ICANN70 | Virtual Community Forum – GAC Public Safety Working Group (PSWG)
Tuesday, March 23, 2021 – 10:30 to 11:00 EST

GULTEN TEPE: I see it's the scheduled start time. Technical support team could you start the recording?

Welcome to the ICANN70 GAC PSWG update session being held on Tuesday 23rd of March we will not be doing a roll call today for the sake of time but GAC members attendance will be available in the annex of the GAC communique and minutes may I remind representatives in the attendance to indicate presence by updating their participant's name to reflect their full name and affiliation. If you would like to ask a question or make a comment, please type it by starting and ending your sentence with question or comment to allow all participants to see your request.

Interpretation for GAC sessions include up a 6 U.N. language and Portuguese. Participants can select the language they wish to speak or listen to. Your microphone will be muted for the duration of the session unless you get into the queue to speak. If you wish to speak please raise your hand in the Zoom room. When speaking please state your name for the record and the language you will speak if speaking a language other than English. Please speak clearly and at a reasonable pace to allow

for accurate interpretation and make sure to mute all other devices.

Finally, the session, like all other ICANN activities is governed by the ICANN Expected Standards of Behavior. You will find the link in the chat for your reference. With that I would like to leave the floor to GAC chairman, Manal Ismail. Over to you Manal.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Gulten, and welcome back everyone I hope you enjoyed your breaks. We will now receive a 30 minute update from the GAC Public Safety Working Group who will provide an update on the work of the working group and their strategic goals of the session is only 30 minutes so without any further ado I'll hand over directly to co-chairs of the Public Safety Working Group Laureen Kapin and Christopher Lewis-Evans. Both of which you've already met during the earlier session.

We will need to finish sharp because we will have the Board joining afterwards so I'll hand it over to you directly. Please. Who will be starting?

LAUREEN KAPIN: I will. Thank you, Manal. So we're going to be very mindful of time, this is a short agenda, we'll go over the work of our Public Safety Working Group which has been very active recently. We will report on our progress of the work plan, all these materials by the way are for your review on the GAC part of the ICANN website. We will talk about our participation in various work streams and then time permitting we will pick up the threads of the DNS abuse discussion that we left off with in the DNS abuse presentation.

Next slide please. So the Public Safety Working Group has very defined goals. Those are in our work plan and broadly speaking we focus on issues that, that focus on protecting the public from malicious or deceptive practices, and in that regard we have 3 primary components in our work plan, and that is to develop DNS abuse and cybercrime mitigation capabilities, and we work with our colleagues, not just around the world in law enforcement, and other public safety agencies but also with our community stakeholder groups since we can effectively do this work together by listening to one another, and ensuring that we have a full sense of those who are best positioned to deal with certain issues.

The second big bucket of activities that we focus on then has been

a primary topic of some of our work -- has been dealing with domain registration directory services which used to be known as WHOIS. And we've stated that information is very a very important tool in the law enforcement tool belt because it provides information on who is responsible for a domain, and that comes into play if that domain is involved in it activities which can be illegal, or deceptive. So it's important to know who is responsible for that, and the domain registration information can help shed light on that.

And finally our other goal is more internally focussed and that's to make sure that one, we have enough resources to do the work that we're tasked with, and two, that we are reaching out to the community and stakeholder groups, and governments to make sure that we are addressing their needs. And, if you would like to touch base with us about any issues, please know that Chris and I, and my colleagues in the Public Safety Working Group are always available to be reached via e-mail, phone, any communication device that suits your needs. We're happy to chat. The Chris, over to you.

CHRIS LEWIS-EVANS: Yes, thank you very much, and go to the next slides, please? So I just want to delve into our first goal here which is around developing a mitigation abuse capabilities of the first I want to concentrate and is two items we lump together a little bit 1.2, 1.3 here and we've made really good progress with the registries and registrars around proactive and preventive measures that they can take, and I really wanted to call out Gabriel Andrews who we heard from earlier. He's been doing some really good work with the contracted parties house around dealing with botnets that are registered by DGAs which is a domain generating algorithm. So that is very much on track work that we're doing.

The -- we've also been looking at how the ccTLDs adopt some procedures and how that can be transferred over to the gTLD space. I think we've got some good feedback so far from the ccTLDs, and now we just need to spend some time working on how this could be transposed over to the gTLD space.

Another item I think we've already touched upon in the previous session is the last one -- and hopefully at ICANN70, so tomorrow I believe we'll pretty much finish this one off and that is around the impacts of DNS encryption so primarily DNS over HTTS on DNS

abuse mitigation. Obviously, there will be further developments, but I think we've done the majority of work on that. So I -- for me that's just a quick overview on the first go. And, Laureen, over to you for the second one.

