ICANN73 | Virtual Community Forum – GAC PSWG Update/DNS Abuse Session
Tuesday, March 8, 2022 - 14:30 to 15:15 AST

GULTAN TEPE: Welcome to the ICANN73 GAC Public Safety Working Group update and DNS Abuse session followed by the GAC discussion on subsequent rounds sessions on Tuesday, 8th of March at 18:30UTC. 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.

To ensure transparency of participation in ICANN's multistakeholder model we ask you to sign into Zoom sessions using your full name. You may be removed from the session if you do not sign in using your full name. 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 all 6 U.N. languages and Portuguese. Participants can select the language they wish to speak or listen to by clicking on the interpretation icon located on the Zoom tool bar. Finally this session like all other ICANN activities is governed by the ICANN Expected Standards of Behaviour. You may find the link in the chat for your reference. With that I would like to leave the floor to GAC Chair, 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 and ready to discuss DNS Abuse for 45 minutes and followed by a discussion on subsequent rounds of new gTLD for the following 45 minutes. And we have our topic leads and invited speakers on DNS Abuse mitigation. We will be hearing from GAC Public Safety Working Group speakers, Laureen Kapin, U.S. Federal Trade Commission and co-chair of the GAC Public Safety Working Group. Christopher Lewis-Evans, U.K. National Crime Agency and also a co-chair of the GAC Public Safety Working Group. Gabriel Andrews, U.S. Federal Bureau of Investigation, and our GAC speaker Sumitaka Shirakabe, Japan, Ministry of Internal Affairs and Communication and GAC representative of Japan, and invited speaker, Ivett Paulovics, co-author of a European Commission DNS Abuse study.

We have a lot to cover, and I think without any further ado I will be handing over to our speakers so over to our first speaker.

LAUREEN KAPIN: That would be me this time. So my name is Laureen Kapin, and I will be speaking this time in my capacity as co-chair of the GAC's Public Safety Working Group. Next slide, please.

So here is a little road map for what we will be covering in a very short, condensed session. Why domain name abuse mitigation is important,

we will hear about a recent study commissioned by the European Commission on DNS Abuse, and we are very fortunate to actually have one of the authors on being presenting information on that study, so many thanks.

We will give a brief overview of other recent developments, including ICANN's new initiative, a technical study group on DNS security issues. Some of the work done by the SSAC which has fed into a private institution, the Domain Name Abuse Institute's new tool for centralized abuse reporting. Another acronym, CART, and also a new small team on DNS Abuse that is composed of representatives from the GNSO.

We are going to give a plug for an upcoming plenary session on DNS Abuse which will be covering a very important topic on differences between maliciously registered domains and compromised domains and what that means for DNS Abuse mitigation, and we will talk about future work, and we will hear from our GAC colleague from Japan. We will mention the issue of improved contract provisions and possible future studies assessments and best practices.

So let's launch right in. Next slide, please. So again we always try to provide some background about what these issues are and why they are important, you're going to hear a lot of discussion/debates on definitions, but we want to give some background about the range of definitions. So one of the things in terms of DNS Abuse and what it's understood as is phrased as security threads and those are known as phishing, malware, botnets. Those come right out of the GAC Beijing

safeguard advice, and that language is actually set forth in the contracts as security threats that must be monitored by registries.

But there's other definitions that have been put forth as well. The competition and consumer trust and consumer choice review team referenced a definition that was part of an earlier study by ICANN or an earlier paper by ICANN that referenced intentionally deceptive conniving or unsolicited activities that actively make use of the DNS and or the procedures used to register domain names. And I'm going to give a great reference to the GAC statement on DNS Abuse which actually contains a more detailed discussion of many different definitions and their sources.

And these activities would constitute a threat to consumers and Internet users including their trust in the DNS—and that could be an individual or a company—or a threat to the security, stability and resiliency. That phrase should sound very familiar because it is an integral part of ICANN's bylaws. A threat to the security, stability and resiliency of DNS infrastructure. When we say DNS we mean domain name system.

So the GAC Public Safety Working Group is actually formed in part because of the focus on DNS Abuse and public safety issues, and it was formed to ensure that there was a dedicated channel for law enforcement and consumer protection folks to advocate about these issues, and also provide advice and support to the Governmental Advisory Committee on these issues as subject matter experts.

