ICANN86 Seville | PF – GAC Discussion on DNS Abuse Mitigation
Wednesday, June 10, 2026 – 11:45 to 13:15 CEST

JULIA CHARVOLEN

Welcome to the ICANN86 GAC DNS Abuse Mitigation Session on Wednesday, 10 June at 11:45 local time. Please note that this session is being recorded and is governed by the ICANN Expected Stands of Behavior, ICANN Community Participant Code of Conduct, and the ICANN Community Anti-Harassment Policy.

Please remember to state your name and the language you will speak in case you will be speaking a language other than English. Speak clearly at a reasonable pace to allow for accurate interpretation, and please make sure to mute all other devices when you are speaking. With that, I will leave the floor over to GAC Chair, Nico Caballero. Nico, over to you.

NICOLAS CABALLERO

Thank you very much, Julia. Welcome back, everyone. I hope you enjoyed your coffee. So, welcome to the DNS abuse mitigation session. We have the topic leads from the GAC, Martina Barbero from the European Commission, Tomo Miyamoto from Japan, and my dear colleague, Susan Chalmers from the United States.

And we also have a fantastic lineup of guest speakers, Diego Alejandro Palomino, Karen Rose, Alan Woods, Graeme Bunton, Steinar Grøtterød, and I hope I'm pronouncing your last name well,

my apologies. Rod Rasmussen, a good friend of mine, Reg Levy, and again, my apologies. Dennis Tan, Vivek Goyal, and Michaela Nakayama. So, without further ado, let me hand over the floor to my distinguished colleague, Tomo, I'm sorry, Miyamoto from Japan. Over to you.

TOMONORI MIYAMOTO: Thank you, sir. Hello, everyone. Welcome to the GAC DNS abuse mitigation session. I'm Tomo Miyamoto from Japan. The next slide, please.

Here's the agenda for this session. I don't read out everything, but we have a lot of items here and thanks to a lot of requests and interest on this session, we have 10 guest speakers. So, the schedule is quite packed. So, please be aware of the time for presentation, question, and any intervention. Susan will be the timekeeper for the session. Next slide, please.

Let me start with a brief introduction. DNA abuse mitigation is our priority and GAC's annual plan includes two expected outcomes. The first is about the policy work, especially PDP and policy development process, and the definition of DNA abuse is in the ICANN remit it's fairly limited. As you know, malware, botnets, phishing, pharming, and spam, and various abuse activities may be out of this scope, and it could be discussed suddenly. But to the reports of DNA abuse under the current contract, gTLD registries and registrars have contracted obligation to respond.

The second expected outcome is about capacity building. Although the abuse under the contract is limited, we observe a lot of problems such as citizen fraud and piracy. And to encourage measures in a broader ecosystem, we covered initiatives of trusted notifiers in the past ICANN meetings in Dublin and Mumbai. Today we will cover the first one about the policy work. Next slide, please. Thank you.

And DNA abuse in a narrow definition is still rampant. In the Prague Communiqué last year, the GAC pointed out the necessity of targeted and narrowly scoped PDPs on DNS abuse, especially bulk registration and associated domains in a timely manner before the delegation of new gTLD of the next round. After some work by GNSO and ICANN staff, final issue report on PDP was published in October. This report illustrated various gaps including transparency of reporting and proactive verification. And the final report prioritized the issue regarding Associated Domain Check, which is called ADC, unfortunately it's a new acronym, and the safeguard for API Access.

And January of this year, GNSO adopted the process and PDP 1 for ADC started in March at the Mumbai meeting. The communities have constructive discussion and Martina and Gabe will cover this topic later, the members from GAC for the PDP working group. And PDP 2 has not started yet. The charter is under construction, as far as I know, but this PDP should also be commenced promptly for

policy implementation in a timely manner before new gTLD delegation in the next round. Next slide, please.

Now, let's move on to the next part, host country presentation. We welcome Mr. Diego Alejandro Palomino. I'm sorry for my bad pronunciation, but from the Spanish National Police. We will learn their efforts and observation on phishing and domain abuse. Welcome and thank you, Diego. The floor is yours.

DIEGO ALEJANDRO PALOMINO Thank you so much. First of all, thank you for inviting me to this event. It's a great opportunity for me, really, but I apologize for my English, so I prefer to make the presentation in Spanish. So, if you need any answer, any question later, I try to answer in English, but for me, I'm [inaudible - 00:05:51] support, but I don't have a miracle. So, I'm going to start my presentation at the start.

Now, I hope I don't want to make the interpreter's life too difficult because I tend to speak quite quickly. Now, I've only got 36 slides for 15 minutes so I think that's okay. So, recently I've been starting at the end. This is actually the last slide that you can see, but really my aim here is with these three images, the formula, Don Quixote, the boat, I mean that's the reason why I'm here is what I'm trying to say. Next slide, please.

So, I am part of the Central Unit for Cybercrime of the Judicial Police of the National Police of Spain, and we investigate crimes which occur on the Internet. Therefore, we, of course, have to deal

with domain names and we have needs during investigations to deal with registrars and all kinds of service providers of internet services. Our unit has three main pillars. So, we have three brigades that are specialized in what they do.

The first one is the technological investigation one, which investigates crimes against people. That's one in the center. So, these are crimes which occur online and especially the protection of minors. The IT security brigade focuses on high-level crimes. So, we're talking about cyber-attacks here, DNS abuse, compromising of login credentials, and last but not least, they have the fraud brigade. Next slide, please.

So, I don't want to go into too many details, but I can talk about the types of crimes that we deal with. So, illicit access to highly technological crimes, IT damage such as leaking data, logging credentials, et cetera. When it comes to social media, it's mostly threats that we're talking about. We have hate crime, crimes against honor. We also have crimes relating to counter suicide measures and we actually have an urgent request system which is done via platforms and that deals with this type of crime.

And also, sexual crimes and especially protection of minors and protecting children from child pornography. And also, we also deal with all kinds of crimes that occur on the internet so large-scale frauds and mass crimes. So, ultimately crimes that happen at a small level, but when we add them all up, the impact is quite

significant, and this really impacts on all members of society. Next slide, please.

