ICANN71 | Virtual Policy Forum - GAC Discussion on DNS Abuse Mitigation
Monday, June 14, 2021 - 14:30 to 15:30 CEST

GULTEN TEPE: This session will now begin. May I ask tech team to start the recording please welcome to the DNS abuse mitigation Monday 14th of June we will not be doing a roll call today for the sake of time but GAC members attendance will be available in the annex of the GAC communique and minutes. May I remind GAC representatives in the attendance to indicate their presence by updating their name to reflect the full name and affiliation. If you would like to ask a question or make a comment, please type it by starting and ending your sentence with question, or comment to allow all participants to see your request.

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

accurate interpretation and make sure to mute all your other devices. This session is governed by the ICANN Expected Standards of Behaviour. You will find the link in the chat for your reference. With that I would like to leave the floor to GAC Chair, Manal Ismail.

MANAL ISMAIL, GAC CHAIR: Thank you, Gulten, and welcome back everyone. During this 90-minute session will be discussing DNS abuse mitigation. And hopefully in 60 minutes if we manage to finish in an hour we will have a quick 30 minute communique review to kick start the discussion on potential topics key messages on pen holders as far as we can reach today I can see we already have a long list of speakers from our Public Safety Working Group, and from our Japanese colleague but also invited speakers from the messaging malware and mobile anti-abuse working groups so without any further ado allow me to hand over to who will be starting? Laureen, please go ahead.

LAUREEN KAPIN: Welcome everyone. My name is Laureen Kapin, and I'm one of the co-chairs of the Public Safety Working Group and I will be joined by my fellow co-chair Christopher Lewis-Evans. And also my colleague from the United States federal bureau of investigation Gabe Andrews who is waking up very early as did I as I'm sure

many others. And we have special guests for this very important topic. Our colleague from Japan, Shinya Tahata and also invited speak others to talk about a very recent study on access to domain name registration data.

In terms of setting expectations as you can see, Manal, we have a full slate so I'm going to ask forgiveness in advance if we take more -- if we go more to the 90 minute edge but we'll certainly do our best and I've done this privately, but I will do it publicly and encourage everybody to be PITHY. We will save questions to the end except for MAAWG and perhaps from our Japan colleague who are welcome to take questions at the end of their presentations. With that we will launch right into this. As is already been acknowledged DNS abuse is one of the topics we have returned to again and again because it's so important, and because it's very much a topic that is in the news these days in terms of threatening critical infrastructure to our energy and financial systems it you the panting people in an everyday level who can be subject to criminal activity, have their identity stolen and have money stolen and often these bad actors use the DNS to facilitate their criminal behavior. So it's very important topic.

So we will be covering a number of issues with regard to DNS abuse and most importantly way that is we as a community, can mitigate that abuse. We will have an update on a recent SSAC

paper which has concrete proposals, and our colleague Gabe from the Federal Bureau of Investigation will talk about some great collaborative work with our contracted party colleagues on a very specific issue that's related to DNS abuse, and methods associated with malware and botnets. We will talk about an important topic that is currently being debated about how long it needs to take to respond to requests for registration data, as folks already know that information can be crucial to an investigating bad behave, I don't are that exploits the DNS.

We will talk about a very specific consumer competition and trust review team recommendation to make sure that there is publicly available data that helps law enforcement and anyone else wanting to get information about a domain name registrant helps them get to the right party and not go through a daisy link of chain to chain folks who may not actually have the information. And then we will have a really interesting presentation from our MAAWG colleagues our Japan colleague will give us some concrete proposals for ICANN compliance which of course is a key player in mitigating DNS abuse and then proposed next steps. So we have a full menu, and I will move right onto the first course. Pass the baton to my colleague, Christopher Lewis-Evans from the U.K. national police.

I'm going to skip over this slide because it basically talks about the schedule and ICANN does a fabulous job about giving you all sorts of information about what event are coming up and what might interest you. With that Chris please give us an update on the SSAC very informative and useful paper.

CHRIS LEWIS-EVANS: Yes, thank you very much, Laureen, and hello everyone. Christopher Lewis-Evans for the record.

So I'm going to quickly cover SSAC's 115 paper which is a proposal dealing with an interoperable approach addressing abuse handling in the DNS. And quite helpfully it's laid out a proposed framework which is a good way of covering the whole documentation. So there are a number of these that are probably of more interest for us as appears to be ... and public policy aspects. And helpfully the first one of those is a primary point of contact effectively for abuse resolution. I think one of the things that ourselves as law enforcement struggle with is knowing where the right place is to go to to get a resolution, and this can actually be seen you know in industry as well, and sometimes what happens is rather than go into the right place, what you get a sort of a scatter gun approach, and you send off abuse notices to everyone that you can think of, and hope one of those has the desired effect so, this discussion point is really about creating a

single point where you can put those requests into, and then obviously they would be able to ascertain the correct contact point to go to, moving on to the next point is an escalation path.

