ICANN82 | CF – GAC: Discussion on DNS Abuse
Tuesday, March 11, 2025 – 10:30 to 12:00 PST

UNIDENTIFIED MALE: Good morning, everyone. Please take your seats. We're about to start.

GULTEN TEPE OKSUZOGLU: Hello, and welcome to the ICANN82 GAC discussion on DNS Abuse session on Tuesday, 11th of March at 17:30 UTC. Please note that this session is being recorded, and is governed by the ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment policy.

During this session, questions or comments submitted in the chat will be read aloud if put in the proper form. Please remember to state your name and the language you will speak in case you will be speaking a language other than English. Speak clearly and at a reasonable pace to allow for accurate interpretation, and please make sure to mute all other devices when you are speaking. You may access all available features for this session in the Zoom toolbar.

With that, I will leave the floor over to GAC Chair, Nicolas Caballero. Over to you, Nico.

NICOLAS CABALLERO

Thank you, Gulten. Good morning, good afternoon, and good evening, everyone again. Welcome to this session on DNS Abuse mitigation. We have a fantastic list of guest speakers. We have Leticia Castillo from ICANN compliance. We have Siôn Lloyd. I'm sorry, is that the right pronunciation, Sean? Okay, he'll get here sometime. We have Graeme from the NetBeacon Institute. We have Reg Levy from Tucows. We have Luc and Jeff. Welcome, everyone.

And the topic leads from the GAC are Martina Barbero from the European Commission and Tomo from Japan. So, we have some interesting discussions about different details and nuances as regarding DNS Abuse. And for that, without further ado, let me hand over the floor to my distinguished colleague from Japan, Tomo. All yours, Tomo.

TOMONORI MIYAMOTO

Thank you, Mr. Chair, Nico. Hello, everyone. Welcome to the GAC DNS Abuse session. I'm Tomonori Miyamoto from Japan. This session is led by Martina from [inaudible] who joins this session online. And I, Tomo, from Japan. For this session, we have distinguished speakers. Leticia from ICANN Compliance and Siôn from ICANN OCTO. Jeff from SSAC and Luc from CPH, and Graeme from NetBeacon. Thank you very much for joining us. Next slide, please.

Okay. Here's the agenda for this session. We will share and discuss the results of GAC survey on DNS Abuse, and the ICANN contract compliance updates, INFERMAL not infernal report and Domain

Metrica. And we will discuss the next step for DNS abuse mitigation. Next slide, please.

Let me introduce briefly some background and context of this DNS Abuse session. As we see, dealing with DNS Abuse is our important issue. We already had some discussions on DNS Abuse here in Seattle with SSAC, NCSG, and ALAC in the previous session. It also has some linkage between the data accuracy issue we talked yesterday. Based on the ICANN contract, the RA and RAA, gTLD registries and registrars must respond to report of DNS Abuse.

These contracts were amended April last year, so it's almost one year. There are various understanding of contexts and approaches towards the DNS Abuse. In addition to the technical cybersecurity issues, some countries are working on online harm such as CSAM, and copyright infringement like manga piracy in Japan. It should be noted that the definition of DNS Abuse in the ICANN contract is clear and limited. Perpetuating malware, botnet, phishing, pharming, and spam. However, there would be some relevance or mutual problem in the route between the DNS Abuse and various type of misuse.

To deal with the challenge of the DNS Abuse, we think it's important to cover ongoing work within ICANN, review some relevant data, and share good practices about efforts outside of ICANN. Next slide, please.

Thank you. Some of you might remember this chart. This shows the landscape of the relevant community. The green square shows the scope of ICANN contracts, and it is fairly limited. To deal with the

problem effectively, we may need to consider the relation in the blue square such as contracts between registrars and resellers. In addition, we may also seek some cooperation between extended community in the red square such as a trusted notifier program. A lot can be done beyond the limit of ICANN contract. Next slide, please.

This is the path we made so far and go forward. Last autumn, we had a discussion in ICANN81 Istanbul talking about what can be done within ICANN. We had briefing from ICANN compliance and discussion with stakeholders including SSAC and CPH. Earlier this year, January and February, we made the GAC survey on DNS Abuse. This survey covered GAC members' understanding situation and cases on DNS Abuse, including approaches, extended community collaboration, data monitoring, etc.

In this session today, we will review the evidence and look forward. We will share the results from GAC survey and have presentations from ICANN about compliance updates, informal and Domain Metrica. We will have a panel discussion on them. Lastly, we will have a discussion on the next steps. Based on our discussion today, we will consider our next step. One of the ideas that will be talked in Prague is cooperation throughout the ecosystem. Let's move on to the next part. Martina, the floor is yours.

MARTINA BARBERO Thank you very much, Tomo. And it's great to be here, and be presenting this session, although from distance. I'm Martina Barbero, European Commission. I'm a DNS Abuse topic [inaudible]

together with Tomo. And in the next part of this presentation, we will focus on briefly presenting the results of the GAC survey on DNS Abuse that we launched at the beginning of 2025. So, if we can go to the next slide already, we can dig directly into the topic.

So, this is a survey that was planned already according to the GAC strategic objective 4 on DNS Abuse. Our idea was to survey GAC members in order to understand a bit better the expectations and concerns of governments in relation to this topic. And as topic leads to understand how we can, through ICANN sessions in person and inter-sessionally address and meet the expectations of GAC members.

We opened the survey in January, and closed it in February, and we received in total 21 responses. You will see on the slide the geographic distribution. So, we do have all the continents represented with different levels of participation, of course. And let me pause here to sincerely thank all the GAC members that submitted a response to the GAC survey because it was really helpful for us to gather this perspective. Although we don't have a statistically representative sample, I think this is already very informative in terms of planning our work on DNS Abuse and understanding a bit what are the GAC member's interest in the domain regarding specific topics to be discussed in relation to DNS Abuse.

So, if we go to the next slide, before we go into the details, what we wanted to do very briefly is to mention the highlights from the survey, and there are three main highlights. So, as you might have

expected, the survey confirmed that DNS Abuse is a priority for GAC members. There is no doubt about that. What also emerged from the survey is that GAC members, they have a wide range of approaches to this topic. And they also have different best practices and different types of initiatives. So, there is a diversity in how GAC members address DNS abuse, which makes the findings of this exercise even more interesting.

What also emerged from the survey, and this is the second highlight, is that in general, there is appreciations from GAC members towards the efforts that are put into fighting DNS Abuse by the ICANN community and ICANN org. But there is also the recognition that this is a topic of extreme importance and urgency, and that there's a need to do more. We need to step up. And a final highlight from the survey is that, there is a belief amongst GAC members that the GAC has an important role to play as part of the ICANN community in progressing on the work on DNS Abuse.

And we will go into the details a few moments later, but there are a number of things that the GAC can do, including monitoring compliance with the contract amendments, but also discussing policy developments, which is something we will do today, producing guidelines, fostering collaboration within and outside ICANN, as well as addressing new trends and sharing best practices. So, these are the key highlights. And if you need to retain only one slide from today's presentation, this is maybe the most important one. But now, let's go into the details of the different parts of the survey. So, if we can go—perfect, thanks.

