ICANN74 | Policy Forum – GAC Discussion: DNS Abuse
Tuesday, June 14, 2022 – 15:00 to 16:00 AMS

MANAL ISMAIL, GAC CHAIR: Hello everyone. If you can please take your seats we will be starting in a minute.

So we are right at the hour. Good morning, good afternoon and good evening everyone in the GAC room and on Zoom. Welcome back to the GAC session on DNS Abuse and this session is scheduled for 60 minutes. The session would continue, GAC consideration of ICANN org and ICANN community initiatives, and it will be an opportunity to get briefed on recent developments, but also an opportunity to continue discussion on possible efforts by the GAC to engage with other stakeholders.

As you saw on the screen, we have quite a distinguished panel we have GAC speakers from the Public Safety Working Group, Gabriel Andrews, U.S. Federal Bureau of Investigation. Cathrin Bauer-Bulst, European Commission DJ chair of -- Laureen Kapin, U.S. Federal Trade Commission co-chair of the GAC PSWG and Chris Lewis-Evans, National Crime Agency, also co-chair of the GAC PSWG. We have also our Japanese GAC representative joining us from remote, so Teruyuki, thank you very much. I hope it's not a painful time for you back home, and Mr. Teruyuki is from the Minister of Internal Affairs and Communications. And last but

not least we have our invited speaker, Graeme Bunton, DNS Abuse Institute.

So, without any further ado I will hand over to the panelists, and Chris you're going to kick start the discussion?

CHRIS LEWIS-EVANS: Thank you, and hello again everyone, Christopher Lewis-Evans and co-chair of the PSWG. So DNS Abuse is very important topic, another one we've been talking about for sometime, we've got quite a full agenda with some really good speakers so I won't take too long in going over the topics that we are going to go through.

We will outline why this is important for us again. There's been lots of discussion around trends in DNS Abuse so we'll cover some of the aspects for that, and then we'll hand over it our colleague from Japan from a presentation of some DNS Abuse within his country. Then we will look at some operational perspectives and initiatives that are going on will lead nicely into Graeme's presentation on the centralized reporting of abuse, and then we will have a look at ICANN's and the community's role in tackling DNS Abuse.

So with that, I'll hand over to Laureen. Thank you.

LAUREEN KAPIN: Hi folks. My name is still Laureen Kapin, but this time I'm speaking in my capacity as one of the co-chairs of the Public Safety Working Group, and so delighted today that we have all 3 co-chairs in the same meeting, at the same table. It's a treat. So we'll start off with the question of why this is important, and if you're talking about why something is important, sometimes you have to first start with what, and the what has proven to be a bit of an issue that has many different perspectives, but there are existing definitions of what constitutes abuse of the Domain Name System that the GAC included in a very good resource, if you haven't looked at it, and are interested in learning more about this topic, the GAC put out a statement that focussed on DNS Abuse specifically and collected a lot of the definitions from within the community.

So, if you haven't looked at that and you're interested in this issue I commend you to take a look at it. But some of these definitions include this concept of security threats, and that originated with the Beijing safeguard advice that ultimately became part of the base registry agreement for new generic top-level domains and those security threats included phishing, malware and botnets.

And then there was also the competition and consumer trust review team and part of their work focussed on consumer trust issues, and they pointed to a definition that defined domain name abuse as intentionally deceptive conniving or unsolicited activities that actively make use of the DNS the Domain Name

System and or the procedures used to register domain names and the CCT review report also contains some very good information about DNS Abuse, and the history of work in the community on this issue.

So, sometimes there's a debate about the contours of the definition. I think the key concept when we're talking within the ICANN ecosystem is that whatever work gets done needs to be consistent with the Bylaws and the contours that are defined.

So the GAC has spoken to this in its statement on DNS Abuse -- and by the way these are links so if you go to the slides you can link to the underlying information with a click of your hand -- but these threats constitute a threat to the public, so that's consumers, folks who are on-line, that would be you and I folks, many of us, maybe all of the -- and their trust in the Domain Name System and it also isn't just the people, it's the infrastructure. A threat to the security stability and resiliency of DNS infrastructure, and again those words should be very familiar because they're enshrined in ICANN's Bylaws. They're crucial to its mandate.

So, part of the reason we even from a Public Safety Working Group is recognizing that DNS Abuse and threats to public safety meant there were -- there was an advocacy role, and an advisory role to the Governmental Advisory Committee that could be constructive, could be helpful, so in 2015 we formally formed the

Public Safety Working Group, and I say formally because law enforcement and consumer protection folks already were advocating on these issues but this was a way to form a specific working group within the GAC that could focus on these issues, particularly, because of their importance.

And it's not just the GAC and the Public Safety Working Group that are concerned about these issues. Many, if not most, groups within the ICANN stakeholder community, prioritize curbing DNS Abuse and I want to be sure to include our registrar and registry stakeholders in that category a lot of the people at the table if not most of the people at the table among the contracted parties with very concerned about their reputation and about their customers and prioritize this work and their efforts including their voluntary effort have been very important in this area.