The point you want to go on is the point that has the direct relationship with the entity causing that abuse, but sometimes they might not be responsive. And the escalation path looks at how to tackle the no responsiveness and how do you escalate the request and actually get action. There's a very good time-line in that escalation path. I will note here that there were some points raised by other SSAC members that disagreed with some of the -- some of the proposals within SSAC 115 and they could be detailed and one of those cast the escalation path and whether there was a 24 hour escalation time-line between each escalation, and some members said that was maybe not quick enough. So that was one point I just wanted to raise but I think you know, as a start that's much, much better than we might see these days. One thing that law enforcement is very used to is making sure there's sort of an evidentiary standard to things that they submit but I think it's really good to create a standard, and you know this could be applied across the different ranges of people that are involved within sort of handling DNS abuse claims, and I think that really would reduce some of the workload on those entities dealing with such requests.

Next one is reasonable time for interactions which really sort of comes into the escalation path. You if you too don't see the reasonable time met how does that escalate? So just there. Then I think one thing that touches across a couple of points is the availability and quality of contact information. So whether that contact information is who do you go to actually get the result we want to? Sometimes that can be hard to find, and I know Laureen will touch upon that around resellers and everything else. And the other aspect is you know, is the actual data you get from an RDS type look out correct or not and is that enabling you to take the most appropriate and effective action so within that... focused and support you know, everything proposed there, but the main ones are the primary point of contact and the escalation paths. Next slide please.

So within SSAC 115 it comes up with these multi-part recommendation, and this takes a little bit of a consideration of you know DNS abuse isn't limited to just the sort of community within ICANN and it looks at how ICANN could maybe start a conversation and show best practice across an industry which you know there are many players outside of the normal ICANN sphere. So as I mentioned one of the sort of PSWGs most liked proposal is the -- that of a common abuse report or facilitator as it's written here. And the recommendation looks at -- or asks for us to start that conversation and see how that could actually be

implemented, and we've had a number of conversations with different parties, and I think you know that's quite widely seen as something definitely worth having a conversation with. And this is something that I would like to see taken forward and put a little bit of weight behind.

Certainly from the GAC I see this as something that we can really support and look to provide a little bit of input into -- with regards to how it might work within each of our different jurisdictions. So with that, and being mindful of everything else we've covered I would like to hand over to Gabe now who is going to talk about the framework

GABRIEL ANDREWS: Thank you, Chris. Good morning. So I'm going to spend ten minutes now to talk about the framework on DGA for malware and botnets which will include definitions of what I am talking about. This is a project that was a joint effort between the registry stakeholder group and the Public Safety Working Group. And I will describe what we've worked on and ask we also give James Galvin of Donuts a chance at the end of the registry stakeholder group to add his thoughts but to define the words when I say DGA because it's technical term it deals with botnets, and botnets are networks of compromised devices controlled by criminal actors and some of the largest and the most dangerous botnets we have

hey to deal with in the past such as configure and after launch which we talk about.

If you controlled by the bad guys via the use of domain generation, algorithms. And domain generation, algorithms themselves with just a piece of code. A tool which you can use as an input at a specific date and time in the future and it will output a domain that is specific for that date and time. It will usually are look like gobbledygook. Law enforcement action against these DGAs, botnets is something we view as relatively low in frequency but we high in impact which means that when we take sweeping action against a large number of domains that are associated with a botnet's DGA it's relatively rare occurrence, but it carries large administrative impact both on law enforcement, and on the registries that we engage. So for example, if there are hundreds of thousands of domains associated with a DGA that are output with each year. Law enforcement has had in the past to often go to the courts on an annual basis to refresh our authority to seize domains associated with that DGA, and that could be something that occurs year after year, which is a burden to the courts, to our investigators, to the registry that is we engage with.

Similarly registries would prefer to the no have to go to ICANN to seek waivers for actions. A goal then for this framework was to set up a pathway for referral of a single DGA by law enforcement

to a registry to enable what we are calling every green action. For the translators that means action in perpetuity going forward. And it would be action that would be enabled for the life of the botnet then for the life of the DGA to avoid the need for yearly court orders or for annual reapplications to ICANN for fee waivers for the registries. Now while this framework is voluntary, and nonbinding, the registry stakeholder abuse group and the Public Safety Working Group are quite hopeful that the common understandings that we framed within it will be helpful to establishing a smoother process going forward for all parties involved. Law enforcement registries all parties that are taking responsible action against the threat posed by botnet DGAs and with that said I would like to ask James Galvin if he has thoughts on behalf of registry stakeholder.