One part of the survey was dedicated to understanding what is the GAC members' definition of DNS Abuse. What are the approaches and best practices towards this topic, and whether they engage in community collaboration. As you see from the slide, the definition of DNS Abuse adopted by GAC members is largely the ICANN definition. Forty-four percent of GAC members who responded to the survey use the ICANN definition. But there are a few, a quarter of them, who have a broader definition including other aspects, for instance, covering online harm, or CSAM. And there are a few respondents who are currently working on a definition, but don't have one adopted yet.

And as I mentioned earlier in the highlight, what we also saw from the responses is that GAC members have different approaches for dealing with DNS Abuse that span from legislative initiatives, and policy framework to cyber initiatives together with the CERTs, as well as collaboration with ccTLDs, collaboration with other players beyond the DNS strict sense ICANN community. So, a wide variety of tools in the hands of the GAC members, which also results in a wide variety of best practices.

Amongst the best practices that were included in the responses, we find proactive measures for addressing DNS abuse. Public-private partnerships, whether it's with the contracted parties like registrars and registries, or with other partners from, for instance, civil society. And then we have, of course, work to promote the adoption of security standards, including through the use of financial incentives, know your customers' initiatives, and interestingly, AI as well. I think we've heard about the dangers of AI

in terms of impersonification, and the challenges that AI pose in terms of DNS abuse. But what we see from the survey is that GAC members also use AI as a way to respond and mitigate DNS Abuse.

And then in terms of community collaboration, again, a great variety of players that are involved in collaborations with GAC members spanning from the internet service providers to law enforcement, agency, CERTs, intellectual property authorities, and else. And as you see, we have actually 60 percent of GAC members that responded to the survey indicated that they engage in community collaboration of this type. If you go to the next slide.

The second part—oh, back one slide. Thank you. The second part of the survey was dedicated to understand how do GAC members monitor DNS Abuse? And here we asked about data sources. Where do GAC members find data about DNS Abuse? There are some common tendencies that we see emerging through the responses. There are some GAC members that do have dedicated websites for the public to report fraud. Most of the GAC members use external sources, and they also engage in information sharing with both governmental and non-governmental agencies.

A lot of them cooperate with the CERTs, of course, and there is a strong majority of GAC members that also use ICANN sources, whether this is publications or reports like INFERMAL that we will discuss later today, different types of sources that come from the ICANN community. So, there are different approaches to gather data, but there are some common data sources that we can identify. And this was important to know to see what type of

evidence we dispose of when we talk about DNS Abuse. If we go to the next slide.

A crucial part of the survey was actually aimed at understanding GAC members' satisfaction and judgment of the efforts of the ICANN community in addressing and preventing and mitigating DNS Abuse. So, there were four different questions, and each of them targeting a different stakeholder in a sense. So, we have a question asking GAC members to evaluate the efforts of—asking GAC members to evaluate the efforts of ICANN org. Then we asked to evaluate the efforts of the registries and the registrars in terms of how effective were the contract amendments obligations.

And then we asked the GAC members to evaluate the efforts of the contracted parties. And as you see from the screen, and then, we go into the details, but there's quite some, let's say, consistency in the ratings. A bit lower satisfaction towards contracted parties' efforts, and we will see why in a second. But overall, as I said at the beginning in the highlights, GAC members seems to be appreciative of the efforts done by the community and rate these efforts quite highly. So, if we go to the next slide.

Maybe a bit more specific on how do GAC members see ICANN org efforts in relation to mitigating DNS Abuse. I think there is a general sense of satisfaction, but also, recognition that progress is not as fast as it could be, and effectiveness may also be higher. So, I think GAC members in general encourage ICANN org, and the new CEO to be even more ambitious in what they set as objectives for themselves in this domain. Regarding the appreciation of the

efforts from contracted parties, I think there is a general sense of satisfaction again in recognizing that the efforts are there and are significant.

But there's also the understanding that there are still a lot of inconsistencies between contracted parties. Some contracted parties doing still the bare minimum, while others are being much more effective in addressing DNS Abuse. So, there are important margins of improvements if we want to achieve industry-wide progresses. And then when we look at the satisfaction towards the registry agreements and registrar's accreditation agreements and the new provisions, strong consideration of the fact that this is a significant step forward, but we're also not having enough data at the moment to measure their effectiveness.

But also, and consistent with the GAC position in this matter, the recognition that the amendments leave some gaps, because some areas are not covered by the contract amendments. For instance, the amendments that do not oblige contracted parties to have proactive measures, nor to transparently report on their efforts. And they also don't cover the entire value chain. For instance, resellers are not included. Some GAC members also draw the link with the question of accuracy. So, these are some aspects that are not currently covered by the contract amendments, but that GAC members also consider important. If we go to the next slide.

And I think this is my last one on the survey. So, the last part of the survey was actually aimed at asking GAC members what they would like the GAC to focus on when we work on DNS Abuse. What

are the priorities? What we should be aiming at? And especially in preparation of the new round that will open next year. And I think we could cluster the responses of GAC members into four pillars that you see now on screen. So, on the one hand, there is a role for the GAC in following up, and monitoring the implementation of the contract amendments. So, liaising with ICANN compliance and ensure that the bar in terms of addressing DNS Abuse is raised before we get to the new round when new players enter this domain.

Then there is a sense of importance of considering targeted policy developments. I think we discussed with ALAC also earlier. So, there are different areas in which targeted policy developments could be helpful on specific types of DNS Abuse or building on the findings from the INFERMAL report, proactive measures. So, there's a list of topics that could be relevant when we think about policy development.

There is another pillar or cluster of responses that relate to the role of the GAC in producing guidelines and fostering collaboration. And what I mean by fostering collaboration is not only ensuring that the GAC speaks with the other communities within ICANN, but also making links with what happens outside ICANN. And some GAC members also felt it was important to highlight the need to develop guidelines on how to address DNS Abuse effectively, and to do so before the new round.

And finally, I think this is also linked to discussions we had, for instance, with SSAC yesterday. The GAC should play a role in

addressing new trends and sharing best practices. So, technology never stops. Technological development never stops. So, we need to look at the new threats that emerge from these technological developments. Quantum related impersonation, anything that has to do with AI, and also, empower best practice sharing, including between the gTLD and the ccTLDs. So, this is really something that some GAC members highlighted.

A final point that is not in one of these clusters, but came across multiple responses is also the link between DNS Abuse and the work on registration data, for instance, on accuracy. So, this is also an element that as topic lead we need to take into account when we move forward. But I think this slide is basically cutting down our work as topic leads in terms of topics of interest for the GAC, and things that we should be addressing when we discuss DNS Abuse. I think at this point, we have a short Q&A if anybody has questions on this, but I give the floor back to you, Nico, to moderate the queue.

NICOLAS CABALLERO Thank you so much, European Commission. Always a pleasure to listen to your presentations. Before I give the floor back to Tomo, to Japan, to my right, let me open the floor for questions or comments, both in the room or online. The floor is open.