So, we have a lot of unanimity around the idea that this is a problem, and that we can do better. In fact, there were some discussions just this morning at the Public Safety Working Group where we heard from some of our ICANN colleagues who, you know readily acknowledged that you know, the contracts that deal with these issues form the floor, the foundation, of how we can expect entities to respond and deal with DNS Abuse, and that floor could be raised and then improvements could be made.

So the point is there's a lot of focus and attention on these issues and there's a lot of good work to be done.

The issue of contracts in particular is an important one because those are the rules of the road in the ICANN ecosystem about what needs to happen, and there has been a recognition by the ICANN Board, and by ICANN compliance that the current contracts could be improved, that they aren't sufficiently clear and they don't create sufficiently enforceable obligations on this issue of DNS Abuse.

And you'll see this in community discussions, and past meetings and statements. There is a very particular piece of correspondence from the Board February 12th, 2020, that explicitly acknowledges that there are some gaps in the current contract that creates challenges for ICANN compliance, and this has also been discussed in various review teams including the consumer and ... trust review people the WHOIS review teams and the security and stability review teams, and also within the new gTLD subsequent procedures policy development process working group.

All of these acronyms, so that's sort of an overview of why this issue is important, and also some community acknowledgments of the work that needs to be done, and a lot of recognition by various working groups and review teams that there are specific things that can be done to make the Domain Name System safer than it currently is in terms of, in terms of DNS Abuse.

So with that I will pass the baton over to Gabe, to Gabe. Yes.

GABRIEL ANDREWS: Hi, folks. My name is Gabriel and I want to piggy-back on the thought of why this is in... to the GAC for a moment. As the PSWG briefed the GAC for some of the most prevalent and damaging forms of cybercrime that are out there today schemes such as ransomware or the business e-mail compromise scheme, often will rely upon embassied phishing to first get their hooks into their victims.

To say this another way, the efforts that we take here to address DNS Abuse categories such as phishing, or the spread of malware, those efforts help to protect all of our citizens against the most prevalent and harmful forms of cybercrime out there today. Some of the tools most important to public safety officials such as the WHOIS tool we use whenever the domain registrations have to be linked to are registrants those tools only exist because ICANN policy created and sustained them.

I believe we are ready for the next slide. All right. Moving on to some of the DNS Abuse updates on the trend reporting that we've been discussing recently, as many of the GAC are already aware, ICANN org has published and recently briefed the GAC on a report that they have put out called the last 4 years in retrospect a brief review of DNS Abuse trends.

Now this is a report in which ICANN took many domains and the count of those domains from what are called reputation block

lists. These are lists of domains that have been observed doing bad things. What kind of bad things? They were looking at SPAM, they were looking at phishing, they were looking at malware delivery, they were looking at the command and control of botnets, networks of computers compromised by bad guys.

They count those domains, and ICANN sought to answer the question, well, if we count up the number of domains seen in each of those categories during the last 4 years are they any observable trends that we can see? And having done so they felt that yes that there are, in fact, and they published this report out on that. Reading the report which we did with great interest because having a shared understanding of the facts is critical to progressing DNS Abuse conversations, we noticed that in the reports the obvious take away right away was that the domains that they counted for SPAM far exceeded the other 3 categories combined, which was interesting to see, and obviously as well as you can see SPAM is in the red beneath lineup.

There was a decline in the number of domains counted for SPAM over time.

Unfortunately, because SPAM is so voluminous it makes it harder for the human eye to discern well what are the other categories and what are the trends there and we tried to in this slide highlight at the bottom where blue I believe is phishing and yellow is malware delivery. It can be difficult to sort of tease out

well, is there a similar trend there? As was observed in SPAM? I don't believe we are quite able to make a determination based off of this alone helpfully ICANN authors behind the report offered to share the data that was used to generate with us and so we hope to be able to look at these potential trends individually in their categories.

Does, in fact,, phishing follow this same SPAM trend? Does malware delivery follow it? And these again are important because they are used by, this is e-mail compromise which is upwards of in the 20 billion dollars range of global loss exposure as of 2019, 2020.

Ransomware, again, uses phishing to compromise victims, so these are very important questions to answer and we look forward to reviewing the data in the future.

Additionally, and finally, I will note that ICANN authors in this report indicated that they would try to determine the cause of the peaks and troughs of the domains that they're counting for these categories of threats. That can be looked forward to in a future report. All this to say that we are not quite led ready to determine what meaning, if any, is to be drawn from this but we hope to dive into it in in greater detail in the near future. And thank you there.

LAUREEN KAPIN: I think our colleague from Japan is next, so maybe we can turn it over to you and I'll ask that the slide to be advanced so that we can get to our colleague's presentation.

TERUYUKI SHIBATA: May I speak?

MANAL ISMAIL, GAC CHAIR: Yes, please go ahead.

