ICANN84 | AGM – DNS Women
Wednesday, October 29, 2025 – 16:30 to 17:30 IST

MICHELLE DESMYTER: Hello and welcome, everyone, to the DNS Women. My name is Michelle DeSmyter. I'm the Remote Participation Manager for this session. Please note that this session is being recorded today and governed by the ICANN Expected Standards of Behavior and ICANN Community Anti-Harassment Policy. During the session, questions or comments will be read aloud if submitted within the Q&A pod. Interpretation for the meeting will include English, French, and Spanish. If you would like to speak during the session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom. On-site participants will use a physical microphone to speak. Please state your name for the record, the language you will speak, if speaking a language other than English. And please speak at a reasonable pace. And with this, I will now hand the floor over to Vanda SCARTEZINI.

VANDA SCARTEZINI: So, thank you very much for all you that have come in today. Normally, there is a lot of conflicts in the agendas around the ICANN meetings. But I appreciate you making room to be with us this afternoon. And as normally, we normally give the floor to our special guests the honorary members the members of the board, and one

special honorary member that is always with us, and Maarten Botterman. The floor is yours.

MAARTEN BOTTERMAN Well, thank you for welcoming me. And I just recognized another honorary man coming in there. It's been truly a pleasure to see ICANN evolve over the nine years I've been on the board. And this network has very much emerged as well in that way. And the value that it brings to you to support each other, but also to get recognition by others of the value of what you do together is tremendous. So I really would think a big thank you is more to you and those who made this happen than to me who happened to come along and appreciate it and being all for that. So I would like to applaud for you. And I really appreciate also the fact that you're going global. So congratulations.

VANDA SCARTEZINI Thank you very much. And now I can give the floor to the other honorary member. Our former chair of the board also, Mr. Steve Crocker. The floor is yours, Steve. You are welcome.

STEVE CROCKER Thank you, Vanda. I felt honored when you made me an honorary member of this group. Multiple things come to mind. Some are more humorous than others, but I'll be serious for a moment. I value this group quite a bit. I think it's very important. My home base inside of ICANN is the Security Stability Advisory Committee, and at this very moment, no, sorry, I'm off a little bit, but there was a different

meeting taking place, and it became clear to me that I wanted to be here instead of there, and so I always give high preference to this. The jokes that I had in mind were how do you meet women at ICANN? Well, there's a way to do that, and here we are. The whole constituency structure of ICANN has some peculiarities to it in terms of where the lines are drawn. This is one of the more important constituencies, even though it doesn't show up on the official multi-stakeholder org chart. So more power to all of you.

VANDA SCARTEZINI Thank you again for being with us. I hope you continue to be with us many years. So I will give the floor now to the other members of ICANN. Other members of the board, please. Catherine is over there. Come over, Catherine, and say you're welcome to the community. Sorry.

CATHERINE Hi, Vanda and everyone. I was just saying we are so many members of the board here, so I won't take up the space, but it's always a pleasure to be here, and I like the joke that if you want to meet women, anyway, let me leave it there. But there's always something to learn from this forum, and I'm so glad we are here, and we are quite a few of us.

VANDA SCARTEZINI Thank you, Catherine. Leon, your turn.

LEON SANCHEZ

Thank you very much, Vanda, and thank you, everyone, for having us again. It's a pleasure and an honor to be with you again, as we do in every ICANN meeting, and all I have to say is continue doing the good work that you do and continue bringing awareness to the importance of gender equality and gender balance within our organization. Thank you for that, Vanda, and thank you to all the women here, Indiana's women.

VANDA SCARTEZINI

Thank you, Leon. I was waiting for the time that we go back to our region to give you the honorary participant on that, but we never go to our region, Leon. It's something that we need to go back to Latin America and Caribbean area. Anyway, you're going to give wherever we go. Thank you very much for your words, and let's restart our… Where is Miriam? Miriam, your turn.