MARTINA BARBERO I think there is a question on the scale for one of the slides that I showed. I think the question is, what does one mean on the scale if

it's from best to worst or vice versa? And I think the question was turned in a way where one was really people not being satisfied or happy with the efforts and for being fully satisfied. So that's the scale that we used.

NICOLAS CABALLERO: Thank you again, Martina. The floor is still open. Any comments, thoughts, questions? I see no hands. So let me get back to you, Tomo. Over to you.

TOMONORI MIYAMOTO: Thank you very much. Next slide, please.

Thank you. Next is the ICANN compliance update. So, I will invite Leticia. So, the floor is yours. Thank you.

LETICIA CASTILLO: Thank you. Hi, everyone. My name is Leticia Castillo. I am a Senior Director with ICANN Contractual Compliance. Thank you for the opportunity to provide an update on the enforcement of the DNS Abuse requirements.

I received some questions in advance whose answers I tried to incorporate into today's presentation. But of course, I'll be happy to answer any additional questions. Next slide, please. Next slide. Sorry. Thank you.

From April 5th through December 5th 2024, we compliance resolved 204 investigations into the DNS Abuse requirements that exist in

the RAA and the RA through informal resolution. This means that no formal notice of reach was required. And this led to the suspension of over 2,900 abusive domain names, and the disabling of over 365 phishing websites. As of March 5th 2025, so last week, we had 46 DNS Abuse investigations ongoing that have already led to the suspension of over 5,400 malicious domain names. So far, our compliance cases resulted in more than 8,000 abusive domain names mitigated.

And this is in addition to the remediation plans that contracted parties implement as requested within our compliance cases to remain compliant. And in addition to the actions that registrars and registries take to combat DNS Abuse and to fulfill their contractual obligations without ICANN compliance ever contacting them. We have sent three formal notices of breach related to the new DNS Abuse requirements. A notice of breach is issued only when the informal stage of our process is exhausted without resolution. And the informal process typically comprises three notifications, two phone calls, where we contact the contracted party. We provide information about the matter, and what is required to provide evidence of compliance.

But the process can be and is expedited when, for example, we discover repeated failures of previously remediated violations. The three notices of breach are ongoing while the contracted parties work on remediation plans that they're implementing to not only become compliant but remain compliant moving forward. And while we continue to monitor and review their situation. And extensions to the deadlines are not uncommon when contracted

parties are implementing remediation plans to take time, but under certain conditions.

For example, no extension is granted if identified abusive domain names continue to be active, and prolonging the exposure of potential victims to the DNS Abuse. Next slide, please.

I mentioned that we have 46 ongoing investigations. Approximately 48 percent of those were results from complaints that were submitted by self-identified information security researchers. We have complaints also submitted by IP lawyers and brand protection associations, approximately 15 percent of those. Thirteen percent of our complainants selected the category other within our form, and these were normally representatives of the companies being impersonated.

And also, users who received phishing emails or phishing texts with the domain name and reported it. Twenty-four percent was composed of other smaller percentages that include, for example, other contracted parties, registrants, etc. Next slide.

In terms of geographic distribution, most complainants indicated that they were reporting the matter from Asia/ Australia/Pacific Region and North America, followed by Europe and Latin America as you can see on this slide. Next slide.

In addition to enforcing all contractual requirements through the processing of complaints, we conduct two audit rounds per year, each lasting about six months. A dedicated audit team within compliance assisted by KPMG evaluates the data gathered from the

contracted parties and about the contracted parties to assess compliance. Something to point out is that audits can also result in formal notices of breach, and that we publish a report that includes our key findings and lists of auditees at the end of each round.

In October, we launched a registry audit that included DNS Abuse mitigation requirements. The questions in the audit aim to confirm, verify that the registries understood the obligations and have the necessary processes in place to comply with them. Considering this, the selection of auditees was partially based on internal and external rankings related to DNS Abuse. It's important to note that selection only does not mean that the TLD is not compliant. We are currently reviewing all the information and records that we gathered to make that determination, and we will publish a report with our findings upon completion of the audit. Next slide, please.

And this last slide summarizes some of the initiatives that we're working on. We plan to release a one year of enforcement report similar to the one that we published for the six months, and incorporating some of the feedback that we received from the community regarding that report. It will include more information about complaint processing and results, audits, the educational materials for complainants and the proactive enforcement initiative that we're currently working on. We're designing it. We don't have a launch date yet, but it's on the works. And more details about enforcement actions taken like the proactive one we recently launched based on information we gathered about phishing campaigns and others.

So now, new proactive enforcement efforts, educational materials for complainants in the works. All complementing our current enforcement through complaint processing and audits. We are committed to upholding new requirements and we are committed to continue reporting on the progress. Going to stop here to make sure we got time for questions

NICOLAS CABALLERO

Thank you so much for that, Leticia. Fantastic presentation with lots and lots of details. So, let's pause here in order to see if we have questions or comments from the floor or online. I don't see any hand online, and I don't see any hand in the room. I have [India] and then Gabe. [India], please go ahead. Please try to speak slowly, [India], because I know you. So, for the benefit of the interpreters, please try to speak slowly.

UNIDENTIFIED MALE

Thank you, Chair. I think given that the reports highlight that the repeat offenders and abuse clusters belong to a few registrars, right? For whatever reason, either because of the pricing model or because of the bulk APIs. Is there any thought process that we developed some kind of registrar risk score based upon the audit findings? I mean, some kind of a star rating mechanism for the registrars I mean, who are doing good and who are doing bad.

LETICIA CASTILLO Thank you for your question. I'm going to try to repeat and make sure that I understood it. Are you referring to the charts that I presented during the presentation or in general?

UNIDENTIFIED MALE In general, I think, I mean, not specific to the presentation, but my question is, these audits have clearly—or all the informal reports, they have brought out that certain registrars are very low on the DNS mitigation measures, right? Am I correct?

LETICIA CASTILLO The audit is still ongoing, so we have not released that.

UNIDENTIFIED MALE The informal reports have brought out that certain registrars—most of the repeat offenders for DNS Abuse or the abuse clusters belong to certain registrars. That's what the informal report findings are, so I don't know who it's supposed to be. So, I mean, the idea was, I mean, do we intend to bring, I mean, is it a good idea to kind of bring out some kind of a star evaluation metric? Some kind of a metric to rank the registrar as to how they are performing in terms of the DNS Abuse mitigation measures. That's the whole thing. I don't know that you are the right person or [inaudible].

LETICIA CASTILLO I'm not sure if I'm the right person, but I can give you attempt of an answer from my compliance perspective limited to our role in enforcing the agreements. We, in compliance, we gather a lot of

data, and we review all the data. So, I was mentioning before, we are part of this initiative that now we're working on as designing this proactive monitoring, the proactive enforcement initiative. So, the data that we gather in our complaints in terms of patterns, in terms of repeated failures, in terms of contracted parties that have demonstrated more failures than others, all of that is data that we're taking into account within the design of this proactive enforcement actions.

And when we enforce through our current process, we always take into account patterns. But I am not sure if I'm the right person to specifically address the question you asked.

NICOLAS CABALLERO Thank you, [India]. Thank you, Leticia. I have Mr. Andrews next.