TERUYUKI SHIBATA: Thank you. Good morning, good afternoon, good evening, my name is you Teruyuki Shibata from Japan minister of... and communications. I would like to express my appreciation for being given this opportunity to share Japan as... with you. At ICANN72 and 73 GAC meeting we shared our sort on the issues of registrar hopping and domain hopping as example of DNS Abuse.

Today I'd like to introduce some recent trends in abuse using domain names, about... and a copyright infringement. Plus I would like to share case... using domain names and popping more, as you can see in the left diagram more than half of major... cites related to Japanese comics a hot domain, February to April 2022. Some major sites have been shut down. This has been... (indiscernible) by large number of (indiscernible).

Next as you can see in the dialogue on the right side abuse using domain name tend to be concentrate in a few specific registrars. Concentrated in specified registries. A few weeks ago they had a meeting with... an area that a domain name that had registrar being abused so we have to carry out first (indiscernible) on this issue. So, we would like to propose some suggestion on how these issues can be addressed to prevent abuse of domain names and registrars. The first is ensuring compliance between ICANN and registrars. According to RA... an ex registrar must collect information from registrants such as names, telephone numbers and postal address. As an action selecting this information registrars should also consider layer 3 verifying this collected information.

For example, I know (indiscernible) between registrar and registrants that registrar we verify -- of the registrants information. As a medium to long-term action we would like to suggest adding registrars (indiscernible) of that information collected from registrants. Next, we would like to suggest appreciation of the provision that registrars should take from step to incorporate, investigate (indiscernible) of abuse.

In addition we also would like to propose that ICANN compliance [inaudible] on this audit. We believe it is important to continue to think about what ICANN can do and implement, to improve the Internet environment. I hope to see progression in discussion on this issue at this GAC meeting. Next page, please.

Next page. Thank you. Next we would like to share the concept of data free flow with trust this. Concept was... at the 2019 meeting and G20 meeting in Osaka. The data free flow of data should... to harness the opportunities (indiscernible) with truss. Strengthening truss by the continuously addressing challenges related to privacy. Data protection. Intellectual property rights, will facilitate the free flow of data in relation to... of this session it is precisely this key, trust which is (indiscernible) based on this concept we would like to share 3 points which should be aimed for.

First, freedom of expression and free flow of information must be protected. Second information need to ensure, third (indiscernible) secure Internet has to be protected. We hope this concept (indiscernible). Thank you so much, very much for your attention. Thank you.

CHRIS LEWIS-EVANS: Many thanks. Interesting presentation. So next slide, and we will cover some operational perspectives and initiatives within the community. So the European Commission afforded us the opportunity to meet up with some law enforcement colleagues and Europol. Considering the proximity to Europol it was handy and we've had some good discussions around DNS Abuse, and the challenges that law enforcement agencies have in dealing with that.

And one of the items on there was -- it's not necessarily just about disrupting the criminal entities causing the DNS Abuse, it's also around identifying and protecting victims of cybercrime, fraud, anything that's carried out utilizing the Internet, and breaking down that trust within the Internet.

We then move forward and talked about the trends. One of the points raised within the meeting is that the reduction in the number of domains does not give a holistic picture of what is happening in the sort of DNS Abuse framework, or overview, and really we need to have a look at the harm being caused; the number of victims, the number of reports of cybercrime.

This is all information that ICANN obviously can't get hold of through its normal collection methods, and something really that the PSWG and law enforcement members can get access to. So, from this, we're going to look at how we can add to some of the statistics around DNS Abuse to see how effective some of the measures that are being taken forward really impact DNS Abuse and contribute to the reduction of DNS Abuse.

So, as the PSWG co-chairs if you have any really good statistics or reporting at agencies that collect this data we will be very glad to hear from you. Europol have offered to do some work on this and I will be collecting some from some other countries as well. And we look forward to presenting this at our forthcoming ICANN.

So then moving on to sort of current and future initiatives, one of the ICANN initiatives that concluded fairly recently and I always struggle with the acronym so I will say it in full is the DNS Abuse security facilitation initiative technical study group, or DSFI-TSG -- I got it first time that time -- one of the regions within there was recommendation 5 which pointed towards an information sharing platform, this is something as public safety groups we're quite used to dealing with, there's some really good examples certainly in the sort of financial institutes.

They have very strong information sharing and assessment centers, and this allows those institutes to share information about threats they're seeing, different trends, ways that they can tackle the abuse that they're seeing, and provide best practices. We really see this recommendation as a good step forward into creating such a platform, within ICANN and the contracted parties and for other constituencies to join to help tackle DNS Abuse, and we would really see this as a one of the top recommendations within that report from the technical study group to carry forward and be prioritized.

