ABU DHABI – GAC discussion on DNS Abuse Mitigation
Wednesday, November 1, 2017 – 10:30 to 11:00 GST
ICANN60 | Abu Dhabi, United Arab Emirates

JULIA CHARVOLEN: Hello, everybody, this is Julia. Very quickly, if you wish to have the head shot, we still have a slot open right now actually with the photographer waiting outside for half an hour. Thank you.

THOMAS SCHNEIDER: We will start in a few seconds. So please, the DNS Abuse team come up and join us. Thank you. [AUDIO BREAK]

So, please, we need to start. Thank you. [AUDIO BREAK]

Okay. This is the session number 32 about DNS Abuse Mitigation. So we're waiting for the slides. Here they are. So, let me not lose time and hand it over to Cathrin, which you all know well by now. So Cathrin, it's yours.

CATHRIN BAUER-BULST: Thank you very much, Thomas. Good morning, everyone. Thank you for coming out for this session on DNS Abuse Mitigation. In the next 30 minutes we want to discuss two main points with you that you will recognize from previous meetings. First of all, the work that we have been doing on behalf of the GAC on the

assessment of the effectiveness of the new gTLD safeguards, and then secondly we want to spend the larger part of this half hour on abuse reporting and on the work that has been going on in the context of the Cross-Community Session and elsewhere to facilitate reliable, transparent and actionable data to better prevent and mitigate abuse and to inform our policy making.

So, coming to the first find, the assessment of the effectiveness of safeguards, you may recall the session that you had with the CCT review team earlier in this week; so the consumer choice, consumer trust and competition review team on their upcoming report. And one particularly helpful piece of work that they commissioned was a report on DNS Abuse that provided a lot of insight into different trends that the review team presented at different occasions during the meetings. And that was open for public comment before this meeting.

The GAC also participated in that public comment period, Public Safety Working Group provided something to basically applaud the work of the study and to emphasize the need to do further analysis on the basis of the work done already. And what was highlighted by other public comments and also in the interactions with the review team was that when it came to assessing the effectiveness of the new gTLD safeguards the study was not yet able to go into the level of detail required to show

whether or not and to what extent the new gTLD safeguards have been effective.

So one aspect that the GAC might consider for further follow up to be able to really assess what the policy has brought in terms of benefits, what the drawbacks are, and where there might be a need for possible adjustments, would be to follow up on this work, specifically on the assessment of safeguards and how their implementation affects the level of abuse in a given gTLD.

And the CCT review team, as they have informed you, will publish its draft final report for public comment in the weeks after this meeting. So, what we would propose to do is to use that public comment period inter alea to highlight this need for further research into the effectiveness of gTLD safeguards and the possibility to perhaps commission a further study or otherwise delve into a bit more detail on specific gTLD safeguards. And we have members of the review team in the audience. So, if there are questions on this issue in particular or on anything else related to the CCT review team and its work, they're here to answer those questions.

So let me just pause here for a minute and see whether there's any comments, reactions or questions on this part. [AUDIO BREAK]

Okay. The second part of the work on the assessment of the effectiveness of safeguards was related to the annex 1 of the Hyderabad Communique, which you may remember, where we asked a number of questions to ICANN to further specify what is happening in terms of addressing DNS Abuse within the organization. And, we've had a very constructive process with ICANN to answer the questions that the GAC asked in its communique and to futher detail how ICANN's processes seek to prevent and respond to abuse.

That conversation is still ongoing at an informal level and there's still information being provided on what is happening including further granularity in terms of the information that can be provided on abuse mitigation measures by ICANN. So what we would propose to the GAC is to continue this informal process with ICANN and to continue that conversation on behalf of the GAC, and to report back at the next meeting on that one.

Then finally, you will also remember that we weighed in on the consumer safeguards role that ICANN, Bryan Schilling, the new Director for Consumer Safeguards presented himself at one of the recent meetings and was warmly welcomed by the GAC which saw an important role to be filled there. And this role is still being defined as we understand that there was a webinar intersessionally where the concepts were being discussed of the

work that the Consumer Safeguards Director could do, and where some of the aspects of Consumer Safeguards were further discussed.