This is just a few examples of the recent measures that we have undertaken. We can see blockages and dismantling of platforms that we have done through international cooperation because technological crimes require international collaboration. That is key. I mean, that's why we're here because all countries have to work together and that's the only way that we can combat cybercrime. Next slide, please.

This is the last thing that we did last year. We seized a drug-selling website and that was the largest platform which existed of this type at the time. And in fact, they disappeared, but then they actually reappeared. So, we can see that the actions of the judicial authorities actually impact on prevention and we basically create obstacles for the criminals when it comes to carrying out their actions. Next slide, please.

So, crimes against people. We monitor the Internet so this includes the dark web and also the clear web. And the aim here is to detect illegal activities which occur on the Internet. As I said, we take special care when it comes to announcing crimes that are going to take place, for instance, announcing of suicide, for instance, this is something that we monitor very carefully, especially when it comes to young people. Next slide, please.

When it comes to protecting minors, of course, the distribution of sexual child pornography and this requires international

cooperation. And that means that we have to get our hands on the information as quickly as possible so that we can protect the victims. And of course, afterwards, we have to prevent the criminals from spreading such damaging and horrible information.

Then we have economic crimes, scams, frauds through online marketplaces, which are not real, banking, phishing, all of these crimes fall under the remit of the work that we carry out. Next slide, please. Next as well because I was talking about phishing here as well so this is the continuation of economic crime. So, to conclude, this is madness, ultimately. Next slide please.

I like to draw a distinction between what cybercrime and cyber security is because ultimately cyber security relates to defense. And that means that private sector companies have to be more involved here because we're talking about protecting data of possible victims. When it comes to cybercrime, we're talking about the actual attacks themselves. So, attacking the security of a system that is used by a system. So, we have confidentiality, authentication and no repudiation.

So, we have this triangle here and in Spain we have a figure called the Cid. He was a great Spanish conqueror and we have used this image for domestic purposes to kind of help us remember what we're talking about when we're talking about cyber security. So, when it comes to cybercrime, we understand this as the use or the committing of crime using IT technologies. So, this can be the means that is used to achieve something. Next slide, please.

In the Europol definition, cybercrime is defined as an interaction between the perpetrator and the victim, which occurs via IT platforms, whatever that is covered by a legal framework. Next slide, please. In Spain, the public prosecutor carries out an investigation, and the public prosecutor, of course, is in charge of investigating crimes at the judicial level, and we work alongside them to build our cases.

So, when it comes to cybercrime, the main aim of the perpetrators tends to be the IT system. So, that means they're using these IT systems as a key part of the process and that also is cybercrime. And when it comes to investigating these crimes, we see techniques that are used with these IT systems. So, what is the starting point here? Nationality, where the crime takes place, so cyberspace and there's no government or borders in cyberspace. And of course, the aspect of perpetrators being anonymous online, I mean, that really makes things a bit more difficult for the investigators.

What is the reality that we're dealing with? Well, we have this report on cybercrime in Spain. 84% of crimes that are committed online in Spain are actually fraud. So, that is a statistic reading of this situation, but we have to understand statistics and what they mean because I always give an example when I talk about this. When a criminal creates a domain name or a website for e-commerce, where they sell, for instance, say fake products or Black

Friday, statistically, that relates to about 200 or 300 reports of a crime.

However, if an individual accesses a database illicitly, that's just one report. So, what is more serious there? Where is greater damage produced? So, it's very important to keep this in mind when we look at the statistics, but we have to be able to properly analyze those statistics. Next slide, please.

Most crimes are based on simple techniques and that's social engineering. So, they're basically obtaining information illicitly from legitimate actors and the user is the weakest link here. Now, as police officers, we can identify someone in the streets and we'll ask them to identify themselves and they can say no, but online, users are happy to share all of their data. So, they often find themselves in situations in which a crime is able to be committed. Next slide, please.

Now, when it comes to this aspect of social engineering, could you tell me which one of these images is real? Which one of these photos is real? Can we put the video on, please? So, imagine that you're a part of the generation, the first generation that is unable to differentiate real from not real because this isn't actually a real recording of me. You might not see me being as animated as I tend to be. Or you might see some small mistakes that might give this away, but really, what you're seeing right now is just a reconstruction that has been created with artificial intelligence of me. It's an avatar.

Now, we can include, for instance, an audio track, and you can see how I'm actually gesticulating. So, with this information we can create a video of me talking for 10 minutes. And this is crazy because when we talk about the future, very soon, anybody will be able to create these realistic videos, YouTubers, influencers, et cetera. We won't even need to turn on the camera to actually make a video, but don't worry that doesn't mean that it's the end of human creativity.

Now, content will probably be more attractive and realistic, but the creativity of people will still be key. And this actual sentence I just said wasn't written by myself actually. It was written by this AI tool. So, you can see the possible implication of what I'm talking about. Now, like all technological progress, there are significant issues that we need to take into account. Now, of course, much like many of you, I also see the possibility for malicious actors to take advantage of this situation, and we're going to have to try to do our best to combat this because fake news and other issues seem more real than ever.

Now, the aim of this video is to show you that this technology exists and it's not science fiction. It's here already and that means that your work is to help us share this information, get the word out so that we can actually combat this situation. So, this situation, or this video rather, was actually created in 2017. Imagine how things have changed since then.

So, there are four points which mean that we will be successful. We all want to help. We all have a tendency to trust. We don't like to say no and we all like to be to be complimented. So, all of this, is this a threat or an opportunity? We have tools such as INTERPOL, Europol, Eurojust, Ameripol, and so on. The problem is that there are technical limitations, time limits, et cetera. Next slide, please.

We have the Budapest Convention. Now, we are the 24/7 contact point to receive all information on the exchange of digital information. The second protocol has been signed and that will allow us to put in place enhanced cooperation measures, so automatic recognition in all of the countries for the judicial authorities when it comes to receiving those requests. The 18th of August is when it enters into validity.

Now, Tycoon was actually a phishing platform and, on this platform, criminals were able to skip over double-factor authentication. And last March, Europol, with whom we cooperate, was actually able to bring this down. All of the information that we received, over 10,000 domain names, well, we got in contact with INCIBE, which is an organization which works with the private sector, so they could carry out analysis. And it turned out there were 300 active domains, but there are also another 150 associated domains. We were able to suspend 20 domains that we had flagged as domains that were committing fraud. So, what are the conclusions here? Cross-border and cross-cutting measures are what are required. Next slide, please.