Graeme is going to talk about another one so I won't ruin his presentation too much but going into that, but there is some really good other voluntary frameworks that have been carried out. With these, these all have a really positive impact on our ability to tackle DNS Abuse, however, it does have a few limitations. This is not Graeme's one, just generally, the voluntary

one just to help you there Graeme -- in that they don't necessarily apply to all of the contracted parties, so we still see the need for improved contract provisions or further policy work to make this apply to all contracted parties and to be able to tackle DNS Abuse effectively.

And then with that, Graeme, I'll pass over to you.

MANAL ISMAIL, GAC CHAIR: So Chris, if I may, I can see a hand up from Kavouss in the chat. Is this a good point to take questions or comments or†--

CHRIS LEWIS-EVANS: Yes, it is.

MANAL ISMAIL, GAC CHAIR: Okay, so please, Kavouss.

IRAN: The floor?

MANAL ISMAIL, GAC CHAIR: Yes, please go ahead, Kavouss.

IRAN: Yes, thank you. Madam, first of all, I would like to thank very much ICANN for the report on this very important issue. I think very

much appreciated all the efforts has been made, all the details has been provided number 1. Number 2 madam chair we request you kindly to carefully take this report in our further action in particular with respect to any future advice or follow up on the GAC advice relating to the abuse because I think this report provided, or meets some of those concerns and we would not to repeat what we have said, now we have some answer, maybe not totally replying to what we are thinking of, but I think at least to the greater extent is satisfying so I'll request you kind through to take that advice when we drafting the Communique, or follow up action of previous Communique, we take that into account. Thank you very much for that.

MANAL ISMAIL, GAC CHAIR: Thank you very much Kavouss. Noted, and I also would like to bring to everyone's attention the chat, so please also keep an eye on the chat and I see a hand up from Indonesia. Ashwin, please go ahead.

INDONESIA: Sorry, I have to -- yeah, thank you. Its security like DNS Abuse and so on is very important today, well not only today but since many years ago -- but perhaps today is more important because now we are more and more dependant and the Internet because of this nice -- no, this bad COVID-19 problem you see.

So my, my comment is that will it be possible for ICANN security team or DNS Abuse abuse group to have a more and more co-operation with the ITU, international telecommunications union as you might away ITU also produced the global cybersecurity agenda many years ago, 2007 but it is†--

IRAN: Are you discussing question 5, 2 or another question?

INDONESIA: No, perhaps it is not related exactly to the question but just something like†--

IRAN: Madam chairman, I have no difficulty for any suggestion but†--

MANAL ISMAIL, GAC CHAIR: Kavouss, please, there is an intervention from Indonesia.

IRAN: I have not finished, I'm sorry. I'm sorry, yeah? Yeah, do you hear me madam now?

MANAL ISMAIL, GAC CHAIR: Yes, so if you may, if you may, Kavouss.

IRAN: Kindly.

MANAL ISMAIL, GAC CHAIR: Kavouss, please.

IRAN: We should not convert your committee to a drafting group. Thank you.

MANAL ISMAIL, GAC CHAIR: Thank you, Kavouss. Sorry, Ashwin, please go ahead.

INDONESIA: What I mean is perhaps a better co-operation can produce a better cybersecurity because IT, for example, also propose global security agenda for example as how to include cyber security many years ago and it was discussed during the WCIT in Dubai, 2012 in Dubai how to one (indiscernible) can be improved to Internet governance can be so cybersecurity is becoming better. By that time in Dubai we did talk further about that, so perhaps in the light of more cybersecurity this is a kind -- this kind of operation can be rediscussed again much that's all. Thank you.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Ashwin. And I see a hand up from the U.S. too, so please, Susan go ahead.

UNITED STATES: Thank you, Chair, and I want to thank the Public Safety Working Group co-chairs for the very comprehensive and wonderful presentation that you just provided. We believe that solutions to address DNS Abuse can take the form of enhanced contract requirements, and Chris made the very good point that voluntary initiatives are different -- are different than contract requirements, and compliance programs which apply to all registrars, and we also believe that solutions can include incentives for achieving relevant anti-abuse metrics and policy development processes as well.

I did want to note that in the discussions from the U.S. perspective and the discussions on DNS Abuse, it seems that there was an equation of equating DNS Abuse to anything that would be harmful on the Internet, is something that I saw but I think through the transcription, but harmful in a legal activity at the Internet content layer is outside of ICANN's mandate, and though we do believe it should be addressed with urgency, whether through normal legal process or other cross-community voluntary and collaborative solutions such as trusted notifiers and best practice initiatives. Thank you.

MANAL ISMAIL, GAC CHAIR: Thank you very much, U.S., and I see a hand up also, please go ahead.

NETHERLANDS: Thank you, madam chair. Good afternoon, colleagues. I would like to address the comment by our Indonesian comment regarding the use of the global cybersecurity agenda. While I would say it's a good thing to look into co-operation with other organizations I do feel that we should find a solution here in house as part of the multistakeholder model and not look too much especially not to the discretions we had in 2012 knowing where those have ended, and also take into respect that is ten years ago and I think the world has moved and quite a bit from there.

