ICANN72 | Virtual Annual General Meeting - GAC Discussions: DNS Abuse Mitigation
Monday, October 25, 2021 – 15:15 to 16:00 PDT

[Recording in progress]

JULIA CHARVOLEN: Thank you, Manal, over to you, please.

MANAL ISMAIL, GAC CHAIR: So we would continue discussion of ICANN Org and community initiatives to prevent and mitigate DNS abuse, and also continue discussing possible concrete proposals by GAC members where we will receive a presentation from Japan.

So with this and without any further ado, allow me to hand over the floor to our DNS abuse topic leads. Laureen, are you going to start?

LAUREEN KAPIN: Yes, I will kick us off. Gabriel, I know you wanted to make sure your microphone worked. Feel free to greet everyone to ensure that.

GABRIEL ANDREWS: Hi all. This is Gabriel Andrews speaking [into my mic.]

LAUREEN KAPIN: Perfect. And you're sounding a little low to my ears. That's my feedback. My name is Laureen Kapin. I am one of the co-chairs of the Public Safety Working Group. Today, we're going to be presenting our focus on DNS abuse. I'm going to be joined by my colleagues from the U.S. and Japan, and when we get to passing the baton, I will let them introduce themselves. I know that time is short, so I am going to launch right in.

I wanted to start to set the foundation about why DNS abuse is important to the GAC. And we'll talk a little bit about cybercrime. DNS abuse is a component of that. And the history of this being a topic of importance to the GAC, and not only the GAC but other stakeholder groups. My colleague, Gabriel, will be presenting on recent developments and there's whole host of very positive developments in that regard. And we will also have a presentation from our colleague from Japan, Mr. Takeda on registrar hopping, and then we'll close with ICANN72 objectives. Next slide, please.

So, why should the GAC care about this topic? Well, anyone who is reading the headlines lately has been reading about cybercrime and ransomware and a whole host of bad behavior. Now, I want to make clear that domain name system abuse is only a component of cybercrime. Not all cybercrime is DNS abuse. But when we think about this issue generally, I want to make people aware—they likely are aware already—that cybercrime attacks across the world grew steeply in 2020. Visa in one of its recent reports lets us know that if cybercrime were measured in the same way we measure gross domestic product, it would value 6 trillion and it would be the third largest economy after

the U.S. and China. And there are many other headlines about the recent surges in cybercrime.

But we are not focusing on all cybercrime. We are focusing on a component of cybercrime which is facilitated by the DNS, the domain name system. DNS abuse at its heart is a threat to the public and Internet users, and their trust in the DNS, and it's also a threat to the security and stability and resiliency of the DNS and its infrastructure.

When you hear the phrase security and stability and resiliency, that should sound familiar to you because that's actually one of ICANN's core missions, to protect the security and stability and resiliency of the DNS.

So let's talk about what DNS abuse is. I know there has been a lot of discussion about perhaps this is a term that is in need of some definition, but there are actually existing definitions that the community has agreed upon. They are in enshrined in the contracts, and DNS as enshrined in the contracts comprises at least security threats such as phishing, malware and botnets. And the consumer competition and trust review team also defines DNS abuse as intentionally deceptive, conniving or unsolicited activities that actually make use of the domain name system and or the procedures used to register domain names.

So the GAC Public Safety Working Group and many other ICANN stakeholder groups have prioritized curbing DNS abuse and recognize that although ICANN contracts do contain provisions that speak to DNS abuse, in many cases there are gaps and the provisions are not

sufficiently clear and enforceable to mitigate the threats to the DNS as robustly as we might want.

And this has been talked about in community discussions, in discussions with ICANN Compliance, in Board correspondence—and I would encourage everyone to look very closely at the Board's February 12th 2020 letter to the Business Constituency where there's specific discussion about the role of ICANN Compliance and the provisions in the contract that it can enforce and some gaps in the contract. And then we also have a whole host of very useful inputs and reviews by various review teams, the competition and consumer trust review team, the WHOIS 2 review team, the security and stability review team, and also, there have been a lot of comments on DNS abuse including input from the GAC on the various PDPs related to the new round of new gTLDs subsequent procedures. Next slide.