GABRIEL ANDREWS Hi. So, thank you very much for that presentation, Leticia. I am very curious, when you talk about the amount of data that you get and you look into for these investigations, I know you've had 46 already this year is what you're saying. That's a lot. I'm wondering what kind of data it is that you tend to request from the registrars. And if that data ever, for example, involves data about the registration information, the registrant information or the account holder info of the persons involved behind those 5,400 malicious demands.

LETICIA CASTILLO

Thanks for the question. This is Leticia Castillo. When we initiate a compliance investigation, it is tailored to the specific obligations that we are investigating for the complaint. So, we will include questions related to data when we're, for example, addressing an alleged inaccuracy. When it comes to DNS Abuse obligations, generally, because again it depends on the specific complaint, we generally require—we provide a copy of the complaint. We provide a copy of the evidence that we have obtained, and any other important point that we consider relevant for the registrar or registry to address, then we require an explanation, a detailed explanation of the review that the contracted party did with regard to the matter. What actions were taken if appropriate to mitigate, to stop or disrupt, why the actions were chosen, and if no action was taken, an explanation why and all related records.

Sometimes when they're explaining their investigation, a registrar, depending on the case, may explain all the steps they're taking, and some of them may perform checks within the account as part of the review, and they explain that to us. But what is requested is really, really tailored to what we're investigating.

NICOLAS CABALLERO

Thank you. I have the Dominican Republic next.

UNIDENTIFIED FEMALE

Thank you very much, Mr. Chair. I will speak in Spanish. Leticia, thank you very much. And I have a brief comment, and then I will ask a question. I feel more relaxed because in the previous session

there was too much discussion about DNS Abuse, and we have seen that nothing is settled. But as a matter of fact, based on your presentation, I can understand that you have a hard work to do. And as the previous speaker said, you have a large number of requests or complaints to be investigated. So certainly, as countries and governments, we feel more at ease with your work.

These audits, these reports, are these published online? Can we take a look at them? Because in our case, based on our cybersecurity strategies, everything that we are trying to follow and monitor in our countries, everything related to system and gender-based violence, the audit may be a good report. It may be a good material, so as to learn a bit more on what is going on, and what are the trends. Thank you very much.

LETICIA CASTILLO

Thanks. This is Leticia Castillo, and I'm going to respond in Spanish. Thank you very much for your comment, and thank you very much for your question. We capture a lot of data and information of all the complaints. We receive all the cases. We receive and we process. And we have some reports that are monthly published. They include not only obligations related to DNS Abuse, but some other obligations included in the ICANN contracts.

With respect to DNS Abuse, there is a specific report that is related to the actions we take based on the requirements. It is published once a month. It includes lots of data, and it's divided based on the type of DNS Abuse. We also publish reports including examples or

more background because sometimes if you see the data in isolation, you need more background or you need an example.

This report was published on November the 8th in our page, and we are working on publishing another report with more context examples. And the idea is to incorporate some of the feedback received from the community from the prior report. So, after one year, we will publish that report, and the audits have their own reports published as well. The Dominican Republic speaking, thank you very much.

NICOLAS CABALLERO: Switzerland next and then I'll have to close the queue for the sake of time because we need to continue with the presentations. So, the floor is yours, Switzerland.

UNIDENTIFIED MALE: Thank you, Nico, and thank you for this session. Thank you especially also to you, Leticia, for this information. Just wanted to share with you some insights regarding conversations with our federal police in Switzerland. They see a positive effect of the contractual amendments, so that's a good sign. They see at the same time that some registrars are not really collaborating as they should, and we therefore are a bit doubtful on what can be done to increase the incentives for such registrars that seem not to collaborate or that seem to be free-riding on what we can do about them. So, whether there is also some direct way of notifying this to

you, to contractual compliance with that data, so that would be an important aspect.

And also, what we received as feedback that apparently the abuse complaints from law enforcement agencies are not always taken as seriously as they should. And there are some concerns because sometimes the legitimacy is apparently discussed even though it's very clear that they are coming from legitimate sources. So, I just wanted to share that also with you. Thank you.

LETICIA CASTILLO

Thanks for the comments. This is Leticia with compliance. So, if I remember everything that I wanted to say. We encouraged them to submit a complaint to us. We have a web forum that are public, and through which we receive thousands of complaints a year. We have several questions within the forums that are aimed to gather important information and including if the complaint is submitted by law enforcement, that is—it is monitor within the system as well. So, we get the type of report and monitor within the system. So, we do encourage everyone that believes a contracted party is not following their obligations to submit a complaint to us.

We have established process through which we enforce the obligations when the process in the informal stage is [inaudible] goes to formal breach, as we were talking before, and the result of a formal breach not cure is either the suspension or termination of the registry [inaudible] or the termination of the registry agreement. So, we do enforce those.

Now with regards to law enforcement, I definitely encourage them to contact us. We don't want them to believe that we're not paying attention to their complaints. We pay attention to everyone's complaints. I am not sure if I'm assuming correctly, but they may be referring to when they submit a complaint indicating that they're law enforcement within the jurisdiction in which the register is located. And if it's not clear that they are within that jurisdiction, we may ask for more information. That does not mean that we're not going to process the complaint. We're going to process it. But we need to know if that jurisdiction part applies to determine which appropriate section of the agreement we're enforcing, but I'm not sure if that's what you're referring to. Happy to speak offline.

NICOLAS CABALLERO Thank you very much, Leticia. Thank you, Switzerland. So, at this point, I will need to go back to Tomo in order to continue with the presentations. Tomo, over to you.

TOMONORI MIYAMOTO Thank you very much. Thank you very much for your updates on the ICANN compliance. And I really look forward to the coming reports and further work. Thank you very much. Next, I would like to invite the ICANN OCTO, Siôn Lloyd. Mr. Siôn Lloyd for the presentation of the informal report and the Domain Metrica. Thank you.

SIÔN LLOYD

Thank you very much. Okay. Hi, there. My name is Siôn Lloyd. And as you've heard, I work for the Office of the Chief Technology Officer in ICANN. I'm going to talk about two very different pieces of work, one Domain Metrica and one the INFERMAL. Next slide, please and again, please. Thank you.

So firstly, looking at Domain Metrica, what is it? It is a system to collect data on domain names, and then make that data searchable, usable, downloadable in as many different formats to as many different users as possible. Next slide, please.

So, we have data at the domain level, and then we can aggregate that to both gTLD level and registrar level. It's searchable. And you can get metadata and context based around whatever entity, domain, gTLD or registrar that you search for. We also have some shareable domain level data. We'll see examples of that a bit later. And a few other visualizations and charts that you can use on a web user interface, along with a couple of different application programmer interfaces, APIs, that allow you to interact with the data via scripts and code. If that's preferable to your use case. Next slide, please.

So, I can't look at all the functionality, but just a couple of very quick examples. If you maybe got an email or a text message with a domain that you're unfamiliar with, you can put that in. You'll get some background information, such as the sponsoring registrar, the creator date, so you can see how old that domain is, some of the DNS settings. Next slide, please.