So we were formed in 2015 and we have a Work Plan and terms of reference, all the formalities that go along with being a working group of the Governmental Advisory Committee.

So, it's not just the GAC, and the Public Safety Working Group, but many ICANN stakeholder groups prioritize curbing DNS Abuse, and recognize, and are concerned that current ICANN contracts don't provide sufficiently clear and enforceable obligations to mitigate DNS Abuse, and there's room for improvement.

This can be found in community discussions, in statements from ICANN compliance, even in Board correspondence there was a very particularly precise letter on February 12th, 2020, from the ICANN Board that referenced its view that certain contract provisions weren't sufficiently clear to give rise to enforceable obligations. And then the GAC has given inputs on this issue in many different places, including review teams, and public comments on the work of review teams and participation in policy development efforts.

So that's a little bit of background. By the way these slides contain very useful links so if you're going to go over them after the fact, click on the links and you can see the underlying material for yourself.

Next slide, please. So we're going to talk about some recent developments, the first of which is a very detailed and informative study by the European Commission on domain name system abuse. I'm

going to give a very brief introduction before turning it over to my colleague.

This was a new study commissioned by the European Commission. It just came out at the end of January, and it was communicated to the GAC at the beginning of February, and we were fortunate enough in the Public Safety Working Group to have a presentation about the study in a conference call in February. So a few general observations about this study. It's very practical. It focuses on roles and responsibility and the whole ecosystem, which is very useful, so it doesn't just focus on the abused parties, and the attackers and abusers but also the intermediaries and not just the ICANN contracted parties for that matter, but even parties -- even entities -- not parties -- that are also part of this system.

So when I say that what I mean is they're not just talking about what registries and registrars can do. They are also talking about what hosting providers and resellers and other intermediaries can do and that's separate and apart from that law enforcement and consumer education can also add to the mix.

A lot of the recommendations and observations that the studies make were also offered in other work by the community for example by the SSAC (the Security and Stability Advisory Committee) and other review teams including the stability and security resiliency 2 review team and the CCT review team which I've already mentioned.

One thing that actually is very meaty and interesting is their observation that it's very hard to distinguish between technical security abuse issues, that's the phishing, pharming, malware, botnets activity, and content related abuse because in many cases that borderline is blurred due to the great deal of overlap between different types of abuse. And there's actually an example in the -- more than one example in the study – but one that talks about phishing so that could involve a maliciously registered domain, and you may get an e-mail from that domain that says click on this link, but then you may get to websites that have malicious content. So it's not only a technical security DNS Abuse issue, it's also a content DNS Abuse issue.

And they give other examples for example, malware, could exploit web vulnerabilities and serve up harmful content. One reason I raise this issue is there's going to be a whole plenary session on maliciously registered domains, and compromised domains, and this raises parallel issues. All for you to understand the complexity of the ecosystem here, and also very importantly how it relates to ICANN's bylaws and what is permissible for ICANN to address and what goes outside its mandate.

Next slide, please. And this is the last observation I'm going to make before you get to hear it directly from the study author. Some of the findings, some of the factual findings that are of interest I think especially to the GAC are that new gTLDs are one of the most abused groups of gTLDs in relative terms. So if you look at that first chart you can see the arrow pointing to a little over 6%. That's the percentage of

the market that new gTLDs are in the market, so of all the gTLDs new gTLDs are about 6% of them.

When you look at abused domains you can see that the percentage that new gTLDs have for domain name abuse is much higher compared to the 6%. It's over 20%. So that's an interesting fact to consider especially when we are contemplating new rounds of gTLDs.

They also observe that two of the most abused new gTLDs constitute about 41% of all the abuse of names. It's concentrated. It's not all of the new gTLDs. There's concentration of DNS Abuse in a few new gTLDs. They also have observations about abuse taking place at the registrar level pointing out again there's some concentration here. The top 5 most abused registrars account for 48% -- that's high -- of all maliciously registered domain names, and they also observe that registry -- I'm sorry -- that registrars and service providers being abused can be very responsive to abuse reports and take rapid and decisive action which can reduce the impact and harm.