So when we talk about DNS abuse, it's very important to understand ICANN's role. And indeed ICANN focuses and is very explicit about what it can and can't do. So when we think about ICANN's role, we can look to its corporate identity as a not-for-profit public benefit corporation that promotes the global interest and the operational stability of the Internet. We look to ICANN's mission which is to ensure the stable and secure operation of the Internet's identifier systems, and of course, we look to the bylaws.

The bylaws specifically state that ICANN can negotiate and enter into and enforce agreements, including public interest commitments, with any party in service of its mission. The bylaws emphasize that ICANN

commits, promises to duly take into account the public policy advice of governments and other public authorities. That's us. That's the GAC.

So let's also think about what ICANN's role is vis-à-vis the contracts. And here I'm going to ask a couple of questions in light of what the contracts say and what they don't say. So the standard registry agreement, at least for new gTLDs, requires registry operators to include what we call downstream provisions in their contract. So the registries tell the registrars to tell the registrants—so we're going down and down, that's why it's downstream—that, "Registrants, you can't do certain bad behaviors," like distributing malware, operating botnets, phishing, piracy, IP infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activities contrary to applicable law.

So that's a very broad "do not violate the law by engaging in this bad behavior" provision. But when we look to what this requirement is and what ICANN itself can enforce, this is a requirement from ICANN to the registries to tell the registrars to put something in their registrants' contracts. It's a paper requirement, but what it doesn't include are actual obligations or consequences in case any of these parties—the registrants, and they're obliged to the registrars who are obliged to the registries who are obliged to ICANN—if any one of the links in the chain isn't enforcing the obligations. This is a gap in the contracts, because ICANN cannot enforce for example against a registry that is not ensuring that its registrars make sure their registrants abide by these provisions.

So we need more than a paper obligation to include certain provisions in a contract. We also need required consequences when that contract is breached. There's also an obligation in the registry contract for registries to conduct a technical analysis basically to monitor for DNS security threats like phishing, malware and botnets.

But the contract doesn't say what needs to happen next. Again there's a gap there that could benefit from some specific obligations that could be enforced. And these are illustrative. They are not meant to be comprehensive. These are some quick examples.

Also, we have the standard contract for registrars for new gTLDs that requires them to investigate and respond appropriately to any reports of abuse, but the Board itself has recognized that the registrar agreement doesn't define with any specificity what that means. What are reasonable and prompt steps to investigate and respond appropriately to DNS abuse? So these are some examples.

So I wanted to set the stage by talking about why this is important in ICANN's role in the contract provisions and perhaps some places where they can be improved, but right now I'm also going to pass the baton over to my colleague, Gabe Andrews from the FBI.

GABRIEL ANDREWS: Right. And can we have the next slide please? Thank you. I am going to talk about some recent developments that have been happening here since the last time we all met virtually, as it may have been.

In February of this year, ICANN Compliance launched an audit to test registrar compliance with abuse specific requirements that are within their 2013 registrar accreditation agreements. In August of this year, they published the results of that audit, and this is an audit that selected the 126 different registrars to review. They chose those to get a lot of coverage the gTLD space, getting coverage of 90% of the total number of generic second level domains out there.

At the conclusion of the audit, they found 111 required some sort of follow up for potential noncompliance, meaning that 15 were marked immediately as fully compliant. 111, some sort of follow-on conversation was necessary there.

The common reasons given with the report for noncompliance were registrar websites that were missing abuse tracking procedures or abuse phone lines not being made available to the public or not being responsive if they were, or abuse phone lines for law enforcement not being responsive, or finally, websites missing abuse handling procedures entirely.

So as a result of this audit, as I said before, 15 immediately compliant. Of the 111 left, 92 of those have taken action to become fully compliant and we're told 19 are still implementing changes, which is all great that those changes have been done, are being done. And while it's appreciated that those actions have been taken, the findings underscored the importance of these regular audits, and we appreciate the amount of effort that went into to ensuring that these abuse

reporting mechanisms are easily found and functional. Next page please.

Okay. Onto SSR2. GAC may recall in January of this year, as mandated by ICANN's bylaws, the second security, stability and resiliency report was published. This is a regular review of the "operational stability, reliability, resiliency, security and global interoperability of the systems and processes" administered by ICANN.