And as far as we understand, this work is not yet concluded. So, what we would propose the GAC here is to continue to follow this actively and to weigh in, because as the GAC has highlighted, there is an interest in having a strong consumer safeguards role here at ICANN and that might also be something that will come up in the context of the CCT review.

So, I will stop here for a minute just to see whether there are any comments on these two points or any questions. And if not, then we should move on to the other main part of this morning's agenda to the efforts on the abuse reporting by ICANN. For this, I will turn the mic to my colleague, Iranga Kahangama. Please.

IRANGA KAHANGAMA: Thank you. To follow up from our session we've been moving along on the DNS Abuse Mitigation efforts, and as a reminder, it's one of the main goals of this is to have reliable, public actionable abuse data. This is transparent data that can be sound and be used as a guidance mechanism to inform the community of available abuse and allow the necessary and appropriate actors to act on them.

And in order to move towards them, I think that we have the concept of these abuse reporting principles. And, you know, one potential model for this is that the GAC has obviously issued principles before on the new gTLD program and the Whois services I believe back in 2007, and this may serve as some sort of model as we kind of see a lot of activity and community interest galvanizing around DNS Abuse Mitigation.

It maybe in our interest, the PSWG's interest, potentially in the GAC's interest and considering their public interest concerns to be proactive in terms of guiding and laying out what the public interest commitments would be in regards to DNS Abuse and the availability of DNS Abuse data.

So along these lines when we had done the Cross-Community Session, one thing that the PSWG had drafted for discussion was a set of potential principles at a high level, and while we did not get agreement within the Cross-Community Session, I think that there's an intersection of these principles and the GAC's concerns and interests and the public interest that may be worth delving into.

So just to give the GAC a very high level overview of some of the categories that we considered in these principles that would obviously warrant further review and development which the PSWG will be working on, will be scope of DNS Abuse, this is a

potential for seeing what would be included if it's phishing, and malware, and botnets, and working with communities such as the SSAC who have some of the more technical knowledge to determine what we can potentially include in there.

This may have overlap with I believe the Beijing GAC advice and the safeguards that were mentioned in there. You know, and similarly we could highlight things that shouldn't be included in this and that we can have a nuanced debate over what should and shouldn't be included, and how different actions and different processes could exist for different types of DNS Abuse as we kind of outlined them.

Then the others are kind of more process oriented, so when we're talking about the identification of DNS Abuse, we can really highlight some principles and standards to be set for expectations of reliability of the data, if they're industry accepted, where else they may be used, how reliable they are, and how available they're made to people. So I think these are all potential items that we as a GAC are in a unique position to identify.

I think your national governments could -- we could explore ways in which governments are using these services already within your countries to keep your citizens safe online with your telecommunications or other service providers. And these are accepted things that the governments use as tools to, you know,

keep their consumers safe. You know, they may be worth exploring. And I think looking at what law enforcement, what the ICANN organization, and everyone else is using, may be worth considering.

I think the third one is the reporting of abuse, and abuse data is an interesting concern that we should have, and we should maybe explore things like the frequency with which this data is reported. We had different members of the ICANN community on the Cross-Community Session mentioning this, too. I think reporting this in an intelligible format and having it reported on a frequent basis allows for a trend analysis to be conducted and that can have its own sets of insights that are put, up and we should have this reported publicly and made available so that members of the ICANN community can analyze the data as they best see fit. Because I think this would enable everyone to be responsible and be more informed over the abuse that exists out there.

And then finally, would be the use of abuse reporting. So trying to determine, you know, how and if abuse reporting should be used in PDPs and review teams and contract compliance and other mechanisms within ICANN. I think these are all vectors that can be better leveraged with the use and availability of data. And I think these are all public interest concerns that keep the public

safe. And it may be worth the GAC to have a set of principles that are guiding the work as this kind of work gets culminated within the ICANN community.

