ICANN78 | AGM – GAC Discussion on DNS Abuse
Wednesday, October 25, 2023 – 10:30 to 12:00 HAM

GULTEN TEPE: Hello, and welcome to the ICANN 78 GAC Discussion on DNS Abuse session being held on Wednesday 25th of October at 8:00 UTC. My name is Gulten Tepe Oksuzoglu, and I'm the remote participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior.

During this session, questions or comments submitted in the chat will only be read aloud if put in the proper form. Interpretation for this session will include 6 UN language and Portuguese. Please click on the interpretation icon in zoom and select the language you'll listen to during this session. If you wish to speak, please raise your hand in the Zoom room, and once the session facilitator calls upon your name, kindly unmute your microphone and take the floor.

Before speaking, ensure you have selected the language you will speak from the interpretation menu. Please state your name for the record and the language you will speak if speaking a language other than English. When speaking, be sure to mute all other devices and notifications. Please speak clearly and at a reasonable pace to allow for accurate interpretation.

To view the real-time transcription, click on the closed caption button in the Zoom toolbar to ensure transparency of participation in ICANN's

multistakeholder model, we ask you to sign in to Zoom sessions using your full name. With that, I will hand the floor over to GAC chair, Nicholas Caballero.

NICHOLAS CABALLERO: Thank you very much, Gulten. Welcome, everyone again. We'll have a very interesting 90-minute session on DNS abuse. Certainly, a sensitive and very important topic for our distinguished colleagues present here in Hamburg. We have a fantastic team of guest speakers, but I will let them introduce themselves starting with my good friend, Graeme.

GRAEME BUNTON: Thank you, Nico. Good morning, everybody. My name is Graeme Bunton. I'm the executive director of the DNS Abuse Institute.

LAUREEN KAPIN: Hi, folks. I'm Laureen Kapin, speaking in my capacity is one of the co-chairs of the Public Safety Working Group.

NICK WENBAN-SMITH: Good morning, everybody. My name is Nick Wenban-Smith. I'm the general council for nominate UK, but I'm speaking with my capacity as chair of the ccNSO DNS Abuse standing committee.

SUSAN CHALMERS: Good morning, everybody. My name is Susan Chalmers, and I work for the National Telecommunications and Information Administration at

the US Department of Commerce. I am here in my capacity is the US GAC representative.

CHRIS LEWES-EVANS: Good morning, everyone. Chris Lewis-Evans. I'm the director of Governmental Engagement and Internet Harms Mitigation, CleanDNS.

SAMANEH TAJALIZADEHKHOOB: Good morning, everybody. I'm Samaneh Tajalizadehkhoob. I lead the SSR research group within the Office of CTO ICANN Org.

NICHOLAS CABALLERO: Thank you very much. And with that, let me give the floor right away to Laureen Kapin who will be walking us through the-- I'm sorry. I'm sorry. Susan Chalmers. I'm sorry. Susan, go ahead.

SUSAN CHALMERS: Thank you for joining us today. We have a very packed agenda for this session. So, I am going to briefly provide a background of the DNS abuse contract amendments, which we all understand are open for voting right now by the contracted parties. And then I will briefly go over the GAC public comment, which was submitted to the public comment process on these amendments.

If we could go to the next slide, please. Okay. Oh, thank you. So, beginning around 2019, the GAC really began to focus on the issue of DNS Abuse and join different parts of the ICANN community in calling for greater action at ICANN and within ICANN's work. The contracted

parties ultimately responded with a proactive proposal to address DNS abuse in late 2022. And that is a proposal to negotiate new DNS abuse obligations, in both of their contracts and those contracts, the names of those contracts are listed there for those who are unfamiliar.

In May 2023, the draft amendments were published, and the public comment process began. In July 2023, the GAC submitted a public comment, which we'll address on the next slide. Just to note that in October, the voting period to adopt these amendments did open, and it is scheduled to close in December.

So, prior to ICANN77, some GAC members may recall that we worked with the underserved regions working group to develop a set of two webinars to give greater context to DNS abuse as well as the aim of the amendments. And so, I would encourage anybody who's interested to check out those webinars, and where these slides will be published will be on the GAC website. Following that, at ICANN77, we had capacity development workshop also led by the underserved regions working group and the United States also worked with the US RWG to produce that workshop. The focus of the workshop was on the DNS abuse contract amendments, but also, and more importantly, how the GAC works together to produce a public comment and to submit it to the public comment process.

And so, we were very lucky to have volunteers who offered to participate in what was quite a tight timeline, to deliver a public comment. And those GAC representatives were from Chinese Taipei, Columbia, Egypt, the European Commission, Mali, Switzerland, the United Kingdom, and the United States. We really did conduct a robust

consultation with the full GAC list and the public comment was also informed by the work of the Public Safety Working Group.

At large, the public comment was very supportive of the amendments. And if there's one thing I'd like for my GAC colleagues to take away from today is that we should all be encouraging registrars and registries in our jurisdictions to vote in favor of adapting those contract amendments. So, please consider that. And the public comment also addressed some areas for future work. And for that, I'm going to turn it over to my colleague, Laureen, from the Federal Trade Commission. Thank you.

LAUREEN KAPIN: Thanks, Susan. And I'm hoping if I say it, I can will it into being, once the contract amendments are approved, there is still work to be done, and this was discussed in the GAC's public comment on this topic. And one of the areas that was discussed were targeted policy development processes to further inform the contracts and the work in this area. And we say targeted, and when we say targeted, we mean that these should be focused narrowly, and hopefully that means they could be done more quickly.

So here are some of the topics that were identified in the comment, and I would say these things as a reminder and also to spur some thoughts about how this could be put into action. So, guidance on key terms. The amendments have some key terms such as appropriate, prompt, actionable, and reasonable, and this refers to, among other things type of evidence that should be submitted and the type of responses that should be taken. So, one thought is that there could be further work on

establishing what indicators or data elements will comprise actionable evidence. And what are appropriate mitigation actions to address certain issues in different cases of DNS abuse.

Another problem, and to echo one of the terms, a persistent problem is how to address issues of persistent abuse. So, if there are repeat offenders of DNS abuse activities, how do we tackle that? And the CCT review team and SSR2 review teams have a lot of thoughtful ideas on these topics, and that was informed by members of various stakeholder groups. So, that's worth taking a look at to inspire further action.

There's also the idea of what incentives we can create for registrars who achieve positive results in tackling abuse. Those could be financial. They could be non-financial. There's always the raw raws and appreciation and affirmation of this activity in public way to at least categorize some of the non-financial ways to incentivize good behavior There's also due process issues. If registrants feel that they have been suspended without an appropriate justification, what process should there be for them to challenge that action? And then finally, training. It's always a great idea to have training about DNS abuse prevention and mitigation so that current and future actors in this ecosystem can promote again good behavior in keeping the space safe.