So, I just want to reiterate once again that cyberspace is where the crime takes place. Next slide, please. The fact that criminals are anonymous and that crime is dealt with as a service is obviously an issue and then we're back to this idea of it being madness. Now, we're back to where we started or we're at the end. Next, please.

What we need is comprehension, generosity, and mutual support. Now, we can't see the boat, but the reference to Don Quixote here is, I don't know if you've read Cervantes, but we all believe that there are giants and that there are problems that only impact us. But we have to realize that we're actually all in a boat going towards a storm and if we don't all act together to change the direction, then we are all doomed.

So, we talked about this formula as well. What are we worth? Our capacities and skills add up, but what's really important is our attitude because that is what multiplies. If we have zero attitude, then we're not worth anything. Next slide, please. Thank you very much. I apologize for going on at length. I just want to say that the National Police is one of the police organizations with the largest number of followers in the world. And thank you very much, and I apologize for going on at length there.

NICOLAS CABALLERO Sorry, it's okay. Thank you so much, Diego Alejandro. We won't have time to take questions at this point, but rest assured that at the end of the session we'll make sure to allocate five or 10 minutes for a Q&A mini-session. So, without further ado, let me hand over

the floor at this point to Karen Rose from the Interisle Consulting Group. Over to you.

KAREN ROSE

Thank you, Mr. Chairman, and good morning, everyone. I'm Karen Rose with Interisle, and I'm pleased to have the opportunity to share with you some findings from our most recent study. Our work examined malicious domain name registrations made in 2025 in the gTLDs and I'll focus on just two questions our research looked at. Number one, how much cybercriminal demand drove new registrations last year, and number two, whether incentives in the market allow that demand to persist.

We used publicly and commercially available data for our research, including blocklists and ICANN registration data. And you can find our full methodology in our report. Overall, our findings were quite sobering. We found that bad actors likely purchased 16.8 million gTLD domain names last year. That's about 20% of all new registrations sold. Put another way, as many as one out of every five domain names were purchased by bad actors to perpetrate phishing, malware, scams, and other harmful attacks.

Imagine another industry where one out of every five products sold was being used to facilitate fraud, theft, or other serious crimes. I think few governments would consider that ordinary misuse and I think many policymakers would ask whether the rules, safeguards, and accountability mechanisms in that market were adequate to the scale of the problem, and if those measures were sufficiently

protecting the public interest. I think those same questions are relevant to DNS abuse policy discussions for the whole ICANN community.

Our study also found that abuse is highly concentrated among certain providers. We found numerous registries and registrars where over half of all of their registrations appeared to be purchased by bad actors. At one registrar, 88% of its registrations, nearly all of its sales, were identified by blocklists as malicious. In one TLD we examined, nearly all of its registrations, some 100,000, were associated with Funnel, a cyber-criminal gang that powered scam farms across Southeast Asia.

So, why does abuse exist at this scale? It's about economics and incentives. Cybercriminals create sustained demand for domain names. They're high-volume, repeat buyers, and they buy millions of domains each year. Fierce competition in the GTL market has driven prices and profit margins down. Sales volume matters. Registrars provide tools that facilitate easy bulk registrations.

Satisfying this demand from cyber criminals appears to be commercially attractive to some registries and registrars. And even when malicious registrations generate little revenue, tolerating abuse can still be commercially rational, especially when there are no clear obligations to prevent it. While cyber criminals and some in the market may benefit from these transactions, the cost of cybercrime facilitated by domain name abuse falls on victims, businesses, governments, and society at large. In economic terms,

this is a classic negative externality, and we need to be frank. It's a form of market failure that undermines the very benefits of competition.

Taken together, our findings make it hard to treat current levels of abuse as acceptable or consistent with the public interest. To be sure, however, our study also shows that abuse is not inevitable. Some providers manage to grow without attracting outside levels of abuse, and our case studies show that associated domain names checks can be a helpful mitigation step, but we need effective steps beyond mitigation. Steps that focus more seriously on abuse prevention and reducing the ability of bad actors to acquire domains in the first place. This is urgent as ICANN prepares for the next round of gTLDs.

The new introduction of gTLDs will intensify competition. It will perpetuate current distortions in the market and risk shifting greater costs and harms onto the public. Measurably reducing DNS abuse needs to be our goal, and we look forward to engaging with the GAC and this community in discussions going forward. Thank you.

NICOLAS CABALLERO Thank you very much, Karen. At this point, let me hand over the floor to Martina Barbero from the European Commission. Over to you, Martina.

MARTINA BARBERO

Thank you very much, Nico. And if we can go back indeed to the GAC slides, and we go on -- Hey, here we go. So, in these next 10 minutes or so, we will discuss about the current PDP. I will not repeat the history of how we got to start a policy development process on Associated Domain Check because my colleague, Tomo, already did trace back that history. What I want to focus on in the next minute is how the GAC is participating in this PDP and how can you join the discussion and the GAC preparation if you wish so.

So, when the PDP was launched, the GAC prepared itself by establishing a small group on DNS abuse and this is an antechamber that allows us to prepare for then the participation in the PDP. We have 17 GAC and PSWG participants from 12 GAC delegations. And this is a rolling call for volunteers, if you, and especially the newcomers in this room, which I know are many, if DNS abuse is a topic of importance for your government and you want to join this small group, please let us know and we will be happy to catch you up on where we stand and include you in the discussions.

So, what we do is we meet weekly to prepare the PDP discussion themselves. And as a matter of fact, myself and Gabriel Andrews are the GAC members in this PDP, and we have also Emanuele from Europol, who is a participant. We need to update this slide, and we will be looking for an alternate soon. If we go to the next slide.

So, let me focus the next five minutes on the progresses that we're making in this PDP, and then maybe we can have a five to 10 minutes discussion if you have questions. But as you know, every PDP has a charter and our objective with the PDP is to address the questions included in this charter. So, what you see on these slides is a very, very basic and very summarized version of what the questions are about and how we are going about to address them.