We previously reviewed for the GAC certain recommendations that were put forward in this SSR2 report noting in particular that the groups 8 through 15 had particular relevance to issues of DNS abuse. Since that review, the ICANN Board has responded to the SSR2 report's recommendations. And while all of its responses to the recommendations groups of 8 through 15 are relevant, here are a few which we thought were particularly noteworthy.

SSR2 recommendation 8.1 asked ICANN Org to commission a negotiating team that included abuse and security experts not affiliated with contracted parties. The Board rejected that noting that ICANN Org negotiates on behalf of the broader interests of ICANN to include public interests and not on behalf of contracted parties.

On the other hand, when SSR2 recommendation 9.4 asked the Board to task ICANN's Contractual Compliance team with making a list of the tools that were needed to address security threats in the DNS, to include any tools that might require contractual changes, the Board reject this as well. The Board said that it could not approve recommendations to "contemplate changes to the contracts."

We note these responses because they may appear to be somewhat in conflict as the Board holds that ICANN alone may negotiate with contracted parties for the public interest commitments but on the other hand, it would seem to suggest it might cross a line to task Compliance with making a list of the tools necessary to address the threats to DNS and provide that list to ICANN's negotiation teams.

Last point on SSR2 recommendations is to note there were a number of them that requested either ICANN Org to consider or to evaluate within the context of its ongoing activities measures to address DNS abuse. This includes improvements to DNS abuse reporting and the potential establishment of a common abuse complaint portal. All of those appeared to be ongoing conversations and we note that we will watch with interest how ICANN Org engages on those conversations. Next slide, please.

Awesome. There have been a number of recently published reports, papers, letters of relevance to DNS abuse topics. Most of these are going to be too fresh to have any detailed commentary on, but we felt it was worthwhile to draw attention to some of these in case others in the GAC would like to obtain copies of those reports for your own benefit.

These include a report on the 2021 phishing landscape by Interisle Consulting which contains many interesting statistics they compiled. For example, a statistic reading that 65% of domains associated with phishing attacks were maliciously registered. Fun stuff like that.

Secondly, there is a report from Technical Study Group that was commissioned by ICANN in response to significant attacks on the domain name system such as the sea turtle hijacking and the DNSpionage campaign. This is going to be a bit technical and a bit in the weeds on sophisticated attacks targeting the very infrastructure of the DNS, but it's something that I look forward to reading. It's 55 or 60 pages long. If there's interest in that, we might give highlights on it later, but too fresh off the presses to have that now.

In addition to written reports like that, we note that there are ongoing conversations within the ICANN community that have been quite interesting and touching upon abuse contexts. Like the Board had a public information session on DNS abuse just last week. Earlier this week. Time is blurring.

We felt it had a very productive dialogue, both by the panelists who were fantastic but also within the chat session as well, which if folks are familiar with is constantly going alongside whoever is speaking. And if you haven't had a chance to see this, it's recorded. No link yet available, but we thought it was particularly relevant to this issue and of interest.

Secondly, there was a GNSO registration data accuracya scoping team. It is currently defining what a potential policy development process on data accuracy could look like, what it could cover and if it's necessary. One additional point on that. The topic of DNS registrant data accuracy has very significant impact on this DNS abuse conversation, and I want to call out why. It's because registrant data accuracy is useful not only in the identification of the subjects, the bad guys that might exist and

be maliciously registering domain, but it's also useful in identifying and notifying victims of crime or fraud or abuse and even dissuading that kind of abuse before it happens. If ae bad guy know they aren't going to be able to provide false information, it's a dissuading factor.

And finally, we will note that informal conversations with members of the ICANN community are suggesting that there is progress being made on the potential development of a common abuse reporting platform. And while it's too early to get into details on this particular issue, it's something that we find is a very positive development and one that we're eager to hear more about as it develops. We really look forward for opportunities to support such a tool being a trustworthy and efficient means of aggregating abuse reporting.

And with all of that said, I am now going to hand over the microphone to our colleague, Mr. Takeda of Japan.

TAKEDA MASAMICHI: Thank you. I'd like to express my appreciation for giving me the opportunity the share. In previous ICANN GAC meetings, we shared our awareness of issues of DNS abuse in terms of strengthening contractual compliance between ICANN and registrars. With regards to DNS abuse mitigation, we would like to introduce our perspective on registrar hopping today.