JIM GALVIN: The DNS abuse framework is important. It's not a separate slide. Not the next one in the series. Yeah, that one. Its DNS abuse framework is an important overarching framework to the 2 things we've heard about here. Multi fact 115 from Chris and the DG... from large ecosystem that SSAC 115 references and you can see here on the right-hand side that the registration system registries and registrars are really only a small part that have ecosystem. And the set of things that we can act on. One of the things in that abuse framework is the definition of DNS abuse and it calls out

that the things that the registries and registrars can directly act on in that framework and the DGAs is just one you subset of that. One piece of the set of things which are directly applicable to registries in particular and it's a space where we can act quite directly and quickly to address those kinds of concerns. But as mentioned in SSAC 115 the framework when it was completed a couple of years ago it has since been adopted by multiple contracted parties and, in fact, it's also been officially acknowledged by both stakeholder groups much it's voluntary framework, but it also calls out the fact there are many people that are part of this ecosystem that are not present.

And similar to what is in SSAC 115 you know we talk about the actions and timelines that can be acted upon inside this framework and the way that it works inside of registries and registrars. You know the unfortunate thing in DNS abuse is just that the problem is larger than just what we can do in our space, and the set of things that we do do. And that's why there's a need for the common facilitator that the SSAC 115 document calls it out. There are many other players beyond the registration system that are simply not present in these discussion and you know have their role to play and are not part of this.

Also, it turns out that many of the actions and the timelines that are called out by SSAC 115 and the reason why having a response

facilitator is helpful is because it really depends on whether are you're reaching out to the right person at the right time. Registries have a limited set of actions they can take under a limited set of circumstances. We does registrars do our part to refer to appropriate parties, but it actually would be more helpful if people would more directly go to the parties that can most directly act on any particular alleged abuse. So the delay in responding to abuse and the action that can be taken you know they all have to be spread around to the right parties. So you know we are pleased as the,ing as registries and I'll speak on behalf of the CPH DNS abuse working group.

Even the registrars are happy to be working with the PSWG quite directly on various elements of DNS abuse that we can handle much the DGA is a specific example of that, and we are glad we are able to work with them and with ICANN to create yet another voluntary framework for those actively engaged in mitigating abuse to get in front of this and hopefully do our part in order to deal with the growing Internet abuse that is out there in the ecosystem. Thank you.

GABE ANDREWS: Thank you, Jim. I want to stress sometimes there is contention over issues but there is opportunity for collaborative action if you can narrow the scope to specific actions and we would invite any

other partner constituencies within the GAC PSWG members and so forth that if you have additional items of actionable potential to bring them up. There is sometimes progress to be made when you really narrow the focus of an issue. And I thank everyone for your time and attention.

LAUREEN KAPIN: Thanks so much to our guest, James, and for Gabe for that presentation. We are going to change topics now, and this actually has been touched on, with Chris's discussion of SSAC 115, and this deals with time-line to respond to requests for WHOIS data. This is a topic that's currently being discussed and debated in the implementation review team for phase one and to give you some context urgent requests or are exactly what they say. They are very limited in scenarios and they are limited to circumstances that pose -- and you will see this this the slide -- an imminent threat to life, serious bodily injury, critical infrastructure or child exploitation in cases barrier disclosure is necessary in combating the threat so by definition these are contemplated to be a narrow category of request which typically are not made frequently at all and the GAC representatives on the IRT team are urging response time of 24 hours.

This is in contrast to the time for nonurgent requests which could be as along as 30 case and in the Phase 1 recommendations it was

specifically contemplated that that time-line for these urgent requests was actually going to be determined by the implementation review team. It hasn't been identified as something that was determined by the policy.

So we wanted to flag this for your attention because the current debate that's being discussed is this 24 hours' time period, versus something that your law enforcement and consumer protection experts deem to be something far too long. The current discussion has an argument for up to 3 business days to acknowledge these requests, and the reason we're flagging this is because when you're getting into something beyond the 24 hour partied and business days you can potentially have a situation where something bad happens over a holiday weekend and then instead of your strict three-day period. Because you have business days you can have an intervening weekend and a holiday, and you can actually be in a scenario where for your very urgent request where there's serious threat to life or bodily injury or critical infrastructure you have a six-day period to respond. So we are currently advocating to keep this to a 24 hour period. So that for those narrow category of urgent requests there is a required quick response so that law enforcement can do their work to protect the public.

Next slide, please.

This also is a topic that relates to domain registration information which again is very important in combating DNS abuse and it actually relates to the slide that James just discussed when he talked about the key players in the ecosystem and besides registries and registrars the third category was a reseller. And this topic was actually addressed in the consumer competition and trust and consumer choice review team. It was recommendation 17. And basically it seeks to close a bit of a loophole where although the registrar is published in the DNS abuse data and law enforcement can go to the registrar to make a request for domain name registration information, sometimes it isn't a registrar who has that information, in fact, it's related party to the registrar, a reseller.

So there was a very simple recommendation that the CCT team made that ICANN should collect data and publicize the chain of parties responsible for ... and the Board actually accepted this recommendation and indicated that it's already taking place. The problem here is that although sometimes this information is in the public domain name registration record it's not required to be. And we seek to highlight this issue because this is something that still needs additional action in order to be fully accepted as we believe the Board intended. Full acceptance and implementation of this recommendation would require the

collection and disclosure of the chain of parties like resellers, responsible for domain name registrations.