There are other areas for future work, and these ideally would be done prior to the next round. One thing is the issue of consequences. The proposed amendments have responsibilities, but they don't say what happens if these contractual responsibilities aren't met. This certainly is in the arena of ICANN Compliance, but it would be productive for Org and the contracted parties to specify what are the consequences, if the

obligations under these new amendments are not met. The ability to monitor enforcement is also very key. It would be very useful to have transparency about what results we're seeing with respect to these particular amendments. And that's something that could be the topic of future work.

And then finally, evolution of DNS abuse. And our SSAC colleagues, wrote about this in their SAC115 paper, that DNS abuse evolves. The bad guys and gals are really good at figuring out new ways to deal with restrictions and they're very creative. And so, we have to do the same. So, no definition should be static. And this could be a topic of review of stakeholders from all parts of the community, consumer protection, cybersecurity, academic and independent researchers, etcetera. So, that's something that could be a very fruitful area for future work.

And we note that the advisory that was published regarding the contract amendments, that should be a living document. There are currently scenarios there, but as the landscape changes, that document should change also to make sure that it's current. So, those are just some of the topics that were identified in the GAC comment and should serve as some inspiration for future work in this area. At least, we hope that it does.

SUSAN CHALMERS: Thank you, Laureen. And now we'd like to open up the floor for discussion. So, we'll have discussion for about 10 minutes and then we'll proceed to presentations by our guest speakers and then have some more discussion, reserved time reserved later before you

conclude. So, if folks would like to intervene, react, share any comments or insights, please.

GULTEN TEPE: Thank you, Susan. We have a queue lining up.

NICHOLAS CABALLERO: Thank you, Gulten. Yes. I have India, China, and Japan. Let's begin with India. Go ahead, please.

SUSHIL PAL: Thank you, chair. This is Sushil Pal for the record. Again, it's a newcomer's question. The DNS, the deal is the worrying issue. I think we are facing these problems in and out almost every day. I think I'm actually intrigued by why calling it future work. I mean, is it not so emergent to be taken up right now?

SUSAN CHALMERS: Thank you for your intervention. So, we're waiting for the-- So, this has been an ongoing subject matter topic for the GAC. We've had, I think, a DNS abuse session every ICANN meeting for the past several years.

SUSHIL PAL: That's not the point. I mean, yes, but the items which are listed in the future work, there seem to be preliminary activity, which should be taken if you actually want to check DNS abuse. But it seems we are still looking about contractual agreements which vaccine can be enforced

actually. And that's the problem we in a country face. We have plenty of litigations going on, and we actually find ourselves completely helpless. We can still take care about the DNS abuse emanating from those domains only which belong to our country domains, but one which are outside, I think we're totally helpless and we have nothing except to throw our hands in the stair.

So at least the contractual agreements need to be taken up urgently on priority rather than-- I mean, I'm sure the community might be discussing it for quite some time, but that's the first thing we ought to be taking up as soon as possible. And because our action is not actually keeping up pace with which the cyber attackers or the hackers are coming up. We are actually lagging behind. I think presently, you can generate, you can do all kinds of hacking, using domain generation algorithms. Do we have all mechanism to actually monitor that? And how do we contain them?

SUSAN CHALMERS: Yes. Thank you. I completely agree with you that this is a matter of priority. And so, that's why it's so important that we encourage registrars in our respective jurisdictions to vote in favor of the amendments. And then in San Juan, I think we'll really have the opportunity to discuss further these specific topics that you mentioned. Thank you.

NICHOLAS CABALLERO: Thank you, Susan, for that. Thank you, India. And by the way, I absolutely agree with you at a personal level. I'm not speaking as the

GAC chair right now, but in any case. I have, China, Japan, and Columbia. China, go ahead, please.

WANG LANG: Thank you, Chair. I'm Wang Lang from GAC China. ICANN opened a voting period for the proposed amendments. And there are two thresholds to be made. For the RAA approval of registrars, accounting for 90% of the total registered domain name under management. And for the RA approval of registry, operators whose payments to ICANN account for two-thirds of total fees paid in the prior year. So, my question is, how well these thresholds have been reached recently? And is the prospect optimistic? Thank you.

SUSAN CHALMERS: So, I believe that there is a tracking link that ICANN has provided so we can watch in near real time, and we can see if we can have access to the link-- Oh, Fabien will be putting it in the chat. So, you can check on the progress there.

NICHOLAS CABALLERO: Thank you, Susan. So, China, you can check the chat room. Thank you for that. I have Japan.

NISHIGATA NOBUHISA: Good morning. And this is Nobu Nishigata speaking from Japan for record. And then maybe first, thank you very much for the great presentation. And also thank you very much for the other work so far to

those who are engaged in this work. And then I have a couple of questions first one, then some comment. And then first question is going to, about the slides, about the key terms just that Laurren mentioned in the presentation.

And some example, the key terms is like appropriate prompt action, or maybe reasonable. This was also used in the current tech study, for example, RAA 3. 18. And then is it going to be, like if we have some guidance on these words and then this guidance, whether this guidance would be applied to the existing text on the use of the same words. That's the first question.

Then second question is about the evolution of DNS, at the end of the presentation. I wonder if some of our colleague has some ideas what type of DNS abuse would be included in a future discussion. Or maybe thinking of some, I mean, I'm not sure about it, but expansion of the current narrowly or appropriately defined of the DNS abuse in SAC115. So, that's the second question.

And the one comment is I just totally agree with the Indian colleague, what he said. I would like to echo in it as Chair did. Looking at the Japanese, the not only the DNS abuse, but also some malicious conduct over the internet. And then we need to have some link between the GAC and those who control the ccTLDs. I'm not saying the ccNSO looking at what ccNSO is doing currently. And maybe Nick can say about it. I just thought I echo, and then maybe I think this is more like a shared issue in each government. So, just we encourage us, ourselves, to do further discussion in your future. Thank you.

SUSAN CHALMERS: I might just respond briefly to the first question, Nobu, and then turn it over to my colleagues for the second. In terms of the first question, those terms are further expanded upon in the advisory that was accompanying the amendments that's also published. So, I would encourage folks to take a look at that advisory, but they do still remain some very, open questions, I guess, you could say. And definitely worthy of discussion within the community.

LAUREEN KAPLIN: And just building on Susan's observations well observed. I think the notion would be if there are targeted PDPs on this action, then I think it would be with the end bit of the policy making process to decide how it's going to run through the contracts. So, if the same terms are used, certainly it's a possibility that then those outcomes could be applied throughout the contract when it makes sense to do so. What I'm saying is there's flexibility and that's going to depend upon the future policy work and the outcomes.

The other thing I would echo that we haven't mentioned that was also in the GAC comment is that there's work to be done both inside and outside of ICANN. And when I hear our colleagues from Japan and India talking about how challenging these issues are, particularly when you're in one country, and there's malicious behavior coming from other countries and you're trying to deal with cross-border issues. I mean, these are topic that certainly also involve negotiations and information sharing agreements and cooperation agreements country to country. All of that work is typically outside of ICANN that is very important work to enable law enforcement and consumer protection

authorities around the world to cooperate with each other to try and deal with these challenges. So, I did want to underscore that as well.

NICHOLAS CABALLERO: Thank you for that, Laureen. Just one thing. Japan, is that an old hand? Oh, okay. Then I have Columbia. Columbia is in the room? No? Okay.