LAUREEN KAPIN: Need to unmute. Thank you. Next slide. So on our strategic goal 2 as you recall this deals with access to domain name registration data. You'll see that our great color code green means it's on track. Yellow is on hold pending some developments, and red means it's challenged, or we've run into challenges I think is more accurate. So, just to highlight a couple of these items you'll see we've signaled from the GAC that we are interested in swiftly implementing EPD phase one you know from our prior presentation that the timelines are a bit uncertain there.

We have had some good developments in interim mechanisms for reasonable access, including the fact that contract compliance now has a dedicated form for complaints about access to WHOIS data, and also reports of those complaints. So those are positive developments. You'll see we've noted the need to improve registration data accuracy, and we're hoping that those policy development work efforts [indiscernible]from with GAC input on

coping. For that policy work. In Phase 2A we are, we are focussing on efforts to correlate e-mail addresses with other domain registrations for law enforcement investigations.

That's a very powerful tool that presently is lacking, and I think -- 2.10 is the final point I'll discuss here. This was a CCT recommendation, and you'll see it's still in a red category. Essentially, we are recommending, and I say we -- where in my prior CCT review team member we were recommending the full chain of parties responsible for a domain including resellers be published in the WHOIS record and the reason that's important is that law enforcement when it's seeking information about a registrant, they need to know who to go to.

And it isn't always the registrar that might be the first link in the chain that the registrar, may be dealing with a reseller who actually then has the contractual relationship with the registrant. And it could be more than one reseller. So it's very important to actually have that information published in the DNS record. It is not required now and that was the recommendation from the CCT review team, and -- that is still something that is under advocacy efforts I will say. We're hoping that that could become a requirement rather than just an option, which is the status quo.

Next slide please, and Chris, back to you.

CHRIS LEWIS-EVANS: Thank you, Laureen. And Chris Lewis-Evans, for the record. The third strategic goal is around sort of maintaining the stakeholder relationship, and obviously detailing the work plan, I think the work plan has been well documented and we've shared it with our GAC colleagues a number of times, and as always you keep us honest to that work plan, and I think we've been able to work along that quite nicely.

I think we have struggled a little bit, and I think with everybody else, with the COVID-19 situation, and you know that's, I think impacted us in able to produce some of the collaboration resources, and share those effectively whilst also understanding experience, from across the sort of PSWG network for want of a better word. So that's certainly something that we are looking to expand, and I think Laureen will touch upon that in the next slide. And with regards to relations with other stakeholders, we've been holding bilaterals with all the other stakeholders within the community, and those have been going really well.

We've had some really good engagement across all the

stakeholders that we've had so far and some really good, interesting conversations where we've hopefully really developed some of our other goals we've highlighted. Laureen, back over to you.

LAUREEN KAPIN: Next slide please. So, as they say in the world of infomercials this is our call to action. This is where we are asking you, our GAC colleagues, to consider who are are the law enforcement consumer protection public safety agencies in your jurisdiction who might be interested in participating with the work of the Public Safety Working Group?

Actually we have, we have had 14 representatives join the Public Safety Working Group since ICANN69, and we can have even more, and we welcome you to contribute to those efforts. The PSWG is very much a contribute, as you can. And it actually -- and I think -- I always hearken back to this, but it's actually the public fundraising for the radio station here in Washington D.C. and their communication techniques are so relevant. It's, give what you can. If you can't afford a whole person, that's okay because they can actually just focus on a particular topic. They can just send it on a path.

They can just participate in our inter-sessional phone calls, which are perhaps about once a month. So we are not asking for someone to devote hours and hours and weeks and week's worth of effort. It's very very flexible and we welcome people to bring their expertise and share their perspectives with us because we all come from different points of view. So, as I said, we have one or two plenary inter-sessional meetings.

We have informal bilateral meetings with different stakeholders' groups. We have topic leads and by the way, we don't say you do this. You do that. We ask people what they're interested in. And we right now have what looks like a lot of members and indeed it is a lot of members, but I will tell you just between us so to speak, the number of members we have doesn't actually reflect the number of members who actively participate in the work.

And what we would love is to have more members who really are interested in participating in the day-to-day work, so if you have questions about that, or have folks who may be interested please have them touch base with Chris or I, and we would be delighted to introduce them to our activities and let them know what might be a good fit based on their own interests. At this point in time I want to shift and go back to some of our discussions on DNS

abuse, and if I could ask -- if I can ask to go to slide 19, perfect.