And the reason this is important is that it saves law enforcement and people acting under time pressure to protect the public time. They can go directly to the party who has the information, not the to one party who will refer them to another party who in some cases may refer them to another 2 or 3 parties if there are a number of parties involved. So we think this is actually -- would be a quick fix and we are hoping who see some action to close up this loophole and make it more efficient for law enforcement to get the information they need to protect the public.

Next slide please.

So now we're also turning to a presentation which deals with access to domain name registration data, and this is going to be about a recent study that the messaging malware and mobile anti-abuse working group M3AAWG for short and the anti-phishing working group released and they will tell you more about this. And essentially just to give you a highlight, this was a survey of cyber investigators, and anti-abuse service providers, and they sought to understand how ICANN's application of the GDBR has impacted access to the WHOIS and particularly anti-abuse work and it's specifically discusses the impact of the

current temporary specification on anti-abuse actors access and use of domain name registration information, which we've discussed, is a very important tool in investigations and law enforcement efforts. So I will turn it over to our MAAWG colleagues and thank them in advance for giving us this update. Thank you, Laurin.

LAURIN WEISSINGER: I see the slides are already up thank you very much. So this is an MAAWG. As Laureen mentioned that was jointly conductively the APWG the anti-phishing working group and MAAWG and the 3 people on screen the principal investigators myself. Dave Piscitello who is well known to people and Bill Wilson, who will be speaking later who is a senior advisor to MAAWG.

Next slide.

The quickly so that everyone on the call knows what MAAWG is it was founded in 2004. It is the messages malware and mobile anti-abuse working group and the largest global industry body bringing together a various stakeholders from within the on-line community. And it is an open forum to develop approaches to are fighting on-line abuse and exploitation. Next slide. So MAAWG does two things. On the one hand it develops and publishes best

practice papers, position statements, training, etcetera, etcetera, to help the on-line community deal with abuse. And also there is public policy advocacy so not lobbying but it is about a technical on operational guidance to governance Internet public policy agents' agencies and so on.

Next slide.

So for this study we had 277 responses. L we sent requests to specific e-mail lists and other contacts so our respondents come from cybersecurity, law enforcement public safety, and so on so it is a pretty specific group. I would also like to quickly mention that WHOIS use is pretty diverse which is something our study under lines so it's about how many record are being accessed and what time-frame what. Happens with the records. What properties are necessary for something to be useful, and how quickly are data required. So for example there is a big difference between a bulk user doing data analysis pulling lots of data frequently and an investigator requesting specific records. Next slide, please.

GULTEN TEPE: Laurin, while I was moving the slides may I ask you to speak a little bit slower, please? Thank you.

LAURIN WEISSINGER: Absolutely. No worries. So looking at our respondents we can see that the majority are cybersecurity professionals at 40% followed by IP and legal professionals 25%. But you can see we also respondents from academia. Business. ISP and hosting as well as law enforcement and public safety. You can see we are comparing on to a study about WHOIS. MAAWG in 2018 and you can see the main movement is that there are far fewer sub security professionals and are more IP and legal in this survey.

Next slide.

So what's important to note is even within this very particular sample -- not that many people are we are interested this had here. Only one out of ten respondents make ... with more than 2/3 below 100 daily ... and as we said like beyond the mere numbers so requests are for and how they are used. That is extremely variable.

Next slide, please.

The so we can see here that in comparison to 2018 and this is combined usage. It wasn't broken up back then -- we can see that there is over all a decrease in query volume, only a few increased their usage. Some have ceased usage but the biggest group as

you can see particularly when it comes to technical data -- so elements that are not redacted -- in 2021 the query volume is the same according to over 50% of on your respondents. Next slide please. WHOIS's access is reflected in the numbers. I told you about before and you can see 36% use WHOIS Web queries and the rest is using a variety of other technologies. There is much more on this particularly on RDAP.

In this the report which I obviously invite everyone to read. This is really a teaser here. Now, the effect of the temp P spec on investigations according to our respondents. Nearly 71% say that the time to mitigate exceeds an acceptable threshold. So this is a big problem obviously. So there is an effect of the temp spec particularly on the timelessness of being able to respond. As you can see less than 10% are saying the investigations are unaffected with a bit over 20 saying yes we are affected but we are still managing within an acceptable time-frame.

Next slide, please.

And if we compare this now to 2018. You can see that there's actually a slight increase for people saying that the time to mitigate exceeds an acceptable threshold from 65.6 to 70.9% so things have gotten slightly worse. Next slide please. And as you can see, and surprisingly more than 80% tell us that the time to

address on-line malicious activity has increased and also that the time to address malicious domains has increased. Keeping in mind what we heard already. I will say it again nevertheless which is that one has to keep in mind that the first few hours the first one or two days are really where it is necessary to act and where cybercriminal activities do kind of make the most money.

Next slide, please.

