where we stand on a host of different issues and then with links to further information.

Now, this you may have seen it was circulated on the GAC list a little while ago on the 7th of March. And we received very positive feedback already from among the GAC as to the usefulness of this exercise.

So, if you have any further comments on this or any further discussions about the format, topics you would like to see

EN

covered, the level of detail, we would very much welcome those via the list.

Then we have also created a Public Safety Working Group newsletter where we try to explain in a little more detail also to stakeholders outside the ICANN community what is happening and why the work that is going on, especially when it comes to public safety issues, can be extremely relevant to stakeholders who are possibly not able to participate on a regular basis in ICANN meetings or even remotely but who still should have a possibility to weigh in on issues that directly affect them and the policies or processes that they're in charge of.

So what we've proposed is to -- we've issued a first version of this. And it was sent to the GAC already before the ICANN meeting. We're going to try to do them again for the following meetings. And we hope that also this will prove useful and would encourage you to also circulate this further to your stakeholders as you see appropriate. So it's really deemed for -- it's destined for public consumption what to explain a bit better what's happening here. Those are sort of our outreach activities as a GAC Public Safety Working Group to you and the rest of the community. And, as part of those outreach activities -- and, particularly following up on GAC advice that has been given several times on DNS abuse mitigation, we were also able to sponsor -- the GAC was sponsoring a cross-community session

on abuse mitigation yesterday, which was very successful. And for more details on this, I'm now going to turn to Bobby Flaim who was leading our work on DNS abuse mitigation. Please, Bobby.

BOBBY FLAIM: Thank you, Cathrin.

So, yes. Yesterday we had the cross-community session on abuse mitigation right here in this room. It was actually a very, very productive session. Hopefully, you were here to hear it. Because the room was full; so, obviously, the attendance and the interest was there.

This also reflects a lot of what we had done in Annex 1, if you remember the Hyderbad GAC communique had Annex 1. And it dealt a lot with DNS abuse mitigation and, in particular, following up GAC advice through the registrar accreditation agreement, the registry agreement.

Some of the concrete outcomes that came out of yesterday's session was to see how we can foster contractual compliance and the security team from ICANN to work a little bit more closely and exploring how they can combat independently abuse mitigation or combat abuse, rather.

Another thing was the ICANN CTO is working on some independent industry-wide abuse reporting system. They reported that that's in a beta phase right now. But that is something we believe would be very helpful. And this also syncs up with what the CCRT is doing, the Competition Consumer Review Team. So we're hoping to marry those two efforts to get a more robust approach, more robust statistics, and also better information on the state of play, if you will.

One of the other things that we discussed yesterday was ICANN has about half a billion dollars in auction proceeds from the new gTLDs. And we brought it up as a point of consideration whether that could be used for any DNS abuse mitigation, whether that's marketing, whether that is giving more money for ICANN to do things that the security and review team can use, whether the security team of ICANN itself can use it for more funding, more staffing to investigate abuse, to treat abuse, whether it's a system for registrars and registries to tap into because we know that cost is a very big factor in combating abuse. And we don't want to disproportionately affect registries and registrars in combating this problem. So maybe that auction fund could be used for that as well.

Just for consideration -- I know there's some policy proposals and some working groups right now considering that. So maybe the GAC can provide some input on that.

Lastly, there was one concern that was mentioned by a couple people. And this, actually, is something that's very important. It's where you have bad actors, registrants in particular, a nefarious person, a criminal, that basically just hops from one registry or registrar to another. The problem isn't being solved. The registrar is being penalized for lack of fees. And how can ICANN, how can the community work to mitigate that?

Those are some of the big takeaways from yesterday's cross-community session. And we're hoping to have a bit more after action and follow up on these. And we certainly look for GAC assistance and input on that as well.

So dovetailing into right that and going into our next topic concerns the Annex 1 that was issued by the GAC in the Hyderbad communique in our last meeting.

Just to give you a little bit of background, the reason the Annex 1 came into being is that the GAC has issued prior GAC advice starting in 2009 with the law enforcement due diligence recommendations, a lot of which went into the 2013 registrar accreditation agreement.