MANAL ISMAIL, GAC CHAIR: Thank you very much, and seeing no further requests for the floor back you to, Graeme, and sorry to interrupt your start.

GRAEME BUNTON: Thank you, Manal, and thank you for having me here today. I'm excited to talk to you about the launch of NetBeacon. I've got a bunch of slides to get through but the one really clear take away is this the DNS Abuse Institute with the support of PIR and clean DNS launch add centralized DNS Abuse reporting service available now to simplify the process of reporting DNS Abuse and to provide value to register stressor and registrars and make it easier for them to act on abuse.

And more substance behind that have the DNS Abuse Institute was created last year by public interest registry who operate the .org TLD and service not-for-profit mission and they saw, like I did when I joined that DNS Abuse is a complicated global problem, and that mitigating it at the individual registry and registrars is follow, and coordinated centralized work is required to fix this problem and reduce DNS Abuse.

And so that is the reason the abuse institute exists, is to combat this problem to educe DNS Abuse and to do it in a way that we can co-ordinate across the entire DNS. Next slide, please.

So NetBeacon the centralized abuse reporting service is directly responsive to a number of community efforts, and so SSR2 recommendation 13.1 calls for a central DNS Abuse -- at SSAC 115 talked a centralized abuse reporting... and the CCRT report alluded to something like a project like this.

And so we looked as we were the institute was looking at the problems it could try and solve it seemed like a place where we could make a difference. Next slide, please.

Right. So there are 2 fundamental problems in abuse reporting today, or there were. Reporting abuse is hard for those of how have done this. You've maybe worked for the law enforcement community or the cybersecurity community it's very difficult to do is across the ecosystem, and for end users it's especially difficult. It requires technical knowledge.

You need to be able to identify a registrar, you need to find their abuse reporting page, there are no real consistent standards for evidence, implementation of these abuse reporting functions and so it's genuinely quite tricky.

And the other side and not often appreciated is that the abuse reports that registries and registrars get are by and large awful. They are unstructured, they are unevidenced they are often for domains that don't belong to to provider, frequently unactionable and so registries and registrars spend a lot of time triaging tickets for very little value in a way that doesn't make the Internet any safer at all.

And so we really felt like there was a solution for this that could sit in the middle al solve both problems at once and that's NetBeacon. Next slide, please.

So it is a free tool. It's free for people to submit and free for registries and register start to interact with that accepts reports for DNS Abuse for phishing, malware, botnets, and SPAM. It takes those abuse reports and standardizes them. It standardizes the requirements for evidence and both the format, it enriches those reports, so not only do we take what was submitted by the end user but we then take that domain name or URL and check it against a number of on-line sources of domain intelligence. Can we find out anything else about this domain? Are there any other hits for it being engaged in illegal activity or bad activity?

And then append that to the abuse report and that's important because this is where we find incentive to use this service from registries and registrars because now what they're getting is more information, and we've moved to a certain extent some of that investigatory burden from the front line compliance person into the service itself. And what we are trying to do there is reduce the barrier to action at the registry or registrar that they can get a robust complete, standardized abuse report where all they need to do at that point is make the choice whether it's harmful and how it respond.

Another key feature is we are distributing these automatically. We remove the burden from the reporter understanding where this needs to go. We are doing that for them. Next slide, please.

So this is important to understand the scale of the problem we are going after here. There is you know some amount of all DNS Abuse an across the Internet. Some of that is discovered in lists and feeds. These are the RBL reputation block list that is form the backbone of a lot of security work and measure DNS Abuse, but there is also this other subset of manually reported abuse and it's really this that consumes a lot of registry and register start abuse cycles of their hours and it's this that they are spend a lot of time triaging for very little value and so this is really the problem that we are trying to target with NetBeacon.

Next slide, please. This is an example of the phishing report. So if you were to go to NetBeacon -- or you have to sign up at app.NetBeacon.org where you can go and create a report for phishing abuse. It's easy to use much the fields are straightforward. We try and provide useful tool tips explaining what information is required. I think the UI is pretty good. And relatively simple for most users to engage with.

I will note there's a bit of friction here. Some people don't want to us use forms, but unfortunately, free text is just unworkable at the scale of the Internet. Registries and registrars require more structured action to act effectively of the other is we require a working e-mail address. You need to be able to verify your e-mail to submit abuse reports that's because what we are just an intermediary. We are taking these abuse reports, making them better and standardized but getting them to where me need to GNSO and a registry or registrar requires more information they need it be able to contact the person who submitted it.

So there's no anonymous abuse reporting through this service. Next slide, please.

Couple of other quick features. There's API for reports submission so that cybersecurity, law enforcement, end users people who can report abuse at scale, can be enabled to do so. We have not turned this on. We have it figure out the rules and the amount of through put to do that and we need to ensure we

keep the quality of the abuse reports really high that registrars see value from the tool but we will be enabling that in the near future.