So, if we summarize some of those issues, and add a little bit more as I said look at the report if this is a topic of interest to you because there will be far more graphs and questions being talked about. So only about 1/4 of on your respondents reported they were able to find alternative data sources to the data they already got temp spec. Attribution is very much impaired surprising to no one. And here 9 out of 10 respondents are reporting issues with doing attribution due to the data.... over 50% consider the redaction of legal and non-... persons to be excessive and only 2.2% think the temp spec is working.

Next slide, please.

So one of the ways we deal with redacted WHOIS data is that you can send in a request to kind of get the data that's been redacted. 34.4% of our respondents tell us that they're not doing this. They

are a he considering it too laborious. A bit under 1/4 do it and then you can see the rest kind of broken up in -- quite a few who didn't know this was available or didn't know it was available or that group that doesn't do requests, doesn't see this as part of their case.

Next slide, please.

Here we are seeing again that in comparison to 2018 response times that are experienced by our respondents on average have increased. In particular what I think is interesting is here the longer than 7 days we are talking a full week obviously. Where the average time one week was reported by 36% in 2018 and by over 60% in 2021. So this means that there's a long wait time for disclosure requests.

Next slide, please.

Is the time-frame of 30 days acceptable to our respondents when it comes to getting disclosure? Well, as you can see, the answer is pretty much no. The researchers, about 50% would be okay with 30 days. Trademark and copyright a bit more than a quarter. Would be fine but everything else you can see there's clear need for faster tendency. So now we are looking at the ten days so, accelerated and you can see this is still not considered acceptable

by our respondents. Again, for trademark and copyright there would be more people who would be happy for that.

Could we go to next slide, please? And this is where we can see what would be considered acceptable by our respondents. We can see here that for malware, phishing botnet and all law enforcement matters we are averaging 3 workdays. For spam it's under 4 and for IP issues people would be happy with between 5 and 6. Researchers would be happy with ten dates. In next slide please. With the disclosure we have focused on the timing here. What is also an issue is that the responses are reported to be very disparate. So a lot of them are just being ignored. Sometimes they are acknowledged and then no response. Sometimes data received are fake or otherwise not actionable, and sometimes there's the request [inaudible].

We also wanted to look at disclosure systems under ICANN consideration. And keep in mind this was a few months ago so this might not be perfectly up to date. So the discussion around a paid system. 61% of our respondents' report that they do not have the ability or the resources to pay for such a system. The 39% who indicated they would be able to pay fees, around 80% would be able to pay a reasonable accreditation fee, 30% overall. And 61% would accept ... pricing at 24% overall. Multiple respondents also underlined they think such a system is

inappropriate having to pay for access to this information can airing that function they have and so on.

Next slide, please.

Last but not least from my side, complaints to ICANN. How satisfied have our respondents been when it comes to complaining to ICANN compliance regarding the accuracy of registration data, and responses to requests, and we can see that this picture is not very positive. 41% are very dissatisfied with 35.9% saying that they're somewhat dissatisfied. At this point I woo like it hand over to bill Wilson who will do the kind of summary of PR presentation and next slide, please. Thank you very much.

BILL WILSON: Hello, everyone. I hope you can hear me well. So there's four observations that I think we get out of this. One is everybody agrees that we need all relative data that's possible while we continue to protect natural person's privacy. The other one -- another one is that the survey responses indicate what's currently being discussed by ICANN is not going to meet the needs of law enforcement and cybersecurity practitioners.

The third one is that we need to -- or ICANN needs to establish a functional system that will allow the registration data to be accessed by accredited parties, and the system needs to be workable for both the cybersecurity professionals and law enforcement but as part that have it's got to work in such a way where it eliminates some of these time delays and the administrative overhead. And, of course, it needs to include strict privacy and security controls and I'll add there has to be some form of accountability in there to keep things aboveboard, and then the fourth one here is that as Laurin mentioned earlier there's sort two types of user, the heavy hitters that use it a lot and the smaller one off or much lower volume folks, and the system needs to be able to handle both types of users.

Next slide, please.

So the four -- or the three summary items that I want to bring to the forefront here is that the temp spec WHOIS access system that's there has been shown it increases the time it takes to address all these things. And so the timeliness of access is a significant challenge for a number of folks, and the other thing is that the system isn't uniform across all registries, and so what you do for one or what you get from one or how do you it with one is different than the next one. And, of course, that in itself is causing a significant issues. There has been a formal request system for

the re-- for access to the redacted data and that -- the one that's their new it fails regularly. Requests are routinely ignored and denied. They are a, he dropped. They just take too long or if they do get responded to it's too far off that it's no long are of value to them.

And then finally the ICANN compliance process, processes they are being described as being too lengthy. Being inefficient and they're frequently providing no resolution or recourse so hopefully something can come out after that. Next slide please. So if you have any questions outside of this forum right now, please feel free to fire off an e-mail to the public policy chair at mailman.MAAWG.org and hopefully we will get back you to to you a little quicker than some of the other ones. All right. Thank you very much.