THIAGO DEL-TOE: Yes. Thanks, Nico.

NICHOLAS CABALLERO: I'm sorry, sir. Because I saw your hand.

THIAGO DEL-TAO: No. I dropped because it was taken care by China. Thank you.

NICHOLAS CABALLERO: Okay. Thank you. Then I have the European Commission and Canada. European Commission, please go ahead.

PEARSE O'DONOHUE: Thank you. Good morning. Pearse O'Donohue, European Commission for the record. Just one observation as we consider areas for future work and the manner in which staff will be dealt with. Let me start by putting on record once again that the European Commission is highly supportive of the contract amendments, and we really do hope that the

voting will proceed and do reach the quotas. We think that this is a very positive step forward in the right direction.

However, we won't hide the fact that we would have hoped to be have been able to go further. And as we consider the manner in which we frame the future work, we have to also bear in mind that there was a public consultation in response to which absolutely zero, none of the proposals made by any of the submissions were actually taken into account in the final contracts.

And this reflects a certain attitude that the contracts are somehow outside of the multistakeholder remit. That they are contracts in the business sense between ICANN org and the contracted parties. When in fact, they are the very substance of the functioning of a key part of the ICANN and IAN in the sense of its remit. And I think we need to assert once again that there is a need and a place for the stakeholders in the multistakeholder process to be able to comment on and influence not just the shaping of the contracts in the way that it has been done, but also then to input directly on the implementation. Because as we've heard from several other GAC members already of the serious challenges that are faced by administrations as a result of DNS abuse.

And that is why I feel that whether it comes to the issue of proactive monitoring, which was not taken up, or a number of these issues, we have to ensure that the policy development process is targeted, but also comprehensive so that it appeals effectively with all of the issues which Laureen has presented to us. Thank you.

NICHOLAS CABALLERO: Canada. I have Canada next.

JASON MERRITT: Thank you very much. Jason Merritt, GAC Canada for the record. I just wanted to take an opportunity briefly before we move to another topic to just once again express Canada's full-on support for the contract amendments. And frankly, a genuine appreciation for the contracted parties OF ICANN for those that came together to negotiate this and come to something that was tangible, something that was incremental, something that was really a positive step forward. I think it's great that we're forward-thinking about next opportunities and things like that.

But from my perspective, we don't, for one second, take for granted that this is a given and that this sort of incremental progress is something that we need to pay attention to and see where it'll-- Excuse me. And excuse whoever coughs. Sorry.

Yeah. I just wanted to get that message out there that we've always been very supportive of this and very appreciative that this was something that the community had brought forward upon themselves and the contracted parties. And that was, I think, a monumental step forward. And there's a still a heavy lift here that needs to happen before we go through this, and we're very conscious of that. So, thank you.

NICHOLAS CABALLERO: Thank you, Canada. I have Iran.

KAVOUSS ARASTEH: Yeah. Thank you very much, and good morning to all. Please correct me if I'm wrong. Last year was some amendment, and I think we are still talking of amendment. Is it a further amendment? Do you know that what is the scope of this further amendment and what is the result of the first amendment? And did ICANN provide some briefing or some information on the scope of the amendment of last year, amendment of this year, and the result of that? Any feedback on that? Thank you.

SUSAN CHALMERS: Thank you so much, Kavouss. So, I'll be very brief, just in the interest of time. But this is the first, as it pertains to DNS abuse, this is the first effort towards amendments there. I believe there were previous amendments relating to RDAP. I could be wrong. I don't want me to mis-speak. But his is definitely the first concerted effort on DNS abuse to amendment contracts. Thank you.

LAUREEN KAPIN: And maybe just briefly, Kavouss. There were some briefing materials prepared on this. And also, ICANN org on its website has very good background about the proposed amendments. They are currently being voted on. They're not final. So, the status is that we're all watching very eagerly in hopes that they become approved in December. I just wanted to give you the procedural stance where we are.

NICHOLAS CABALLERO: Thank you very much for that, Laureen, Susan, Iran. Any further questions before we move on, in the room or online? Seeing none. Sorry. Indonesia, go ahead.

ASHWIN SASTROSUBROTO: Yes. Thank you for not putting it in the Zoom. What I want to know is we have the agreement on what the registrar should do for the DNS abuse and so on. I just want to know whether it is also something like certification system for the registrar, something like if you have to follow ISO security 27001, for example. There is a standard procedure that you have to follow, then you have to be certified and so on. How about this, the possibilities for that kind of process in the DNS abuse agreement? Thank you.

SUSAN CHALMERS: Thank you so much for the question. I am not sure about ISO security requirements and procedures, but I think perhaps we can discuss that further offline, if that's all right with you.

NICHOLAS CABALLERO: Thank you, Susan. Thank you, Indonesia. Any other question or comment? Seeing none. Let's move on with the agenda. Back to you, Susan.

SUSAN CHALMERS: Thank you. So now we will dive into our guest speaker presentations, beginning first with the DNS Abuse Institute.

GRAEME BUNTON: Thank you, Susan. Good morning, everybody. Apologies to the people who were in here on Saturday during the capacity building. You will have seen some of these bits and pieces before. My name is Graeme. I'm the executive director of the DNS Abuse Institute. The Institute is a project of public interest registry which operate the dot org TLD. And they created the Institute to try and solve problems related to DNS abuse across the industry. And so, we work moderately independently from the registry itself.

And I apologize for the somewhat rudimentary nature of these slides. I was added to this panel last night, and so they haven't had a lot of time put into them. So briefly, I'm going to talk about our Compass project and then about measuring abuse in general and then specifically about measuring the impact of the amendments that are being voted on right now. I'm also going to try and do this in eight minutes or less, so hold on to your hats.

So, we created this project called Compass. We really felt that the ICANN community really needed to engage in data-driven policy development around this issue, but also that registries and registrars weren't empowered with information either. And so, we really wanted to build a robust academically rigorous, transparent approach to measuring DNS abuse. And so, we launched this project last year.

We provide monthly abuse reports that are public. If you search for Compass DNS Institute, it should come up. I'll put a link in the chat in a moment. And so, we do this monthly reporting that includes aggregate trends across the industry, as well as sort of top 10 lists where we talk

about specific registrars and registries that have both high rates of abuse and low rates of abuse. So please check that out if you're interested in this topic.

This is a complicated slide that I don't expect everyone to fully ingest at this moment. In fact, if this is a topic measuring abuse that's important to you, I would suggest attending the ccNSO desk. There's a session this afternoon that my colleague Laureen will be presenting at, I believe Samaneh is presenting at, and is going into this topic in quite a bit of detail.

The short bit about this slide is just how measuring DNS abuse works in general. You have to consume some form of information about abuse. This is primarily done by RBLs, Reputation Block List. These are sources of information about abusive domain names. There are issues with those sources that is a much longer discussion. You need to clean these lists. You need to deduplicate them. And then what we're doing is that we're fingerprinting these sites, these abusive domain names, and the websites they point to. We run an algorithm to determine if they're malicious as in registered explicitly for harm, or if they're a compromised website, most often, a hacked WordPress, if you will.