For instance, the first question that we're asked to address is, what is the trigger for conducting Associated Domain Check? And the PDP is working on a trigger that is based on actionable evidence of abuse, of DNS abuse, which is consistent with the current contractual obligations and gives a very strong start and a strong signal for a registrar on when the ADC needs to be conducted.

We're also working on criteria to define associated domains, so how do you decide whether two domains are associated or not? And here we are looking at which kind of information can our registrars have available that can allow the registrar to associate domains. So, this can be linked to the account or can be technical indicators or behavioral indicators and a registrar will be free to see what association makes sense. We're also looking at what a reasonable investigation means and we're trying to also be consistent there with the practices in the contract amendments and what compliance has arguably established as the minimum required to meet the obligation on DNS abuse.

But we are also looking, of course, at safeguards and remedies, of course. This is also important because there could be cases in which things go wrong, but we're quite confident that existing practices and procedures and as well as existing laws, especially on privacy and data protection, constitute a sound ground.

And then important point as well, the question of timeline of conducting Associated Domain Checks, here we learn from registrars that some registrars they do the ADC immediately when they receive the trigger before mitigating the initial abusive domain. Others they do the full investigation and then they mitigate altogether. For the moment, we are discussing the use of term prompt for the timeline which is again consistent with the contract amendments and the existing practices.

So, in a nutshell, this does not cover the extent of our PDP discussions, but my message to you today is twofold. Please join us if you want to discuss DNS abuse in a small group, if you have opinions. If what we are doing is not enough or is too much, please join us and let us know. And secondly, I think we're having very productive discussions in the PDP. I think that the GAC position has been very much grounded into the reality and we've been very pragmatic in trying to meet the expectations of the community in terms of not overreaching, but also achieving the results that we expect with this PDP.

And it is the GAC opinion that this PDP can achieve great results because as we heard DNS abuse is still a very big problem, a priority

for the GAC. And extending the tools that ICANN compliance has to ensure that the registrars have the highest standards possible in addressing DNS abuse, it's something that will produce results. We're confident of that. So, I think I have 10 minutes and I think I wanted to do this rapidly to check if my GAC colleagues had questions or comments or feedback or thoughts. So, I'll stop here and back to you, Nico.

NICOLAS CABALLERO Thank you very much, European Commission. Very quick and narrowly scoped questions at this point. I see no hands in the room and I see no hands online. So, over to you, Susan.

SUSAN CHALMERS Great, thank you. So, that concludes the first part of our session. This is the second half of, thank you, Tomo, GAC's DNS abuse session and it is divided into two parts. In part one, we will address the PDP. In part two, we will hear a presentation from Graeme Bunton at NetBeacon, a not-for-profit organization that does two very positive and helpful things to address DNS abuse.

One, NetBeacon receives DNS abuse reports and routes them to registries, registrars, and web hosts. And two, measures DNS abuse on the internet. We will also hear from Michaela Nakayama Shapiro from Article 19, which is a human rights organization that works on two interlocking freedoms, the freedom to speak and the freedom to know.

Before we get to the PDP discussion, part one, GAC colleagues, please recall that the purpose of the Associated Domain Check PDP that is currently underway is to develop a framework requiring registrars to proactively pivot to investigate domains linked to malicious actors particularly in cases of high-volume domain registrations used for DNS abuse campaigns. So, in part one, we are asking participants in that PDP who are here today, one, to address one, two, or three questions, and those questions are on the screen. So, I'll just quickly read them since we may be ahead of time.

Question one, based on the current state of the discussions in the PDP, can you highlight areas of agreement and areas of disagreement from your SO or AC's perspective? For example, do you align with the spirit of the initial strawman answers to the charter questions already discussed? If yes or no, please explain why. Question two, what aspects of the PDP discussion seem to be mature enough from your perspective and could lead to an agreement relatively soon? And the last question, what is the main challenge that remains to be solved according to your supporting organization or advisory committee?

So, let me just say very quickly that the United States strongly supports the ICANN community's concerted efforts to more effectively address the problem of DNS abuse. Thank you for joining us today, everyone, and we appreciate your time, which for this part is limited to four minutes per speaker. So, I apologize in

advance, but I will hold up this page when you have one minute left in your intervention. Let's begin with Alan Woods from CleanDNS.

ALAN WOODS

Thank you very much. So, yes, as I'm not actually speaking, I suppose, as an SO or an AC, I'm going to kind of maybe do a little bit of an operational point of view from us. So, we do, do a lot of anti-abuse work on behalf of contracted parties. So, my task, I wanted to kind of think about three main questions and I will slow down, apologies, the Irish in me comes out very easily.

So, the first three of the questions I want us to think about as we listen to my colleagues as they talk about this will be, first, what does reasonably trigger that ADC? The second would be, what would that ADC then comprise? And then, how would that impact the registrant at the end of the day? So, these are not academic questions, these are things that are billions of people who will be impacted by this therefore, we need to take this exceptionally seriously, as there will be consequences.

So, operationally, I think we need to start with a very core concept, and that is an ADC is not a takedown of a domain. An ADC is a tool that is used in investigation. Once that investigation perhaps shows that there is a linked domain or domains that are linked to an evidenced case of abuse, as was talked previously by Martina, then it goes into a normal anti-abuse investigation process. That is where maybe at the end of that, based on evidence being found, that there will be a potential takedown. So, that's an important

thing. The ADC does not take it down. It is a tool that is to be used in order to aid the takedown.

I suppose I would like to think, as we listen as well to our colleagues, I would ask there be two demands in your brain as you're thinking about this. The first thing is, I would ask you to demand reliability in the data that you're hearing. It is absolutely vital that we are getting correct data. It must begin with evidenced cases of abuse. It cannot be on inference. It cannot be on reports of abuse only.

So, to confirm to people, a report of abuse, and there are millions of reports of abuse every day, a report of abuse does not mean that that abuse is occurring. If you're just measuring the reports of abuse coming in and you are not validating that that report is occurring or there is a reasonableness in stating that that is happening, that is merely an allegation of abuse. That is noise, it is not signal. And on the operational side, that is what the job that companies like CleanDNS do. We take all that noise and we try and find that signal.