And you will also see, if we're aware of any reported abuse on that domain, and which of our feed providers has reported that domain for abuse. Along with a trend line showing the popularity of that domain. So, we use the Tranco ranking, which gives you some idea about how well used, how well considered that domain is. Next slide, please.

You can do similar searches, but at the TLD level. And in that instance, again, you get some background information, you get the registry, you get the size of that TLD, and the net change since we last measured it. And you also get some statistics, then, about the amount of reported abuse that we've seen, both as unique counts and as a percentage of the zone in total. Next slide, please.

And along with that, you also get some other information, such as trends in those reported abuses, and we geolocate the domains in question, so we can see where they're hosted as well. Next slide, please.

So, we talked about shareable domain-level data. As a registry or a registrar user of the system, you get access to the list of domains that are under your management. So, in your TLD, you're sponsoring registrar for that name. And again, we tell you who's reported the particular domain, and what form of abuse it's been reported for. So, here we see some have been reported for botnet, command and control, for malware, but the vast majority have been reported for phishing. Next slide, please.

So, Domain Metrica, as it stands today, is not a finished product. In fact, we imagine it will evolve throughout its lifetime. We'll add new

metrics, new data sources based on what research we've done. It's a platform where we can push the output of our research, but also from feedback that we receive from the community. Because this is now available to anyone who has an ICANN account. So, the account you use to sign up for an ICANN meeting, now gives you access to all of this Domain Metrica data. There's a couple of links there. One is like a mini page that gives a lot more detail, and links to other things like the FAQs and documentation. And there's a link to a webinar that we gave that gives a lot more detail, and shows a lot more of the functionality that we have within Metrica. Next slide, please.

So, I'll move on now to talk about the INFERMAL report that came out towards the end of last year. I think that it's been reported a few times previously. Next slide, please.

So, this was a project that was funded by ICANN, but the actual work was conducted by a group working under Professor Maciej Korczyński, who's at KOR Labs and University of Grenoble. And it looks at registration policies and practices to look at patterns that might give an attacker a preference to a particular TLD registrar combination. So, the final report, as I said, was published towards the end of last year. And there's more details on that link there. Again, it's a mini page. It gives a link to the actual report, which is very detailed and very comprehensive. And also, there's an extended webinar that was given earlier this year. Next slide, please.

So, the way INFERMAL worked, it looked at different features of a registration. So, for example, pricing. Were any discounts in place at the time? So that could be discounts. For example, if you register a large number of domains, do you get a reduced fee per registration? What bulk registration facilities are available? The presence of one of these application programmer interfaces again. So essentially, looking at how much automation is possible in the interaction between the user and the registration process. What payment methods are available? So, can you pay with cryptocurrency? Can you pay with PayPal, etc.? And also, what other services do you get as part of your registration fee? Do you get web hosting? Do you get a certificate? How much of that stuff is taken care of for you as part of the registration process? Next slide, please.

So, another group of features that was examined could be thought of as verification or security practices. And some of these are proactive. So, for example, validation of contact details, but before payment is accepted for the registration. What sort of restrictions may be in place? So, do you need local presence in the jurisdiction, the country where you're registering? What sort of documentation is required? And then also things like what proactive measures might be taken in order to prevent clear, abusive, or clearly potentially abusive names being registered?

So, for example, if my name contains a string like Office 365 or Facebook, it's more likely to be targeted for phishing. So, is that sort of thing checked before the purchase of the domain? And along with the proactive measures, there were some reactive

measures looked at as well. So, for example, the uptime. How long do reported domains remain active before the abusive content is mitigated in some way? Next slide, please.

Various different datasets were used in the study. I won't go through them all. But essentially, it's a mixture of third-party data. Some manually collected data, so just looking through what's available through the process, and then some active measurements, such as DNS measurements, WHOIS measurements, and so on. Next slide, please.

So, the report itself is very detailed, and there's a lot of nuance and sort of context given to all of these figures. And I can't really do it justice in five slides, but it's a sort of rough idea of things that were seen. The strongest correlations with increasing abuse were things around the availability of that API, so the automation piece. The extra service is provided, so the DNS hosting or web hosting, and registration discounts. And then looking in the other direction, the strongest correlations to decreasing abuse were around the proactive measures, so the validation of contact details before the purchase of the domain is possible, and the presence of those registration restrictions.

So finally, a couple of things that the author has been keen to point out when he's presented this work himself is that it's likely that the attractiveness to attackers will result from a combination of factors. So, no one factor on its own will be the deciding factor in levels of abuse seen. And also, it's important to consider other implications of any decisions made based on this data. So, for

example, yes, a decision may mean that attackers have a lower preference for that particular TLD and registrar, but it will also affect legitimate users as well. So, any measure will affect legitimate users as well as attackers, and any attacker is likely to respond to measures that are put in place.

So finally, I'd just like to extend our thanks to Professor Korczyński and his team for the incredible work that they've done and for the very comprehensive report that they've put together. And with that, I would invite questions. Thank you.

NICOLAS CABALLERO: Thank you so much for that, Mr. Lloyd, very interesting presentation indeed especially regarding that very simple fact about the phone number and the email address requirements, so to say, and how it makes DNS abuse go down. But let me open the floor for quick questions. We have about five minutes for a mini-Q&A session at this point. The floor is open. And I see a hand on the back of the room. Please take any of the microphones and go ahead with your question.

ALEX URBELIS: Sure. My name is Alex Urbelis from the Ethereum Name Service. I have a question about Metrica, and the statistics that you're tracking with respect to threat actors. You mentioned that you are tracking the actual location of the hosts. In my experience in tracking numerous threat actors, hosts often hide behind Cloudflare. So, do you have any kind of methodology to request the

actual host information from Cloudflare, or are you just tracking that the NS records would point over to Cloudflare, and that would equate to the host.

SIÔN LLOYD It's purely a geolocation of the resolved IP addresses for the domains that we see reported for abuse. So, yes, we're aware there will be inaccuracies, inconsistencies in that data, but potentially it shows something unexpected or interesting to the party involved.

ALEX URBELIS Right. And is that data updated in real-time in Metrica, or is it kind of after the fact?

SIÔN LLOYD Daily.

ALEX URBELIS It is.

SIÔN LLOYD Daily updates.

ALEX URBELIS So, if I understand correctly, we could report a domain. ICANN well investigate it, and update Metrica on a daily basis?

SIÔN LLOYD So, the data input queue is the reputation block list that we ingest into the system.

ALEX URBELIS I see, I see, okay. Thank you.

SIÔN LLOYD No worries.

NICOLAS CABALLERO Thank you for the question. I have the UPU next. Tracy, go ahead, please.

TRACY HACKSHAW Thank you, Nico. Tracy Hackshaw here. On the Metrica site, I was just checking it, and I'm wondering if there's an opportunity to do comparisons. It seems like you can only do one at a time. Is it possible to do comparative like for TLDs, for example, one TLD against another? Is that coming soon?

SIÔN LLOYD Yeah, we can do that currently if you interact with the charts. Maybe if you catch me after this session, I can show you. I'm happy to do that.

