ICANN81 | AGM – GAC Discussion on DNS Abuse Mitigation
Tuesday, November 12, 2024 – 10:30 to 12:00 TRT

DAN GLUCK: Hello and welcome to the GAC discussion on DNS abuse on Tuesday, the 12th of November at 07:30 UTC. My name is Dan Gluck from the ICANN Policy Development GAC Support Team. Please note 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 will only be read aloud if submitted within the chat pod. Interpretation for this session will include all six UN languages and Portuguese.

If you would like to speak during this session, please raise your hand in Zoom. Please state your name and the language you will speak, if other than English, and remember to speak at a reasonable pace. As a kind reminder, tables with microphones are reserved for GAC members, observers, and invited guests. I'll now hand the floor over to GAC Chair, Nico Caballero.

NICOLAS CABALLERO: Thank you so much for that. Welcome everyone to the DNS Abuse Mitigation session. We are privileged to have our GAC topic leads, Martina Barbero from the European Commission, Owen Fletcher from the US government, and Hajime Onga from Japan, and I hope I'm pronouncing your last name well. We're also honored to have our guest

speakers, Mahmut Esat Yildirim from the ICT Authority of Turkey, Leticia Castillo from ICANN Contractual Compliance, Reg Levy from Tucows, Dennis Tan from VeriSign, and Jeff Bedser from CleanDNS.

Welcome, everyone. Without further ado, and for the sake of time, I will hand the floor directly to Mr. Hajime Onga from Japan, who will be walking us through the details and nuances of our conversations today. Please go ahead.

HAJIME ONGA: Okay. Thank you for this, Chair. Good morning, everyone. Welcome to this session today. I am Hajime Onga, the new GAC representative from Japan. This session will be co-lead by the European Commission and the United States and Japan. And in this session, we welcome wonderful guests from the Turkish government, ICANN, and the Contracted Party House, CPH, and SSAC.

Okay. This is the agenda for today. After this brief introduction, we will have a presentation from the host country. Next, the ICANN Compliance team will provide a briefing on DNS abuse update after the implementation of the amendment of Registry Agreement (RA) and Registrar Accreditation Agreement (RAA) this year. Then we will have a panel discussion on the situation after the amendment with CPH, SSAC, and ICANN. And then we will have a GAC discussion. Lastly, we will explain the next step toward ICANN82 in Seattle and discuss for the Communiqué.

First, DNS abuse mitigation is one of the main topics in the GAC. In Japan, this problem has attracted a wide range of attention from phishing in a narrower sense, as defined by ICANN contracts, to manga piracy in broader sense. Second, under the updated RA and RAA, the registries and registrars of gTLDs have to deal with the report of the DNS abuse as a contractual obligation. Thirdly, in this contractual agreement, DNS abuse is defined as malware, botnet, phishing, farming, and some cases of spam. This time, we will discuss what measures are being taken, mainly within the scope of the ICANN limit. And the next ICANN, we will discuss the effort by the DNS ecosystem as a whole.

Here is a big picture of ICANN's scope on DNS abuse mitigation. The green square, which means ICANN contractual authority such as RA and RAA is limited. This is the relationship between ICANN and registries and ICANN and registrars. So, relevant actors such as resellers, registrants, and ccTLDs are not in this box. Today, we will discuss the relations impact and effect in the green one. Actually, DNS abuse stakeholders' communities are larger than the green square.

First, many cases of DNS abuse are ccTLDs. This issue of DNS abuse is prevalent in the DNS industry, which is represented in this blue rectangle. In addition, bad guys generally use services such as hosting providers and CDNs represented by the red box in this picture. To mitigate the DNS abuse, we have to work together collaboratively.

Last month, we held a pre-ICANN webinar, and Jeff, who will be in the panel discussion today, introduced SAC115, which is one of the most

important references in the updated RA and RAA. In the presentation, Jeff introduced a number of discussions on our framework for mitigating DNS abuse. It highlighted the importance of cooperation among the extended DNS community. Today, our session will cover the bullet point enclosed by the red box.

First, the Turkish Information and Communication Technology authorities will introduce their approach to DNS abuse. As the ICANN80 Kigali Communiqué stated, learning from case studies is important to consider the further measures against DNS abuse. This representation will introduce Turkish initiatives, including collaboration with ccTLD administrators and other relevant organizations.

Next, we will discuss what can be done within ICANN. First, ICANN will give a briefing on RA and RAA compliance. Second, we will have a panel discussion with stakeholders about the effort and effect of the amendments. Lastly, we will have the GAC discussion taking this input into account. Then, in the next ICANN, we will expand the scope and discuss what can be done with the extended community or the ecosystem.

As the closing of today's session, we will give a brief explanation of further steps for the next ICANN meeting. As you can see, the agenda for today is very packed. So, everyone, please respect the clock like Japanese, but I'm not a good teacher for this today because a little bit running out of my time. Sorry. Anyway, let's move on to the presentation from the host country, Mr. Mahmut, the floor is yours.

MAHMUT ESAT YILDIRIM: Thank you so much. Hello, everyone. My name is Mahmut Esat Yildirim. I'm the head of department at Information Communication Technologies Authority of Turkey. Today, I will be talking about the abuse mitigation mechanism that we are building in Turkish National CERT and ccTLD as well. So, I think we are going too fast. Okay.

NICOLAS CABALLERO: Mahmut, if you could please speak closer to the microphone.

MAHMUT ESAT YILDIRIM: Sure.

NICOLAS CABALLERO: Thank you so much. Thanks.

MAHMUT ESAT YILDIRIM: So, Turkish National CERT and the ccTLD of Turkey reside in the same department. And Turkish TR CERT is the National Cybersecurity Incident Response Center of Türkiye. And its primary role is to detect, analyze, and mitigate the cyber threats and incidents across the country. And as well as the, as I mentioned, the ccTLD, which name is TRABIS in Turkish, resides in the same department. That's why we can combine two powers at the same time to combat the DNS abuse and other cyber threats.

We have a National Cybersecurity Strategies and Action Plans. Actually, we have four of them. And in these strategy and action plans, there are

some bullet points about abuse to detect and mitigate about the abuse mechanisms and about the cyber threats. The latest version of the National Cybersecurity Strategy and Action Plan has 4 themes and 6 strategic objectives, 18 targets, and 61 action items.

These points are, first of all, human-centered cybersecurity approach. Safe use of technology and its contribution to cybersecurity, cyber resilience, proactive cyber defense and deterrence, domestic and national technologies in combating cyber threats, and the last, Turkey brand in the international area. They are all in our National Cybersecurity Strategy and Action Plan.