And then we check uptime. We're monitoring that website in increasing intervals of time for up to 30 days. So, something like 5 minutes, 10 minutes, 30 minutes, an hour, 2 hours, 6 hours, 12 hours, and then every 12 hours for 30 days. That allows us to be able to measure not just mitigation rates, but time to mitigation as well. And then we produce that into these monthly reports that are available. Anyone can look at. Also, if there's any TLDs or registrars in the room, regardless if you're a

gTLD or a ccTLD, we provide custom dashboards to the community. All of this is free. To those specific gTLDs, ccTLDs or registrars, flood them to see their abuse reports, to see the data and have a sense of where they are compared to their peers.

So, this is our current reporting on the overall rates of abuse. I don't think it's sort of appropriate to make really broad suggestions about trends here. There's a bit of a step change between December 2022 and January 2023. This is almost certainly because a particular provider of free TLD services went offline. And I think we saw a lot of change within the industry there. If you pulled those out from the historical data, I don't know that there would be a large change in rates over time.

If we're thinking about the amendments and what impact they're going to have, my hunch is that over an extended period of time, we will begin to see the rates of abuse decrease as registries and registrars are incentivized to do more about abuse of registrations. I do not think that happens right away. I think it will take some real time. This community should think about the impact of those amendments and where that abuse is going to go. It does not solve cybercrime. Bad guys got a bad guy. And so, where does that work go?

So, this is, again, from all of our public reporting. This is about measuring mitigation rates. And so, as I said, we're checking these domain names over time to see what's happening. And mitigation could mean that the domain was suspended by the registrar. It could have been suspended by the registry. The registrant could have changed the website, fixed the compromise. It could be the hosting company got engaged. It could also be that the criminal finished

whatever activity they were doing and turned it off. And so, this isn't really talking about who's doing the mitigation, just that the harm is no longer present.

And you can see by and large across the industry, the green being was mitigated, orange being was not within 30 days, and the sort of peachy color is where we were unable to determine effectively. And the peachy color gets smaller because we got better at detecting what was happening over time. And so, by and large, the industry standard is somewhere around 80% of abuse that we see gets mitigated inside of 30 days. Which is pretty good. I think we'll see that creep up a little bit post-amendments. And that I would expect to happen relatively quickly where we can see these mitigation rates improve.

This is a screenshot from our dashboards that we provide to registrars. This is a particular registrar's median mitigation time So, this is how long they took within each month to mitigate abuse, and you can see there is some variability. But by and large, their median time is around 24 hours, which is pretty good. And so, all of that is to say the pieces that I think are going to be useful for understanding the impact of the amendments are going to be what I was just showing. Overall rates of abuse, overall mitigation rates, and median time to mitigation. And so, I think abuse rates will come down slowly over time.

Again, I'm very optimistic about this. It's my job to make a difference. So maybe take that with a grain of salt. I think mitigation rates are going to improve as the industry is incentivized to do that. And I think they'll get better at mitigating over time, and the time to mitigation will come down. And I think that's all I had for you today. Again, if you're really

interested in this measurement of abuse, please check out the ccNSO session this afternoon. Thank you.

NICHOLAS CABALLERO: Thank you so much for that, Graeme. Questions for our distinguished guest speaker, in the room or online?

GRAEME BUNTON: I should add because I'm terrible at adding it. We do all of this for free. None of this is a commercial service. So, if you're a registry or registrar or you're trying to understand abuse, please feel free to reach out. Our job is to help educate and work with the community. And don't be shy about doing that. Thank you.

NICHOLAS CABALLERO: Thank you again, Graeme. A very important point. So, I see no questions online or in the room. So back to you, Susan.

SUSAN CHALMERS: Thank you, Chair. I think it'll be-- The prospect of using the set at a kind of measure the effects of the contracts amendments in the future is very exciting. So, it'd be interesting to have that discussion as we go forward. So now going to pivot to ICANN. Please. ICANN OCTO.

SAMANEH TAJALIZADEKHOOB: Thank you, Susan. So, I'm Samaneh again. I'm a director of Security Stability and Resiliency Research at ICANN office of CTO. And I lead the

DNS Abuse Activity Reporting tool, which most of you may have heard of, the DAAR tool. This presentation is also made very quickly, so I hope it's informative, to being on the panel last night.

The DAAR tool is already existing since 2017, and the general fits is that it aggregates the Reputation Block Lists domains listed on Reputation Block Lists and it aggregates at the TLD level. So, there is counts per TLD. It maps them and combines them with the counts of domains from zone files and maintain counts per day and aggregates per month since 2017.

The tool has monthly reports that are published on public on ICANN Org DAAR web page, and registries have daily access to the numbers, to their own numbers via their most API, which is the ICANN API that registers use. Since the tool is in use for many years, it also is capable of creating longer term trends and reports.

This is the simplified visual of how it works. The inputs are domains listed on RBLs and zone files, and there is a process of cleaning, aggregating, dealing with coronary cases, and then producing metrics. These metrics are two types of metrics. Either raw counts or normalized percentages by size of TLDs. I'm trying to explain how the tool works in simple terms because that's what's we were asked the other time when I presented the tool to the GAC. And due to lack of time, I'm not going into many, many details of the tools, but please feel free to either interrupt me now or ask me later after the presentation, if you have questions.

So, this is one of the types of the plots that the tool creates and that is in the monthly reports. And this visual shows the distribution of the 4

different abuse types in legacy and new gTLDs. Basically, the message of the visual is that, depending on the type of the TLD, threats concentration could be different. Malware domains seem to be more concentrated in legacy gTLDs, whereas new gTLDs seem to contain more spam domains.

This is another example of visual that comes out of the DAAR monthly reports. This is the percentage of-- so on the y-axis, you see the percentage of abuse, and on the x-axis, you see the size of the TLD. And each circle is also a TLD in the plot per thread type. So do you see the higher the dots in the plots and the bigger the circle means the more abuse there is in that gTLD.

This is not included in the DAAR monthly reports. As you can see in the x-axis, this is a very long timeline I generated, especially last night for this meeting, because I thought it might be interesting to you to see a timeline of almost five years. That's why the title axis is a bit mixed, but this is basically how DNS abuse looks like from ICANNs perspective in the last five years that we are collecting data. For phishing malware, spam as a delivery mechanism, and command and control domains.

So, I know that DAAR project has been perceived in many, many different forms in the ICANN community. But the fact is the DAAR project as it is now has also certain limitations. There are things that the project can do and cannot do. The current state of the project can only report on threat activity at the level of TLDs. It can report on historical trends and time series data of the 4 thread types that a system collects. And that data, since it's aggregated and anonymized, cannot

be taken as to actions right away, but it can be indicative of where security threats are concentrated.

What the project cannot do is the project at the moment, so DAAR system at the moment does not provide data at the registrar level, only registries. And it does not provide any information about mitigations or mitigation strategies. The system does not have any mechanism to distinguish between malicious registered domain and compromised domains, and it does not publish names of TLDs, or registries based on their abuse.