And I wanted to talk first in terms of DNS abuse on the topic that very much tracks my Japan colleague's presentation, and that is the enforcement of ICANN contract provisions and indeed our contracted -- our contracted parties themselves have pointed to enforcement of ICANN contract provisions as one of the key, and existing tools we have to combat DNS abuse, and, of course, we're in absolute agreement with using that.

And I want to look back to some prior GAC advice and I can see this is from the Toronto communique and this was before the new gTLD launch, and the GAC had advised that if there are commitments set forth in gTLD application that is those should be transformed into binding contracts, contract obligations and I'm stressing the world binding, and then in the GAC Beijing communique of course the GAC provided very specific safeguard advice about what should apply to all new gTLDs, a special subset of safeguards for GT and regulated sectors and even more safeguards that would apply to highly regulated gTLDs, and those are for example those gTLDs that deal with very sensitive topics.

The banks pharmacies, accounting, certain health organizations,

charities. Domains where you may be engaging in very sensitive transactions or disclosing sensitive financial or health data. And that is what led to the public ... commitments set forth in the registry agreement specifications 11.

And specification 11 we have certain specific obligations but as was pointed out in the prior discussion that we had regarding SSR2 recommendations there have been questions raised by ICANN compliance, and indeed the ICANN Board, about GAC's [indiscernible] from contract.

So just to drill down a little bit, the specification 11 requires -- this is what is known as a downstream requirement -- the registries require registrars to include in their agreements with registrants -- and that's why it's downstream -- it goes from the registry level to the registrar level to the person who's buying the domain, the registrant -- there has to be a provision that basically says don't do bad stuff. So that's my high level para phrase, but more specifically it prohibits the folks who own the domains.

The registered name holders, from distributing malware, botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engages in

activity contrary to applicable law and that's why I call it the do not do bad stuff provision because it is quite broad, and it has the catch all at the end otherwise engaging in activity contrary to applicable law. And importantly it provides consequences for such activities so -- says to registrants don't do bad stuff and we can get you with consequences if you do said bad stuff. So that sounds great in theory.

Next slide please. But, in fact, when you look at that, what it's requiring is basically it's a check mark. You have to include this it provisions in your contract, but it doesn't say -- it doesn't go beyond that. At least at the registry level. ie; the registry should be making sure that the registrars enforce their contracts but it doesn't go beyond that, and for the registrars they are in the position of making sure that their agreements with their registrants contain that provision. And they are supposed to act, and when I say they -- the registrars are supposed to act if there is a problem.

The other obligation registries and these are the public interest commitments as the registry level is that registries have to conduct this technical analysis to monitor for security threads like farming, phishing, malware and botnets and have to maintain

reports and if ICANN requests those reports they have to provide it to them. So where are there gaps here?

The gap is that the contracts don't specify what type of actions need to be taken in if response to these security threats. And we know that when ICANN engaged in audits and this came up in our last discussion as we will. ICANN does, in fact, audit these contracts for compliance, that they experienced some challenges in obtaining detailed information. So there are there are contract positions but there are also gaps here.

I do want to point out that in a very focused part of step 11 -- and that is what should registries do when law enforcement has a complaint or issue regarding security threats -- there has been a framework worked out -- this is a voluntary framework, ie;, it is at the discretion of the particular registry. It's not a requirement. It can't be enforced. It's voluntary framework but that is example of how law enforcement has worked together with registries to come up with a best practice to response to security threats. So that's at a high level, some of the existing obligations but also some of the gaps at the registry level.

Next slide please. As I pointed out, and I think we referenced in

the discussion in the DNS abuse session, the ICANN Board itself has raised questions to the intellectual property stakeholder group about enforcement, and I thought this was worth actually repeating because, you know you're getting it right from the source here. The contract provisions as they currently stand, and the reason I'm discussing this is I think it provides a road map for gap that is we can fill in -- it doesn't -- it doesn't grant ICANN enforcement or right against registrars who fail to include the required contract in their agreement or how to determine whether the registrars imposed consequences for the domain owners who may engage in bad activity.

So that is a gap. Also in terms of the registrar agreement, it doesn't set forth specific consequences that the registrars have to impose if their registrants are engaging in bad behavior, and ICANN enforcement therefore, doesn't have the authority to tell registrars to delete or suspended domain names or to take certain specified actions. That is not something that is set forth in the contract. ie; it doesn't say what those consequences have to be. It just says there should be consequences if they engage in illicit behavior.