There's also an API to report consumption to registries and registrars can consume the reports not just via e-mail. So they can get them into the abuse management systems and these forms are imbeddable so that registers and registrars anyone else can imbed them on the web sites, enable the reporting of abuse, get the valuable of the standardization and enrich without doing the development work themselves. Next slide, please.

This is important because I want to make sure we cover what it is and what it isn't. It is not abuse management. Registars and registrars will get these in the system where they could be comfortable. It's not a place where they're going into this manage their abuse complaints. It also doesn't make determinations. It's always going to be up to the registry or registrar who has the liability to determine ultimately if this is abuse, and how to respond to it.

We are also not building a repository of abuse complaints. It's a risk for the institute, and also registries and registrars would not be thrilled if we were storing their dirty laundry for forever, so we have a relatively short data retention policy. And this is all not about providing access to registrant information. Registrars have that already. They don't generally need it to submit data abuse.

This is really about disrupting abuse. It's not about trying to have a long back and forth or gain access to information.

Next slide, please. We have a pretty ambitious agenda for this service. We really want to build it new know a central robust tool that is a public good to make the Internet safer. That includes integrating ccTLDs hosting content distribution networks and e-mail service providers so we can accept reports for a broad array are harms and route them to where they belong. That allows us to do things like have escalation paths so that report -- or abuse can be reported to hosting companies, and then we can escalate those to the registrar where appropriate.

The best example would be for compromised websites where someone unknowingly has been hacked and acting at the DNS layer first is often inappropriate so then we can send that to ET host first, you know we can see if they take action and escalate that further.

Ultimately we want to get to reporter reputation as well so that people who report abuse and do that commercially and want to demonstrate a reputation for being very good at reporting abuse can have a neutral third party in NetBeacon to demonstrate that they are a he good at that. At the same time registries and registrars want some reassurance the people they are getting abuse reports from -- or doing so in good faith and do so you know

in a robust quality fashion, and so we are working towards that as well.

Next slide, please. Couple of frequently asked questions. Is it easy for end users? I think it's pretty easy. We probably need to do nor UX work and think about that a little bit more but by and large just about everybody could use it now. Currently, it's only in English. We need to keep cleaning up the text but ultimately we will be translating this to make it available around the world.

I often get questions about whether we will publish data that's going through it. Like reports, and the short answer is that we will probably produce some aggregated statistics, but we think adoption of this tool is more important than shaming registrars that have abuse reports that go through it. The DNS SI has a separate initiative to measure DNS Abuse that I think is going to be academically rigorous and far more robust in answer to this particular question.

Closure and notifications. We can't close tickets for registrars that's always going to be up to them. I think there's some interesting work to be done around expectation management within this community and hopefully that becomes a discussion piece. Another FAQ I should add to the -- is do registrars have to sign up and the answer is no. Registrars are obligated to have a public abuse reporting contact and that's with we are sending to

by default. Registrars and get for value creating an account, but we don't need them to do that. Next slide, please.

This one comes up as well as a more general FAQ. Why are we doing this? And I think this is important on answer when you're looking at abuse and how to report it across the Internet very quickly it becomes apparent that to do it effectively requires working cross more than just registries and registrars. You need to engage with other bits of the Internet's infrastructure and doing so very quickly crosses ICANN as remit. So we really felt as a, you know well supported agile and respected member of this community we would well positioned to build a service like this.

And the there's another piece here about registries registrars and hosting companies having multiple places to report abuse, and so they end up you know if there were just an ICANN initiative, you end up bifurcating your abuse reporting processes and that doesn't work. It creates confusion for end users and people trying to report abuse. Next slide, please.

Right, supporting the work. So some of this early definition of this project we worked on with the Internet and jurisdiction project so thank you to them. And then PPIR is a supporter of the DNS Abuse Institute and this work and clean DNS hasten an extremely generous partner and donated the technology as well as the development hours to customize it for our purposes so a big thank you to all of them.

Next slide, please. So this is live. Anyone can go and visit it. You can create an account if you have abuse to report. Please do so. You can reach out to me directly for more information. And then I'm always interested in making connections with organizations that wish to disrupt DNS Abuse and we can talk about how to integrate with the tool. So that's it. I hope there's questions. I'm happy to answer any we've got. Thank you very much for the time.

MANAL ISMAIL, GAC CHAIR: I can see already a hand up. So in the Zoom room so please ... I'm sorry if I'm mispronouncing and then I have Nigel Hickson from U.K. please.

SPEAKER: .... is it possible for domain owners to receive reports from NetBeacon? We are a highly -- domain and it would be helpful for us to know the abusive domains were being registered which were either similar to us or sort of impersonating us so would it be possible for us to get a feed of what's being reported which relates to our specific domain.

GRAEME BUNTON: Thank you for the question. It's interesting, and not one I've thought a lot about so we certainly don't have that built much the similarity is an interesting problem. I think we would have to have

something relatively sophisticated to do that but I will add to the list of features because there's lots of work to be done and we will look at it, thank you.