So, for law enforcement, consumer protection, and government folks out there, encourage folks to report abuse because many times the registrars and service providers take this very seriously, which is all to the good. And with that, I would like to turn it over directly to the European Commission study author, Ivett, please take it away and many thanks in advance for agreeing to come here today and letting us have a deeper dive into this very important study.

IVETT PAULOVICS: Thank you very much, Laureen, and thank you for having me here. Due to time constraints I will directly jump into the, into my presentation. So I will talk about the objectives of the study that was commissioned to us by the European Commission, the methodology that we used, the timeline, the definition that we proposed for DNS Abuse, the magnitude that we measure, the good practices that we identified and the recommendations. Next slide, please.

So the objective of this study were quite broad, so it was commissioned to us to assess the DNS Abuse phenomenon to find the definition, to identify the recurring, the typologies. The role -- to assess the role of the actors, and to assess also the magnitude of the phenomenon. To give an overview of the policies and the laws at international, EU, ICANN level and also to identify industry practices, and if possible to identify good practices that could be extended also to, to other intermediaries or at the EU, international, and ICANN level and to identify the technical and policy measures needed to address the DNS abuse phenomenon.

Next slide, please. The methodology that we used was from one-part primary research, so we carried out real-time measurements, surveys, in depth interviews, and we organized also workshops. We did participation of many experts, the -- during the real-time measurements we analyzed over 2.7 million incidents and 1.68 million abused domain names using blacklist, domain and URL blacklist and as for the secondary research we reviewed -- we had a quite extensive review of third-party reports.

Next slide, please. This study took one year, and we carried out the measurements in the second quarter of 2021 so from March until June.

Next slide, please. Regarding the definition of DNS Abuse, Laureen already mentioned about the limit of many terminologies that were used so far. So what we found that it is quite difficult to distinguish between technical and content related threats due to the broad overlap between those types of threats, so our proposal is to use a broader definition which is domain name system abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity.

Our approach is based on a bottom-up approach so to analyze each incidence and the most important thing to point out that our approach distinguishes between maliciously registered domain names and compromised domain names so those domain names that were registered by legitimate registrants but at later stage compromised due to web hosting vulnerability or other reasons by malicious actors.

Next slide, please. How do we categorize DNS Abuse? We have 3 categories in the study. Type 1 comprises abuse related to maliciously registered domain names. Type 2, abuses related to the operation of the DNS and other infrastructures. And type 3, abuse related to domain names distributing malicious content. It is important to highlight that this third type may take advantage of maliciously registered or compromised domain names.

Next slide please. This approach is important also and distinguishing between maliciously registered domain names and compromised domain names to arrive to the question and to the response who should take action to mitigate DNS Abuse.

The first category, abuse related to maliciously registered domain names, for example algorithmically generated domains used for command and control communication, in our opinion the remediation path should be at DNS level so the intermediaries that should take action are at that level, DNS level.

Regarding malicious content as we mentioned it can be distributed using a maliciously registered domain names for example the typo squatted domain names serving phishing content. In this case the remediation path should take place at hosting level and also at DNS level. This is because mitigating this kind of abuse only at one level would not be effective.

In case of malicious content distributed using compromised domain names so for example compromised domain serving phishing content it is not useful to address such kind of abuse at the DNS level because it can cause collateral damages to the legitimate registrant and also to users, so in that case we propose the remediation at the hosting level.

Regarding the abuse, abuses related to DNS operation it should be addressed at DNS level. So from the definition that we propose it comes also who should take action to mitigate the DNS Abuse.

Next slide please. Let's now talk about the magnitude of domain abuse. Laureen already mentioned the -- one of the graphs of the study so we measured the overall health of TLDs, we measured also where does the abuse occur, so malicious against compromised domain names. Registrar reputation. Hosting provider reputation, and other issues such as uptimes. Regarding the overall health of TLDs as Laureen mentioned we concluded on this graph you can see, on this figure you can see because it compared the market share of five groups of TLDs with the distribution of blacklisted domains, and we concluded that EU ccTLDs are the least abused in both absolute terms and relative terms to their market share. You can see that for example EU ccTLDs have 14.44% of market share, and less than 1% of abuse.