So, when an action is taken, at the end of the day, that action is based on evidence, and it is not going to unnecessarily impact a registrant, and also the contracted party or the hosting company, if you're going beyond, that is taking that action. And I think that needs to be core. So, if we're going to be using statistics, we need to cite, and we need to make sure that those statistics are reliable, and we are all professionals in this room with billions of people

being impacted by this. And I think we need to be very clear on those methodologies that we are looking for evidenced cases of abuse, not just mere inference and reports of abuse. I want you to think of that as you're listening to the other speakers today.

The second thing, and I will wrap up on this, is talk about operational experience. You need to know how this affects individual people, how it is achieved on the pointy end of the stick at the registries, at the registrars. So, we are very lucky in the multi-stakeholder model that there are people who do this day in and day out and I would ask you to think of them. So, I'll wrap up by saying ask the questions as you're thinking, is the data reliable? Is the operational experience present? And therefore, at the end of the day the framework for an ADC will be operational, effective, and not punitive unnecessarily. Thank you.

SUSAN CHALMERS: Thank you. Thank you, Alan, for setting the table here. Now, let's proceed to our participant from the ALAC, Steinar Grøtterød

STEINAR GRØTTERØD: Thank you. This is Steinar Grøtterød from ALAC. I am one of the two members of this working group. Answering very simply your first question, we definitely are in line with the spirit of this work done. At-Large should be the voice of the end user, the users of the internet services whatsoever. So, with that aspect, we're trying to see what we debate and discuss during the working group, not only

as the registry, registrar, registrant factors, but also the end user stuff.

The way we do this is that we have something called the Consolidated Policy Working Group, which is the policy forum for the At-Large. And the working group members, we bring weekly, but every time there has been a meeting in the DNS abuse ACD working group, we bring reports back to that one. And for those cases where we need, let me see, input, consensus and so on, we're trying to get tools to identify so we have something to report back.

And I'm very pleased to say that so far in the process we have not seen anything that is in the category cannot live with. For those who have read the report so far, there is a category cannot live with meaning that you definitely need to have something there. We have comments into the can live with stuff and that will come up and we will tune that, but we are monitoring the process very, very well.

I think maybe that's covered the bullet point number two. What is the challenge that remains to be solved, and it's not necessarily been solved in this PDP, but we need to have some sort of requirement, no, not requirement, but, sorry, policies that will assist an end user when, as an example, you are evicting of a false positive decision and we don't have that today. So, thank you very much.

SUSAN CHALMERS Thank you kindly. Now, let's turn to SSAC. Please, Rod Rasmussen.

ROD RASMUSSEN Thank you. I'm Rod Rasmussen, one of the voting members of the PDP representing the SSAC. This PDP is addressing one of the areas that was identified earlier as potentially one of the most effective at dealing with the large scale of abuse that we've seen. So, we're very encouraged just the fact that we're doing this.

In general, this PDP has been going along, from my experience, extremely well. It's being run efficiently and things are staying on schedule. Differences of opinion are being worked out rather quickly, and I think there's been a very good spirit of camaraderie and willingness to work through differences of opinion. So, that has all been very positive signs, and that kind of gets to the second question there. I think, with some luck, we're maybe, you know, on schedule or even better for doing this. We'll see, knock on wood. And that gets to the policy side, because that's what we've been concentrating on.

I think the challenges that we're going to see are in implementation advice because that's where a lot of the real interesting stuff ends up happening, in particular areas around how do you do this and how do you track it, how do you report it, how do you measure it? On the first part, how do you do it? There are already suggestions in there.

The SSAC itself, we have a work party that is supporting the team that's on the PDP, and we have been working on a fairly extensive document looking at various ways of pivoting their pluses and minuses and when they might be applicable that we hope to share very soon. It's not done yet, and the SSAC processes make it a little challenging for us to be very quick on some of these things, but we hope to get that out and share it.

Measurement is something else we're keen on, trying to figure out, how do you look at this from the outside? What kind of data you need to be able to understand whether the policy is effective or not. So, those are areas we're working on and we look to contribute to our technical expertise from the SSAC to bring to the work. And as, again, I say, the challenge, I think, is going to be getting good implementation advice so that at the end of the day, both with a good effective policy and effective enforcement, we can actually see a good impact from taking on this policy. Thanks.

NICOLAS CABALLERO: Given the time that we're kind of okay in terms of timing, let me just mention an important thing at this point. Today's Rod's birthday, so let's give him a big round of applause. Happy birthday. Over to you, Susan.

SUSAN CHALMERS: Thank you. Thank you, Chair. Now, let's turn to Reg Levy from the Registrar's Stakeholder Group. Reg.

REG LEVY

Thank you. Reg Levy from the Registrar Stakeholder Group in Tucows. And I want to echo what Rod just said, that throughout this process, the registrars have taken the perspective that this PDP is going so well. We are using the term cautiously optimistic throughout. The straw proposals that have been put forward are reasonable and are data-based, which is exactly what we're looking for.

The challenge for us as well is measurement because as Alan indicated, a review, an ADC check is not necessarily always going to result in suspensions. That doesn't mean it wasn't done. So, trying to figure out how we're going to identify whether or not this PDP was successful in terms of reducing DNS abuse is a bit of a challenge for all of us.

That said, we continue to be heartened by the straw proposals being submitted and by the summaries of our conversations that are getting presented both in public and to the PDP group itself. And we have hope for the future.

SUSAN CHALMERS

Thank you, Reg. Now, let's turn to hear from the Registry Stakeholder Group. Dennis Tan, please.

DENNIS TAN

Thank you, Susan. This is Dennis Tan for the registries, also with VERISIGN. So, I want to echo all the points on the making progress.

We are doing the work in a good pace and finding the compromises. On a substantive level, I will say that we are pleased that the policy recommendations that we are coming up with or the preliminary policy recommendations that we are working on are grounded on the current DNS abuse framework and the contractual amendments. So that we are building on, evolving it, not trying to do a revolution here.

And so, that's a good thing because as we see these policy recommendations, at the outset, we always said that the DNS abuse amendment was going to be the first step into a much more continued work on bringing solutions to the community and having the community part of it. So, in that regard, we're pleased to see that, again, policy recommendations are building upon the contractual framework.