So, our legal basis to mitigate these cyber threats and DNS abuses are implemented in accordance with the provisions outlined in the Articles of Turkey's Electoral Communication Law, 5809. In Article 60, Paragraph 11, it says the organization takes or has someone to take all kinds of necessary measures to protect and deter against cyber attacks to government organizations, private and real entities. So, with this law, there are so much responsibilities given to Turkish National CERT to deter and take actions against the cyber threats.

In the next paragraph of the same law, it's saying the organization can receive and evaluate information, documents, data, and records from the places within the scope of its duty. And so far, with this law, we can ask for data about information to detect the cyber attacks from different organizations or from different systems.

The ccTLD's legal basis, especially within the framework of legal regulations, that .tr ccTLD supports law enforcement in combating the

cyber crime. And we are working closely with all the law enforcement and also with the courts, and we are providing the information and documents requested by authorities such as courts, and sometimes we are also working closely with CERT and law enforcement all together to detect and deter against those kinds of abusive activities.

So, what type of abusive activities that we are dealing with almost every day? Phishing, malware distribution, spams, domain hijacking, botnet command and controls, sometimes the child exploitation materials, fraud and scams, DNS abuse, technical DNS abuse like DNS spoofing or DNS hijacking, and sometimes the privacy violations. These are all things that we are trying to detect and deter against all these categories, and we built some tools and mechanisms to detect them.

First of these tools that we built is AZAD, called AZAD. This is the project software actually built in-house, which uses the AI mechanism, machine learning and AI mechanisms, to detect phishing domain names. For example, we are gathering all the newly generated domain feeds and also some other feeds from different sources. We are gathering millions of domain names every day, and by using the machine learning and artificial intelligence, we are gathering the phishing-related domain names out of these millions of domain names, so that our operators in the ccTLD can check manually if that phishing-related domain name is actually phishing or is it a false positive.

So far, this software succeeds in like 97%. In this way, the phishing addresses targeting users in Turkey are detected and blocked before or as soon as they become active. Since we are using the CERT power,

Turkish National CERT power, and the ccTLD's power together, we can work closely in cooperation with the ISPs in Turkey as well, so that we can act really fast to mitigate these phishing activities. All these feeds, all these abuse-related complaints are gathered in a specific software, again, that we build in-house, which is KULE. We are gathering all these notifications and separate them to different divisions.

So, this is how our DNS abuse flow works in TRABIS in general. We are gathering so many notifications from different sources, like registrants, registrars, or end users, or as I mentioned, AZAD. We are gathering all these notifications in the KULE application. Then we are forwarding it to TRABIS, which is ccTLD. Then they are analyzing all these notifications by using AIs and everything. Then they can suspend the domain name, or they can escalate it to the ISPs.

So, there are some statistics about this KULE software incident response statistics. We gathered more than 13,000 complaints, and out of these 13,000 complaints, 8,000 were actually an incident for us. That means we should check these notifications if they are an abuse activity or not. So out of these 8,000, 5,000 were actually an abuse, and we either canceled the domain or blocked it. So far, we found more than 900 phishing websites, more than 3,400 banking phishing websites, and 3 malware and command and control centers, and 26 malware emitting names. All of these by using the AI tool that we built.

And there are some common patterns and restricted name list words, such as complaint. Actually, maybe in English it doesn't make sense, but complaint, implication, dues, cancellation, loan in Turkish are used

for identity theft. And the number of words are containing banking doesn't exceed 20 because we have a restricted domain names list. So, we included all these official bank names in this restricted domain names list so that the abuse actors or cyber actors cannot register bank-related domain names.

In Turkish, opportunity, discount, trust, online campaign, these words are really highly used in these phishing activities or abuse-related activities. Again, maybe in English doesn't make sense for some of you, but we are building and we are improving our artificial intelligence mechanisms by expanding these kinds of words. And every day we are teaching new mechanisms and new words to improve the AI mechanism to detect abusive activities.

So TRABIS established in the 2022 and there are some turning points after 2022. So before TRABIS, all the domain-based registrations were document-based for com.tr, net.tr, or org.tr. You had to provide the official document. But after TRABIS, it's first-come, first-served. That's why abuse-related activities picked up. That's why we have to improve our detection mechanisms. And also, after 2023, we start using the CERT capabilities with TRABIS so that we can mitigate them faster.

Our complaints methods, it can be by email from the CERT complaints methods or by webpage or by hotline. They can just call us and tell about any abusive activities. So, if you check usom.gov.tr website, you will see the blacklisted addresses. It's publicly available to everyone. We are sharing this list with the world so that you can implement this blacklisted domain names or IP addresses, malware domain names, or

phishing domain names in your own projects, in your firewall, or in your other blacklist.

So we are open to collaboration with the GAC members and find most effective policies for mitigating the DNS abuse. And we are curious about abuse policies of other ccTLDs and other countries, how they detect and how they mitigate it. We can share experiences and we would like to contribute our experiences, how we implement these policies or these mechanisms to our processes. And if you have any questions, feel free to ask. Thank you so much.

NICOLAS CABALLERO: Thank you very much for that, Mahmut. So, the floor is open for questions at this point for Mahmut. I don't see any hand up yet. And I do have some questions regarding the kinds of techniques you're using right now in order to identify anomalies in DNS traffic or DNS queries or spam in general.

So, what kind of artificial intelligence techniques are the most successful from your point of view or according to your experience for these cases, like, I don't know, random forest or deep learning? And in that case, what kind of deep learning? Neural networks, convolutional neural networks, or in general? I don't want to get too deep, but just to have an idea of what works best from your point of view and according to your experience.

MAHMUT ESAT YILDIRIM: It's a really nice question. And actually, I love the technical side of this. So, there are two different sides of this machine learning processes. First, we use the machine learning methods to detect the newly registered domain names to check the similarity. For example, I registered the mahmut.com and our machine learning models check if it's a 90% phishing website or not that we taught before.

NICO CABALLERO: Random forest.

MAHMUT ESAT YILDIRIM: Yeah, generally. But on the other hand, we are working closely with the ISPs, with the CERT power, so that they are using their own network systems, the ISPs, huge network systems to detect the other kinds of DNS abuses, like DNS hijacking or DNS technical-related networking attacks. And they are using other different machine learning methods to detect the flowing packets. And they are reporting to us. When ISPs detect such an attack, they report to us. Then with the ccTLD experts and with the CERT experts, we go to incident response to detect and mitigate those attacks as well.