MANAL ISMAIL, GAC CHAIR: Nigel, please go ahead. You can†--

UNITED KINGDOM: Yes, thank you very much and thank you so much, Graeme, for that. Well, thank you for the whole panel it's been excellent. But in particular Graeme for the incredible work you're doing in the DNS Institute and this NetBeason.

IRAN: Madam chairman, I have a firm proposal†--

MANAL ISMAIL, GAC CHAIR: Kavouss, Kavouss†--

IRAN: As long as the issue†--

MANAL ISMAIL, GAC CHAIR: Kavouss, please†--

IRAN: Network is properly†--

MANAL ISMAIL, GAC CHAIR: Kavouss, we have an intervention here. You're interrupting an intervention, so please if you can wait until Nigel finishes and I'm going to give you the floor next. Thank you. I'm sorry, Nigel. Please go ahead.

UNITED KINGDOM: Not at all. Good afternoon, Kavouss. I've lost my thread but I wanted to thank you for what you know, for what you're doing at NetBeacon. This sounds incredibly you know positive and I really mean that because I think you know having this wealth of information is just really positive. And I suppose the question, the question I had, and I know you partly covered this, but you know, you go to -- you put a lot of work in terms of analyzing the information reporting back to the, to the registrar giving them lots of different information, and, of course, at the end of the day it has to be their determination what they do with that information, but I guess you're intrigued and we would be intrigued as governments I suppose as well that you know, that a positive result took place, and I know positive is a bit of a subjective word, but you know where there really was abuse taking place that that domain was taken down or whatever. But anyway, thank you.

GRAEME BUNTON: Thank you, Nigel. I appreciate these kind words. We are looking at how to measure the outcome of abuse reports, I think it's relatively complicated to do so, and it's hard to say. It could be that the -- you know the report was wrong or incorrect and so actually leaving a domain up was the right thing to do but we are investigating that and so partly for selfish reasons we want to show the service is working and making the Internet safer and so that is on our list ever things to try and look at.

MANAL ISMAIL, GAC CHAIR: Thank you very much. So I have Kavouss then I have Rwanda and then I think we need to proceed because we may be running out of time. So Kavouss, please over to you and to help me do a better job, please, if you can raise your hand so that I can be able to know the queue, I'm sorry. Go ahead Kavouss. Kavouss can you hear me? So Rwanda, please go ahead.

RWANDA: Thank you for DNS Abuse Institute, it's well done, and we appreciate it. And I just want to ask some qualification if you do have kind of (indiscernible) that you can help developing countries in DNS Abuse, and (indiscernible), and as you know, many many countries don't have the Danish (indiscernible) and I think this would be -- just I would recommit to make a

co-operation with the country code domain and (indiscernible) engineer to be able to prevent DNS (indiscernible) help to increase the security for the domain (indiscernible), and the final one, I just want to inquire the frequency of publishing your report. I don't know if it's an annual report or just how you publish your report. Thank you.

GRAEME BUNTON: Thank you for that question. On the capacity-building front some of the other activities that the DNS Abuse Institute is engaged in is around education and best practices, we've published a few of those for registries and registrars as well as end users for keeping their websites safer and secure and reducing DNS Abuse that way. And that's work that we will continue to do as an institute over time.

And, look forward to engaging with you on that. Thank you. Oh, and re-reporting, unclear what sort of reporting we will put out of NetBeacon but as we publish in a separate project measuring DNS abuse, I expect that on start coming out in this August or September and we will be doing that monthly.

MANAL ISMAIL, GAC CHAIR: Thank you very much. I see a hand up from the U.S., and I'm wondering how many slides do we have? 2 slides? So U.S. very briefly because we need to move on. Go ahead.

UNITED STATES: Thank you, Chair, and thank you to Graeme for the presentation. The U.S. recognizes the introduction of the DNS Abuse initiatives NetBeacon abuse reporting tool and also we note its consistency with regions made in both sack 115 and SSR2 final report and we look forward to learning of further developments around NetBeacon's use and deployment in advance of ICANN75.

More generally, on DNS Abuse reporting the U.S. believes that better more comprehensive and rigorous reporting activity to include abuse reporting may granular to the registrar and registry level more detailed break-downs of the types of DNS Abuse measured and availability of raw aggregated data should assist in developing the contract provisions mentioned previously in the presentation. Thank you.

GRAEME BUNTON: Thank you for these very kind words and it -- I should probably mention that the service is live and it's working. We've had the first real abuse reports flow due it and bad domains are coming off the Internet and I think it's a really positive initiative looking forward. Thank you.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Graeme. And Cathrin, thank you very much for your patience. Please go ahead.

EUROPEAN COMMISSION: Yes, and thanks from our side. We move from horrible to great, free and easy too use. Quite an advancement indeed.