MIRIAM SAPIRO

Oh, Vanda, I was a few minutes late. I apologize, but it's so wonderful to be here and look around and see so many friends and familiar faces and see new people that I really am excited to get to meet. I'm starting now my second year on the board, having been appointed by the NomCom, which was a tremendous honor, so in a way, appointed by all of you. And I just want to say Catherine, who's a fabulous colleague, I don't want to take time away from this great program, but I do want to say something to Vanda I've said privately, and that

is you are a one-woman powerhouse, and so we all owe you a debt of gratitude for what you do, what you have built, and how much you inspire me and I think all of us every day. So let's carry that forward, let's help mentor the next generation, and as they say, pay it forward, pay it back, but really try to inspire also the next generation of leadership here.

VANDA SCARTEZINI Thank you, Miriam, for your presence. I want to remember that Becky is not here, but she is a very presence any time, and sometimes it's almost impossible for the conflict of interest, but I would like to raise the voice to thank you, Becky, also for all those time running with us and giving us support since the beginning. So I appreciate also the presence of everybody. So now we should change a little bit exactly because of the conflict of interest. Our founder member, Cheryl, is taking picture in another room and maybe will not be able to start with her talking about our remembering that we, ten years ago, exactly ten years ago, we have been here in Dublin, and we had one of those, not the first one, but over there. We are, look at the bridge over there, and we are there, very nice weather, not so many winds, not so many cold, so we were there, and we had this breakfast, sponsored by Amazon, that started to give us some support in that time, and we took that photo with the people from the beginning, some of them not anymore with us, others still with us over there, so it's, but Cheryl will come back after the picture section a model, I believe, and she will come and talk about those times the elapsed time that have passed on that. just in time to start the lecture. I've

been waiting outside for minutes. I believe to show up with applause. Thank you. So, sit, take your time, and the floor will be yours, so we will not change the agenda.

CHERYL LANGDON-ORR Well, hello ladies, and a few gentlemen. Vanda asked me, first of all, my name's Cheryl Langdon-Orr, part of the original founding group. We once sat around, quite literally, a single table and had breakfast, and I think it was seven, perhaps only five of us, so look at it now. And we can say in the last decade since we've been here at Dublin, remembering we formed in 2009, so we are a lot older than this reflection of 10 years. Sorry, I'm still catching my breath. My apologies to the interpreters listening to me huff and puff.

Now, when you look at that photo, it's a goodly number of women, but when we line up for our photo today, just look at where we've come to. But I wanted to just give a couple of moments, thank you so much, a couple of moments of reflection. There's many of those women who have now gone on to hold very senior roles in the world of internet governance, in naming and numbering management. Some of these ladies were literally very fresh, very new, just good tech people who thought, oh, I wonder what I might be able to do in this space. So in the 10 years, the graduates, for the want of a better word, that we've had, and I believe, and I think, Vanda, you'd probably agree with me, it's about confidence and comfort. It's about knowing that you're not alone and that there are a number of women and stories from women that can inspire you, and let's hope you then can

inspire others, to just give some of these things a try. We've also had, and I'm immensely proud, a number of women say, I'd like to do this with a group of like-minded people locally. So we've now, in the last decade, which wasn't the case back then, spawned a number, and Vanda can give you the stats, of local chapters of DNS women. Now, I want to mention that to you because that's something that should you be interested in, whether you're in a small island state or a very large country. It's always possible to do. I know somewhere in this room there's someone who's already said, I've talked to a few people and I would very much like to talk to Vanda and you about starting up a chapter. And I went, not me, that's Vanda's job. So Vanda, you've got at least one in the audience right here today. So to that end, I just want you to take a moment and think of not even with that picture, but from the original six or seven or five or seven of us, we had a few good ideas about networking and confidence building and sharing success stories and discussing opportunities to make females' journey in this part of ICT a successful one. Back to you, Vanda, unless you wanted me to say something else.