NICOLAS CABALLERO Thank you, UPU. Any other question or comment before we move on? Is that an old hand, Tracy? Oh, all right. So, thank you. Thank

you again. Back to you, Tomo. Oh, I'm sorry, I'm sorry. Please go ahead, Cambodia.

UNIDENTIFIED MALE: Good morning, everyone. My name is [inaudible] from Cambodia. My question is maybe going to GAC chair. May I ask you about the GAC or ICANN? Is any regulation or guideline for breakdown of the DNS Abuse or any regulation decision for protecting of the DNS Abuse? Because this morning, you are talking about the survey, about the compliance, about the mitigation, but there is no regulation about protecting of the DNS Abuse. This is my question. Thank you.

NICOLAS CABALLERO: Thank you, Cambodia. I'm not sure I entirely understand your question. Could you please repeat what is exactly that you're asking?

UNIDENTIFIED MALE: Yes, the question is GAC or ICANN have a regulation or guideline for protecting of DNS Abuse or DNS breakdown, something like that, yeah?

NICOLAS CABALLERO: The short answer is no, GAC doesn't have any specific. There are many recommendations coming from ICANN, and from the NetBeacon Institute, and from many different institutions, and we can certainly point you to the right place for that, including DNSSEC

implementation, and we have a fantastic team within ICANN that can certainly help you with that. Not only DNSSEC implementation, but also RPKI and many other things including, for example, MANRS, Mutually Agreed Norms for Routing Security and many other measures that you could implement in your country. No problem. But the GAC itself doesn't have any specific guidelines, though it's not a bad idea to have some sort of package pre-prepared. Thank you again, Cambodia, for the question. And now, for the sake of time, I will need to go to Tomo. Please go ahead.

TOMONORI MIYAMOTO

Thank you very much for the information from ICANN. Thank you very much. Next, we'd like to move on to the panel discussion. We welcome the distinguished panelists, Graeme from NetBeacon, and Reg and Luc from CPH, and Jeff from SSAC. Could you move on to the next slide, please? Thank you.

These questions on the slides are the topics for the discussion today. We asked panelists their reactions to INFERMAL and Domain Metrica. Again, comment is further step to address DNS Abuse and other data needed developing the trends in this field. Our panelists, Graeme, Reg, and Jeff will present or make short remarks for these topics at first, and then we have a discussion open for further questions. So, first, Graeme, please.

GRAEME BUNTON

Thank you. Hi, my name is Graeme. I'm the Executive Director of the NetBeacon Institute. We work to make the internet safer for

everybody by reducing the prevalence of malicious domain names. So, I've put together a couple slides. I'll try to go through them quickly in the interest of time, because I know my colleagues here would like to have a moment. Next slide, please.

So, first up is kudos to Professor Korczynski, ICANN, Samaneh, the entire OCTO team for their work on INFERMAL. Truly, it's an excellent report. It's interesting. It's important. If I had one problem with it, it's that they got to it before I could. This is work we really wanted to do, and they got in front of it, and it's great. And one of the great things about that report is that it really highlights the complexity involved in DNS Abuse. INFERMAL identified 73 different features that were important factors in DNS Abuse. And imagine each one of those factors as a dial at a registrar that they can adjust. And adjusting each of those dials causes them to interrelate. And so, that's the context in which we need to think about this problem. Next slide, please.

I think INFERMAL did a really good job of providing concrete data on issues that we've long assumed as a community to be involved in rates of DNS Abuse. That we now have something to build upon around things. Boy, I'm not going to get into price, but ungated APIs for sure. We were asked about surprises within that data. Boy, I was really surprised about the low relationship between mitigation speed at a registrar and their rates of abuse. I had long assumed that if a registrar was quick and proactive at mitigating abusive domain names, they would be less attractive to bad actors. And that was only a little bit present within the INFERMAL report, which

I think is pretty informative for this community as well. Next slide, please.

So, what do we think we should do as a community? I think there is a lot of interest in a PDP on abuse. And I think before we get there, we need to establish some principles. And I was listening to the GAC survey on DNS Abuse with interest. One of the things identified in your survey was about making more progress faster. So, how do we do that? Well, the first thing is to identify a specific problem that we think we can make incremental progress on. We cannot start a PDP on abuse. It's too big. It won't work. It will take years. We'll all be frustrated.

What we need to do is identify a specific problem and move forward with an incredibly narrow scope on that problem. The scope should be so narrow, the narrowest thing. You almost want people to be uncomfortable that the outcome seems predetermined because we've made it so narrow that we can make meaningful progress in a short amount of time, and then we keep doing that. We keep moving the ball down the field. Apologies for a sports metaphor, so that we can improve abuse for everybody and then whatever PDP, if we get there, we really need to make sure that it's technology and business model agnostic. That this can be applicable across the ecosystem. Next slide, please.

So, a couple other points as we're thinking about what that work would look like. It's important to remember that criminals are faster, smarter, unconstrained. They're often better resourced than we are at this. And they're not playing by our rules. And so, we

cannot produce policy that specifies things like limits on particular services. Criminals are going to automate and adapt in hours and it takes us currently years to produce policy. And we know that they are already scripting and automating against registrars that don't offer services like free APIs. And the technology to do that becomes easier to use right now, every day. So, what do we do?

Well, I think we need to identify potential policy changes that incentivize registrars to adjust those available dials that I was talking about, those 73 features, in their specific context. That they find the ways to implement friction that impacts criminals but not benign registrants. And we need to make sure that those things are enforceable and auditable. So, let me see if I can make that a little bit more concrete. So, if you've read INFERMAL and you're like, boy, that free API access really drives up rates of abuse, turn your mind from specific limits to access to those. But really, how do we incent registrars to be more cautious with who they allow access to those features?

And that's the sort of, I think, place where we can find effective policy that is adaptable in the marketplace and can adjust not just the abuse we see right now, but potential abuse in the future. And so, a couple last thoughts on data and abuse reports. And [inaudible] can issue reports of abuse to registrars and registries all day, every day. We monitor that through our data project called MAP, very similar to Metrica. And it's early days and it's not conclusive. It's not hard science but we are beginning to see an uptake in mitigation rates post contractual amendments. And so, we'll keep looking at this very carefully. We'll keep publishing

content for this community as well, but I encourage everybody to check that out. Those are my comments. Thank you.

TOMONORI MIYAMOTO: Thank you very much for your comment. And Reg, over to you, please.

REG LEVY: Thank you, and thank you, Graeme. This is Reg Levy from Tucows, a domain name registrar. I wanted to highlight something that the EU raised in their presentation. The speaker asked for a website that was a centralized place for people to submit reports. That's exactly what Graeme has. NetBeacon is a centralized portal for reporting domain name abuse to any registrar. You don't have to go to the specific registrar. So, I just wanted to highlight that because I know that was a specific thing that the EU was asking for.

GRAEME BUNTON: Thank you, Reg.

TOMONORI MIYAMOTO: Thank you. Next is Jeff, please.