In relative terms new gTLDs, as already mentioned by Laureen, with market share of 6.6%, are the most abused groups of TLDs. Laureen also mentioned from the study, study's result that it doesn't mean that all new gTLDs are abused because we observed that the two most abused new gTLDs combined account for 41% of all abused new gTLDs.

Next slide, please. The next figure shows the distribution of compromised and maliciously registered domain names per abuse type. Here we observed that about 25%, and 41% of phishing and malware domains are presumably compromised at hosting level. While

the vast majority of Spam and botnet command and control domains are maliciously registered.

Next slide, please. This figure shows the distribution of compromised and maliciously registered domains per TLD type. Next slide please. Then as I mentioned we measure those already through reputation. Hosting provider reputation and we observed that the top five most abused registrars account for 48% of all maliciously registered domain names. And we also observed among hosting providers disproportionate concentration of spam domain names.

We also observed that the overall level of DNS security extensions and e-mail protection protocols such as DMARC and SPF remain very low. Next slide please. Finally, we -- after analyzing all the policies applicable at international level, EU level, ICANN level and also some self-regulation we identified good practices of different types, so we divided such good practices in preventive, reactive good practices and also regarding the transparency and the availability of information, and we then identify different intermediaries so you can see the examples of ccTLDs and also some gTLD registries.

So, due to time constraints I cannot go much into details regarding the good practices, so the study extensively analyzed that, so I would go to the next slide.

And finally, in the study we identified a set of 27 recommendations in six different areas in order to improve the measures to mitigate DNS

Abuse. Also here, obviously I cannot mention all recommendations. There are some technical ones, and also some policy related recommendations. So for example, these recommendations also address different intermediaries. So, for example, for registries, registrars and resellers we recommended to build standardized or centralized system for abuse recording to verify accuracy of domain name registration data through know your business client procedures, to use predictive algorithms to monitor the abuse rates and also to use sanctions and incentives in order to keep the abuse rates under determined thresholds.

Regarding the hosting providers we also identified similar recommendations so to monitor abuse rates which should not exceed the determined thresholds. And within the, let's say, last area of collaboration, awareness and knowledge building at EU level we recommended to harmonize ccTLD operation by the adoption of the good practices that were identified and also to collaborate with the governmental institutions, law enforcement authorities and trusted notifiers so there are several recommendations which as Laureen mentioned could also be observed in different other kind of studies, but this study tried to give a complete overview of the -- of the phenomenon, what we observed in 2021.

So this was my last slide, and maybe on the last one you can find the -- sorry, the -- on the next one you can find the links to download the study, and also then you can reach out to, to myself or to my co-author Maciej Korczynski from the Grenoble University who cannot

be here in this session because he is presenting in the Business Constituency at the same time, so thank you very much for the time.

LAUREEN KAPIN: Many thanks, and I know that Manal suggested -- and I already see questions in the chat and raised hands -- that we take a bit of a pause for those who may have questions specifically about the study, I'll also note that we have a lot to pack in before our end time, 2:15, and ask for everyone's mindfulness on that.

Finn asked if there was any low-hanging fruit -- is there anything in terms of recommendations that would be especially easy to act on as soon as possible? And I think that question is directed to you Ivett.

IVETT PAULOVICS: Yes. Thanks, sorry, I was muted before. So, it's obviously not an easy question so it depends on -- this study was commissioned by the European Commission, so if -- for the European Commission, for example, it might be much easier to reach out to the ccTLDs within the EU in order to harmonize the ccTLD operations adopting good practices. Within ICANN maybe there are other priorities and other recommendations that could be more easily adopted, also because there are many other parallel works running out there.

LAUREEN KAPIN: Susan, I believe you were next.

UNITED STATES: Thanks, Laureen. So we sincerely appreciate the study on DNS Abuse which seems to be a comprehensive resource for policy makers seeking to better understand the technical and commercial layers over which both illegal and legal activity on the Internet take place.