LAUREEN KAPIN: Thanks so much, Laurin, and Bill for that very interesting presentation with some really concrete examples of some challenges experienced by our cybersecurity investigators and law enforcement. It certainly gives us a lot of food for thought on the challenges ahead. To make these systems workable, and appropriately balanced it make sure data is protected appropriately and the public interest is also served.

So we are going to move on now to an entirely different topic. And this is going to be presented by our colleague from Japan. Shinya Tahata, and I will turn it over to him right now.

SHINYA TAHATA: Thank you, Laureen. Hello, everyone. At first, I like to express my appreciation to PSWG working group co-chairs for giving me this opportunity to speak. . Today, I have some updates regarding our proposal at the GAC meeting at ICANN70 in... at such I would like to present some information along with our ideas on discussing concrete measures to... and compliance by registries and registrants. After the ICANN70 meeting we have come to understand there have been some cases against the RAA for example we have... some threats do not correct the quiet information from registrants at the time timing of registration and some registrants do not follow ICANN rules, and they... registrants... domain names in spite of knowing that they are using accurate WHOIS data.

As mentioned in the 2019 GAC statement on booze, and CCT reports abuse domain names tend to involve -- of specific registries and registrars. For example according to the study group 11 out of 15... malicious domains have been registered by a single registrar. This registrar does not follow the provisions of the RAA, nor correct required information from the registrants.

Therefore, ensuring compliance and he will be noncompliant businesses can be very effective for tackling DNS abuse.

I would like to emphasize three points regarding the RAA compliance. First, it is important to collect accurate information from registrant at the time timing of domain name registration. According to the RAA registrars can collect information from registrants such as telephone number and postal address, and most of the registrars follow the ICANN rules. Meanwhile there are some registrants that do not follow the rules. That could be a hot bed of DNS abuse. Therefore, it is necessary to collect the... situation through audits. By ICANN complies.

Second, it is important to verify the identity of this registrants in the RAA. Registrants can take necessary measures including suspension of domain names when the accuracy of WHOIS data is not solved to are 15 days that. Malicious registrant willfully provide inaccurate data in many cases. Therefore it is effective to suspended the domain names of malicious registrants on this provision. Beside for the purpose of precise identification. Phone number verification could be effective. It is important to restricting... to abuse networking from ICANN compliance as well as confirming that registrants have reacted to abuse networks following the registrant compliance program. It is also important to ask for evidence to provide that domain names are not abusive.

Also, standards for DNS abuse handling in SSAC 115 is very important for enforcement. We will come to a report and the expect that... standards including... for mitigation DNS abuse will be established. And enforced bares... and RAA.

In addition to these 3 points it might be worth discussing the effectiveness of the... in the future and request the registries and the registrants to take appropriate measures. It's essential for registrars to suitably respond to abuse reports and verify the identity of registrants based on the RAA it guarantees the safe and secure usage of the Internet and we could share our concern regarding DNS abuse at this GAC meeting and can discuss measures to tackle these important issues. Thank you very much.

LAUREEN KAPIN: Thank you so much, Shinya, for sharing those concrete proposals with us. We're very grateful for your participation and this interest in these topics. So we've certainly had a variety of items on our DNS abuse menu. Then I think a lot of things to think about. I'm going to briefly talk about some next step that is might be possible, and then I will leave some time for questions. I know this flag is also part of Shinya as presentation and is more of a reference to the specific contract provisions to speak to DNS abuse, so if you're going back to the slides this is a great reference that our colleague from Japan has put together.

Next slide, please.

So in terms of next steps there have been a lot of proposals directed on DNS abuse and mitigating DNS abuse to the subsequent procedures policy development group. But the GNSO subsequent procedures group has indicated that DNS abuse their view should be addressed with respect to all gTLDs not just new gTLDs. In other words, this is is something that should be handled holistically, and not just in connection with the next round of gTLDs. But something to recall is that for the first round of new gTLDs, it actually served us an opportunity and an incentive to raise the bar and create more robust contract positions to combat DNS abuse and those contracts for new gTLDs, contained those provisions and that was a positive development. And we could have a similar if not more improved positive development in this next round of new gTLDs because we've actually learned from our experience with the contracts for the new gTLDs program.

They were, in fact, more robust but there are still some grandparents and loopholes that we've discussed in prior meetings that could be dealt with and the second round of new gTLDs presents a real opportunity to are that to take place. So that's is certainly is a potential next step notwithstanding the PDP's view on this. There's still I think debate to be had on that

issue, and here really the perfect is the enemy of the good. I think we all agree that DNS abuse needs to be addressed across all domains. But that doesn't mean we shouldn't do what we can in if the time that we can, to address it sooner rather than later. Another shoe that continues to be discussed and debated is well what is DNS abuse?