NICOLAS CABALLERO: Thanks. Thank you so much for that. I have the European Commission and then Mustafizur. European Commission, go ahead first.

GEMMA CAROLILLO: Thank you very much, Nico. Gemma Carolillo from the European Commission. Thank you to the Turkish colleague for the very interesting presentation. I have a couple of questions because we also have in the European Union for our own ccTLD .eu, we have a very similar approach. So, they are using AI and machine learning in the prevention phase, so basically to prevent the registration of malicious domain names.

But your approach seems to go even beyond. It seems more interesting because for what I understand, you integrate threat intelligence from the CERT and hence you're capable also to go into not only into the preventive phase, but when it comes to detection and even response, if I understood correctly. So, if you could clarify that.

And then I don't know if you have the information, if you can share it, because we have discussed about these tools a lot in this group. You say that this is developed in-house by the ccTLD. If you have information about the costs of such system and whether you think these systems, whether they would be made open, whether they could be used easily, integrated easily into other registries. Thank you.

MAHMUT ESAT YILDIRIM: Thank you so much. So our CERT mechanisms, generally we use our own developers, our own R&D activities in-house. So, it took almost a year to build this mechanism. Actually, it could take less, but we took more than a year maybe to teach the machine learning algorithms to create the new models. Before these algorithms, before the software was made, by manual, we had number of operators. By manually, they

were tagging the domain names like phishing, malware, or other types of. That's why we have a really huge tagged domain list. So with this domain list, we teach, we create new models and we are improving it every day. That's why it's really successful.

On the other hand, with the CERT mechanism, we can, as you mentioned, directly prevent the abuse activity. The ccTLD can detect the abuse activity or someone can notify ccTLD, there's a phishing website, or they can detect. And with the CERT, by cooperation with the ISPs, within maybe five minutes, we can block the access of this domain name. We can do domain cancellation as well, we can do takedowns, or we can directly block it. It depends on the case. If it's a cyber-related malware command and control, we directly block it with the ISP level. Thanks.

NICOLAS CABALLERO: Thank you so much for that, Mahmut. I have two more questions. We're not going to torture Mahmut with a thousand questions. I myself have many other. I have Bangladesh and then India. Please keep it short and straight to the point. Go ahead, please.

MUSTAFIZUR RAHMAN: Thank you very much, Mr. Mahmut, for a wonderful presentation. As you said in your presentation, that after checking the documentation, the number of the complaint reduced. So my question is that checking of documents needs times, but on the other hand, the customer, they need quick service. So how do you balance this issue? Thank you.

MAHMUT ESAT YILDIRIM: Actually, that was before TRABIS. So until 2022, as you mentioned, it was a really slow process. So you could try to register for a com.tr domain name and you submit your official documents, maybe four or five pages, then operators had to check and had to check if it's a valid documentation or fraud by using different mechanisms, then they can give you domain names. But now after 2022, it's not like that. Now, it's like first come first serve. We don't require any documentation.

NICOLAS CABALLERO: Thank you for that. And there's a phone ringing somewhere. So I have India next. Go ahead.

T. SANTHOSH: Thank you, Chair. This is T. Santosh for the record. And thank you, Mahmut, for the presentation. So my question is, is .tr open to the globe? If yes, what is the verification validation you do for those? Thank you.

MAHMUT ESAT YILDIRIM: So .tr is open globally, but we have a number of allowed registrars in Turkey. So you can use only those registrars to register a .tr domain name. And you have to have the WHOIS data correct and you have to provide the WHOIS data correct, like with the email address or the physical address, phone numbers as well. It's similar to .com or some other gTLDs.

NICOLAS CABALLERO: I have one quick last question. This is the only chance I will have to ask you. So I need to do it, sorry. Before I give the floor to Owen from the US. For DNS tunneling, what worked better according to your experience, like multi-layer perception in terms of neural networks or naive base? What worked better in your case?

MAHMUT ESAT YILDIRIM: Actually, in that context, I think by using this flow data and using the neural networks could be better. Because we could not be sure how they are using, how they're implementing that DNS tunneling mechanisms. We cannot be sure what they are pushing through those tunnels. So maybe we can gather the packets. Maybe we can gather the packets and using neural networks to teach, to detect the DNS tunneling in the huge number of packets, then we can analyze it in detail by hand.

NICOLAS CABALLERO: Thank you very much. I have Bangladesh, and then I'll give the floor to the US. Bangladesh, please go ahead. I'm sorry, I'm sorry, it was an old hand. So, I'll go to the-- Sorry. I saw a hand. Is that Libya? Libya? Go ahead, please.

KHALED ALTARHUNI: Thank you, Chair. The question is for Mahmut. Thank you, Mahmut, for a good presentation. I'd like to know, is the system addressing a legal content in the domain like text, pictures? Thank you.

MAHMUT ESAT YILDIRIM: Yes, actually, this software that we built, AZAD, I didn't mention in detail, but it checks the similarity of the domain name and also the context of this website. First, it pushes an alarm when it detects from the similarity check, like 95% it's phishing, it pushes an alarm. But there is no context in this website, so that we cannot do anything about it. For example, let's say a person is holding a gun, doesn't mean he's going to shoot someone.

That's why we have to see there's an abusive activity in this website. And the machine learning algorithm checks the context of the webpage, if it's updated or renewed, then when we see actual abusive activity in the context, like a phishing website or other kinds of things, then we take measures and prevent it. Thanks.

NICOLAS CABALLERO: Thank you very much, Mahmut. Indeed. Thank you, Libya, for the question. At this point, let me hand the floor to Owen Fletcher from the US government. Sorry to keep you waiting. The floor is yours.

OWEN FLETCHER: Thank you. Hi, this is Owen Fletcher from the United States. I think we're running a little behind on time for our session, so I'll be very brief.

And I think all of our speakers for the rest of the session also know we'll try to be quick. But we have Leticia Castillo here from ICANN Contractual Compliance to present us with an update on the DNS abuse contractual amendments that the GAC welcomes earlier this year, and which the GAC has expressed interest in following regarding their impacts and enforcement. So I'll turn it over to Leticia. Thank you.

LETICIA CASTILLO: Thanks, Owen. Hi, everyone. My name is Leticia Castillo. I am a senior director with ICANN Contractual Compliance. And like Owen said, I'm going to provide an update on the first six months of enforcement of the new DNS abuse requirements that became effective on April 5. I also want to highlight that last week, on November 8, we published a detailed report on the first six months of enforcement. It's 17 pages with a lot of information regarding the investigations conducted, outcomes, examples of the responses and actions that were deemed compliant. So please take a look at the report if you want even more information about the enforcement actions taken.