But at the same time, it seems that the definition for DNS Abuse in this study may be over broad for use within, within ICANN, because the definition could sweep in harmful and illegal activity on the Internet that falls outside of ICANN's authority on the bylaws, but having so said, we think that this is -- this venue is ideal for facilitating an exchange on issues between government experts and DNS policy, including on the commission study.

Even if some of those issues fall outside of ICANN's bylaws or -- so I think in sum, we appreciate the study, we recognize its utility, and we also recognize that under broad definition DNS Abuse can be dealt with within ICANN but also outside of ICANN, so thank you so much.

LAUREEN KAPIN: Thank you. Gemma, you're next.

GEMMA CAROLILLO: I hope you can hear me well because I'm -- had some small audio problem. I also see myself, so thank you very much first of all to Ivett for the presentation and also Maciej indeed is in parallel in other sessions so this is for two reasons, first of all because our contractors of course have been very helpful and are being very helpful in

disseminating the work they have done and also because from our side there has been a bit of a push for them to be really in a dialogue with the ICANN community in so much -- so many forums as this was possible.

So thank you, Ivett, for your presentation, and as Laureen has mentioned at the beginning, there was also quite extensive presentation at the PSWG. I was actually surprised, and positively surprised by the summary that Laureen has made at the beginning because indeed there are things that were discussed inside the PSWG that could possibly be considered -- and this partially replies to Finn's question -- as low-hanging fruit considering what could perhaps be suggested in the context of the ICANN contracts as regards DNS Abuse because this is a subject that has been discussed in ICANN.

This was subject of discussion after the issuing of the SSR2 reports and this is something which also the PSWG group is working on in terms of possible suggestions.

I want to say a couple of things, first of all, our approach is that our study is an independent one, so we commissioned it to experts outside of the Commission. We procured this study even, I would say, without a specific timeline for a policy initiative, which is usually the case inside the European Commission simply because this is a topic of great importance to us and the need to prevent and find DNS Abuse has been central to the chapter on Internet security and openness in the European cybersecurity strategy of 2020.

Our intention to give the broadest possible visibility and time for discussion inside ICANN for this study is linked to the fact that ICANN equals to DNS for -- to use a simplistic approach and we keep being reminding that ICANN is the place DNS needs to be discussed and where actions needs to be taken. Therefore, we want the study to be highly visible on ICANN agenda and, of course, it's very important that the different constituencies have the possibility to comment because of course this is an independent study. It's not a Bible.

And therefore, there are elements that may need to be reviewed or comments that are -- that can be expressed given also the different interests stakes but this is by no means a study on ICANN. So I would like to -- hopefully -- this is already the second or the third time this study is presented that we a bit stop the rhetoric about what can ICANN do? This is outside of ICANN's remit.

I mean, I think everybody in the community is interested in preventing and fight DNS Abuse. DNS Abuse is a very complex topic because of course, as presented very well by Ivett this does not begin and end with the registering maliciously domain names. It can happen after the domain name has been registered. It can happen at a later stage, and it can involve several actors. I think the tremendous effort that the contractors have done precisely in looking at the DNS Abuse holistically should, you know be -- this is I think actually the main added value.

We are looking at DNS Abuse from the side of those who suffer from it. So perhaps the strict definition on -- and I would say the contentions about what is exactly DNS Abuse, could be stopped or at least -- I mean paused to see this is what is happening under the umbrella of DNS Abuse, happening through the use of DNS or by registering maliciously domain names, and these are the actors involved.

We can see this very clearly and the study which is, of course, very long and not all details could be presented in this context, explicitly looks at what registries, registrars, resellers, because I've seen of course there's a very complex environment after the registrars but this is identified precisely in the study, and what the hosting providers could do.

And in some cases the study identifies DNS Abuse type 1 and 2 and 3 depending on what level it's happening, the abuse. More than one actor needs to be involved so the first step is that the actors actually have the capability to inform each other that something is happening. This is why one of the, of the low-hanging fruit is, please do have contacts where abuse can be reported. This was one very, very clear and small recommendations which can make a whole set of difference.

Make sure that somebody has the responsibility inside the organization to tackle with such requests, and make sure that the actors who want to communicate at the hosting level or at the DNS level they have the possibility to get in touch with the responsible ones. And, of course, this points also clearly to the need to have good WHOIS records in place. This is another clear conclusion from the study.