JEFF BEDSER: Thank you. Having already spoken in the context of SSAC with GAC earlier this week, I'll just emphasize some of the points. I think that the INFERMAL study was excellent. And I do again commend the researchers at OCTO for commissioning that report. But as I made

that point earlier, it was not a recommendation report. It was a findings report, and it confirmed some things for us that we all kind of suspected for a long time. But the confirmation is that it's economics. People always buy the cheapest resource, and they will always use the resources that give them the best ease to get them, whether it's for crime or anything else.

When we're looking at cybercrime, we're looking at a one to $10 trillion business annually that is largely facilitated by domains. The incentives for the criminals to use domains for the work they do, to steal from the citizens of all your countries are simply priced, and they will always go for the cheapest ones. If you make the cheapest domains $1,000 when they're making hundreds of thousand dollars per domain, you're not going to impact their bottom line much. But you will stop all the citizens of the world being able to afford domain names.

So, to me, the real solutions moving forward are not about what do we do to stop domains being sold for abusive purposes or used for abusive purposes, because with a $10 trillion economy of cybercrime, there's very little we can do to stop the sale of them. What we can do, though, is work on better detection and better reporting. We are in an environment where the majority of the reports and RBLs being used to measure this problem, there's five to seven of them, sometimes eight. They are looking at the top of the iceberg. That's pretty much the public data that almost anyone in this room can get their hands on.

Every single registrar and registry get hundreds of thousands of reports annually that never make those lists with domains, and they act upon those. There's also the reality that everyone in this room, and if you deny it, raise your hand, has gotten a phish or a smish, and you've deleted it, and didn't report it. Probably five times today is significantly unreported. We don't know how big this is, but we do know that it's very big, and the best way to fight this is to work on better models moving forward as a community to detect. The faster you can detect it and report it, the faster you can mitigate it. And working on technologies within the community that allow you to quickly measure the evidence. And that's one of the things in the new contractual obligations, is it must be an evidenced report.

Why is that? It's because the contracted parties and the ccTLDs, given an evidenced report, can work faster. They don't have to reinvestigate that report to verify it. They can take that report, look at that evidence, and quickly make a determination that it's actionable, and then mitigate from that. So, that's where we need to move. I think the INFERMAL report did a wonderful job of making it very clear that in the economy, tied into the realities of cybercrime economy is that the scale is extensive, and the solutions are going to be based on better reporting, and better detection of the abuses. Thank you.

TOMONORI MIYAMOTO Thank you very much for your remark. Now I'd like to open the floor for the Q&A. So, do you have any questions or comments? Reg?

REG LEVY

Thank you. Reg Levy for the Registrar Stakeholder Group. I also want to highlight the good work that Jeff and his team are doing. His technology powers a lot of NetBeacon's stuff. They work closely together at CleanDNS. And another thing that the delegate from Europe was asking for was AI models to help combat DNS Abuse. Primarily, what we as registrars are seeing is LLMs being used to create more DNS Abuse. Super fun. But Jeff's technology does have LLM tools that help us get more information, and so that we can take action better and faster.

NICOLAS CABALLERO

Thank you, Reg. The floor is still open for questions or comments. Yes, please go ahead. Grab any microphone and ask your question.

DEAN MARKS

Thank you very much. Dean Marks, I'm with the Intellectual Property Constituency. And I had a question for Jeff about—you emphasized reporting and detection. And my question for you, with all the work that you've done is, that all seems more reactive. Do you have any suggestions or thoughts about steps that can be taken that are preventative with respect to DNS Abuse? You mentioned pricing and you said it doesn't matter. If there was a minimum price of $1,000, cyber criminals would still be buying up domain names quickly. So, the implication of that is that pricing doesn't matter for cybercrime. Can you identify what you think are preventative measures? Is know your customer a preventative

measure that might be useful? That's my question. Preventative measures, and what you think of them

JEFF BEDSER

Thanks, Dean. And that's a great question. I think that historically, better know your customer processes with identity verification and validation were good. I think it was in a previous presentation I made this week. I think the realities of generative AI and the potential of using it to create identities that look exactly like you need them to look using a real person's name, but using a different person's photo is here. It's already here. So, you're not going to see that grow until—if everyone puts in identity validation, then you'll see that grow.

They're going to go to the places where that's not happening now, but they already have a solution for that problem. And if they really want a domain with a particular extension on it, because that extension helps them convince someone of the lure to get into the harm, they will go to that process to get that domain. That's already been seen, demonstrated.

I think that the key is going to be that, and I've already seen efforts between the registrars and registries on this, and I look forward to more of it is collaboration. Every one of them processes hundreds of thousands if not millions of reports a year, and the underlying infrastructure related to every one of those reports can be a pattern that can detect more, so that when a bad operator registers a domain that Tucows catches and shuts down that pattern in a share, every other registrar can see that pattern and say, no,

putting some friction in the system here and we're not going to allow that to proceed.

And I think that's the type of thing that, it starts to happen when you've got communities collaborating because domains are perishable, right? They register. They drop them annual period. The infrastructure underlying, it's a lot more expensive to maintain, and keep a clean reputation on. So, there's a friction point there, and I think there's some other efforts that are interesting when you look to payment processors where a lot of these sites, whether it be fake shops or phishing, if they're using credit card facilities in any way, their merchant accounts can be targeted because they're also very hard to get their hands on and shut down.

So, it's not just shutting down the domains that are being used as the frontend, but if you can attack them on the payment processing side too, you're not just taking away a tool they can replenish easily as far as a domain, but you're making it much more difficult for them to process the monies they're stealing.

NICOLAS CABALLERO Thank you, Jeff. And before I give the floor to the UK, Graeme, is there anything you would like to add at this point?

GRAEME BUNTON Thanks, Nico. This is Graeme again from the NetBeacon Institute. I'll try and be very brief. I think Jeff covered a lot of good ground on that question, but I'll just highlight that one of the pieces inside of the INFERMAL report is that they highlight that increased KYC

seems to incentivize identity theft. And we're also seeing AI become better and better at generating fake convincing identities. So, I find myself a little bit less convinced that that is going to be the solution. It may be a piece of a puzzle, but I don't know that it's going to solve as much as we want it to.

And then other opportunities I think that are interesting that are yet to really be explored, and are outside the ICANN context are going to be the relationship between fraud and abuse, and seeing if there's technologies and tools that we can leverage there. But boy, I've talked to a party this week who were describing that all of their abuse was purchased with legitimate credit cards, and my mind exploded. And so, the overlap there is not as great as I think we all want it to be. Thank you.

NICOLAS CABALLERO Thank you, Graeme. Sorry to keep you waiting, UK. Please, go ahead, Nigel.

NIGEL HICKSON No, no, not at all, and thank you very much for this session. One wonders, it's an incredibly complex area, and clearly, there's a lot going on. But increasingly, our adversaries are working on new issues on how to conduct the fraudulent foreign acts and cybercrime. I mean, I found the INFERMAL report really interesting. I remember discussions on bulk registrations some years ago, and there was no real evidence, and now we have the evidence. I mean, clearly, we're not going to—well, I'm probably not going to issue

GAC advice this afternoon saying all domains should be priced at $100 or more, or anything like that. These are competition issues. These are very difficult issues.