VANDA SCARTEZINI No, thank you very much for your words of applause to that. And yes, that is quite important if you are living wherever you live. Certainly there is a lot of women there that need some support and be together and be part of our group and share stories, share experience, even business. We have done some business around, so it's interesting to be part of a worldwide community because what is the opportunity you have sitting back in your home to meet people around the world

that has the same ideas, that share the same intentions of growing and make the Internet more open, more inclusive and much more interesting for the future generation. So we welcome the youngest, of course. Well, we are the party.

CHERYL LANGDON-ORR Oh we are definitely the party.

VANDA SCARTEZINI We are the party. Our time is going and we're still here because we are stuck in that.

CHERYL LANGDON-ORR The word she's looking for is stubborn.

VANDA SCARTEZINI Probably. But anyway, it's something that I appreciate the contact, and I'm this kind of a nerd people that can answer all the emails, can enter into WhatsApp and LinkedIn, whatever, and to keep in touch. So keep in touch with us, and let's make this expanding around the world and give more opportunities in your country, in your region, for other women to grow in this field. Thank you very much. So now we're going to have a very interesting panelist talking with us this time. So what we're going to have is some ideas what we around the world are doing related to the DNS abuse. So we're going to exchange some experience, some ideas, how we can deal with that, because it's a complex situation. So I ask Hadia, Margarita, Samaneh is correct?

Samaneh and myself, because we have an interesting experience in Brazil that maybe can use in other developing countries because it's very easy. So it's something that makes more contribution for the world about the problem we are facing with the DNS abuse. So are you going to start to give the floor to Hadia, our chair of the chapter from Egypt? Thank you. Go ahead.

HADIA ELMINIAWI

Thank you so much, Vanda. But if I may take just a minute to thank you and thank Cheryl, the founders of the DNS Women. And I would just like to note that the reason for which I joined a leadership position in ICANN It's my pleasure to welcome you to ICANN's second meeting with the DNS Women Cocktail Party. It was, I think, my second meeting ever with ICANN, and at the DNS Women Cocktail Party you were speaking about leadership roles at ICANN and encouraging us to apply, and I took the brochures that you had, I went to the website and looked at the leadership positions I applied through the NomCom, and that's how I started. So this is a true story, and so, and let me now start the short, the brief presentation that I have.

So the DNS is the backbone of how the Internet functions. It translates domain names into IP addresses, allowing us to reach websites and services easily. But because of its central and essential role, the DNS is also a frequent target for abuse by malicious actors. So in this session, we will take a closer look at how the DNS is being exploited, drawing on recent reports that identify the most common

forms of DNS abuse, and then finally, we will explore how the At-Large community can play an important role by raising awareness, promoting best practices, and contributing to efforts that make the DNS more secure, trustworthy for everyone. So if I can thank you so much.

So DNS abuse could be explained as malicious or harmful use of domain names or the DNS infrastructure in ways that undermine the security and security stability and trust of the Internet. So malicious use of domain names happen on purpose. When someone intentionally uses domain names or the DNS infrastructure to carry out harmful activities, such as registering a fake banking account or setting up domains that spread viruses or malware, a harmful use of domain names may refer to a legitimate domain that gets hijacked or infected by malware without the owner's knowledge. Or maybe even a domain collision where a private network name unintentionally overlaps with a public domain. And then here the harm is real, but there was no deliberate intent to cause the damage by the person who registered the domain name. So ICANN refers to the following forms of DNS abuse, botnet, malware, pharming, phishing, and spam, when spam serves as a delivery mechanism for any of the aforementioned forms of DNS abuse. If we can have the next slide, please.