At a very high level, this is kind of what was included in your briefing that we submitted a little while ago,. and are the kind of general broad themes that we had revolved around and we're happy to take questions, and I think maybe the document may be loading up. But I just wanted to take the opportunity to inform the GAC of kind of the PSWG's perspective on this and that we would obviously love to seek your input and advice as we go through this process and kind of flesh out what some of the PSWG and GAC priorities around some of these themes may be.

Any questions? All right. I'll hand it back-- Okay, so as you see the document here to highlight some of the points that I mentioned earlier, these were the proposed principles that we had given, so I can just briefly run through them. We have a few more minutes.

Okay. So for scope of DNS Abuse should include misuse of domain names and DNS infrastructure that raise public interest concerns and can be addressed through ICANN policy and contracts. They should be evolutionary to address the threat landscape. Obviously, the threats we see today aren't ones we haven’t seen, and if you asked someone years ago, things like ransomware and things like that obviously had not existed, so

this is obviously an evolving landscape that ICANN should be flexible in.

As I mentioned per the Beijing safeguards and the GAC advice, phishing, malware and botnets were all mentioned there, and so stressing the need to kind of continuing this, including it in scope is important.

The issue of spam, give how much of the industry recognizes that this is a common vehicle and mechanism for other forms of malware to be distributed for botnets to happen. These are things that the DAAR project is considering, and so it's something worth noting of importance and significance.

And then the general use of trusted feeds that are used for illegal content such as child sexual exploitation materials. These are allissues of concern and things that can be nuanced and incorporated but addressed differently, and just highlighted as something as a general public interest concern. And I think developing specific principles that delineate those, give the community more flexibility to have different positions on these items.

The identification of DNS Abuse, again we want to stress the reliability of industry standards and sources, that they should be used for trends over time and include actionable metrics, things

that we can really help inform different communities to make better decision making and be responsible community members. We would like this to be very transparent, so publication on the website in a very intelligible format, things like updating it daily, and showing an allowing for identification of those parties involved in the abuse and behavior.

We think that DNS Abuse reporting should be incorporated within the policy making process. This is ultimately -- the ultimate goal is to have informed decision making based on facts and data, and to have that drive a lot of the decision making so that people can be more responsible as we mentioned before.

This would also apply to contracting and contractual compliance. Given our future amendments to the RAA, DNS Abuse should obviously be something that's considered as this is an evolutionary process and these documents are obviously ones that guide the business methodology going forward.

And then finally with contractual compliance, we always love to see contractual compliance being transparent and having the tools that it needs to be an effective mechanism within the ICANN community. We'd like to have a feedback and communication mechanism so that all the information is being fed to the proper channels so that no gaps exist, and that we could use effective DNS abuse reporting.

So this is at a very high level, was the preliminary document that we had thought of; obviously, this will change and evolve as we have more conversations, as we consult with GAC members and PSWG members and community members, but we just wanted to give you a very broad-level overview of some of the things that we're thinking about and welcome your encouragement, participation today and on mailing lists for future comments. Yes, Ashley?

ASHLEY HEINEMAN: Thank you. Could you scroll up, please? Under principles? Thank you. Under the Scope of DNS Abuse -- but first of all, thank you for giving us a presentation of these principles. I think this is very interesting and I understand it's preliminary and it will need to go through some discussion within the PSWG, the GAC and the community, but I do want to just flag as a point of concern, as it does move forward and continues to be discussed, that the last bullet under Scope of DNS Abuse, particularly a specific reference here to illegal content.

As a mother myself, of course child sexual exploitation materials is of tremendous concern and is a serious issue that needs to be addressed. But my concern is how is it going to be addressed in the DNS context and the ICANN context. So I just want to make sure that as we proceed, that we're very careful and maybe even

reconsider whether this is something to include as part of a scope section. I mean, I think it should always tie back to that first bullet which is, you know, making sure it kind of pertains to what can be done through ICANN policy and contracts.