Do we all agree on the definition? And we have heard there's a lot of disagreement but, in fact, there's also a lot of common ground and the GAC gave a concrete statement on DNS abuse in September of 2019 focus on this common ground which is actually based on the contract language that's in effect regarding new gTLDs and prior community work by other stakeholder groups. It's also important to note that our colleagues across the multistakeholder community have proposed definitions and are doing really significant work on voluntary efforts in this arena, and we certainly applaud that as well.

Next slide, please.

I wanted to reference, and I do want to leave time for questions, I wanted to reference that various definitions of DNS abuse that were pointed to in the GAC statement on DNS abuse, the CCT review team had a definition. One broad focusing on intentionally deceptive conniving or unsolicited activities to

actively make use of DNS and or procedures used to register stories domain names and talked about DNS security abuse which is more technical that would include malware, phishing, botnets and spam when it's used as a delivery tool for this abuse. And then we have the language and the ICANN contracts which also is actually quite broad. There's broad prohibitions against dystopian malware, Botnets, phishing trademark or copyright. Fraudulent or deceptive practices. That covers a lot of ground even using that definition would provide a lot of latitude to mitigate the most abusive behavior, so on and so forth.

I wanted to give a little reminder about the fact that we have definitions that we can rely on here. And they certainly serve as a foundation for future work on these issues. Next slide please so in terms of next steps and this is very high level we are encouraging the GAC to participate... improved contract provision and also something that's been mentioned several times even in this meeting and earlier meetings particularly by our ALAC colleagues is that public education on avoiding DNS abuse is also a great tool because if you can spot it and see it and avoid it then you aren't going to be victimized by it so that's absolutely something that the GAC could work arm and arm with other colleagues, and with that we have -- I'm going to ask Manal if we can permit perhaps five minutes for questions or if not maybe we can save that opportunity perhaps for another session

if we have extra time, but I'm mindful of wanting to do so many things in the short time we have available so I'll turn it back to you Manal, and govern myself accordingly.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Laureen. I fully understand that we have had had a lot to cover during the session. That said, let's continue with the questions, I know we had plans to have a quick review of the communique in the remaining half hour, but we can try to reschedule this tomorrow, we have another opportunity during tomorrow's session the one on WHOIS. And EPDP so let's allow for a few questions. I saw many in the chat, but I see also Olivier as hand up please Olivier go ahead and please everyone we will prioritize questions from the GAC but if there are none we will go through the rest of the questions. Olivier, please the floor is yours.

EUROPEAN COMMISSION: Thank you and hello to everyone. So I would like for us to commend really the work of the PSWG I mean this session shows the breath of the work that is being upped taken and I think this is really a very important topic DNS abuse, I would like also to pour the, the proposals from Shinya from Japan. I think in the end a lot, a lot of the issues we are considering here can be solved through compliance with contractual obligations through enforcing contractual obligations. I think SHS something ha has

been said in a number of reports so it's of course very good that we try to improve these provisions but already compliance and enforcement I think are two very important tools, and these are tools which would allow as Shinya was saying to address the wrong to us because I'm sure many -- most of the contracted parties follow contractual obligations but some of them are not doing -- who are not doing it. And these are the ones that we need to speak to, and address, and I would also agree with the point on the -- on accuracy.

Accuracy of registration data is very important tool in the end to tackle DNS abuse. I was very interested by the report by Laurin, and I hope it will be shared with everyone, but it confirms that access to registration data is a very important tool for cybersecurity, for law enforcement, expert and this is something we have been pushing for many years here in the GAC. And finally, I think the SSAC 115 report contains very useful recommendation and I'm really supportive of the fact that for example we will see with the Board tomorrow what they think about it report and what are the next steps on the recommendation. So these were the points -- these were reactions not questions. Thank you, Manal.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Olivier, and I see many plus ones in the chat, and indeed, thanks to the PSWG for the tireless efforts to bring all the information back to the GAC. So I saw a comment from India in the chat. It reads educating end users about DNS abuse and the accuracy of the WHOIS data will help in mitigating DNS abuse, the lack of awareness related to DNS abuse in Internet users need to be addressed by developing course content in different languages to do so. A group should be formed will form the course content and also help the interested countries in developing courses in regional languages.

So I saw also Brian... replying in the chat with a few material links to material and I'm also -- I understand we will be bringing this up as well with the ALAC during our bilateral, but I'll stop here, and maybe see if there are any comments from our presenters?