And the takeaway here, I think, although I know that our

subsequent procedures review team doesn't necessarily agree -- but in 2013 the new gTLD contract provided an opportunity and contained more specific safeguards than the prior gTLD contract contained. They raised the bar on DNS abuse safeguards, and it certainly is an opportunity, if the next round occurs to advocate that that round could do even better in terms of contract provisions that are clear, and enforceable regarding obligations on mitigating DNS abuse.

And I fully take to heart that in an ideal world, as our subsequent procedures review team has stated -- we would deal with DNS abuse holistically ie; across all gTLDs, but in the meantime I think we can deal with it incrementally by focussing on how contract provisions can be improved, and if there is a subsequent round to seek improvement of those contracts as a starting point.

Final slide in my final 3 minutes, getting to the definitions of DNS abuse which I think is part and parcel, and I touched on this in the last, in the last discussion. What I really want you to take away here is that we don't need to re-invent the wheel. Here I'm borrowing someone's very APT comment we don't need to reinvent the wheel on the DNS abuse and a lot of that work has already been done and this is [indiscernible] from review team

rely on prior work done by reports by ICANN org staff. Also consensus definitions based on the contracts.

Again, those are already in the contracts. They're already existing policy, and certainly we can look to these sources to come to an agreement about what comprises DNS abuse, and lastly, our colleague Kavouss had asked to look at one of the slides again, slide 16, I wanted to put that up on the screen to allow Kavouss to follow up with any questions, and also, in our last 2 minutes, if anyone has any questions, I'm happy to take them along with my colleague.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Laureen, and Chris. I see 2 hands, Kavouss, and also Steve Crocker so Kavouss please go ahead.

IRAN: [Inaudible] sorry to take your colleagues back to the previous session. If you --

GULTEN TEPE: Kavouss, I'm so sorry to interrupt, but we cannot hear you. Your line is choppy.

IRAN: You hear me now?

GULTEN TEPE: Yes, it's much better now, thank you.

IRAN: Sorry to take you back to the previous slide. If you look into the third bullet point contracted parties, what do you think about these claims? Are you that they have limited and not always appropriate tools and so on and so forth. So I'm not going to do them one by one but what we can do about this? How we could convince them? How the situation could be improved?

It is also related to what you said 2 minutes ago that going to the provisions of the contracts, or contracted party provisions and improve them but if we want to improve them and we have this argument that they mention that they have a limited and not always what we can, could? Thank you.

LAUREEN KAPIN: It's a challenge absolutely, Kavouss. I think that first of all I don't discount some of their arguments because in in certain regards they do have limited tools, and sometimes it is challenging for them to figure out who is best positioned to deal with the abuse, and I'll give the example of when there is particularly troublesome content on a domain. Content that may be deceptive. I'll give an example of a deceptive claim about COVID-19 relief, financial relief.

That has been really prevalent currently. And a contracted party may say well we're not responsible for that content that's the registrant or that's the web host provider and in that case, I think one thing that really needs to be explored is terms of service, what terms of service does the -- is the registrar have with its registrant, and are those terms of service being enforced? And how does that relate to the current contract provisions which do create a responsibility between the registrar, and the registrant?

So that would be you know an example where we need to understand the business realities, and we also need to make sure that the existing contracts are being enforced. I also would point to some of the existing work that is going on with voluntary efforts, which we think are very useful, but don't take the place of

requirements because it's requirements that are coming into play when you're dealing with truly bad actors or havens for systemic DNS abuse which we know regrettably has occurred from time to time. Manal, I know we are a little over time but I also know that Steve has a question. I defer to you.

MANAL ISMAIL, GAC CHAIR: Yes, please, Steve, very briefly because we are already over time.

STEVE CROCKER: Thank you very much. How hard for public safety organizations to obtain the detailed registration information for domains that appear to be involved or implicated in bad behavior snow would it be helpful to require explicit response to requests for registration data. Just focused on the gathering of the date to to begin the investigation. Not the rest of the enforcement.

LAUREEN KAPIN: I know that is challenging not across the Board, ie; I'm not saying that every time law enforcement makes this request they don't get it or it takes a long time but I know there have been challenges particularly when dealing with privacy proxy providers which

demand a formal processes that a subpoena or a court order and the answer to your sec question is, yes, that would be very, very, very helpful.

STEVE CROCKER: That's three verys, right?

LAUREEN KAPIN: Yes, thank you.

MANAL ISMAIL, GAC CHAIR: Thank you very much Steve, and there is another response from Gabriel also in the chat if you would like to read it, and a comment from [indiscernible]from with that allow me to thank Laureen and Chris, thank you very much for this informative update, this concludes the PSWG update. We now have the second discussion on subsequent procedures, and please support staff let me know when we're ready to start.

[END OF TRANSCRIPTION]