So I will quickly go through this. So a botnet is a network of devices that have been compromised and are controlled by a cyber attacker. These networks can be used to launch DDoS attacks or denial-of-service attacks, where the botnet floods a target service with large

volumes of fake traffic, overwhelming it and causing disruption. Botnets are a common tool in DNS abuse and other cyber crime, of course, because they allow attackers to scale attacks across many devices at the same time. If we can have the next slide, please. Phishing. And this tricks users into clicking malicious links or visiting fake websites that impersonate real services. So attackers often use deceptively named domains or compromised sites, making it a form of DNS-related abuse when the domain itself is malicious or hijacked. So a quick tip here. Users need to check their URLs carefully. They need to enable email filtering, multi-factor authentication, verify requests before clicking. And we'll talk about, At-Large, a role in that regard. If we can have the next slide. Malware. So malware, you don't really need to click or accept or download anything. Just opening a compromised website could allow code to be installed on your device, run in the background, and your device is compromised. So what do we do in that regard? So it's very important to make sure that our browsers, apps, operating systems, all of these are up to date. And again, At-Large, and the At-Large community could have a role in this as well. If we could have the next slide, please. So parming. It's a form of DNS abuse that directs users to another website, just like phishing. But the difference here that the abuse is happening at the DNS level. And for that, we have DNSSEC, for example. Implementing DNSSEC could protect from that form of abuse. If we can have the next slide. It's about spam. So those are bulk emails, recipient has not granted permission for the message to be sent, and messages were

sent as part of a larger collection of messages. If we can have the next slide, please.

So on the left, we have a graph from the Interpol Global 2020 report, which shows phishing among the most common forms of cyber attack. The Interpol Global Financial Fraud Assessment 2024 as well finds phishing a major source of cyber crime, identifying it among the most common methods used to facilitate financial and identity fraud worldwide. If we can have the next slide, please. The Interpol Africa Cyber Threat Assessment Report of 2025 highlights most frequent reported cyber threats across African Interpol member countries in 2024, based on low enforcement survey data. So the report highlights that phishing continues to be the most frequently reported cyber crime among Interpol member countries. If we can have the next slide, please.

So what can At-Large do? The At-Large community can play a key role in combating DNS abuse through awareness campaigns, technical mentorship, regional cooperation, and research. Yesterday, during the AFRALO-AfrICANN Statement discussion, we agreed on creating a think tank group to work on various topics. The At-Large community, along with ICANN Global Stakeholder Engagement Teams, can help educate users, promote best practices, and use surveys and feedback to ensure that awareness and capacity-building strategies are relevant, user-focused, and effective. If we can have the next slide, and that's the last one. This one is about AFRALO and the outreach engagement and engagement plan. So AFRALO continues to work on a strategy which all WALOs have similar engagement plans. So

AFRALO continues to work on a strategy to build an informed and resilient user community against DNS abuse. Key outcomes include promoting and developing technical skills, such as promoting the implementation of DNSSEC and mentorship programs via the capacity-building webinars team. Running relevant campaigns to educate users about forms of DNS abuse, such as phishing, and how users can protect themselves through checking URLs carefully, enabling email filtering, multi-factor authentication, and verifying requests before clicking, as well as updating their browsers, apps, and operating systems to protect themselves against malware. Also collaborating with Africa Global Stakeholder Engagement to increase DNSSEC adoption is essential. Collaboration and regional cooperation is as well very important. AFRALO members can share their success stories either through dedicated webinars or via AFRALO newsletters and monthly calls. Leveraging the think tank idea, which we discussed yesterday, AFRALO has many previous statements on DNS abuse. And if we can only start by reviewing those statements, looking back at them, and looking back at them, it could be a good start. With that, I thank you and turn the floor to Vanda.

VANDA SCARTEZINI Thank you, Hadia. That's an interesting experience. I believe the RALOs need to go further and have more, in my opinion, interaction among all those. Because those malwares or phishing or whatever is the abuse, it's not coming normally from your own country. It's mostly circulating in other countries to make it more difficult. So we need to start a agreement among the Brawlers to help ourselves to

deal with that more effectively. Let's find out what they do. Thank you. Let's put the next one. What is it? Margarita, the floor is yours.