But it does appear to me that, and we discussed this with the ALAC earlier, that there might be some room for policy development processes on bulk registrations in some areas, and particularly on where you've got a bulk registration, and perhaps the registration is completely for free. Perhaps the registrar is offering free registrations for this particular domain. Then there does seem perhaps room for extra questions to be asked. Are you doing it because you've got a sports event or whatever, and you need all these new domains because of your process, or it's a new school. There's lots of legitimate uses, of course. But I think we need to do more at the frontend to find out what is going on. Thanks.

REG LEVY

Reg Levy from the Registrar Stakeholder Group. Thank you very much, Nigel. We're actually looking into bulk registration along with the team that developed INFERMAL and published INFERMAL, because in this case, I believe, it was defined as 50 domain names at a time. If we decide that we are going to ban 50 domain registrations at a time, then they'll just turn into 49. So, what we're going to do with INFERMAL next is they want to know if the data is bad in a certain way. So, they're going to give us some hypothesis, and then we're going to—and by we, I mean, a number of domain name registrars that are involved in INFERMAL. We're going to look at the data that we see on our end and provide back to them

information about whether or not there's correlation there. So, they're going to send us lists of domains and some hypotheses. So, yes, absolutely looking into that right now. Thank you.

NICOLAS CABALLERO Thank you, Reg. The floor is still open. Martina, is there anything you would like to add online while we still have you? Sorry, Jeff. Yeah, go ahead.

JEFF BEDSER I made the analogy earlier this week in a presentation, and when it comes to the bulk registrations, considered the same as a licensing model, right? So, if you were in most countries, if you drive a scooter, the licensing requirements are a very young person on the verge of adulthood can get a license to drive a scooter. But to drive a semi-truck, I'm not going to convert imperial to metric here. So, say a really big semi-truck. The licensing requirement is always a lot higher. And why is that? Because the risk to human life is significantly higher to drive that larger vehicle, and it may simply be that any registrar that wants to have a bulk registration model is required to have a much higher standard for access to it and licensing to use it.

And maybe that's even something like a certain amount of money on hold. If you misuse it, you lose the money. There're all types of ways where you can almost do an insurance around the misuse of a tool that is, if misused, very damaging. And I think that might be the direction to take that discussion.

TOMONORI MIYAMOTO: Thank you very much for the panelist. Thank you very much for the panel. Actually, we have the GAC discussion last. Well, already the GAC discussion has started, but I'd like to introduce Martina for some points. So, could you explain it.

MARTINA BARBERO: Thank you very much, Tomo. So, we had hoped for a great session. I think we are getting a great session. But indeed, we wanted to close with some question for the GAC, and gathering input from GAC members on what we have heard today, and what do you think are the key insights from the presenters, and the different topics that we have covered. And how what we have heard affects the next steps on DNS Abuse.

So, some of you already pointed at some directions in particular. But we're keen to hear in the next five minutes, what would be the next the ideal next steps in the interviews. And finally, as asked by GAC leadership, we also can communicate considerations. So, anything that we want to put in the communique stemming from this discussion and related to expectations for future work and consideration for the new round. Brief recall that, as some of you mentioned, there's been discussions within the GAC on possible PDP. There's also been discussions with other communities. I heard that ALAC was interested in collaborating further with us on this topic. So, back to you, Nico, and let's maybe have the last three

minutes to see if there is any perspective that we want to include in the communique.

NICOLAS CABALLERO Thank you very much for that, Martina. Indeed, we have the UK. I see your hand up. Please, go ahead

UNIDENTIFIED MALE Oh, it was an old hand. Sorry.

NICOLAS CABALLERO Oh, I'm sorry. So, again, we have three minutes for quick questions or comments online or in the room. Please, go ahead. Yeah, just grab a microphone.

DAVID HUGHES David Hughes, IPC. I wanted to ask Jeff and Graeme a question, which is, we have seen some ccTLDs, for example, but not necessarily, that have extremely low levels of DNS Abuse. What can we learn from those?

JEFF BEDSER The largest concern with answering that question is that while the gTLDs have a common set of rules they run by, the CCs do not, and it varies significantly. So, many times, those low rates of abuse also correspond to the low rate of growth. They're not processing that many. They're not growing that quickly. But there's two different types of abuse at the meta level, and that is domains registered for

an abusive purpose, and of course, those compromised at the host and used for an abusive purpose. And I think that we do see a larger preponderance of compromised domains within the ccTLDs by most studies than we do in the gTLDs just based on the model.

So, I think that continuing to focus on low levels in certain places, there's also a CC that has one of the highest rates. And again, I'm not going to name and shame here, but it does go the gamut from G's and C's as far as their rates within, and there's plenty of gTLDs that have super low rates as well. So yeah, I don't know if I have anything constructive to point on that.

GRAEME BUNTON Thanks for the question. It's tricky to answer. Go back to INFERMAL reports, 73 different features that they were manipulating and looking at. And so, it's hard to say that there is one solution, because I don't think there is. And I also think that looking at abuse rates alone is a mistake because cyber criminals got a cybercrime, and they're going to pick a TLD for whatever reason sometimes, because of one of those dials that the registry or registrar may not have known about or had the ability to adjust at some point.

And so, we need to be aware of that complexity, and then look at not just rates, but also mitigation rates, as well as median time to mitigation, more sophisticated views of the entire sort of abuse chain. Thanks.

NICOLAS CABALLERO: And I'll give the privilege of the last comment to Reg. Over to you, Reg.

REG LEVY: Thank you so much. Reg Levy from the Registrar Stakeholder Group. This is actually a very interesting question and the ccTLD group and some of us here on the stage right now are going to be discussing it, I believe, tomorrow. So, check the schedule for more information on that. But not only do ccTLDs have different policies, they have different markets. And so, there are some types of abuse that might actually target a particular ccTLD because that's the way that they can get those clicks. So, there are all different kinds of factors that go into this, as Graeme said, but I encourage people to attend the ccTLD session as well.

NICOLAS CABALLERO: Thank you so much. Oh, sorry, Denmark, very quickly. We're over time. Go ahead, please

FINN PETERSEN: Thank you, Finn Petersen from Denmark. And thank you for giving me the floor so late. I think actually it's a good idea to look at certain of the ccTLDs. I know at least in one country, the bulk registration has been limited to five, and if it's above that, then there's a deep investigation in the identity of who have applied for that. You can have many things. But looking at what we have heard today, perhaps the GAC should look into, and see whether we can propose a kind of PDP on bulk registration. And if I understood

	right, it should be quite narrowly scoped if we should have a good possibility to have it adopted, and start the work so we can have, let's say, that could be a low-hanging fruit for the GAC to suggest that. Thank you.
NICOLAS CABALLERO	Thank you so much for that, Denmark. Good idea. Narrow in scope and in timing, I would say. Anything less than five years would be more than welcome. So, thank you so very much for that. Thank you, Reg, Graeme, Jeff, Tom, Leticia, and Siôn. Thank you so very much. We're going to pause now. We're going to have a lunch break. Please be back in the room at 1:15. Thank you very much, everyone. The session is adjourned.
GRAEME BUNTON	Thank you, all.

[END OF TRANSCRIPTION]