So, what is next? It's been almost a year that we at the Security Stability and Resiliency group at OCTO are working on taking the project on to next level. We have received reviews, different reviews from the community teams, and we have taken those into account. We have been in consultation with different parts of the community. I have presented personally many times the project, got feedback from you. And so, we are in incorporating all of this and taking it to next level.

We are now defining requirements for the project. The projects is done internally, and it's perceived to be a measurement platform where it's modular. So, we are going to add functionalities and modules over time. Since there are many things that we want to do with this project, we are starting small and extending over time. The first module will be having metrics for registries and registrars, something that we are adding specifically on top of the DAAR system. There will be a dynamic dashboard to share visuals. There will be a search functionality for users. There will be different user levels. And there will be also

functionality for ccTLDs to participate in it. There will be also an API to pull data for researchers and academics who would like to use the data.

After the first module is released, these are just high-level things that we want to add to the projects in general, not at first. But after the first module is released, which is probably in a year time, this is also future work that we want to add.

STEVE SHENG: We perceive the system, the platform to provide domain level Reputation Block List data so that the community can have access through that. We perceive to add modules that measure uptime in a robust manner to be able to distinguish between types of malicious domains, meaning malicious registrations versus domains that are hacked or compromised. We want to add detection for parked domains, prediction, abuse prediction, etcetera.

I would like to note that we the researchers at the SSR team are working on the science behind each of the modules and we expect each year to add a module to the system. Again, more information on this will be shared in the same session that Graeme pointed, the ccTLD task session later today this afternoon. And I'm happy to receive questions.

NICOLAS CABALLERO: Thank you so much, Samaneh. Do we have any question? I mean, I have India. Go ahead.

T. SANTHOSH: Thank you, Chair. So, nice presentation, both the DNS abuse team as well as the one. So, basically, I would like to know whether one can mitigate the malicious domain under DNS over HTTPS or DNS over TLS. Because it is very difficult to detect the traffic. Ivan is also here. This question is for Ivan as well. Will you be able to detect the malicious domain through DOH or DOT? Thank you.

SAMANEH TAJALIZADEHKHOOB: Thank you for the question. The question that you asked has two levels. One is the detection part which is basically what you pointed is a mechanism to use to perform a malicious activity over TLS or HTTPS. That would involve the entity who does the detection. At the moment, at least what ICANN Org does is that for the DAAR project, we have other projects that we do a detection on DGAs or other things. But for the DAAR project, we don't do detection ourselves. We just use domains that are reported to other third-party sources. So, basically, we are not involved in that detection process. We just take the domains that are listed on the Reputation Block Lists and do further investigation to find evidence of abuse.

NICOLAS CABALLERO: Thank you, India. I have China.

WANG LANG: Thank you, Nico. This is this is Wang Lang from GAC China. We know that there's a committee against abuse in ccNSO, I mean DNS abuse standing committee. And there's also a small group in GNSO against

abuse. So, what's the difference between these groups, the responsibility or the focus or the outcomes? Thank you.

NICK WENBAN-SMITH: I'm happy to speak to that in more detail but I think it might be covered in my presentation to some degree which is yet to come. So, if you still have that same question after the presentation, let's have a chat conversation about it.

WANG LANG: Okay.

NICOLAS CABALLERO: Thank you, China. Any other question in the room or online? Seeing none. Back to you.

SUSHIL PAL: Can I just ask a question?

NICOLAS CABALLERO: I'm sorry. India, go ahead.

SUSHIL PAL: This is Sushil Pal for the record. What does ICANN-- I mean, do you have any plan to engage with those countries which are facing multiple cyber-attacks in terms of capacity building or engaging with them to what precautions they need to take?

SAMANEH TAJALIZADEHKHOOB: Sure. I think at least from OCTO, there is a technical engagement team that maybe you have already been engaged with or having contact with. We at the SSR are working with the dot IN ccTLD from India for the DAAR project. I know that they are very involved. Maybe we can connect offline, and I can connect you to our technical engagement team if you need trainings or help.

GRAEME BUNTON: If I can add briefly. Sorry. This is Graeme from the DNS Abuse Institute. We were recently at Vietnam to do outreach to the APAC region help do capacity billing within the registry and registrar community there. That's work that we undertake all the time to try and provide best practices and education to anybody who needs it. And so, feel free to reach out. We're also working with trying to bring more partners on board to our abuse reporting system called NetBeacon. That's a free service, and happy to engage there as well. Thank you.

NICOLAS CABALLERO: So, thank you so much again, Graeme and Samaneh Tajalizadehkhoob. Did I pronounce it well? So, any other question so far? If not let me give the floor to Chris. Chris, go ahead.

CHRIS LEWIS-EVANS: Yeah. Thank you, Nico. And Chris Lewis for the record. So, it's really good to be speaking to you. I've almost had withdrawal symptoms from speaking to the GAC. So, it's been a while since I was speaking as a

PSWG. But now I'm director of governmental engagement and internet harms at CleanDNS. And we managed DNS Abuse on behalf of registrars, registries and hosting providers. And today I'm going to go over how we do some of that evidencing of the reports of DNS abuse and the sort of information that's required and some of the reporting that helps with that mitigation.

So, number one is key is receiving reports. I know the PSWG have talked about it because I think I did is the lack of reporting from people in each of our countries. I think that's a standard thing that happens is driving reporting is really, really important. So, tools such as NetBeacon, which Graeme's just mentioned, are really important. We feed that internet beacon. So, thank you for that. We also take feeds from abuse lists. As Graeme mentioned, some of those need a of cleaning up. They're not very consistent. They're not a great source. However, it all adds to the evidence of abuse if you're able to get multiple sources.

Our clients have abuse ingest forms the registries and registrars and hosting providers. So, when you enter into one of their systems, that gets fed in directly into us if they're one of our clients and that gets managed. That's either a web form or an email address. We receive all of those. And then importantly is the cybersecurity side. So, there's a lot of information that they have. A lot of abuse that they detect and receiving stuff from that, from governmental search is really important.

I know the UK has a project about reporting suspicious emails that generally have links for phishing or credential stealing. So, receiving those sorts of reports at scale is really important to be able to mitigate the abuse and the harm.

So, continue on the reporting a little bit because it's really, really important. As CleanDNS, we understand that you need to mitigate as much as you can as soon as you can. And we will receive abuse reports from any source and for any registrar, registry or host. When we get those, they're processed, enriched, and evidenced. If they are our client, we will obviously deal with that, if they're not, we will get that to the appropriate party by using the DNS abuse institute's NetBeacon, they then relay that onto the appropriate party.

One of the things that we've seen from research that's really important on reporting is the feedback. Reporters don't like to report and for it to disappear in a black hole and never know what's happened to it. Especially if you've been a victim, it's really important to see some things happened because of their report. So, we do provide feedback on what's happened to that domain, and that in itself, we've seen has facilitated better outcome, more reporting. So, it's just another mechanism that we can get more and more reporting.