LAUREEN KAPIN: I would just add that there is a real interest, on the part of the ALAC and the Public Safety Working Group to work together, and those issues and I certainly am aware that our colleagues the contracted parties are also thinking about these issues and have developed materials and I think with all of that energy and expertise we can come up with something and the point is well taken it's not just us coming up with material. It's then making

sure that that material is translated into the many languages that it needs to be so that the public can actually benefit from that content. So I this I these are very important and promise being opportunities for collaboration.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Laureen. Fair point. And I see no other hands up, and I don't think there were further questions from GAC colleagues. But if I missed in, I please retype them in the chat or feel free to raise your hand. Meanwhile I saw a question from Dean Marks saying given that ICANN org appears to be taking the position that it it is not a controller or joint controller of WHOIS data, and therefore is unable to auditory enforce any data accuracy requirements how cost the GAC expect ICANN compliance to undertake the complete proposals that Japan has proposed. So I --

LAUREEN KAPIN: That's a tough question to answer. I think, I think perhaps certain position that is are taken about ICANN's controllership have taken some of us by surprise, and we need to consider it a bit more fully. So I think further thinking needs to happen on these issues but I think dean ACs main point is that the accuracy issues are important and that the issue of who is going to take ownership over that is an important one, I certainly will point to the existing

contract provisions which have direct obligations on accuracy, and robust enforcement of the existing permissions certainly will be beneficial but there's more work to be done as we all know since we have those contract provisions and yet there's still is a problem with domain name accuracy, and indeed that is why there's future work being flagged and identified by the GNSO issue which the GAC is eager to participate in. So hopefully we will be able to make inroads there.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Laureen. Yes, Chris, please go ahead.

CHRIS LEWIS-EVANS: Thank you. I would just like to add that certainly they know the section in the RRA that covers actually around be WHOIS but I think some of the provisions within GDPR a slightly different and as Laureen highlighted, I think that does require a little bit of further work from the community which I know the GAC have offered to help with the scope and exercise of the GNSO is currently looking to undertake.

MANAL ISMAIL, GAC CHAIR: Thank you, Chris, and -- yeah indeed it was a tough question. It's good thing to think about. But already answered on the spot. And while we are on the Japanese proposal, allow me maybe to insert

my question here before going through the rest of the questions. If there is a certain experience how to prove that domain names are not abusive because I think this was one of the points raised in the, in the presentation, are so if there is a certain experience here, a best practice that could be shared it would be very helpful. And meanwhile I will continue with the rest of the questions.

I saw a question from... asking Laureen to reference a GAC proposed definition of DNS abuse and I think, Laureen, you already touched on this?

CHRIS LEWIS-EVANS: Manal, I think Laureen referenced the GAC statement on DNS abuse which I put a copy to the link on the chat.

MANAL ISMAIL, GAC CHAIR: Indeed. Thank you. So this one is done. I saw another one from Susan. Laureen, how would imposing new obligations on... which do not exist yet have an impact on those which do? TLDs which already have a contract will have no incentive to adopt different processes. Recall by volume the vast majority of abuse is in legacy TLDs so why is the focus not being applied there?

LAUREEN KAPIN: Those are fair points, and I think the -- observation about the where the bulk of DNS abuse lives is very accurate. It lives in the legacy TLDs and that's largely by virtue of their size. Not by proportion and I think the answer to this question, and I think the observations are very fair, is that we do what we can where we can. The legacy gTLD contracts are in the currently being negotiated, what is golden opportunity are the new gTLDs but there is no contract for them. That is too to be developed so this is an opportunity to improve those provisions.

Will it have a spill-over effect to the first round of gTLDs or to the .com contract? Well I would point out the current .com contractually adopted some of the new gTLD safeguards in its revision of its contract. So I would say yes it has that it has that potential for a positive impact, but I think the main takeaway is we have to seize the opportunities that are before us and the perfect can't be the enemy of the good.

I would love, love, love to deal with DNS abuse across all gTLDs. I'd love to do it as soon as possible but I also am realistic in that we have to deal with the opportunities we have and sometimes the incremental work can then have oh, overstating it -- but wouldn't it be great if that was a title effect. That would be my hope. But in the absence of said tidal wave I'll settle for some

improvements in the specific situations we have before us and that is the next round of new gTLDs.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Laureen, and apologies if I have missed any questions. And while I'm waiting if there are any more questions I -- and thank you Laurin for sharing the link to the survey in the chat. I think it's very interesting, and very informative. I was wondering whether there was also any questions regarding potential solutions, I mean that those who expressed dissatisfaction if there was an opportunity for sharing solutions could be interesting too.

LAURIN WEISSINGER: Thank you very much. This one will be coming so I can tell you that MAAWG again, some called elaboration -- will be looking into potential solutions including as many stakeholders' ones possible on the practitioner angle and we will be getting back to you with kind of a second document later this year. So we have collected the data first and now we will kind of look more into the policy as you could see we mainly kind of gave kind of some observations of what the data say, and obviously some of the questions kind of spoke to here as well. Reporting in is different from finding a solution so next step that will be coming hopefully by the next ICANN meeting we will have something.

MANAL ISMAIL, GAC CHAIR: Perfect. Thank you very much, Laurin, and thanks to everyone and to our speakers from their PSWG from Japan, also from M3AAWG.

Very informative session, and this will conclude our DNS abuse mitigation discussion but for GAC colleagues please stay in the room. We may benefit from the remaining few minutes in quickly reviewing where we stand on the GAC communique so thanks everyone and to support staff please let me know when we can start a quick discussion on the communique.

[END OF TRANSCRIPT]