With that, let's go to the data. From April 5 2024 through October 5 2024, we initiated 192 DNS abuse investigations with registrars and registries. These were cases that involve at least one type of DNS abuse that for the purpose of the ICANN agreements means phishing, farming, malware, botnets, and spam, when spam is specifically used to deliver one or more of the other four forms of DNS abuse. As a result of these investigations, two of the cases ended up with a formal breach notice

to a registry operator and one to a registrar for failing to comply with the DNS abuse requirements.

We resolved 154 DNS abuse investigations during what we call the informal resolution stage of our process, which is the process in which we resolved most of our complaints across all types because the registrar or registry demonstrates compliance or takes action to remediate a noncompliance before escalated compliance actions are taken.

And because one compliance case can involve one domain name or multiple and because one compliance investigation regarding a number of domain names may result in the discovery of additional abusive domain names within the account, for example, those 154 investigations that were resulted in the suspension of over 2,700 malicious domain names and the disabling of over 350 websites in these cases because the registrar or reseller was also acting as a web hosting provider for those domain names.

I also want to point out that these are the numbers for the period, the first six months, April 5th through October 5th. We currently have multiple investigations ongoing, hundreds of domain names, part of them, others were closed after October 5th, so these are not counted toward this mitigation number but will be included in future updates.

During these six months, we also participated in multiple outreach activities with the community to raise awareness of the new requirements. For example, in September, we were part of a workshop with contracted parties in Beijing where there was a focus on the new

DNS abuse requirements. Same here in Istanbul, last month. We do work closely with our colleagues in GDS and GSC that lead this type of capacity building activities as part of the ICANN's multi-faceted DNS abuse mitigation program.

We just launched an audit dedicated to validate compliance with the registry agreement, including DNS abuse requirements, not limited to DNS abuse requirements but including them. In June, we began publishing monthly reports on our enforcement of the DNS abuse requirements. These reports are broken out by the type of DNS abuse and related enforcement actions.

They start with April 2024 data and are updated every month. The format we used for these reports really provided a comprehensive picture of these cases when also complemented with regular updates with insights and outcomes, like the ones we have presented before and the November 8th report, but the intention was always to continue building on these reports and improving them over time. So, we do welcome feedback from the community to do so. I mentioned the November 8th report before. It's also linked at the bottom of this slide.

I was mentioning before the 154 DNS abuse cases that we resolved. This slide provides a summary of the reasons why those were resolved. With respect to the cases with registrars, the number is 151. In approximately 52% of the cases, the registrar confirmed the DNS abuse and took action to stop it by suspending the domain names. In approximately 21% of the cases, the registrar did not find actionable evidence of the DNS abuse and the response was deemed compliant

because they provided us with a reasonable explanation of what was done to investigate and how they reached that conclusion.

For example, a registrar assessed all the information and evidence they had regarding the domain name, including account information, including communications with the registrant and the account holder and determined that the registrant was actually acting with the knowledge and consent of the entity that was believed to be impersonated to conduct a simulated phishing program using the domain name. That's one of the examples.

In approximately 12% of the cases, the registrar took action to disrupt the course of the DNS abuse by, for example, forwarding the claim to the registrant who then took action to disable the URL where the DNS abuse was placed. In approximately 3% of the cases, the registrar took other actions to stop the DNS abuse. For example, sync calling or redirecting the name servers so that users trying to reach the malicious domain name were instead redirected to IPs that were controlled by the registrar. This is for registrar.

Let's talk about registries. We resolved three cases with DNS abuse cases with registry operators and all the cases, all domain names were suspended by the registry. Again, these were the cases resolved. We have many others ongoing. We also had one case that it was limited to problems with the abuse contact. Those were also resolved. The difference in numbers between cases resolved with registrars and registries is consistent with the fact that of all complaints received, 94%

referred to registrars. Of all investigations initiated, 97% referred to registrars, the rest to registries.

But we do not have a minimum or maximum for us to initiate an investigation or escalate an investigation. Proof of that is that during the same period, we issued a public formal notice of breach to a registry and a public notice of breach to a registrar. As I was mentioning before, these are the numbers for the first six months. We have a lot going on. We have a lot that was resolved after October 5th, and we intend to continue providing updates and issuing reports with details regarding those as well. I want to stop here so we have time to answer questions.

OWEN FLETCHER: Thank you. I found that information very useful, and I imagine everyone else did as well. This is a topic I think is important for the GAC. I'm sure we have questions from the audience. Nico, did you want to?

NICOLAS CABALLERO: Yes, we have time for a couple of questions. I have India.

T. SANTOSH: Thank you, Chair. This is Santosh for the record. That presentation was quite briefly explained about the role of registries and registrars. From India, during the period, we have raised three such complaints through this contractual complaint's website, but the thing is that we don't have any status of that complaint. It doesn't come through our mail also. So,

what is the status of the complaint we are raising? It is not being reflected. Can you explain about that? Thank you.

LETICIA CASTILLO: Hi, this is Leticia Castillo. Thanks for your question. If I understood correctly, you submitted three complaints, I think you indicated, and you did not receive a status update to compliance. I do believe that I'm aware of the complaints that you are referencing, and I believe we requested certain information and we're asked to grant additional time to provide it, and we are waiting on those.

But I can certainly look at those offline with you just to make sure that I'm thinking about the right complaints. But it is part of a process when a complaint is submitted, there's a confirmation that provides a case ID, and then there is additional communications that the processor sent out to the complainant either to request additional information. This happens often. We do a comprehensive review of each complaint.

Many times, we need clarification, we need more evidence from the complainant, and we send that we receive it, cases like such as the example several times, and also receive requests from our complainants for more time so they can gather that information that we're requesting and provide it to us. And when the cases are resolved, they also receive an explanation why the case is resolved and how to contact Compliance if they have any question about the case that was resolved. That's also sent out with every communication that we sent. So, I'm happy to talk to you offline and give you further updates about those complaints.

NICOLAS CABALLERO: Thank you so much for that. I have Netherlands and then the US. Please try to keep it short and sweet. Go ahead.

ALISA HEAVER: Thank you. This is Alisa Heaver for the record. Thank you for the presentation. I was wondering to what extent have these been numbers or how are these numbers compared to half a year ago or a year ago when the new measures were not in place yet? And my second question is, what is the average duration of an investigation before a registrar undertakes action? And to what extent were the investigations that have been started based on the new contractual measures? So, the additions to the previous set of regulations. Thank you.