And the last point is really a point that Graeme raised, I think is really key for the mitigation of abuse is the time that it takes to take it down needs to be as short as possible. The shorter that is, the less chance that someone has click on it, the less chance that someone has to download the malware, the less amount of victimization that can happen. So, I think really good is the reporting on uptime because it's really hard to quantify the impact that a phishing domain or malware domain has had without all the reports. So, the best way of doing that is to have a shorter time as possible.

So, at the CleanDNS, we evidence each different type of abuse differently. A phishing email is not the same as a site that's deploying malware. You can't evidence those in the same way. So, you have to be able to qualify each of the specific harms. A lot of those can be captured visually, but not all of them. As I say download of a malware is really hard to take a screenshot off. Just doesn't work. So, you have to think about how you can evidence them and having proper procedures and practices put in place.

So, we automate that and make an actionable evidence record that then can be passed on to that appropriate party to do. So, I've listed some of the things that we look for when we're doing that. So, the actual report is really key because that shows that impact and that first initial harm. And then you will look at screenshots, header information, log data, URLs. A hash or the content is really important. For malware, we don't recommend you download the malware and send it to us as part of the report. We would much rather we don't have that, or you wouldn't expose yourself to that. And then any metadata yeah is really important.

So, from that list, the question we get is, well, is there a lot of PII in that? And on the evidencing of the report, we do not collect any PII. We do not need the PII to evidence the abuse that is going on. So, as much as possible, we try and automate that to keep the time down and collect all that information and gather it together to combine it to make the most actionable evidence package that we can so that the registry, registrar, or hosting provider can take the appropriate action.

Appropriate action, do we use PII in that? Mostly not. However, sometimes the most appropriate person to act on an abuse type might be the registrant. So, in that case, we would need to use either contact with the registrar to contact their registrant, or if it's a host of providers side, we might use the WHOIS to gather that data, to then help them with sorting out the compromised host that they have.

And over to questions or I don't know if you want to do that. I'll wrap up a bit. Thank you.

NICOLAS CABALLERO: Thank you so very much, Chris. So, now let me open the floor for questions or comments in the room or online. Laureen, go ahead.

LAUREEN KAPIN: Very quickly. You heard it but I wanted to underscore. Our last couple of speakers were asked very late in the game to help us with this session. And I just wanted to give a huge thank you and express my appreciation for them being able to join us and just really step up and present some very useful informative materials. So, huge appreciation to them.

NICOLAS CABALLERO: As a matter of fact, I was actually going to ask for a big round of applause for-- and I already have two requests for the floor. I have India and then Iran. India, go ahead first please.

T. SANTOSH: Thank you, Chair. This is Santosh for the record. So, basically on a SubPro or SubPro track or the new gTLD, as well as the other track on WHOIS. We get communication regularly from the GAC secretariat. But whereas on DNS abuse, we have to go to the ICANN site to find all the reports. So, I have a request to the GAC secretary that if the reports, which is the monthly report, could be shared in email to all the GAC representative it will be very good. Thank you.

NICOLAS CABALLERO: Thank you, India. I have Iran.

KAVOUSS ARASTEH: Yes. Thank you very much. I joined Laureen for the big round of applause. It was very rich and very exciting sessions. What I suggest that perhaps we should see that what are the ways and means to take a follow-up action for these things that we proceed further to see what are the feedback and what is yet to be done in order to bring back for instance the 80% will be increased to a higher level and so on and so forth. Any of these things that we need to concentrate on the follow-up action how we do that, because a lot of information has been provided yesterday and today on the DNS abuse and we need to find out how to proceed further. Thank you.

NICOLAS CABALLERO: Thank you, Iran. Chris, would you like to take that one or?

CHRIS LEWIS-EVANS: I think what we can do is support the registrars and registries in accepting the contract changes. Understanding, I think as Canada very well put at the start, that this is a really big step change for them. It really raises the floor in being able to tackle abuse. And us as a separate company really think this is a very positive step forward and welcome the amendments.

SUSAN CHALMERS: Thank you, Chris. And Kavouss, I'll just suggest that we turn to the GAC email list and exchange information and updates there and especially in anticipation of ICANN79 and send one. So, I would just encourage that we connect and collaborate there on the GAC email list.

NICOLAS CABALLERO: Thank you, Susan. Thank you, Chris. And I have Iran again. Go ahead please.

KAVOUSS ARASTEH: Thank you very much for the follow-up action. Yes. Our colleague from Canada mentioned that the issue relating to registry and registrar are outside the multistakeholder. And this is something between ICANN and these two contracted parties. How we could reinforce the situation to have some sort of active, I would say, participation or influence or active role in this issue that with between the ICANN and the registry and the registrar. What are the ways and needs that we could enforce this situation or send in the situation to have more active participation? What are the ways and means? Thank you.

SAMANEH TAJALIZADEHKHOOB: Thank you, Kavouss, for the question. From the research perspective, you can always-- the DAAR project takes on volunteer participants, ccTLD participants to the project. So, that's one of the ways where if you are volunteering to participate, you can provide zone file and also receive personalized monthly reports. And there are also trainings that the TE group provides regarding abuse and capacity building which are the resources that we have that can help.

NICOLAS CABALLERO: Thank you for that, Samaneh. Any other question? Any other comment? And this is certainly a fascinating topic and we could talk for hours and hours. But for the sake of time, at this point let me give the floor to Nick. Nick, please go ahead.

NICK WENBAN-SMITH: Thank you, Chair. If you can move on to my slides, please. Excellent. Thank you. So, just a quick overview of the agenda of what I'm going to be talking about now, if we move to data slide, that's it. So, just a little bit about the ccNSO, the task, the DNS Abuse Standing Committee. And then we do provide some tools and resources to the ccTLD. So, I'll take you through those.

We as a baseline project to understand a bit more about practices within the ccTLD community, we conducted a survey. So, I'll talk you through some of the interesting findings on that. And then it's been thankfully, very grateful to the promotion of my two-hour session this

afternoon specifically on deep dive on tools and measurements for DNS abuse is quite a complex area. So, we're having several presentations looking at this from different angles. And so that's a session we have this afternoon. And then our future work plans. I'm quite interested in the next sort of 6 to 12 months of evolution of what we're going to do going forwards.

So, you need to, for a moment, don't think about contract amendments, contracted parties, gTLDs, SubPro, all of that stuff. This is outside of all of that. These are the country codes which are very diverse as you can see from the slide. So, my role in that as the general council for dot UK, I've been there for 16 years. I've spent many years dealing with cybercrime, cyber issues, abuse, all of these types of policy questions. So, for better or for worse, I'm the chair of the standing committee on DNS abuse for the country codes.

And you'll see there's massive diversity. We have IDNs. There are just over 300 ccTLDs in total, if you include the IDN variants. So, it's a very diverse and interesting group of people. And we are not, and we won't be contracted to ICANN. We are sovereign entities essentially and we have a very strong relationship with our national representatives. We reflect the culture and diversity of every one of the different countries in the world, which is why we're all different as well.