On challenges, I think echoing what Rod said, in terms of coming out with a good quality final report with implementable policy recommendations and then how that is going to be implemented, yes, challenge ahead, but I think we're going to continue our support through the implementation review team and beyond. And I think short and sweet. Back to you, Susan. Thank you.

SUSAN CHALMERS: Thank you, Dennis. Now, let's turn to the Commercial Stakeholder Group and Vivek Goyal, please.

VIVEK GOYAL

Thank you, Susan. Vivek Goyal for the record. Echoing some of the things other members have said, we are very happy and content with the way things are progressing. The CSG were initially discussing that there should be some timelines implemented on how long it does take, in what time period should an ADC start and in what time period should an ADC conclude, but based on discussions, we agree promptly works best. And the stock proposals out there are quite encouraging and we look forward to working with members of the community to get this thing through the door and out into implementation.

A few aspects of this PDP that we would like to highlight are, in the PDP and the way we work can implement regulations that the contracted party members have to follow. But in this ADC check, ICANN compliance has to play the biggest role. If you report a normal abuse, as long as the abuse is up, you can complain to ICANN compliance and then see whether action was taken or not. But in case of an ADC, once I submit a complaint to a registrar, I do not know what happens.

There is no obligation for them to report back to us to say, "Yes, we conducted an ADC and we took down five more domains." That information I will never come to know. The only team that will ever come to know that information other than the registrar, registry is ICANN compliance. So, to measure whether the ADC which will be put into contract is being followed thoroughly is for ICANN compliance to do proactive checks.

So, while we are discussing the ADC and bringing it to a closure, I would encourage ICANN org to also look at ICANN compliance and booster them so that they have the capability to do these proactive checks. And check every registrar and do it frequently so that they can very confidently say, "Yes, this has been implemented and it is working."

Another thing that we foresee in the future is, as AI is making our lives easier, it's making our life more difficult. Today if number of threat actors are using some registrars to register large number of domains, using AI it will be very easy for them to register those domains over say 100 registrars, 200 registrars. In that case, while ADC will give us benefits initially, in the long run, we might see diminishing of its impact on DNS abuse.

So, moving ADC checks from one registrar to enabling registrar to share this data and do checks across registrars will become important to continue to see the impact of ADCs. So, we hope that as we are working very hard to get this policy through the door and implemented, the ICANN compliance is coming up with automation or coming up with more ways so that they can proactively check whether registrars are following this policy or not. And are doing it effectively within the promptly time that we believe they should be doing this. And what next? How can we make sure that this policy works across registrars and continues to give the benefits in fighting DNS abuse for which we are all working so hard here? Thank you so much.

SUSAN CHALMERS Thank you for your intervention, and now we will turn to the Non-Commercial Stakeholder Group and we will hear from Michaela. Michaela, please, the floor is yours.

MICHAELA SHAPIRO Thank you, Susan. Thank you for having me. Michaela, Non-Commercial Stakeholder Group. I prepared some very, very short slides. I don't know if it's possible to get that up there. Fantastic. So, we can just skip ahead to the next slide already.

So, I have the pleasure of going last, which means I get to say, it's so great to be in agreement with so many of the folks who have already spoken before me. So, the Non-Commercial Stakeholder Group is also cautiously optimistic. We were a little nervous about the tight timeline, but I think, as others have said, having the kind of basis of the interventions here be so strongly tied to the realities of domain operators' operations and to be tied to the business realities that we're seeing has been really positive.

And so, I don't want to rehash what we've already discussed, but I want to draw attention to two key areas. So, one being what the scope of a reasonable investigation will look like and as others have mentioned, let's already look ahead about topics that we want to see coming next. So, next slide, please.

So, here, the Non-Commercial Stakeholder Group's position, and this echoes a bit of what others have said, like Alan and Reg, when

it comes to the investigation, conducting an ADC should not necessarily presume an outcome. And sometimes the outcome might be that we've already taken care of it already, and that's great and brilliant. And we might not know until the ADC is done, but again, we don't want to go in with the presumption what the outcome will be.

And so, for that reason, we recommend calibrating to the severity of the reported abuse, perhaps the portfolio size or registrar business model. These are just a few ideas, others have been tossed around and also want to acknowledge I am not a domain operator, so operators will know best what that could look like, but I just wanted to throw that out there. Next slide, please.

And here, this is not to say we want every single one of these changes to be in there per se, but a few recommendations on textual changes. So, I'm not going to bore you all with all of this text, but just to say the main gist is, we want to see some criterion around keeping this narrowly scoped.

A little bit to echo Nico's comment earlier about the questions from GAC, we also want to see a narrowly scoped investigation here, tailored to what we're trying to achieve with the Associated Domain Check. Similarly, again, we don't want this to necessarily generate new data, but it should be based on data that's already readily accessible. Next slide, please.

And the next point that we really want to reiterate is, what comes next, right? We're all excited about this to be moving at a fast pace.

To quote our fair list leader, the chair, we're doing this at record speed, but we also want to make sure that we don't forget about when it comes to the registrant, for example, if something goes wrong, if we get something wrong in the side of a mitigation, let's make sure that there are ways that we can remedy that. So, that's really what we're excited to see.

As a potential priority topic coming up next is thinking about what a standard dispute or recourse mechanism for registrants could look like when it comes to mitigation actions taken in response to DNS abuse. And I give a lot of credit to folks in the room, including my esteemed colleague to my left, who has also written extensively about what this could look like in the ICANN context. So, I guess to quote Reg again, you know, positive, what is it, optimistic, optimistic about where this will go and thank you again for your time today.

SUSAN CHALMERS: Thank you so much. Since we do have a little bit of time, ICANN compliance's role was mentioned, and I just wanted to reach out to see if ICANN compliance is in the room, so if they'd like to -- Oh, here we are. Jamie, please.

JAMIE HEDLUND: Thank you, Susan, and thank you to the panel for this discussion. As ICANN compliance, of course, we don't have a role on what policies or obligations should be developed or would be the most

beneficial. But we are very pleased that we've been able to actively participate and follow the discussion of the working group. We have a serious and deep interest in ensuring that what policies and obligations come out are clear and enforceable.