MARGARITA VALDES

Thank you very much. Thank you, Vanda. Thanks for inviting me. My name is Margarita Valdes. I'm from the .cl registry, which is the entity in charge of the TLD in Chile. We belong to the University of Chile, which is the main public university of the country. So thanks, Javier, to explain very technical matters, because I will skip the next slide. And, well, the DNS we had at the very beginning numbers. And after that, we need to remind the sites. And the DNS and domain names were built. And, John Postel, thanks for to build this system. Basically, the DNS, it's how we normally set something like it's a tree, but inverted. You have the roots at the top. And all these branches, which is the domain name system, divided by generic top-level domains and ccTLD domains, top-level domains. And you will find the difference just because the CCs are two-letter codes. And the other part is three or more-letter codes. Next, please. And, well, I said basically the main actors of the DNS are gTLDs and ccTLDs. Next, please. The technical abuse, well, Hadia explained it better than me. And normally, that's the way that our use domain names or the DNS in order to abuse or make scams or all the things that are the bad behavior in terms of using the Internet for frauds. Next, please. In the case of Chile, because this is the experience that I will share, before 2020, we have regulations to allow validation registration data according to Article 17 in our registration terms of service. We call it reglamentación in Spanish. And the mitigation times were

excessively long, limiting the effective response capability. In 2020, we made a regularity change, and regulations were modified to incorporate a new Article 6D, introducing the condition of deactivation in cases of technical DNS abuse as preventive measure. In the practical world, we have currently the opportunity to suspend a deactivation is not delete the domain name, it's just to put it on hold as a service, and we could analyze in a very short period of time what is the activity that is related to the domain name, and this is the way that we could help in order to avoid the misuse of the domain names. The current protocol, we can now suspend the domain operation when it's verified that we're registered specifically for phishing malware or bot sets, and this is significantly improving our response systems. Next, please.

Basically, you can see in this slide how is the flux of our work. We are available to receive any reports in this email box, abuse at nic.cl, and after that we have a technical analysis that is detailing the case evaluation of the use of this suspect domain name, and we can classify if it's compromised or malicious, because sometimes the report, it's about a site that is compromised in terms of it's not a domain name that was registered to be used in abuse way. Sometimes it's a problem of security in the website or the server that the registrant have in their systems, not the domain name itself. So we have this difference between compromised and malicious, and after that we can take an action that notification or deactivation in the case of we have the strong opinion that is an abusive domain name registration. In the first case, compromised site is hacked.

When the legitimate domain has been breached, the owner is immediately notified to resolve the security issue in their infrastructure, or in the second case, malicious registration is an abuse case. It is determined that the domain was created with malicious intent. It is immediately deactivated according to the established protocol. And the suspension criteria, as I said in our new article 6D, the evaluation considers whether the domain was created in a specific type of abuse registration, date and time associated similar domains, contact information, behavioral patterns, and deactivation requires a unanimous response from the evaluation committee that we have in Chile, composed of about 11 cybersecurity experts inside the registry.

In this graphic, you can see the total of the reports that we have, and how much were real DNS abuse cases, and we have these two other numbers, and when we use, as we call it, article 17, which is something that we can do before the deactivation in terms of ask to the registrant that they could give solid information that they are real registrant and serious registrant, and they have a term of five days that they have to reply this email and say I am XX, and this is my address, and so on, and I'm a personal or a legal entity, and we could have this information and put out of the abuse system. Or, in the case of article 6, we have these 92 cases that were deactivated by the abuse process.

Our future plans basically try to have an incremental automation of this process, and try to use artificial intelligence that helps us to be more proactively and fast, because the speed is critical in cases of

abuse, to have a ticketing system, centralized management for the tool, in terms of tracking the reported cases, improving incident traceability and documentation. We are planning to have a control panel, a specialized dashboard for real-time monitoring DNS abuse activities, and continuous renewal, a permanent update of the action protocol base of new threats, international best practices, and operational feedback.