So, of course I mean, this is a very long topic, and I don't want to replace the presentation from Ivett, but I really wanted to say I think people in ICANN, in the ICANN community take from the study what you find is useful. There is many recommendations addressed to the operators, we can as European Commission look at what we as policy makers could do, and this is what we are doing from our side. We are assessing the recommendations from that point of view.

But we would really like to see whether the community takes stock. If there is something that is considered valuable, and in time-frame we see, we reassess what has happened, if anything, and if improvements have been made. But I would really like to say let's see what is possible to do instead focusing on the narrow or broad remit of ICANN. This is not the point. We are not asking only to look at ICANN. This is part of the ecosystem. Thank you Laureen. Sorry for the very long intervention but I thought I had to clarify a few things.

LAUREEN KAPIN: Thank you, GEMMA. I'm hoping, Manal, we might be able to have perhaps a few more extra minutes since the study questions and statements were so very useful, and naturally when things are useful they take more time. But before -- you don't have to answer that question now. We are going to go back to the slides, and we are going to reorder things so if I can ask -- great. If we can go straight to my colleague from Japan side because we want to make sure absolutely that we get to that material and then maybe we can assess if we can do

a very quick overview of the remaining material. So to my colleague from Japan thank you so much for your patience.

SUMITAKA SHIRAKABE: Thank you very much. This is Shirakabe speaking can you hear me?

LAUREEN KAPIN: Yes.

SUMITAKA SHIRAKABE: Okay, thank you very much. Thank you, Laureen. I'm very appreciative taking this opportunity and also I know there is quite limited time remaining. So I will quickly share this slide today, just one slide, showing to you.

So today I take this opportunity, I would like to share this slide. During the last ICANN72 GAC meeting we shared the issue of so called -- we called register hopping. Which registrant is continuing abuse by transferring the same domain names from one registrar to another registrar. As a new and current issue today. We would like to share a case which the registrant who seemed to be the same continues abuse by using different domain names registered to the same registrar.

So the -- this is the current issue. Our point of view from Japan side. And today we would like to suggest two points for you all. The first point is ensuring compliance between ICANN and the registry and the registrar.

Of course the -- so many colleagues have already mentioned this point. I know, it is still important to correct the information from the registrant at the time of domain registration and to ensure the accuracy of the information, and also, it is very important to conduct effective and continuous audit of registrar compliance by ICANN contractual compliance.

The second point is the considering the effective measures against abuse using domain names. One of the ideas that we think is that concerning the possibility of using the so-called trusted notifier program. I think it would be useful especially on the case of the DNS Abuse which contains a content issue especially. And also I would suggest the co-operation, the discussion with the other supporting organizations or advisory committees in ICANN.

As far as I remember the last -- ICANN72 GAC, ICANN72 meeting with ALAC there was a discussion to promote the discussion regarding the DNS Abuse between GAC and ALAC and mentioned making a small group.

That would be a good point and we really expect that action. And also, the -- this morning the -- there was a mention by the ccNSO groups and we really expect such a proactive approach and action in the several groups, and also we expect that collaborative work between GAC and the other groups.

So, as many colleagues already mentioned there is some organizations, there is something limited way in ICANN, but we really expect the ICANN take more action, proactive regarding the abuse issue. So that's all for today. Thank you very much Laureen to take this opportunity. Thank you.

LAUREEN KAPIN: Thank you, so much, Sumitaka. We appreciate your presentation.

MANAL ISMAIL, GAC CHAIR: So--

LAUREEN KAPIN: Go ahead, please.

MANAL ISMAIL, GAC Chair: Laureen, this is Manal speaking. Very sorry to interrupt you and thank you very much Sumitaka. So working on my back channels we have borrowed ten minutes from Luisa and Jorge, so you have until 25 past the hour please. Over to you.

LAUREEN KAPIN: Okay. Perfect. So Gabe, I'm passing the baton over to you, but can I ask ICANN staff to go back a few slides. Keep going. Keep going, keep going. Okay, one more slide down.

GABRIEL ANDREWS: The fourth one.