LETICIA CASTILLO: Thanks for the question. So, with regards to numbers, what we are observing for the last few years, even before April 5th, we observed an increase in the number of complaints that we received regarding abuse. Just to give you a data. In 2023, we were receiving in total an average of over 1,300 new complaints a month that added to existing cases. From January to September 2024, the average was almost 2,000 new complaints a month. So, there has been an increase for sure, and even before April 2024.

With regard to the time that investigation takes, it totally depends on the type of investigation. We have the DNS abuse cases with one domain name. Very straightforward. We contact the registrar. The

registrar says yes. The domain name needs to be taken down. It's taken down.

It can be done within the same day. We do have an investigation that has thousands of domain names included where the contracted party is requested to not just address the abuse report, but also, we detect patterns that indicate they do not have a process in place to address the DNS abuse. So, it's not just that report. It impacts future reports and how they overall address the DNS abuse.

So, we request them to provide a remediation plan and how they're going to implement it and milestones and implementation dates to make sure that they put that process in place. And we wait until that process is in place and we test it and then we close and monitor that because if recurring issues happen after that's implemented, escalated complaint action happens. So, it totally depends on the case, how long it's going to take.

NICOLAS CABALLERO: Thank you very much. I have one more request for the floor, USA. Laureen, go ahead, please.

LAUREEN KAPIN: Yes, this is Laureen Kapin speaking in my capacity as a member of the Public Safety Working Group. I wanted to express gratitude for all the work that's being done here and just to also say that this is very encouraging that we're seeing these very specific responses to mitigate DNS abuse and it's a sign that these are welcome and effective changes.

My question is there's a category here on the slide that's up. The registrar took action to disrupt the DNS abuse, which is separate and apart from suspending the domain name. Can you speak to what types of disruption you're seeing?

LETICIA CASTILLO: Thanks, Laureen. So, the obligation in the agreement is to take mitigation actions to stop or disrupt the DNS abuse and the specific actions will depend on the specific circumstances of the case. So generally, a clear case of DNS abuse domain name that was registered to perpetrate that domain name abuse generally results in the suspension of the domain name. There are other cases like the example I was giving.

For example, in this particular case that I'm thinking, it was a compromised domain name and the registrar contacted the registrant and informed this is happening. You need to do X and Y to make sure this doesn't continue happening. So, the registrar went ahead and took care of the URL itself. That was a disruption on the part of the registrar and that was found compliant with the agreement.

NICOLAS CABALLERO: Thank you very much. I'll go back to Owen now.

OWEN FLETCHER: Thank you, Nico. This is Owen Fletcher. I agree it's great to see the metrics being released related to enforcement of the contract

amendments and great to see the results that you're reporting already. We're going to move on to a panel discussion with the slides up. We have Reg Levy from Tucows, Dennis Tan from VeriSign, and Jeff Bedser of CleanDNS and also the SSAC. They will be answering a few questions on the next slide, please.

One of these is only really aimed at Reg and Dennis as it specifically says, as a Contracted Party, what have you done since the amendments? Please help us understand that. The questions two and three are for everyone. What have been the impact and consequences of the amendments in your view? And what are the lessons learned from the first six months of implementation of the amendments? So, this will help us continue to get more views and learn about follow-up on the amendments. We are trying to keep each of you to three minutes. Sorry if I interrupt you if you're going over, but I'll try to keep us a little on track. And can we start with Reg?

REG LEVY: Thanks, Owen. Reg Levy from Tucows, a domain name registrar. Tucows was intimately involved in the negotiation of the amendments. So, a lot of, well, the main thing that I'm going to say is not much that we have changed since the amendments because we think we were doing things right in the first place. But we are very pleased that the amendments are now part of our contractual obligations. I have a team of seven DNS abuse professionals who review all of the reports that come in to confirm the alleged abuse and to take mitigation action.

One of the things that we have started doing that has changed since the amendment, although perhaps not because of the amendments, is that we've started sinkholing rather than suspending a lot of the phishing domains. Sinkholing means that we direct the NS records of a domain to a particular set of DNS servers that are actually run by CleanDNS over here on the panel so that they can get additional information about the phishing campaigns, and they can see trends across registrars. So, we can see certain things that take place in our namespace, but a group like CleanDNS can see broader trends in the industry. And we hope that this information that we are providing to them will help them better identify campaigns across the industry.

OWEN FLETCHER: Thank you, Reg. That was well under three minutes. Good job. Dennis, would you like to go next?

DENNIS TAN: Thank you, Owen. There isn't much to add to Reg in terms of the impact of the DNS abuse amendments. In terms of the registry operators, much of the responsibility lies on the registrars who have the direct relationship with the registrant. At the registry level, we tend to look at the scale security threats like, for example, botnet DGAs, and that's where something the registry operators are more capable in preventing the registration of those domain names because those are reverse engineering and no specific list of domain names that could be acted upon at the registry level.

In terms of registered domain names, we most likely will refer those to the registrar so they work with the registrants in the most appropriate way to handle the mitigate or disrupt the DNS abuse happening. I think I just want to say in general, and I'm speaking for in general all the registry operators, one of the aspects that the abuse amendments have helped in a practical standpoint is to raise the level of the quality of the abuse reports. Now that the abuse reports require evidence, that makes us easy to evaluate and determine, verify what the abuse is and take the appropriate action in that regard.

I also want to note something that our both groups, combined CPH, DNS abuse working group, have been doing since the institution of the DNS abuse amendments that we always said that was going to be the first step in multiple activities in terms of helping mitigate DNS abuse. We have been working and doing outreach to other ICANN community groups in order to find common issues that we can work on, whether it's a policy work or just finding best practices or finding solutions to those problems.

Just recently, and maybe some of you have attended the session earlier in the week with the NCSG, the CPH collaborator, looking DNS abuse mitigation practices through the lenses of human rights impact assessment. That's one of the examples of our outreach and the work with the ICANN community. I think I want to pause here, yes, in the interest of time and go back to you, Owen.

OWEN FLETCHER: Thank you, Dennis. That's great. Jeff, let's move on to you. And you have some slides, so.

JEFF BEDSER: Thank you. And I'll breeze through the first several slides because they're a repetition of what was already provided. Okay. So, what I want to do is a bit of a data comparison. I apologize. I've been fighting keeping my voice for the week. So, I'll do my best to enunciate so you can understand me clearly. I've got some data to share that is about the broader volumes, DNS abuse. So, we can kind of put things in perspective for the volumes we're talking about.