And we are very committed to the digital security, so we are very aware that we are a key actor at the Chilean digital ecosystem, and we normally maintain a very close relationship with other entities involved in security in Chile, and try to help to mitigate the DNS abuse. And our mission is to ensure that .cl namespace is a secure and reliable environment to users, businesses and institutions operating in the Chilean ecosystem. And basically, a key insight, an anonymous evaluation protocol by 11 experts ensures that each deactivation on decision is technically sound and fair, balancing security with the rights of legitimate domain holders. Next please. And we have these channels, this presentation is with the help of my colleague Guillermo Lama, who is our CISO, and the channel that we have is our email abuse at nix.cl, and you can see also our emails, personal emails, and mvaldes at nic.cl, and glama at nic.cl. Thank you very much.

VANDA SCARTEZINI Thank you. We always know that the CC has more capacity to deal with the systems, and because of that, they can, if they want to, but to make something more efficient for the community they serve.

MARGARITA VALDES Actually I could add something very important. At the ccNSO we have a DASC, which is the DNS Abuse Standing Committee, with our colleagues at the ccNSO we are very keen to help in order to avoid the DNS abuse.

VANDA SCARTEZINI Before I give the floor to Samaneh, Maarten wants to make a question.

MAARTEN BOTTERMAN Thanks Margarita. Thank you for the presentation, and thank you for doing that. The curve proves that at least something has been achieved. My question to you is, the enormous value of these case studies that these 11 cybersecurity experts do, is there a plan or the intent, or is it possible for you to put that together and have a good practice document resulting from that? Because these insights would be immensely valuable.

MARGARITA VALDES Well, the answer is yes. It's a very interesting way of work that we have in NIC Chile, because we, these panelists or experts, are from mostly the old sections of our organization. So there is engineers,

lawyers, client services, and all the participants in this system of registry systems. So the good thing is that they have different views and different perspectives, not only technical, which is very helpful in order to understand what is the behavior behind these registrations.

VANDA SCARTEZINI Thank you. So, Samaneh, for you, for your presentation, the floor is yours. There is time for one short question? Raul?

RAUL ECHEBERRIA may I?

VANDA SCARTEZINI A pleasure to have you here. I didn't give the floor to you, but it's an opportunity to at least say welcome, and please participate in the future meetings that we're going to have. Thank you for your presence.

RAUL ECHEBERRIA For sure. Thank you very much, Vanda, and for sure I will participate. Congratulations for this initiative. It's really a pleasure to be together with so many inspiring and strong women leaders in this field. Thank you, Margarita, for the—oh, so I didn't introduce myself. I'm Raul Echeverria. I will start my term in the board of ICANN tomorrow. Thank you very much, Margarita, for the presentation. It was very good. And I have one question. The changes that you introduced in the regulation, in the ccTLD regulation, that says that now you can

take actions with domains that were registered with the purpose of doing some malicious activities. What about other domains that were not registered with that purpose but are used for that purpose? You take actions, too? Or is it more complicated?

MARGARITA VALDES: Very good question. Thank you very much, and it's great to have you here, Raul. The answer is, this is a preventive actions that sometimes, it's not always, or not all the ccTLDs have, because you have a very slight limit between the law enforcement entities and the registry. When sometimes we do not have enough evidence to say that this is an abusive registration, normally we could, as a registry, give enough hints to the law enforcement entities and they could investigate if it's malicious or not. We have a limited scope as a registry, but we are always available to help these law enforcement entities to continue the work if there is some smell that perhaps is an abusive registration.

VANDA SCARTEZINI: Thank you. So, let me give the floor to Samaneh, please introduce yourself and go ahead.

SAMANEH TAJALIZADEHKHOOB: Thank you, Vanda. I'm Samaneh Tajalizadehkhoob. I'm the Director of Security, Stability and Resiliency Research within the office of CTO ICANN organization. It's my pleasure to be here, and thank you for inviting me among all women and men of this room. Today, I will walk you through some of the core idea behind our group and an overview