Second piece of GAC advice that we were hoping to follow up on through the Annex 1 was the registry agreement, the new gTLD registry agreements. And, if you remember, in the back, the Beijing GAC communique, there was safeguards, GAC safeguards

that were addressed and actually put into the registry agreement, in particular Spec 11.3b.

So in November, in Hyderbad there was a series of questions in the Annex 1 on how ICANN is following up on this GAC advice. Because some of the provisions of the 2013 RAA have not been implemented yet. Here we are four years later. So we were just asking how that is coming along, when can we expect implementation?

Also with the registry agreement and the GAC safeguards, one of the things registries were due to do was report back on any abuse statistics, how they're combating security problems, and how those reports sent to ICANN. But we haven't seen those.

So what we're really questioning or really trying to do is see what the effectiveness of GAC advice is.

And that's the purpose of what we're trying to do, especially through the Annex 1.

So can we go to the next slide?

So what we did is we provided ICANN with the Annex 1 at the last meeting. And on February 8th, ICANN replied to the GAC questions.

Unfortunately, a lot of the responses provided by ICANN were not sufficient. Some weren't answered or there was not enough specificity to actually answer the question in full.

In particularly, about the WHOIS accuracy provision of the WHOIS specification of the RAA. That was supposed to have been enacted and implemented about three years ago. And ICANN did look into the matter, and there was some talks with registrars. But nothing came of it.

So we asked about that in Annex 1. And ICANN has replied that they're going to start that process again. But it would be a little bit more helpful if there were more specifics surrounding that.

With the registry agreement and the answers that were provided, we're still looking for more specificity, more substance when it comes to the contractual compliance of enforcement complaints. And also the reports, the reports that the registries are generating per Spec 11 of the registry agreement, are those reports being helpful in mitigating abuse? Are they helping the security team? Are they, basically, accomplishing the goals in which the GAC set out? So those are some of the -- part of the analysis that we are working on and will provide to the GAC.

So the next steps is that we will provide an analysis of ICANN's answers to Annex 1 and pass that to the GAC. And we're looking to see how we can be effective in getting more specific answers.

And one of the things we thought about is maybe having someone from the GAC appointed to work with ICANN to develop a scorecard to track some of these issues that were addressed in Annex 1 to ensure that the implementation is complete and GAC advice has been followed to the best efforts possible.

So that was it. And then, pursuant to that, we are going to meet with the ICANN board tomorrow.   So the analysis of the questions and this proposal to have a scorecard with maybe someone from the GAC to follow through on that, would be something that we would mention tomorrow.

CATHRIN BAUER-BULST: Thank you, Bobby. Just to clarify on the scorecard, this would sort of be in addition to the general scorecard that we have for the implementation of GAC advice? We've tried to come up with something more specific to actually track the answers to the questions that were asked to the ICANN board.

And where we've also provided some more details on what exactly might be examples of types of data that would assess us the efficient and effective implementation of GAC advice on these familiar and quite technical issues. One central concern here that I'd like to raise now is that really comes back to GAC advice on the whole, is that, when we've submitted GAC advice,

it has turned into policy, in particular, policy that has a public interest background, this policy, of course, now has been mostly turned into contractual clauses between two private parties that don't necessarily fully share the same interests.

So, in a sense, in implementing these clauses, we, as the GAC, still have an important role to play in holding the parties accountable and in asking for the right levels of transparency to actually be able to assess that what has been added on paper at our request is actually also implemented in practice. That's the type of transparency and accountability that I think is still missing from many parts of the contracts, in particular, when it comes to the public interest side of things.

And that's where we think with this process we can make a concrete step forward and establish some standards for how such accountability and transparency can be created.

And we very much, of course, hope that you would all share this suggested approach.

BOBBY FLAIM: The other thing that's not directly related but related to abuse mitigation is that one of the things that we as PSWG have been able to do is work very effectively with ICANN and the registrars and the registries in operational matters.

ICANN 58
COMMUNITY FORUM
COPENHAGEN
11–16 March 2017

One that we spoke about yesterday was Avalanche which was a very big cybercrime case where we worked directly with ICANN, the security team, and the registries. And a lot of that came from our work here.