LAUREEN KAPIN: There we go. So Gabe your mission, if you choose to accept it, will be to give a very brief overview of the remaining material until I take over for the very end. Go!

GABRIEL ANDREWS: We will do this fast, folks. Excellent presentation on the EC study notwithstanding it was not the only important study to publish results recently, and I wanted to take just a moment to highlight the excellent work that came out of what was called the DNS security facilitation initiatives and their technical study group. For background this is something that ICANN's CEO requested back in 2020, and it was in response to some very high-profile attacks that targeted the DNS infrastructure. 2018, 2019, attacks like Sea Turtle and DNSpionage which you might have seen in the news. The TSG here, the technical study group, looked into not just those attacks but many other real-world attacks and issued examples -- took from those actual incidents and they issued best common practices in order to address those real-world security incidents.

So, without diving too heavily into this, all of the recommendations are going right back to ICANN's office of the chief technology officer who actually was one of the contributors to the report. There may be additional communication coming back out from ICANN as a result of

this work later but no immediate need for GAC action. I merely wish to highlight the excellent work conducted herein.

Next slide, please. You may recall that about last year the Stability Security Advisory Committee, SSAC, published their SAC 115, a report about addressing abuse and how to handle that. It had one recommendation, and that recommendation dealt with the creation of a common abuse response facilitator.

Now since then, we, a year later, are starting to see what one possible candidate for what such abuse response facilitator might look like, and we see this from the DNS Abuse Institute, which was created by the Public Interest Registry. They are testing now something called a Centralized Abuse Reporting Tool, I do not think that's the official name -- right now we are calling it CART. It might launch as early as June. And it seeks to automate the routing of abuse complaints. Perhaps even enrich them with additional reporting that might make it easier on the contracted parties to ingest and act to that reporting. So this is very preliminary. But it's something new and interesting, and we hope that perhaps at the next ICANN we might be able to dive deeper into review of this tool.

Next slide. Right. Wrapping up the other developments we note that the Generic Names Supporting Organization, the GNSO, has recently created a small team on DNS Abuse. And as part of their work they have started to share questions including questions submitted to the GAC to, "better understand what its expectations are of the GNSO", and

whether further policy work might contribute to their existing initiatives.

So those questions are included here on the slide. I'm not going to dive into them now but be aware that these questions have been asked, and the small team on DNS Abuse within the GNSO is looking perhaps ambitiously, for response by March 21st. If anyone would like to contribute, please do engage.

Next slide. Finally, there is very soon, tomorrow, a plenary session on maliciously registered versus compromised domains. We note that the European Commission study talked about how there might be different escalation pathways on how to route abuse reporting depending on the nature of the abuse at hand. This is a panel that will dive into that very issue, and I think it will be interesting.

And with that, I hand the reins back to you, Laureen.

LAUREEN KAPIN: Thank you. Next slide, which I believe is our final slide. We've heard from our colleague. This is the future work slide in the last minute just to highlight one of the things we continue to want to provide work on is improved contract requirements, and we actually had some language in this, in our last communique that pointed to provisions in the bylaws that authorized ICANN to negotiate agreements including public interest commitments in service of its mission. So we think that work could be done jointly with stakeholders and ICANN to accomplish these

goals to improving contract provisions to be even more responsive to DNS Abuse, and also that there's further assessments of DNS Abuse to be done.

In particular, our Security and Stability Advisory Committee recommended certain work, particularly prior to launching the next round of new gTLDs which I think is a great segue to our next session, because when we are considering an additional round of new gTLDs of course it's always good to look on lessons learned about DNS Abuse in the last round and in general.

So with that, I'm going to apologize that we didn't have more time for questions, which you might have but I'll certainly extend an invitation for you to reach out to the Public Safety Working Group at any time, not just during these meetings -- if you have questions we are happy to have conversations with you. So with that, I will turn it back over, and I think I'm right on time with my extra time.

MANAL ISMAIL, GAC Chair: Thank you. Thank you very much, Laureen, Chris, Gabriel, Sumitaka and Ivett, very interesting and informative and I want to thank Fabien for the support he's providing to the PSWG. And without further delay I'm handing over to our topic leads on subsequent procedures.

[END OF TRANSCRIPT]