So I just wanted to urge some caution here as we proceed and just be careful not to get into areas that really perhaps are not within the remit of ICANN. Thank you.

IRANGA KAHANGAMA: Thanks, Ashley. Yeah, I mean we're totally on the same page with you with that. We do note it and I think part of the reason the bullet is there is because we believe that, you know, within the remit of ICANN and the public interest that there can be differences where we just acknowledge that those are issues of concern that are worth highlighting for data purposes and can have a role in terms of just being identified, but that there can be nuances that are drawn versus things that you would obviously find in the first bullet.

And, you know, as Public Safety Working Group and as law enforcement, it's always tough to not address some of those concerns. But having different branches within it of that would I think easily -- or not easily but, you know, accommodate for different levels of address for those. Do you want to add to that?

CATHRIN BAUER-BULST: And just to add that this actually goes back to a comment from within the GAC also. So other GAC members have highlighted, and the UK has done it in the past, Italy has concerns related to how we deal with child sexual exploitation. And mainly this, but of course that touches upon this very complicated issue of illegal content. And of course, you see that these principles are also categorized in terms of identification reporting and actual use.

And of course, when it comes to the use, differentiations can be drawn. But just creating transparency around some of these issues might then help actors make informed choices while understanding that of course [inaudible] contracting and compliance there are very specific limits to be drawn around what is within scope of this community. Nonetheless, it might not hurt to create a bit of transparency because the people who are part of this community are the people who could choose to do something to address these issues if they were made aware of them.

So, I think that's part of -- and I don't want to speak for those parts of the GAC who are concerned about this;hey can speak for themselves of course also, but that is how we've understood these concerns in the past. Yes, we have a comment.

INDIA: Thank you, T. Santhosh from India for the recorde. This is regarding the fourth item, that is Use of DNS Abuse Reporting in ICANN policy making. So here I would like to say that DNS Abuse Reporting could also be used to amend already developed mitigation measures developed to protect the ccTLDs, both two characters, as well as the three characters; also country and territory name, geographical names etc. And also [inaudible] work upon the risk involved in releasing these top level domains, both at the TLD, as well as the second level domain in the forthcoming new gTLD program. Thank you.

CATHRIN BAUER-BULST: Thank you.

UNKNOWN SPEAKER: Thank you very much for the detailed information about the DNS Absuse. My question is about the DNS Abuse reporting. You mentioned in 4, 5, 6 bullets about the reporting procedures, how [inaudible] in the principles.

My question is that I saw on the ICANN website, ICANN also has some facility to report DNS Abuse if a registrar has no reporting, no compliance as part of the contract. And [inaudible] one to

submit complaints and there is no active response from the registrar. So is there such principles that's support that ICANN have its own continuity of reporting the DNS Abuse directly from the registrant?

CATHRIN BAUER-BULST: Thank you. So, this is a small part that we're highlighting now of the efforts that ICANN is undertaking. So there are clear terms in the contracts between the accreditations agreements between ICANN and the registries and the registrars that set out the roles of the contracted parties in terms of abuse mitigation.

And then there's also of course ICANN compliance that is in charge of enforcing these contracts, and one aspect that you will see show up in these draft principles is how DNS Abuse reporting could inform compliance possibly in the further iteration.

And we had a very interesting discussion around that also in the Cross-Community Session on Monday because, of course, while the current abuse reporting tool as it is set up at the moment, the DAAR tool, shows trends and can help inform about for example the fact that a particular registry has a large number of malicious registrations, there is for the contracted parties to take action they flag the point that they would need further evidence to

actually go after individual cases. And I assume the same will be true for ICANN compliance.

So now of course, the question will come back to what those parties need to do to further investigate on the basis of the indicators that the reporting can provide, and then to get to the level of specificity that they need to take action. So what the reporting can provide is indicators, and then on that basis, further action will need to be taken to investigate on the compliance side and on the side of the contracted parties to then take action on that abuse.