So, we are not here to set policy. Policy is set domestically for the ccTLDs. We're more around sharing information and insights and practices, understanding awareness outreach, capacity building. We have a very strong community of open and constructive dialogue. it's a lovely community. And fundamentally, we want to do the best we can

to mitigate the effect of DNS abuse. And so basically, we are trying to push down the levels of abuse globally, not just in one place but everywhere.

So, in terms of our resources we provide, the first thing is a repository. This is led by David McAuley of VeriSign. And this, basically, provides dedicated resources specifically tailored towards the ccTLD community about abuse. So, that's the first thing. And you can see here on the record, we encourage members to if it's helpful for ccTLDs, then please share it.

We also have a dedicated abuse email list which is being launched this afternoon in fact. So, that is going to be another resource so that the ccTLD community will be more connected with each other and information can be shared quickly. It is not confidential as such, but it is a closed list restricted to the ccTLDs.

Okay. So, this is really where you are. I wanted to give a little bit of time on this survey. So, in fourth quarter of 2022, we conducted a global survey of ccTLDs practices when it came to abuse. They didn't have to be members of the ccNSO, but we did get 57 unique responses as you can see here. Some of those responses reflect more than one ccTLD. So, it's not a compulsory survey. It's an opt-in. So, you need to just remember that this is a self-selecting sample of people who have responded to the survey.

And in order to encourage participation, some people are sensitive about confidentiality. We don't want to give threat actors information which might be helpful to them. So, some people wanted to do this on a confidential basis which we respect.

So, we had the survey. We've had had three sessions of presenting the survey details in three different goes and they set out here. Very interesting and it was very useful in terms of formulating what we're going to do next and understanding properly attitudes and behaviors within the ccTLD community.

So, it was very interesting. Like I said, the ccTLDs are so diverse globally which is sort of obvious when you think about it because all the countries are diverse globally. But it was very interesting that there's the huge range of ccTLDs from the governance models registry, abuse levels. Obviously, we had regional variations but even within regions, there's a huge amount of diversity. So, that's just was a striking finding.

So, if you just go to the next slide, I will summarize. So, in ICANN76 Cancun meeting, the survey results focused on the top-level actions that different ccTLDs take when they encounter DNS abuse because it turns out it's not necessarily the same across the mitigation practices and response to abuse is different. And that actually is quite interesting because take my example. We do not define DNS abuse. We have criminality and abuse. And those are the things that we take action on. So, depending on what has happened, the mitigation and intervention might need to be tailored towards what's specifically you see.

So, that was an interesting example there. A lot of us I think look at the abuse on a risk-based assessment. But some will automatically suspend the domain or take it out of the DNS immediately upon notification by an appropriate notifier. Moving on to the DC meeting ICANN77, we had a lot of focus on the different registry models. Because as you can see, some ccTLDs do not permit a new registration

to be created without certain preregistration information being collected and validated.

And what we were trying to do is to look at whether there is a correlation between the preregistration, data validation, post-registration data validation. Nearly all of us do some sort of data validation, but we were trying to see if there was a relationship between data validation and DNS abuse levels observed. So, that was also a very fascinating actually exercise.

So, what I really want to emphasize, and I think if there's one thing you remember from this presentation is that your ccTLDs are almost the safest TLDs globally. So, the levels of abuse that are observed either through our own analysis and self-reporting or through the objective analysis and reporting we get through the DNS Abuse Institute. Maybe this is a little bit like checking people's homework, but we did check against the DNS Abuse Institute data, the self-reported data to see whether or not people were being truthful I suppose. And it turned out if anything they were overestimating the amount of abuse.

And one of the reasons why we're having a dedicated session this afternoon on specifically how you measure abuse, the tools and procedures that are available. The reason we're doing that is because 38% of our respondents in the survey said that they were not sure or did not know the amount of abuse that they had in their TLD. So, we want to make sure that after this afternoon session. that 38% goes down to 0%. Everybody should have a good handle on one of the most fundamental things about running a good TLD which is are your systems being abused by bad actors. And if so, to what extent? Are

there policy interventions that you can make which would reduce it? This is what we want to empower people, hence the session.

I just want to say that one of the reasons that people were not sure about the amount of abuse is because in some small TLDs, where they do quite a lot of checks and registration checks or they may have a nexus requirement to that nation state, they're not open. The amount of DNS abuse was so small that it's actually very hard to observe. So, in some months they have zero and some months just single digits. So, it's very, very low levels. Hence some of those respondents genuinely had a good reason to come back and say "we're not sure" because they didn't see enough to measure it fundamentally. So, very interesting.

Personally, I was always suspicious. And we talked a little bit about the free registrations model which was good for us in terms of timing because that basically stopped just as we were doing this work. But one of the hypotheses is that very cheap domain names should have a positive correlation with high levels of observed abuse. And actually, what we tend to find is that the larger TLDs, so we're in beautiful Hamburg, the host nation is Germany. One of the largest ccTLDs you probably know is the dot de, the German country code.

It's run very efficiently. It's in Germany. They have lots of domains. It is very cheap to register domain in dot de. Their levels of observed abuse are incredibly low. So, that we found that it wasn't easy to prove the hypothesis that very cheap equals lots of abuse because there's some really good examples of very large excellently run cheap TLDs with actually not very much abuse. So, that was another sort of

interesting finding. It helped us give a little bit more sophistication to the nuances that you get with these sorts of topics.

So, I'll just wrap up. We had a webinar which we covered the final set of questions around the regional variations. And within our definitions of abuse, there's the ICANN definition, but actually, for most ccTLDs, the definitional question is not limited by the constitutional divide between content abuse and technical abuse. So, actually it was very interesting to look at the fact that most of us say, for example, with CSAM, would count that as DNS abuse even though it's on the content layer and not on the technical layer.

Yeah. So, as I said, relatively low levels for the ccTLDs. There's a huge variety of different responses and the ways that we tackle abuse is very different, but we generally do all tackle abuse in our own way. Registration checks is a fascinating area. It is different from region to region. But basically, we do quite a lot of registry validation. Sometimes not necessarily with the target of reducing abuse, but just because as the custodian of a national database, we actually like the data to be accurate and that is in itself a laudable objective.

And finally-- Oh, I have this problem myself when you press the thing and-- Anyway. Two goes forward too actually. Yeah, just a plug for this afternoon session where we're having a two-hour specialist deep dive on different perspectives and tools for measurements of DNS abuse. We have four excellent sets of presentations including the DNS Abuse Institute, the DNS Research Federation from the ICANN DAAR team. And we also have, there's a collaboration between two ccTLDs, the Dutch and the Belgians where their technical teams are doing a collaboration

using AI techniques to try to be more predictive and more effective in terms of mitigation. So, that is this afternoon.

And I think to answer the question from China earlier. That session is followed by a discussion between myself and Bruce Tonkin, who's the vice chair of the DASC and the leadership team of the gTLDs Registries Stakeholder Group. So, they have a leadership team on DNS abuse and we're going to have a conversation between us around the commonalities between gTLD abuse and measurement and ccTLDs abuse and measurement.