We're very pleased with the language that was included in the DNS abuse amendments, we think, to effectively enforce those. Obviously, there's more that we can do, and the more that we are going to do, as we've talked about elsewhere, we're going to launch a proactive enforcement program, which means not waiting for complaints, but going out to identify where abuse is happening and enforcing them, enforcing the obligations.

We would like to be able to do the same with the ADCs. I think with the Associated Domain Check, as others have mentioned, there is a challenge in making sure that an effective domain check was actually carried out because we in compliance are not going to have the same level of visibility as we do when there is DNS abuse and there's evidence presented that we can verify.

So, it will be really important for us, for the working group, to be clear on what registries and registrars would have to demonstrate that we can enforce to show that they've actually complied with the obligations. But like everyone else, we're very pleased with the progress and the seriousness of the discussion that's happening. Thank you.

SUSAN CHALMERS

Thank you, Jamie. Now, before we turn to part two, I'm actually going to give the floor to Martina to see if she has any observations. Martina is, of course, one of the two GAC representatives in the working group, along with my colleague, Gabe Andrews from the FBI. But, Martina, please, over to you.

MARTINA BARBERO

Thank you very much, Susan, and thank you to all the community members that shared their reflections with us today on how the PDP is going. I think this is appreciated. Maybe from what we heard, I think something that I forgot to mention in my previous presentation is that, there are a number of topics that cannot be covered under this PDP, but that are staying on the radar.

For instance, transparency of reporting was just mentioned by Vivek and by Michaela, and it's definitely something that is on the radar. But also, cross-register collaboration because we will be able to reduce and ensure that ADC checks are done within a single registrar. But of course, you know, there is more that can be done if registrar collaborates and also remedies, which is, of course, as well, something that the GAC is interested in.

So, I think this is just to say that this PDP is not the beginning and the end of everything, but it's a good conversation going on. We are uncovering topics that need to be addressed elsewhere. And I also hope that we can beat, I think it was Rod who said, maybe we can beat the speed of this PDP or, you know, we're going as fast as we can. And it's true that we're on time so hopefully we have

something by February next year and to be adopted by the board before summer next year. So, in one year's time, maybe we're already good to go, but let's see if we can even beat the odds and be the fastest PDP ever recorded in ICANN. Thank you.

SUSAN CHALMERS Let's hope. All right, now I'm going to turn to Graeme.

GRAEME BUNTON Thank you, Susan. Good afternoon, everybody. My name is Graeme Bunton. I'm the Executive Director of the NetBeacon Institute, and I've got some slides. It would be handy if we could get those up, please, and thank you. Thank you kindly. All right. Next slide, please. Briefly about who we are.

The NetBeacon Institute was created by and is a part of Public Interest Registry, PIR. PIR operates the .org top-level domain and is a not-for-profit. And so, this work is in service of its public interest mission. We're also not a commercial organization, the institute. All our products and services are free. We do a lot of education, innovation, outreach, collaborating across parties, developing white papers. Here, I'm really talking about that innovation bucket around the services we offer to try and disrupt abuse at scale across the entire DNS. Next slide, please.

So, we have two key projects. One, NetBeacon MAP. This was created to try and understand abuse. We partnered with a European academic to measure abuse across the entire ecosystem

in a robust and transparent fashion. If you're interested in understanding more about abuse rates across the ecosystem, I would encourage you to check out those reports. Today I'm going to more focus on Reporter, however.

NetBeacon Reporter is our abuse reporting conduit. We saw two problems. One, people with knowledge of malicious domain names had a really difficult time reporting them. And at the same time, registries and registrars were getting unevidenced, unactionable, duplicative reports. And it seemed like a really good thing to do was to build a conduit that sits in the middle, that provides value to reporters and value to registries and registrars, and helps facilitate the disruption of malicious domain names. And so, I'm going to speak pretty quickly, actually, about what we've learned in operating that service. Next slide, please.

So, this is a sort of high-level architecture of what we do with NetBeacon Reporter. We accept abuse reports from anybody, any Internet user, but we also see a lot from Internet security, brand protection, law enforcement, consumer protection, as well as we take our own data from our MAP project based on feeds and turn it into evidenced abuse reports. We distribute those to web hosts, CDNs, all ICANN-accredited domain registrars, participating registries, both gTLD and ccTLD. And then we monitor those reports and collect feedback on false positives and unactionable reports from those who receive them. Next slide, please.

So, NetBeacon Reporter does tens of thousands of malicious domain abuse reports every month. May was our biggest month on record and we sent something north of 42,000 abuse reports to registries and registrars. Those reports, as I said, come from blocklist that we've cleaned, verified, and evidenced to the best of our ability, as well as through third parties. And we do this monitoring so that we can do quality control, that registries and registrars can flag false positives, unevidenced abuse reports, and we can work with reporters to try and improve their work. Next slide, please.

So, key learnings. A big one is that the raw feeds, such as those used in other measurement projects, are often woefully insufficient for mitigation. And the path that we see from suspicious name to actionable abuse report is really quite long and challenging. We spend a lot of time and energy building opportunities to enrich abuse reports that we get, to add actual information to every single report that we see to ensure that it's possible for a registrar to mitigate their risk and take action on an abuse report.

A tricky one is that abuse where it's in an email only, there's no corresponding website to resolve, is exceptionally difficult to evidence and this is a problem that requires some more thought. It's interesting to look at mitigation rates, not just at registry and registrar, but also by reporter, by the organization that is submitting that abuse report through our conduit to registries and registrars. It's clear to us that many of them have had insufficient feedback. They've not had enough quality control and guidance on

how to submit those abuse reports. They are often unaware of reporting standards published by the registrar and registry stakeholder groups and they are occasionally unwilling to adopt them. Next slide, please.

So, a brief summary. You know, I really want to highlight that Reporter facilitates the disruption of tens of thousands of malicious domain names every month for free. I also want to highlight that a domain name on a blocklist is not in and of itself actionable. Registrars do mitigate well-evidenced reports and report quality, especially including screenshots, is the single biggest predictor of mitigation. We see reporters getting 90 plus percent mitigation rates when they submit simple, clear, evidenced, actionable abuse reports.

If you're really interested in more of this, as I said off the top, please check out our MAP project for more information about mitigation rates and time to mitigation, and know that we're really working towards more transparency in that data, that we will work towards publishing all of that across the entire DNS. And so, I know we all know this, but I'll leave it with you one more time, that effective disruption at scale is happening now, but it really depends on strong collaboration between our stakeholders and quality, evidenced, actionable abuse reports. Thank you, Susan.