of some of the research we do. So, when we talk about security or insecurity or DNS abuse, in this case, in the DNS space, we talk about domains and DNS infrastructure and components or processes that are not adequately secured. This is basic. I think this is discussed many times in ICANN meetings. This creates opportunities for malicious actors to exploit certain vulnerabilities or engage in various forms of DNS abuse that involves domains or DNS infrastructure. The examples that involve domains are phishing malware, botnet command and control, and spam. For the sake of this presentation, I only included these three categories. But if we look deeper into why these certain misuse of the DNS, at least at the domain level, exists, there is a vast field of study that claims that security failures are at least caused by bad or misaligned incentives as it's caused by bad technical design. So, basically, systems are particularly prone to failure where the person who is guarding them is not the person who suffers if it fails. Having that in mind, that's the core idea behind our research. The question is, how do we align and improve incentives so that we get better security and less DNS abuse or insecurity exploitations? That is what we do. The answer is simple. By having high quality metrics. These metrics could be ... You have seen them all over the place. They are called KPIs, performance metrics, other names, but the core is they are just metrics. Metrics influence decision making by quantifying security performance, allocating resources and impacting priorities. Poorly designed metrics, on the other hand, can create perverse incentives, leading to unintended consequences and short-term focus. In this case, again, we are talking about DNS abuse. This is what my team does. We have data

and we do multiple line of researches on how do we take this data and create robust metrics out of it. Metrics that we can present to the community, metrics that can be used to talk about mitigation, metrics that can be used to talk about how a landscape looks like when it comes to DNS abuse. On this slide, you see some examples of the works that we are doing. Now I will walk you through some of them.

Here is my team. So the office of CTO consists of four teams, research, technical engagement, operations and SSR. I have a team of three scientists who work on the SSR-related issues. Our projects, probably you have heard ICANN Domain Metrica is the most talked project that we have in the ICANN community. Also it's the biggest project that we have because it's a platform, it includes metrics and interactive dashboard and DNS abuse, all kinds of visuals. Everything that is produced from research perspective in our team is going to be a module inside ICANN Domain Metrica. So over time we will add new information to the platform, new modules. This is how we built it. Some example of other projects that we work on. So how we work, basically we create science and then our technical engagement team goes to the community and shares that science and trains different part of science community with the results of our research. Another very useful, at least from our perspective, line of research that we did is basically creating a method on how third party or users of a reputation block list can evaluate whether it's good, whether it's fit for the purpose of the use. We created a peer-reviewed academic publication. We also published an OCTO 37 document where you can

use any niche part of the community you are, if you are using reputation block list for filtering, for whitelisting, for count observing and quantifying DNS abuse, this is your way to go to know which list is the most useful for your use case. At the moment we are, part of my team is working on discovering associated domains. Probably you have heard this topic during this week a lot. This is a topic of the upcoming PDPs also and it's originated from the Infermal report which is a report that our group has been funded and worked with parts of the community. The idea behind this research is basically, and also Margarita talked about this in their registry practices, the idea behind it is to use simple models, so less resource consuming models to identify domains that are malicious and they belong to the same pattern or group of domains. They are different from DGAs, the algorithmic domains that are similar in terms of numbers. These are domains that are similar in terms of patterns that we find in them. We are also working on measuring mitigation time or domain uptime. The idea is that we measure from the amount of time the domain is up from the moment that is seen or registered for malicious activity down to the moment that it's taken down. We published, we also, the research of this work has also submitted and accepted into an IEEE conference and will be published soon. We are building on community work on this topic. There has been work already. This topic is very hard or relatively hard to quantify because as the defenders try to measure or see the domains that are up still for malicious activity, attackers also adopt techniques in order to hide domains or flux them so that you do not, you think they are down but then they are up again at some point. This is also why it's hard to

measure uptime because you also, you need proxies to go from one location to another in order to see even the content of that domain. And we also look into how domains are parked, what are the different categories of parked domains and how the parked domains are actually utilized in distributing DNS abuse. This work is also, the earlier version of this work is published, accepted and published in an IEEE conference and we are working on the follow-up. This is a continuation of the work from the CCTRT recommendation to the ICANN org, which we are doing now. With that, I would like to conclude my presentation. I would like also, since we are in the DNS woman space, I would like to make myself available for women who are interested to do research in these topics or research in general, technology in general, to mentor or answer questions or be of help if I can be useful. Thanks for giving me that stage.