I think I'm acutely conscious. We actually operate a number of gTLDs as well as the ccTLDs. There's no point the ccTLD is being brilliant and clean if we're just pushing the abuse into other places. So, we're trying to get better coordination across all of the TLDs because that's the idea we're really to effectively combat it on a global level. And I think I will say just going if you move on to the next slide, you can see our plans for the future which is more stuff on data and registration policies and mitigation governance models.

And also, I'm personally very interested in the vertical cooperation between registries and registrars and how good examples of that could be discussed and used, socialized for everybody's benefit. So, that's our work plan going forwards. And that is the end. Sorry. We are a little bit tight for time, but I'll hand back to Nico. Thank you.

NICOLAS CABALLERO: On the contrary. Thank you, Nick. Does the GAC have any questions or comments on this topic for Nick? And I see Japan. Go ahead please, Japan.

NISHIGATA NOBUHISA: Thank you very much for the great presentation. And I have two questions to ask your opinion or your view or how you observed internet. The first one is, I saw there's some great good practices to prevent or maybe discourage the DNS abuse via the ccTLD. Is there any way to leverage the ccTLD's good practice to aspire gTLD related guys, I mean, the registries and registrars for at least some better practices to, like you said, in other words prevent or discourage the DNS abuse or some other malicious conduct in the internet?

The second question is about I see some diversity in the ccTLD, I mean the countries. You presented some good practices and good countries including Germany. But on the other hand, I see some countries who has the ccTLD with some vulnerabilities to do some malicious conducts over the internet which is worse than the gTLD and the registrar. So, if there are any further activity from your side to encourage or evangelize these countries to aspire the activities in these countries. Thank you.

NICK WENBAN-SMITH: Thanks, Nobu, for the question. So, in the first question, our philosophy is to show not to tell. But I think we all, particularly the ccTLDs tend to have either not profit or some sort of public interest public benefit sort of constitution. I think reputation is extremely important. So, I think by encouraging good practices people can see the benefits of reputational

benefit. It's good for the country. It's good for the digital economy. It's a great driver of growth. That sort of reputational thing is really important.

So, if you can see good examples, we hope that people will copy good examples and very happy to share. So, we hope that sharing good examples in and of itself raise its standards because people will choose to do the right sorts of things.

Secondly, in terms of the gTLDs. I think we can't create policy for gTLDs, but you shouldn't forget that many of the good gTLDs do many things over and above the minimum required by ICANN and their contracts, and that is totally fine. So, we like to see people to adopt things voluntarily because it's the right thing to do, not because of legal obligations and other sorts of things. I think reputationally, we all live or die by the quality of the TLD. And I think we all try to encourage an innovation and best practices in these areas.

NICOLAS CABALLERO: Thank you for that, Nick. Reputation is indeed a very important thing. We can go all the way back to the Romans and Julius Caesar. But I have Chinese Taipei. Please, go ahead.

KEN-YING TSENG: Hi. It's Ken-Ying from Chinese Taipei. My question is short. Are there any DNS abuse preemptive measures taken by the ccTLDs that are different from those taken by the other TLDs? Thank you.

NICK WENBAN-SMITH: That is a good question. I think there's a lot of commonalities and I think-- I don't think it's easy to generalize like that. Because for example, some gTLDs are very closed and specific. If you look at say pharmacy or dot bank, they pretty much have no abuse because they do a huge amount of registration and those gTLDs are only eligible to licensed banks and registered pharmacies.

So, you'll see that sort of check sometimes is done in some ccTLDs, but some ccTLDs, and I would put the UK and Germany in the same thing, were quite similar in philosophy to gTLDs, they open TLDs like org. net. So, I think there's a lot of overlap, but I don't think you can generally say that there's something that only ccTLDs do which makes them better.

And I think just to reflect on that, I myself am a bit surprised that we have in the ccTLD, is basically about, I don't know what factor, but it's a fraction of tenth. So, it's a factor of 10 less than the gTLDs in terms of the observed abuse. And I think part of the reason I'm so interested in the tools and measurement is that I really want to understand why this is, because I can't really understand. I mean, I know obviously the British people are very honest and we don't have any criminals but it's not a tenth of the global level of criminals. So, there must be something going on. And I think I'm very interested to try to get under the skin as to what it is that makes these ccTLDs so good. Thank you for the question.

NICOLAS CABALLERO: Thank you for the question, Chinese Taipei. Thank you, Nick, for the answer. Chris, go ahead.

CHRIS LEWIS-EVANS: So, not to do Nick's job for him but one of the different things that the ccTLDs are doing differently from the gTLDs at the moment is with center. They've created an information sharing center which I think is really key to learning what abuse is occurring, what best practices and being able to share that amongst the different ccTLDs at the moment. But I know there's probably some hope to expand that as well and that's a really welcome step that I know the GAC has talked about before. Thank you.

NICK WENBAN-SMITH: Just briefly. I think that is a really important point. And we've talked a lot about specifically DNS abuse through a very narrow prism. And I think it's important to consider cybersecurity, whether that's infrastructure resilience or other forms of cybercrime in a more holistic way. And certainly, the ccTLDs, we do have specific information sharing bodies to tackle cybersecurity and cyber resilience more holistically than that, and that may be part of the answer. I don't know. Thanks.

NICOLAS CABALLERO: Thank you again, Nick. Thank you, Chris. Any other question or comment at this point? I see none online. So, if that is the case, I will give back the floor to Susan Chalmers from the US. Bear in mind, you're the only one separating us from lunch. No. I'm joking. Go ahead.

SUSAN CHALMERS: Just very briefly. Graeme, Nick, Samaneh, Chris, thank you so much for dedicating your time to informing us during this session. We really, really appreciate it. And whether you are an end user, registrant or government, let's all encourage our registers and registrants to vote in favor of those amendments. All right. Thank you so much and let's-- Yes.

GULTEN TEPE: Susan, thank you. Before we close this session and, Nico, I'm very sorry to interrupt. We have Iran on the queue.

NICOLAS CABALLERO: Go ahead please, Iran.

KAVOUSS ARASTEH: Thank you very much. Sorry to take your lunch time. I think during this discussion, which was very useful and important, reference made on several times on the cybersecurity, cybercrime, cyber threat and so on and so forth which has direct impact on the DNS and DNS abuse. If and only if we have to also take that into account, I am a little bit surprised that in other area outside the ICANN, there is a resistance from some government present at the same meeting that you are to do anything with respect cybersecurity, cybercrime, and cyber threat in regard with the DNS.

So, we GAC members with the government, we should not have two hats, we should have one hat. Either it has some impact or does not have impact. If it has impact, why not? We could also study outside the

ICANN as it was mentioned. It was about a week ago in ITU, there were council working group dealing with the DNS, dealing with the IDN and the issue was on the table and there was a rejection from some countries. I don't want to name any country but there was a rejection and the issue about ourselves.

So, we should have more or less a confirmed position in all areas but not having two different hats and speaking in two different positions with respect to the same subject. Thank you.

NICOLAS CABALLERO: Thank you very much, Iran. Anybody would like to take that question? We're absolutely out of time. Thank you for your comments, Iran. A big round of applause to our fantastic presenters today. So, we're going to break for lunch now. Sorry.

[END OF TRANSCRIPTION]