And the one thing I guess I'm asking of all of the GAC representatives here is that, if we can encourage your law enforcement from your -- you know, in capital in your respective countries and also your public safety officials to get more involved, especially when it comes to cybercrime and abuse mitigation, because that is where the rubber meets the road. That's where there's a lot of applicability. That's very, very important.

I wanted to make that pitch. Because a lot of times, when we're doing these policies and contractual obligations, it gets a little bit lost and a little esoteric and a little bit cloudy. But there is a lot of real world applicability to what we are doing here with cybercrime. So I would just encourage all of you, if you could talk to your national police and especially your cybercrime agents, this is something that is very important and actually will get a lot of benefit in combating cybercrime on very specific cases. So I just wanted to add that one point.

CATHRIN BAUER-BULST: Thank you, Bobby.

Are there any comments, questions, remarks on the abuse mitigation point?

Okay. Then we can move on to a brief presentation on the security framework for registries where we can start seeking your endorsement again. I'll turn it over to Iranga for that one.

IRANGA KAHANGAMA: Thanks, Cathrin. To give you a brief overview, the security framework is coming from the new gTLD safeguards creation of a framework for how registry operators can respond to security threats. It's been an ongoing process for about two years now. We were put together in August 2015. There were multiple versions that went back and forth. And I think since Hyderabad the last iteration a very successful draft has been emanating. And I think -- I'm very confident that we are very close to an agreement on draft language that we've worked on. We met with the registry operators once early on during this ICANN meeting. And then each side, both the registries and Public Safety Working Group, were given private meeting time to do their own consultations. And then yesterday we finalized, as a PSWG, edits that they had submitted to us.

So there's going to be one more final meeting at 5:00 today. It's an open session with both sides coming back to the table. And then we're going to hash out any remaining issues. But that

draft proposal is looking quite optimistic. And it looks like we're getting very close to an agreement.

 Can we go to the next slide, please.

 So to give you a little bit of an idea of the framework, it's a voluntary practices document, best practices document for how registry operators can respond to security threats. As the PSWG, we have given insight into a number of common ways that we've work with registry operators and things registry operators have done in response to security threats. In addition to outlining the specific actions and methods that registry operators typically take, we also tried to put a framework together of defining certain high-risk categories of security threats, and then suggested timelines for responses and issues such as what the content may -- may be.

 So -- And then how to prioritize those requests, and then communicate that effectively so that both the registry operators and the public safety law enforcement agencies are on the same page and able to mitigate the threat in as best and efficient way as possible.

 In terms of process, as I said, we're having a meeting 5:00 today where we're hoping to finalize the language. Should we finalize the language there or shortly after, from our perspective, the next process item would be to come to the GAC, propose it to

ICANN 58
COMMUNITY FORUM
COPENHAGEN
11–16 March 2017

you all and then have the GAC comment on any edits as necessary.

So once you all are able to take a final look and we endorse it, then we'd move on from there to a public comment period. And then obviously if the public comment period brought up anything significant that would change the outcome or the content of the document, we'd bring it back to you all for formal approval.

But as I see it right now, I think either by the end of this meeting or shortly after the end of this meeting, both the Public Safety Working Group and the registry operators should be close to final text for submission to the GAC.

Happy to take any questions.

Thanks.

CATHRIN BAUER-BULST: Thank you, Iranga.

Okay. If there are none, then we can take a couple more minutes for the update on the privacy/proxy services accreditation.

Nick, do you want to come up here or do it from the floor?

NICK SHOREY: I'll do it from the floor, if that's all right with you.

Okay. So privacy/proxy services. We're now at the implementation of the policy phase. The GAC will recall that there was advice submitted against the final recommendations for our privacy/proxy services accreditation where the GAC stated that there were certain elements of the recommendations that were of concern. And the suggestion was that we could address these in the implementation phase, and the board agreed. And so now there are several GAC representatives on that implementation team.

We were tasked to develop a straw man proposal for a disclosure framework. So we've had a small team working on that over the last two months or so. That's still ongoing. We've sent some initial ideas around the PSWG for feedback and comments. And then once we've got something in -- in sort of good order, the plan is to send it to the GAC, the full GAC, to get -- to get agreement and approval from the full GAC. And then we can send it back to the IRT team. And then it will be further discussed and debated.