UNKNOWN SPEAKER: Thank you. Basically my observation is that there should be a monitoring from the ICANN level if a registrar is reluctant to provide the DNS Abuse reporting [inaudible] compliance. So there should be a principle in this document to which ICANN has a supervisory role because there are many things in the contract obligations signed by the TLDs, but they do not obey.

And how ICANN is monitored, it's not feasible that there are more than 250 ccTLDs, and now there are many TLDs [inaudible] and the second round is also in the progress. So are there principles for this supervisory role? Thank you.

IRANGA KAHANGAMA: Yeah, I think that can be a consideration. I think that's something we have to delve a little deeper into. Because, I think there is already a role for that in contractual compliance and enforcement that they do have that, and there is -- you know, ICANN does keep track of the different types of complaints that comes in and I think contract compliance has gotten better about being transparent about the types of complaints it has, but I definitely recognize your point that this should also be considered, like the role ICANN has to play in all of that. Thank you.

CATHRIN BAUER-BULST: The gentleman in the front, please.

UNKNOWN SPEAKER: My comment has to do with items 3 and 4 on the publication of indicators, which are important. So I would like to focus on the fact that we need to concentrate on the fact that indicators should be achieved in a reliable way. Because, we usually see some indicators that are published that have a great impact on the activities, but unfortunately, sources are not reliable. So it is really important to be able to have indicators, official indicators and reliable indicators that are kept on a regular basis showing the engagement of authorities.

I would also like to mention that we need to establish a relationship between certain indicators so as to be able to go deeper or to analyze this information for the benefit of the community. So this is my comment about items 3 and 4. Thank you very much.

IRANGA KAHANGAMA: -- the domain abuse reporting tool that ICANN is currently putting together. So to your comment on indicators, in our Cross-Community Session ICANN went over the fact that the data and the feeds that they are aggregating this data from are coming from pretty reliable sources. Sources that are already used right now in browsers, in social media feeds and different internet security mechanisms to provide safety and security where those feeds are directing action anyway.

So it's industry reputable standards and indicators that I think we can imitate to the best that we can. And I think that the reliability is there, it just needs to be fleshed out and very clearly communicated and educated to the community.

CATHRIN BAUER-BULST: And maybe just to provide further detail on this, we'll check with David Conrad the CTO presented at the Cross-Community Session on this, whether we can share his slides with the GAC because he

went into a lot of detail on the specific methodology of DAAR, which is reproducible by anyone because it relies on open source data which will provide further reassurance I think to the members of the GAC as to how the data that is in DAAR is sourced and the reliability of those sources. So we'll take an action item to provide that to the GAC. [AUDIO BREAK]

Iran, please.

IRAN: Thank you. I think some parts of this report is related to the child abuse, whether the issue is followed in ICANN or ITU, or in others is to be protected. We have activities in the ITU council, a working group dealing with the child online help and protect. Do you have any relation with that group? How do you share some of your information relevant to that part of the issue with them in order to assist them, to further pursue the matter or in order to get further information from them, what they are doing.

So I suggest that perhaps you consider this sort of information sharing which helps. There is only a one day meeting, sometimes half of day, sometimes one day maximum; because of time limitation, they may not have sufficient resources and I believe some of this material will help them or vice versa. Thank you.

CATHRIN BAUER-BULST: Thank you, Kavouss. And taking off my Public Safety Working Group co-chair hat and putting on the European Commission one, I can say that at least from that perspective we're already working on that and indeed if there's data to be provided, so in particular there actually was data in the report that was commissioned for the CCT review team on child sexual abuse and the prevalence in the DNS. So we can go back to that data and make sure that we create the link with the working group that you're referring to. Thank you.

UK: Yes, thank you, Iran. That was very helpful cross referencing to important initiatives internationally in the area of child online protection. I think we can set up some some communication channel along those lines, and of course, the ITU are observers on the GAC; I don't know if their representative is here who will be able to comment on that. But, that's certainly worth noting as a possible cause for the PSWG to pursue with the help of our advisors on child online protection and the membership. Thank you.