So, the period of April to June, we processed about 628,000 abuse reports. That represented about just short of 160,000 unique domains. So multiple reports to a smaller number of domains. The average monthly volume pre-obligations change was about 225,000 reports per month. And post the obligations change, it was a slight increase up to an average of about 240,000 reports per month.

In conversations I've had with registrars and registries and some hosting companies, that is an increase that they've seen. I think it comes about from the knowledge of knowing there's a change in obligations and many reporters started generating more reports. Though one reporter might report the same domain to the hosting company, the registrar, and the registry, thus it could count for three reports for one incident.

So, here's an example, again, of the monthly phishing volumes of report volumes between September of 2024 back to October of 2023. And you can see that within the averages per month, the report volumes have, there are spikes occasionally and a couple of dips. But for the most part, the volume of reporting continues roughly the same across phishing.

So, this is something I thought was very interesting. The registry that was breached, it's a public breach report from ICANN, was .top And we looked at, on the date, the month of the breach notice was July. That month, there were a total of about 7,000 abuse reports for .top. The volume in August was slightly higher, just short of 8,000. September went up again by another 2,000. And in October, it's 13,000. So, this is a great example of how ICANN Compliance picked a very good party to breach on this issue.

Because obviously, despite the breach notice and an extension, the volume of reports of abuse within that zone continue to grow. So, this is not showing that ICANN Compliance has not done their job. This is a great show that they are doing their job. This is the type of parties that the change in the obligations were made to address, parties that weren't addressing the abuse. And volumes like this are a demonstrative of that.

So, what we're measuring now, of course, is the total number of reports processed, total number of domains involved. And on average, it can be a 3 to 1, 2 to 1 ratio, number of reports to number of domains involved, number of actions taken by Compliance per registry-registrar,

and of course, number of breach notifications. I'd like to suggest on the next slide, what we should be measuring, because it's more impactful to understand how the obligations are changing behaviors and thus changing victimization through DNS abuse.

How many reports were evidenced adequately for mitigation? Because a number of reports is great, but being a company that processes somewhere close to 8 million reports a year, I can tell you about half of those aren't evidenced well enough to take any action. They're wrong, classified wrong. The harms were mitigated before they were reported.

So, it's really good to know, with this new evidencing standard, how many reports are really being given to the parties that are at the right standard to be actioned. How long did the harm last? That's something that I tend to get very passionate about, because the shorter the lifecycle of a domain being used for abuse, the less victims. And currently, the mean is about 48 hours. I think using AI technologies and machine learning, we can definitely get two minutes into these processes. So, it's reported, validated, and mitigated.

The next measurement point, and I know that's another part of ICANN with the domain metric and the OCTO office is working on this, is how effective was the mitigation at reducing overall volume? Because right now, the American term, of course, is whack-a-mole. You take one down, there's another one, another 100 to replace it. But when we get the effective point of taking enough down, enough mitigation work where we start seeing a change in behaviors of the bad actors. And then finally, how much effort is involved in getting a non-compliant party

into Compliance on abuse mitigation? I'll leave that question to be answered by the Compliance functions at ICANN.

OWEN FLETCHER: Jeff, sorry to interrupt you. We're over time. Can you wrap up? Thank you.

JEFF BEDSER: Well, this is my last slide. But I'll summarize it very quickly in that I think the change in the obligations was good. I think the change in behaviors from all the parties, the parties that report harms, has gone up significantly. I think I continue to see those trends going up. I'm seeing that the parties that are the problems, which is the parties that are outside of the ecosystem and not taking the actions, are being noticed for not taking those actions. And I think that's a bigger story to be told here, good or bad, is how the amendments are having an impact systematically. And I think that with six months under our belts, I think it's a good sign things are going in the right direction.

OWEN FLETCHER: Thank you, Jeff. We also have a quick statement from ICANN Global Domains and Strategy, Mukesh Chulani. Mukesh, you can go next. Thanks.

MUKESH CHULANI: Yes, thanks, Owen. I just wanted to underscore our belief that we are seeing case-level impacts from the amendments. We're six, seven

months in, and you've heard both from contracted parties, we've seen some aggregate-level reports from contractual compliance. You've also seen from a third-party metric specialist that there are some positive impacts.

There's some momentum going in here. The abuse amendments, as Dennis also mentioned, was never meant to be the definitive step forward. It's meant to be the first step forward. And you can expect preferences to change, you can expect attack vectors to change. So, we should continue to keep on top of it, keep on top of the discussions.

From our perspective, Compliance is there to enforce the contractual obligations. We have contractual data very focused on that slice. Of existing cases. And that should be complemented by wider angle lens of market abuse. So, the wider angle. We have existing projects through our OCTO team. One is Metrica, which is a platform for data measurement.

And we should be hearing more about that in the coming days and in the coming months. And then the other one is INFERMAL, which is a study being launched to evaluate attacker preferences. So, those are some of the work we're doing internally. We also, as Leticia mentioned, continue to look for ways to facilitate exchange of good practices through platforms like this. So, we thank you all for the invitation. Let's keep at it. Thank you.

OWEN FLETCHER: Thank you, Mukesh. I think it is very helpful for us to get views and research and analysis from a broad range of stakeholders on this issue, so the GAC can have evidence-based discussions about possible next steps, as you and others have mentioned, since the contract amendments are meant to be only one step of many to follow. So, we have allotted some time for more Q&A right now before moving on to GAC discussion. Nico, can I turn it back to you for any questions from GAC members? Thanks.

NICOLAS CABALLERO: Thank you so much, Owen. Thank you, Mukesh. And thank you to the panelists, Reg, Dennis, and Jeff. I don't have any hand online or in the room at this point. So let me just handle the floor to Martina in order to walk us through the GAC discussion. Martina, over to you.

MARTINA BARBERO: I notice a hand raised.

NICOLAS CABALLERO: Yes, there's the European Commission. Go ahead, please.

GEMMA CAROLILLO: Thank you, Nico. I'll be very brief. I would have a question to the speaker, I believe, from Verisign. I hope I'm not-- Yes, that's you. You mentioned that you are exploring a possible area for policy developments. You mentioned one example of engagement you had with the community. I wanted to know whether you have already a few

ideas because we are discussing the same in the GAC. It would be very useful to compare notes. Thank you.

DENNIS TAN: Thank you for the question, Gemma. So, we're exploring the next item to work on. Not necessarily a policy development process because early, a few months back, I think we've heard from the community that a policy development process is very time-consuming, cumbersome, and takes a lot of resources. And that's how the idea of people to target and narrowly focus PDPs, which that's on the table. So, PDP, it's one of the possible ways forward. That's what we're trying to explore, having conversation with the ICANN community. We want to learn more from the infirmary report that was just published. So, I've just skimmed it. I haven't consumed it just yet, but I believe that's going to help also be, it's going to be a catalyst for conversations, which we, of course, welcome.