That is a case that a domain name is transferred to another registrar every time a third party reports that domain name for abuse. In Japan,

this is called registrar hopping. I would like to explain the whole process for this hopping. Please see the diagram.

First, a registrant commits abuse with the domain name which is registered with registrar A. Second, a third party reports the abuse to the registrar A. And third, the registrant transfers the domain name from registrar A to registrar B. It is my guess that a registrar investigates a report of and warns a registrant before the registrant transfers the domain name to another registrar.

This flow keeps repeating and abuse using the same domain name continues. In specific cases, that's how it happened in Japan. Registrar hopping has taken place less than [three months] after third party has reported the abusive domain names to the registrar.

[How we assume that it takes about three months for a] registrar to investigate [inaudible] report of abuse. We think the purpose of registrar hopping is to prevent registrars from identifying the identity of registrants and suspending them from using domain names. Hopping without any regulations allows registrants to continue abuse while using the same domain name. Next slide please.

Okay. I would like to highlight 2 challenges about registrar hopping. First, even if a third party takes appropriate action such as reporting abuse to a registrar, the third party has to keep repeating this procedure because of registrar hopping. Second, under our RAA 3.18, if a registrar receives a report of [inaudible] abuse, the registrar shall take prompt steps to investigate, but we don't know whether a registrar can investigate a registrant who has transferred to a different registrar.

Thus, today I would like to propose that GAC begin discussion on the issue of registrar hopping and the need for action in terms of strengthening contractual compliance between ICANN and the registrars. I'm grateful we can share our concerns regard registrar hopping at this GAC meeting, and I hope to see progression in discussions on the issue. Thank you all for your patience.

LAUREEN KAPIN: Thank you so much to our colleague from Japan for the presentation. Next slide, please. So this is the part of the presentation where we just give a little bit of an overview to some prior GAC advice and statements.

But before that, I do want to also give a lot of credit to many of the voluntary initiatives and work that is going on. In the chat, there was a reference to the DNS Abuse Institute, which we really welcome all the work that they have identified as topics for future endeavors and the hard thinking that they're starting to do on this topic. It's a very welcome development, particularly because it may serve as a clearinghouse where contracted parties can actually confer and communicate about best practices and issues of common concern.

We know that the registry and registrar stakeholder groups have also engaged in various initiatives particularly related to best practices for creating trusted notifier programs, which can really streamline reporting of abuse. Also procedures related to business e-mail compromise, which is a particularly nefarious form potentially of DNS abuse.

So there are lots of initiatives and thinking going on, and we also confer regularly with our colleagues from the registry and registrar groups. And our focus on this topic and the potential for improved contract provisions should not take away from our recognition that there's very good work being done, and also that many of the registries and registrars that participate in ICANN processes are the good guys and gals who care about their reputation, who care about the health of the Internet and who care about their business reputations and want to make sure that they are seen as good players.

For the most part, the good guys and gals are not the ones we're worried about. When the consumer trust review team was looking at DNS abuse and actually commissioned a study on this topic, there were findings that a lot of abuse is concentrated in very few domains, and in very few registries and registrars so that there's an outsize concentration of abuse in a few outlier parties. Not exclusively, but there is those statistics to look upon.

And it's the bad guys and gals that create a need for strong contract provisions so that they can suffer consequences if they don't abide by their responsibilities to make sure that DNS abuse is not happening within their systems.

And indeed we don't want a framework of contracts that will actually drive business towards the bad actors, because it might be seen as a place that can be a haven for those who want to take advantage. We want there to be an even playing field so everyone has to play by the rules. But in order for to that happen, of course, you need clear rules.

So with that said, I'll continue on with our discussion of some prior GAC comments so you have a sense of the context here. And even though we're starting with ICANN 68, I will tell you that the GAC's focus on DNS abuse actually goes back many years, and this has been a topic of concern consistently.

But most recently in our ICANN68 communique, we welcomed the efforts of various stakeholder groups, registries and registrars, SSAC, ICANN itself, and the focus on capacity building and training by ICANN Org for countries most affected—and I'll give a shoutout to ICANN Org which consistently does training and capacity building that is really excellent, and I know appreciated by the people who are able to take that training. And also, we note that new efforts to tackle DNS abuse should be alongside of existing initiatives and that we have urged the Board to commit to different work streams on DNS abuse.