And for the record I'm Cathrin Bauer-Bulst. I am with the European Commission and absolutely thrilled on see so many of you again in person after such a long break. Hi, GAC followers. So we are going to runned round it out and come back to ICANN's role. What is ICANN's role in this? And what should it be? Now we've made great strides in creating STRANS patience around abuse. Not just outside ICANN. ICANN itself contributed through the DARR and the DNS sticker initiative and here we are taking great strides when it comes to utilizing tech, automation to help the whole of the ecosystem be more efficient in tackling abuse.

We will come full circle to Laureen's first remarks about the floor. ICANN today has easy means to take action when a registrar not paying its dues. But not if the registrar is repeatedly in overtime violating its responsibility to contribute to a safer and resilient Internet in now this status quo does not fully reflect ICANN's mission and we have eat heard a lot of echos of it view around the community. There's widespread agreement we need to do more and we welcome industry support for a number of the valuable initiatives that are already on going within ICANN and beyond.

Now, we need to build on the one side on the transparency that is now being created. Information sharing has already been cited

can play a key role. We need to build this out and get a better understanding of the factors driving DNS Abuse in it's forms and supporting recreational industries and registrars and complement the data from the cybersecurity perspective with what public safety authorities and others see in their investigations on the economic and also on the human impact of various forms of DNS Abuse. And we believe that this is precisely in line with ICANN's role as defined in the articles of incorporation and Bylaws as set out as a reminder here.

Now, of course we can create transparency and facilitate all we want. We also need incentives. Because at the bottom line taking action against DNS Abuse is a cost point even if it is just reactive that is in response to reports, let alone proactive. Now, we've also often discussed it is usually not the contracted parties who are in the room actively contributes to ICANN who are less engaged.

When I mentioned industry support many of those contributing to ICANN already committed to doing more and are actively engaged, it is often those who do not participate here and I think the Japanese example is a case in point -- there are registrars who are not aware of what they might be doing here or that they have a problem. Now this can be a question of capacity building of course, but we also need to create incentives and raise the contractual floor and here we come back to some of the inventions that have come from the floor, and Laureen will now

take us through the gaps we see today and possible future steps that we as the GAC might wish to...

LAUREEN KAPIN: Thanks. Next and final slide. I know we are a bit over time. So again, the contracts form the floor and I think ICANN compliance, and the panel would agree if it's not in the contracts it can't be enforced. So the real question is, what is currently in the contracts? And is there a room for improvement because ICANN compliances power emanates from the contracts.

So, one of the places where we see a provision that is in the public interest commitments of the standard based registry contract is a prohibition against distributing malware, abuse, unfortunately, operating botnets and you can read the bank yourself but this is directly from the registry contract and you may think upon first glance that that means oh my goodness, there's all this behavior that is being prohibited so if this happens we can just go out and enforce against it.

But that's actually not what the prohibition is. This is what we call downstream requirement that just obligates the registries to say to their registrars -- the people who are dealing with the customers who buy domain names -- make sure you put in your contracts with those buy buyers that they can't do this so if you're looking at the relationships and the enforcement relationships, ICANN and the registries have a promise to one another about this

paper requirement being included in the contracts with registrants but there is no obligation for the registries to make sure that registrants don't do this.

There's no obligation to make sure -- to have registrars take certain actions, so these are, these are things and issues that should be discussed under the general issue of how do we think about enforceable provisions regarding how do respond to DNS Abuse? And I say conversations because it should not be up to the Governmental Advisory Committee in isolation or any stakeholder group in isolation to develop these. We are identifying an issue, how to respond to DNS Abuse, and what should be the way to improve contracts in this regard but that has to be a conversation with all the stakeholder groups especially with the contracted parties who have their business reality to contend with, they know things that we don't.

We know things that they don't. It has to be a dialogue so really our big picture suggestion is there need to be good conversations about this so that we can work together.

Another example where there is a potential gap in the contracts deal with the registry obligations to conduct a technical analysis to find out whether there's security threats but the contracts don't say what needs to happen next after the security threats with identified. So more questions.

And then the standard registrar contract calls for registrars to promptly investigate and respond appropriately to DNS Abuse, but the Board it severe has acknowledged that the registrar agreement the base registrar agreement doesn't define with specificity what that means, what does reasonable and prompt steps to investigate and respond appropriately mean so there have been discussions. There have been voluntary initiatives, there's a lot of good thinking on this, but we need to have these discussions that focus on the broad topics, of reporting and handling responding to Domain Name System abuse, and how contract terms with be put in the contracts and then enforced grappler even more suspect I have with the issues. I want you to thank you for running over time.

MANAL ISMAIL, GAC CHAIR: Thank you.

LAUREEN KAPIN: Apologies, we don't have time for questions.

MANAL ISMAIL, GAC CHAIR: Very sorry, but thank you very much to all speakers here and on-line, and thanks to GAC colleagues for the active participation, and to community interest as well. GAC colleagues, please be back in the room at half past. Thank you, everybody.

[END OF TRANSCRIPTION]