NICOLAS CABALLERO: Thank you so much for that. I have the USA next.

OWEN FLETCHER: Thank you. This is Owen Fletcher again. Quickly, I just wanted to note, I recall, I believe the Board offered at one point to convene listening sessions on the scope of any possible PDPs going forward that could address more nuanced considerations flowing from the amendments and follow up on those. I think we'd be interested in any update on that, although that's probably not a question for anyone here.

NICOLAS CABALLERO: Of course.

REG LEVY: So, this is Reg Levy representing the Registrar Stakeholder Group DNS abuse subgroup. Dennis and I, as co-chairs of the Contracted Party House DNS abuse subgroups, have been conducting listening sessions that don't necessarily-- they're not exactly these Board sponsored ones, but we've reached out to various members of the community, various official groups and unofficial groups within the community to find out from each of them what they want us to do, what they are seeing, the sorts of trends that they are interested in and how we as contracted parties can take that on and not necessarily turn it into a PDP, but listening sessions, having those conversations.

We've already met with the ALAC. We are hoping to meet soon with the SSAC to, again, have these individual conversations so that each of the different groups within the community have an opportunity to speak to us directly.

NICOLAS CABALLERO: Thank you, US. Thank you, Reg. I don't see any other hands, so let me give the floor to Martina Barbero from the European Commission, who's going to be walking us through the next steps and whatever Communiqué consideration we might have. Martina, over to you.

MARTINA BARBERO: Thank you very much, Chair. In fact, we still have two short parts of the agenda before we leave you and we free you for lunch. I know it's the last part before lunch, but please bear with us because this is important. So first, we wanted to just open the floor for a discussion on what we just heard today. And we have put together a few discussion questions to see if you have any feedback to share. Mainly, what we would like to discuss within the GAC right now is if you have any reaction to today's briefing on the implementation and the impact of the contract amendments. I think we've heard many interesting things. So, if you have any reaction or comment to share, that would be a good moment.

Also opening the floor to see if there is any other lessons learned from the previous round that would help us to prepare for the next round in relation to DNS abuse mitigation. I think we heard a bit. We spoke briefly about PICs and RVCs yesterday with the contracted parties, but there is also, and I was not there, there is also a very nice report on DNS abuse from the previous round that had some conclusions that we could take on Board when we prepare for the next round.

And finally, also, because we heard a very nice presentation from our Turkish colleagues, if there is any other ccTLD best practice that could be considered and could be food for thought for the gTLD space. That's also a moment to share those. So, before we go to Communiqué consideration, Nico, maybe we can open the floor on these points and see if there is any reaction from GAC members. Thanks.

NICOLAS CABALLERO: Thank you for that, Martina. So, there it is. The floor is open. We're more than happy to take any question, comment, or anything you would like to share with us at this point. And I have India. Go ahead, please.

T. SANTOSH: Thank you, Chair. This is Santosh for the record. So, during ICANN80, we had proposed that proposed for DNSSEC deployment, which should be made mandatory, particular in the sectors like financials, financial services, health care, government and telecommunication. So, this would align with the global security measures and ensure the protection of vital national infrastructure. So, any thought about that on DNSSEC deployment? Thank you.

REG LEVY: This is Reg Levy from Tucows. DNSSEC is one way of securing domain names and HTTPS seems to be the currently adopted security protocol that the market has decided is what they want. We offer DNSSEC. We are happy to assign DNSSEC to any domain name that is purchased from us. It is not a very popular option. It's not a security standpoint that a lot of our customers seem to be interested in taking advantage of in the way that, as I said, HTTPS seems to be. You'll also note that a lot of browsers are starting to require HTTPS, which is pushing that more as well.

I don't see a problem with asking certain sectors, encouraging certain sectors-- Sorry, I'm being told to slow down. I don't see a problem with

asking certain sectors to look into additional security pathways. But I have discovered that most customers are not interested in DNSSEC in the way that perhaps we at ICANN would want them to be.

NICOLAS CABALLERO: Thank you for that, Reg. I have the UK next.

CHRIS: Yeah, hi. Just introduction. So, I'm Chris. It's my first time at ICANN, but here from the UK, involved with the Public Safety Working Group in particular. I just wanted to comment building on India's point just now that just from a bigger picture perspective, it was only a few days ago, so last Friday, that under our UN Security Council presidency, for this month, we actually chaired a ransomware session. And there was quite a number of UN member states that signed up to a statement, particularly on impacts to CNI and healthcare, particularly on ransomware, but obviously as a form of malware, it's very relevant to this discussion here.

So, there is an increasing appetite, I think, from quite a number of certainly UNSC members at the moment. It also expands to bodies such as the Counter Ransomware Initiative, which again India are very active in alongside the UK and others in the room. So, it's not so much a question, but I think more a comment that other multilaterals that a number of government members here are involved in are pushing these issues higher up the agenda. The fact that it was on UNSC at this time, obviously it's quite pertinent. And so, I think there'll be a bit more

emphasis, certainly through the PSWG route up that we do perhaps need to look at risks to particular CNI sectors and sort of move forward towards that. Thank you.

NICOLAS CABALLERO: Thank you for that, UK. I have the USA next.

OWEN FLETCHER: Thank you. This is Owen Fletcher, USA. I wanted to respond briefly about DNSSEC as well. I recall that at ICANN80 we did have some texts in the Communiqué, which I think followed Santosh from your question about it at the time. So, we could review the text, but I think I would just say, I'd point out that our text then did note supporting promotion for adoption of DNSSEC, which seems like a good idea in general to me. But I'm not sure about the idea of calling for it to be required. That seems like something we might need to-- before considering that, we would need to get a lot more information and be well informed about implications and whether that would be a feasible idea.

I was also remembering that the SSAC noted in their bilateral meeting with us that they follow this topic a lot, of course, so they may be a good source of input if we determine that we want to seek more information. Thanks.

NICOLAS CABALLERO: Thank you for that, US. I don't see any other hands online or in the room. So let me get back to Martina Barbero from the European

Commission in order to deal with next steps and whatever Communiqué considerations we might need to be aware of at this time. Over to you.

MARTINA BARBERO: Thank you very much, Nico. And thanks to all the GAC members who intervened today. I think it's Christopher made a good reminder that this topic is pushed high on the agenda, so we surely take that into account. And that leads us to the Communiqué consideration. So, if you could go to the next slide.