VANDA SCARTEZINI Thank you, Samaneh. Wonderful. I have no deeply idea about this group. I don't know the others. I heard a little bit about that, but not so discussed around the groups normally. I'm here 25 years, but it's something that we passed through, but we don't go deeply on that and the discussions don't take you there. That is very important for us to have your presence here. Thank you very much. My experience is very simple, but we are an association of software companies in Brazil, so we have more than 2,000 companies associated, and there is a large one, but not really involved in the industry of internet industry. But we know that our population in the count suffers a lot with the DNS abuse, so we need to do something. Even the governor

normally, you are technical guys, you need to do something about that, because nobody understands really what we are talking about. And the general population has no idea to talk about DNS abuse. What the hell is DNS abuse? So first, abuse is some word in Portuguese too, but DNS, what the hell is that? So we need to do something. We don't need to explain for the others, but I took some pictures from our website and translated to English, because it's all in Portuguese, and just to make, giving some idea to the population that we are talking about that. So we talk about that, and you need to be alert about what's going on. What do we have decided to do? To create a hub to receive complaints, to analyze those complaints, and address these complaints to our partners around, out of Brazil, inside Brazil, to deal with the mitigation or eliminate that abuse. Because like I said to Margarita, we have no power to do anything. So what we could do to help is just facilitate the operation, and remember that in Brazil we talk all, it's just facilitate the operation, and remember that in Brazil we talk Portuguese. In our neighbors, we talk Spanish. And there is no way people will address anything in English. They cannot do this for a registrar in some other part of the world. So, it was something that we need to do. So, go ahead with this. I'm going to try to read this. I'm going to read this. I'm going to read this. I'm going to read this. I'm going to read this. I'm going to read this. I'm going to read this. I'm going to read this. I'm going to read this. I'm going to read this. I'm going to read this. I'm going to read this. Change this. So, it's another picture. Explain a little bit what is that. Go ahead. So, how we report that. We don't talk about abuse. We say cyber crime. In Portuguese, it's the same. Cyber crime. We alert people that we are

talking about crimes. They need to be alert about that. So, and then we collected under this email, people should, and there is a lot of explanations for people, webinars, and tests to explain how to do things. We ask them to send the very email they receive. It's not to call us and send to us your idea. We need the very email. We need to analyze that. And to address the problem, we need to have this clear, and this is very difficult when you talk to the population around. So, you talk about more technical people, not so difficult, but talk about the population is very hard. You need to really go deeply to make it easy for them to send correctly the information and to allow us to address that. So, if they want to be follow up and to understand what is going on, we can also ask for the names and we can send emails and updates about what we have done. So, our association cooperates with the partners outside the country, registrars and other ccTLDs to help them to go and do the business they are supposed to do as mitigate the problems in their environment. So, this service is open at all, and nowadays it's just in Portuguese, but we are open to Spanish to serve Latin America, and, of course, it's free of charge. So, that's our contribution in some way because our association is also part of a business constituency on that. So, that is the issue I would like to share with you because it can be copied around and help everybody to mitigate those problems that we have. Thank you very much.

CHERYL LANGDON-ORR So, ladies and gentlemen, time is our enemy, as is often the case. I think particularly based on Samaneh's very generous offer to explore

research possibilities in this area. We might also want to accumulate any particular questions you have for any of our panelists today. We will do our best to make sure they receive their questions, and we'll do even better than that to try and make sure they give us any answers. But time is our enemy, and we do have to let the fabulous interpretation team go. Thank you very much. A note of thanks back there to those. The tech team have had a very long day, and they'll just start pulling plugs on us shortly. So, Vandra, if you want to have literally the last word, we also need to gather you, well, at least the girls amongst us, for a photo. So, that better happen pronto because I know all of you have somewhere else to be right now.

[END OF TRANSCRIPTION]