CATHRIN BAUER-BULST: Just to complement, there is an international association of 71 countries around the world who come together in the

WePROTECT Global Alliance which is also currently supported by the UK Home Office with the Secretariat.

And I'm also in another capacity on the board of that and they have -- or the commission is on the board of that and they have a current initiative to actually provide data to both us here at the Public Safety Working Group and other initiatives such as at the ITU and elsewhere to basically look at also creating a better evidence base there. So we can also take that back there and see how we can follow up on that. The US.

US: Since we're having the conversation, I just would like to ask a question. When we're talking about protecting child online abuse materials and the like, in what context are we talking about it? Are we talking about it -- there was a reference made that there is child online abuse materials on the DNS. And I'm not sure exactly what that means.

And is the intent here to be utilizing the DNS as a mechanism to stop this type of material? I'm just trying to understand the scope and how it would pertain to the remit of ICANN just for a little bit of clarity. Thank you.

CATHRIN BAUER-BULST: Thank you, Ashley. That's why I said taking off the PSWG chair hat and putting on the commission hat, I think here this is about providing information so that's where policies are being developed that is based on reliable data. And what form that will take remains to be seen. But I think we have an intervention from the ITU. Yes, please.

JIE ZHANG: So thank you very much. My name is Jie Zhang, I'm the representative of ITU here. As Iran correctly pointed out, actually we do have a council working group on child online protection. And I just checked the website for this council working group and their next meeting will be January 23rd, 2018 in Geneva.

So if there's any information here we provide to this council working group to help them, I'll be glad to act as a liaison to tansfer the information to ITU, and if there's anything we can do, I would be glad to do that. Thank you very much.

UNKNOWN SPEAKER: Thank you.

UK: Yes, Mark Carvell, UK again. Just to add to your response to the US. Of course, online child protection came up in the context of

the new gTLD application round where there were applications clearly targeting children, children's affairs and so on. And we were very alert to the risk that was becoming apparent that new gTLDs might become opportunities for that kind of content to expand under the new gTLDs.

And recently, the Internet Watch Foundation reported that the number of cases that they were aware of under new gTLDs was increasing substantially by over 200% or something of that order. So, it's highly appropriate I think for the PSWG to be active in this area in looking at the implications and what can be done within this community. Perhaps an association with other initiatives like WePROTECT and the ITU's child online protection program to mitigate that risk and adjust those issues in a multistakeholder way. Thank you.

CATHRIN BAUER-BULST: Thank you, UK. Christina, European commission, please.

EUROPEAN COMMISSION: Thank you, Cathrin. Just to support what UK just said, we think that online child protection is an important topic, especially for the GAC, and the Public Safety Working Group could help a lot in focusing a bit more attention on this issue.

Of course, it's a complex issue, so also the definition of the scope is important, and we should look at that and what is achievable in the context of ICANN. But it is an area where governments have a role to play, definitely. And again, we are eager to contribute to this effort. So just to support this. Thank you.

CATHRIN BAUER-BULST: Thank you, Christina. And we're running over time, so we're going to close the discussion here, but just to inform you on the next steps. So as Iranga was saying, these principles were originally drafted just as a basis for discussion to prepare the Cross-Community Session. So these are a couple weeks old. We've had a very robust discussion on these concepts in preparing the Cross-Community Session.

There was no agreement on these across the community, so we did not submit them as principles for discussion in the context of the Cross-Community Session per se and have not published them anywhere. And a possible next step could be for us as the GAC to further reflect on these draft principles to see whether we can come to a common position on these, and then possibly take them forward in the next months through a series of discussions on our list to then be reviewed again at the next meeting at ICANN61.

So unless I see any objections here, we would proceed as we have proposed, and then share these principles again with you for your consideration in a little bit of an updated version also taking into account some of the feedback we've received from you today. And with that, if there are no further comments, thank you very much for your attention and we wish you a good rest of the day.

UNKNOWN SPEAKER: Thank you.

[END OF TRANSCRIPTION]