So as just to recall, as topics leads what we're putting now on the slides are some possible elements for reflection, but the input comes from you as GAC members. As always in the Communiqué, we have the possibility to go for advice or issues of importance. And in terms of elements that could be considered to be put on the Communiqué, following the presentation we had on the implementation of the contract amendments and the measurement of their effectiveness, we might suggest to continue following on that as the GAC. I think that would be interesting.

And then, of course, I think we already heard it this morning from ALAC, and then today, there might be some expectation of further work, whether policy or otherwise. Just to recall that when there was the contract amendments public comments, the GAC put together a response which indicated there were some topics that could be conducive of further work. Those are listed here. So proactive monitoring, enhanced transparency, periodical review of DNS abuse

definition, addressing DNS abuse within and outside ICANN, guidance on key terms, compliance consideration.

Sorry, sorry, sorry. You're totally right. I was trying to raise, to open the floor as quick as possible, my bad. And so, these were just some of the topics that were included in the-- these are topics that were included in the response to the contract amendments public consultation at the time. And then in Kigali and also yesterday a tiny bit, we discussed about any consideration in preparation for the next round TLD, which will open soon.

So, these are all elements that could go into the Communiqué. But the point of the next eight minutes is to see whether these are points that you could consider relevant. If there is anything else or you have any other consideration to share before we go in Communiqué drafting mode. Thanks a lot.

NICOLAS CABALLERO: Thank you for that, Martina. So, the floor is open. Any comments, thoughts, questions? USA, go ahead.

OWEN FLETCHER: This is Owen Fletcher, USA. Already mentioned earlier today was the informal report and somebody earlier, perhaps Jeff was it, also mentioned domain Metrica, the upcoming OCTO platform. So perhaps we note our interest in further sources of information and research that could help us identify possible future work on DNS abuse amendments. I also, I mentioned listening sessions earlier and Reg noted the

contracted parties seeking input on that as well. So perhaps further engagement on that is something the GAC could note interest in. Thanks.

NICOLAS CABALLERO: Thank you, USA. I have the European Commission next.

GEMMA CAROLILLO: Thank you, Nico. Gemma Carolillo. I would like to echo what Owen say that we could reflect on the sessions that we had yesterday and today as well. So, there was, I think, a lot of interest in the GAC about the report from SSAC, including on the impact of emerging technologies on DNS abuse. I think we should-- I mean, there was really a lot of questions and interest in moving that work forward. And also, I think the welcome proposal from the ALAC for the two groups to work side to side as regards a topic of mutual interest, they referred in particular to the subject of the report. So, the maliciously registered domain names. But I think the topic in general is a shared concern between the ALAC and the GAC. Thank you.

NICOLAS CABALLERO: Thank you for that, European Commission. Any other comment or question? Yes, go ahead, please.

SAMANEH TAJALIZADEHKHOOB: Thank you, everyone, for all the presentations. I'm Samaneh, the Research Director of the SSR Research Team within ICANN Org. Since

the name came up a couple of times, we are the lead of the ICANN Domain Metrica Project and also the group who funded INFERMAL project. I wanted to invite you all to tomorrow's session at 1:15 on DNS abuse updates, where we talk about both projects, the feedback we got, what we are going to do for the next steps. Thank you.

NICOLAS CABALLERO: Thank you so much for the invitation, Samaneh. Unfortunately, the GAC will be having a session. We'll be drafting the Communiqué tomorrow at 1:15, but thank you so much for the invitation, even though that doesn't preclude anybody from attending. Of course. Thank you so much. I have the UK next.

NIGEL HICKSON: Yes, thank you, Mr. Chairman. Very briefly. This really excellent dialogue. I just wondered, I mean, obviously, we haven't got time to touch on it now and it's a new issue, but in previous meetings, when we had discussed the RDRS and looked at that, we'd also noted the dialogue that had taken place about having sort of mini PDPs or micro PDPs on specific aspects of DNS abuse, such as phishing and malware. And this had generally been welcomed by members of the GAC to do this. This hasn't been taken forward. I know there's many other issues on people's agenda, not least on the GNSO policy agenda. But I think it is something we need to come back to, because clearly there are specific issues on some of these issues, on some of these aspects of DNS abuse. Thank you.

NICOLAS CABALLERO: Thank you, UK. Well noted. Any other comments? I don't see any other hand in the room or online. So, let me just give our distinguished panelists or the European Commission, USA Government, Reg, anybody for any final remarks. The floor is yours.

GEMMA CAROLILLO: Just to thank all the GAC delegates who participated in the discussion today. Thank you very much. The co-leads might suggest some texts for the Communiqué. Maybe under the issues of importance, this is a topic that remains an issue of importance for the GAC. So, we will put together something for your consideration.

NICOLAS CABALLERO: Thank you for that, European Commission. Any final remarks from our distinguished guests?

DENNIS TAN: Thank you, Nico. Now, I appreciate the invitation and being part of this conversation. We think it's a very important one. So, Reg and I, we are reachable. So, any discussions, again, the amendments were the first step. And now we look forward to the next conversations. And whether that's a PDP or something else, we want to be part of it. Thank you.

NICOLAS CABALLERO: Thank you so much for that. Jeff, Hajime-- Go ahead, Jeff.

JEFF BEDSER: I'd also like to take the opportunity to thank for the invitation, the opportunity to speak on this topic with this group of people. Thank you.

NICOLAS CABALLERO: Thank you so much, Jeff. Mahmut, Hajime?

HIJAME ONGA: Thank you very much for your fruitful discussion. It's my first time, but it's a really memorable situation. So, I'd like to do my best from the next session. Thank you so much.

NICOLAS CABALLERO: Thank you, Jimmy. Mahmut?

MAHMUT ESAT YILDIRIM: Thank you so much for giving me the opportunity to share our experiences with you and hope to see you here again to exchange information and share experiences. Thanks.

NICOLAS CABALLERO: Thank you, Mahmut. And we hope to come back to Istanbul soon. I have Colombia next.

THIAGO DAL-TOE: Thank you, Nico. Thank you, everyone. Just to remember for those who are joining us that don't know, but the DNS abuse is one of the topics that we have for our strategic objective, actually number four. And I just wanted to thank the topic leads as well for putting together this great session and hope we can continue to do some great work on this issue. Thank you.

NICOLAS CABALLERO: So, thank you very much, everyone. The meeting is adjourned. Please be back at 31:15 sharp for the meeting with the Board. Thank you so much. Enjoy your lunch.

[END OF TRANSCRIPTION]