For ICANN69, we noted our advice to the subsequent procedures working group—we took note of the subsequent procedures working group position that DNS abuse is not just an issue that should be for new gTLDs, but it should be addressed holistically. And indeed our conversation today is very much with the holistic view in mind rather than just focuses on new gTLDs.

And we also have noted the importance of review team recommendations coming from the competition and costumer trust review team and the SSR2 review teams and that we stand ready to work with the Board and with the community on these issues,

particularly through proposals to improve policies and contract provisions to curb DNS abuse. Next slide, please.

In our more recent communiques, we pointed out that DNS abuse is an issue that should be addressed by the community before a next round, and this is sort of the good housekeeping role. We want to make sure our house is in order before we start doing a renovation and adding to that house.

We also focused on taking measures to ensure that not just registries and registrars but privacy proxy providers comply with contract provisions, and we welcome the recently launched DNS Abuse Institute which our colleague, Chris Disspain, has highlighted in the chat.

And in our most recent communique, we noted the collaborative efforts taking place to develop voluntary mechanism. Again, we welcome that, but we doesn't think it can take the place of required provisions will encompass not only the good actors but also the bad actors with consequences. And again, the GAC has highlighted this need to develop and implement improved contract provisions and also signal that we're going to closely follow developments related to improving the measurement, attribution and reporting of DNS abuse. And this has to do with the reporting that ICANN itself does to let the community know about what is happening with DNS abuse, where it's happening, so that there can be transparency that can inform community action.

So with that, I will actually take a pause. We wanted to make sure and allow time for questions and discussions. And in fact, we do have time. I think this is the last slide if I'm not mistaken. So then I will turn this

back over to Manal for questions and discussions and give ourselves a pat on the back for allowing sufficient time for that instead of going right up to the end which sometimes we do.

MANAL ISMAIL: Thank you very much, Laureen, and thanks to Gabe and Takeda for an informative presentation. So I'm just looking to see if there are any comments or requests for the floor or questions. And I have also shared in the chat the scorecard on SSR2 for those interested. It's a table indicating the recommendations and the action of the Board on each with the rationale, and I understand they belong to five categories or maybe more. I cannot recall off the top of my head, but at least there are recommendation that are accepted, recommendations that are rejected, and quite a bunch that is pending, either with an expectation to be accepted, pending with the expectation to be rejected, and pending subject to further information to decide whether they will be accepted or rejected.

So it's an interesting table, and this is an important topic as Laureen and Gabe have already explained. It's also in our questions to the Board. So if you would like to skim through the whole thing, I have shared the URL in the chat. Last call for questions or comments.

LAUREEN KAPIN: And Manal, I can also note we do have ICANN72 objectives on the screen. While people are considering perhaps their last opportunity for

questions at least for this session, we of course are always happy to take questions.

You'll see that we are focusing on the ICANN Board's scorecard for the SSR2 review team, to consider the results of the ICANN audit for registrars, to consider the SSAC's proposal for an interoperable approach to addressing abuse handling in the DNS, which was put out in March, including the creation of a common abuse response facilitator. And then also consider noting ICANN's ability to negotiate agreements including public interest commitments with any party, and that would include registries and registrars, as long as it's in service of its mission, and to note that ICANN as a public benefit corporation tasked with ensuring the stability and security of the Internet's unique identifier systems is particularly well placed to receive public policy input and negotiate updates to the standard agreements to ensure that the contracts promote the public interest, including by providing clear and enforceable obligations to detect and respond to security threats and DNS abuse. So some topics to consider for ICANN72 while people are considering if they have questions.

MANAL ISMAIL: Thank you very much, Laureen, for the excellent compilation and very useful links on the screen. So I hope everyone will benefit from visiting the links and engaging in the discussion.

Seeing no hands up, I would like to thank you very much, Laureen, Gabriel and all PSWG members involved, and special thanks to Mr. Takeda for the informative presentation on Japan's experience with

registrar hopping. And many thanks to everyone for your attention. This concludes our DNS abuse mitigation discussion. We have a little bit more than a 30-minute break. We have a 35-minute break now. We will reconvene at 16:30 Seattle time. 23:30 UTC for our meeting with the GNSO. Thank you, everyone.

[END OF TRANSCRIPTION]