So that's -- that's pretty much the status. My question to the GAC is when our little team has got our -- has got our proposal doesn't, does the GAC require to see the -- see the documents and approve it before we send it to the IRT or would they be

happy with us, in the interest of time, to give it straight to the IRT where there may be further sort of discussion and debate around elements that we propose before we get any final document, final policy stuff that would go out for public comment.

So it's a question to the GAC, really, just on process.

Thank you.

CATHRIN BAUER-BULST: Thank you, Nick. And I'll pass that question to the floor.

So the question is really there is a straw man proposal which is a rough outline of what could become the basis for a law enforcement disclosure framework which will be subject to a lot of further discussion and will, of course, also be submitted for review as it matures through the process of work with the IRT team. And the question would be to what extent you want to take a look now or whether you want to wait until the work has matured a bit further before taking any views or opinions on this document.

Does anybody have any views on this?

Let me ask it a different way. Does anybody feel strongly about taking a look at the document now? Or would you -- Yeah. I'll

ICANN 58
COMMUNITY FORUM
COPENHAGEN
11–16 March 2017

leave it there. Does anybody feel strongly about taking a look at the document now?

CHAIR SCHNEIDER: Thank you, Cathrin.

Well, to answer -- to answer Nick's question, basically whatever goes out as a formal document needs to be validated by the GAC. There are different ways that can be done. One is for adoption at the meeting. One is for an online procedure where you give them a certain amount of time and nobody objects, then it's -- then it's adopted.

If this is urgent, maybe if we have time, why not have a look at it now and then see, give people a chance to quickly check whether they are fine with this or under what conditions they would be fine with it.

Thank you.

CATHRIN BAUER-BULST: Nick, is there something that you could share now?

NICK SHOREY: Well, I wasn't planning on sharing anything today, but my plan was to sort of get some feedback from the PSWG and then circulate sort of the product of that to the GAC on the mailing

list. And sort of as Thomas suggested, like open a period for GAC comment before we then send it back.

 But I'm just wondering if -- you know, if people feel strongly that they would want to have the -- the full GAC would want to have the opportunity to do that before we send it to the IRT, mindful that then we enter a period of sort of further discussion with the members of the IRT, and there may be a risk of a kind of a back-and-forth between the IRT and the GAC. And in the interest of workload, I wanted to know sort of what the best way of going forward was.

CHAIR SCHNEIDER: Thank you, Nick. Well, as I said, if something is a formal document, no matter what stage, it needs to be validated by the GAC.

If it's just a brainstorming, very first draft of something and clearly marked as such, you can share it with others. But if it's -- if it's considered to be a document, an input document that is a formal document, it needs to be validated by the GAC in one of these ways. That doesn't mean that we have to take two months to validate it if there's nothing controversial in it. But people need to be able to see it for a few days, at least, and then -- okay. Thank you.

CATHRIN BAUER-BULST: I think Kavouss had a question.

IRAN: Yes, and the expression says when the oven is hot, put your bread on. Yes, oven is hot but the bread is not prepared. So let us have it, think it over, and come back. Two months, one month, two weeks, two days, two hours, but we are not prepared to do it now.

Thank you.

CATHRIN BAUER-BULST: Kavouss, we appreciate your flexibility.

Thank you. So I guess we'll share the document, and then also based on your reactions, we can gauge whether this is the type of early brainstorming document you would rather not be bothered with in the future or whether really you find this helpful to also take a look at these early documents.

So we will share as soon as it is ready for sharing and then give you two hours, two days, two weeks, some appropriate time frame to take a look and come back to us with comments. And we very much look forward to your input on this and on the other files.

ICANN 58
COMMUNITY FORUM
COPENHAGEN
11–16 March 2017

And let me just come back to the newsletter and the update and the meetings here. We really want to do what we can to support you in shouldering the immense workload. So do let us know what we can do differently, what we can do to support you most effectively in the work of the GAC.

And thank you for your time here.

Thank you.

[END OF TRANSCRIPTION]

ICANN 58
COMMUNITY FORUM
COPENHAGEN
11–16 March 2017