SUSAN CHALMERS Thank you. Thank you, Graeme and I'm just going to pause and see if anybody has any questions for Graeme before we move on to

Michaela. Okay, I see no hands. Michaela, the floor is yours. Oh, wait. Oh, sorry, there was a hand. Sushil.

SUSHIL PAL

Thank you. Thank you, Susan. I think just a question both to Graeme as well as maybe to Karen from Interisle. Thank you for this research, but all of this, you know, lead us that whatever action we take will be reactive. I think, can your research also throw out certain policy measures we need to take which are more proactive and let's those down, you know, in terms of the priority?

GRAEME BUNTON

Thank you for the question. This is Graeme Bunton again for the transcript. So, I think two things. One is, we wrote a white paper last year, time has no meaning anymore, proposing a number of policy development initiatives within ICANN, and the Associated Domain Check is one of them. And while that does seem predominantly and it is predominantly reactive, there is a component of this that I think will be helpful in reducing abuse proactively, which is, effectively doing an Associated Domain Check is a tax on registrars for how many domains they let exist in, say, a customer account. And so, it's going to incentivize registrars to be thoughtful about who they let large volumes, register large volumes of domain names. And so, that's a positive piece.

And then I think also the next policy development process in the queue is around limiting access to APIs for registering domain

names. And putting some friction in that process is going to reduce the volume of large-scale abusive campaigns. And so, I think those two pieces that we're all working on collectively or gearing up to work on are really positive steps.

SUSHIL PAL: Just to follow up, I mean, how does ADC handle those domains which are not verified?

GRAEME BUNTON: I'm not on the PDP, so I'm not sure I'm the best person to answer that question, and I'll defer to my colleagues. But the Associated Domain Check, from my understanding, would apply to any domain name at a registrar, whether it's verified or not.

KAREN ROSE: Yeah. If I can just make a comment. I think prevention and mitigation are two very important pieces of the puzzle. And I think the progress that has been done on the PDP is very promising, and we hope it has a good continuation and conclusion.

At the same time, I think if we focus on prevention and we know that there are techniques that can help reduce domain name abuse on the front end, for example, I would encourage you to look and see what some ccTLDs are doing in this area to prevent domain name abuse on the front end. And I think the prevention and mitigation go hand in hand because the more that we can reduce

these domains from being registered in the first place, the less burden we have on the mitigation side on the back end.

So, prevention and mitigation are two very important pieces of this puzzle. And I think like Graeme was saying, I think there's incentives both ways. If mitigation is more effective and prevention is more effective, then we'll have a reduction in abuse overall.

SUSAN CHALMERS: Thank you, Karen. All right, Michaela, can we turn to you for your presentation, please?

MICHAELA SHAPIRO: Sure. Thank you so much, everyone. Michaela, Non-Commercial Stakeholder Group for the record. My name's right there, I realized, so also that helps. So, the title of our latest report which came out a few weeks ago, is Damming a River to Catch a Fish. Why the DNS Must Enable Expression, Not Silence It, and I will be talking a little bit about the scope of the research that we did and where we would like to see it go. So, next slide, please.

So, some of you may be wondering why as a human rights organization like Article 19 we do work on freedom of expression, why are we at ICANN? Why are we talking to you today? And the main question that we are trying to answer with this research which we think will help answer those other questions is because there is a relevance to when it comes to DNS abuse mitigation and freedom of expression online.

So for this purpose, for this research I had the opportunity to speak with a number of domain operators, both on the general top-level domain side and the country code top-level domain side, to try to understand, as my fellow co-panelists have shown, we are dealing with a very big DNS abuse issue, right, and we have to address it. And absolutely, Article 19 is supportive of that. We're supportive of supporting those victims of abuse.

At the same time, how we do that is also important and we want to draw attention to the way in which mitigation takes place. So, here, what I put on the slide is that the domain name system, it's a tool. Things like domain suspensions and deletions are tools, similar to the Associated Domain Check. And the way that we do address abuse, it can be a powerful tool for addressing things like online abuse. On the other hand, when it's not done carefully, there's a risk that it could lead to censoring of content, stifling the free flow of information, or silencing critics.

And I do want to also caveat with this is not always done with malicious intentions. More often than not, it happens because you're trying to do the right thing, but sometimes there is a perspective that might be missing and that's really where this report came from. We wanted to talk to both the operators who are dealing with these requests and are facing pressure to do something about this, as well as the registrants who have been kind of caught in the crossfires. So, next slide, please.

So, as I mentioned, why does this matter, this is probably not news to a lot of you, but a domain suspension impacts a lot more than just, quote-unquote, the DNS, or as in it's much more broader. It's broader in scope than just, for example, a URL block. It means that your email won't be accessible if you have social media handles that are tied to your domain name. It goes quite broad, and so that's why we also wanted to kind of put in one place what actually is the DNS and again why taking action at the DNS should be done very carefully with clear safeguards and guiding principles to ensure that it is proportionate and to the abuse at hand. So, next slide please.

It's like damming a river to catch a fish is kind of the metaphor that we came up with. My boss is Dutch so that was kind of the idea there, is that if you're trying to catch that one fish of abuse, but you're damming the entire river, there's a risk that you might catch some fish that otherwise should be swimming happily in the sea. So, next slide, please.

And what you probably want to know is, you know, what did we find as we spoke to folks? And one of the things that we found from speaking with operators is, there's a broad spectrum of how we define DNS abuse, right? So, ICANN has its five categories, which is fantastic, but that's just a baseline.

And what happens is you have registries both on the G side and the CC side who can then go beyond. And that makes a lot of sense given the context, particularly when it comes to the country code

side. But what that means is, you report abuse in one place and how it's defined there versus somewhere else could lead to another outcome. And this just can create systemic vulnerability and confusion, more often than not, for the registrant themselves. So, that was one of our findings.

Secondly, that registries and registrars are operating under growing and often conflicting pressures, right? We've spoken a lot about the policy development process at ICANN, so we're seeing a lot of changes happening in this space, but we're also seeing national laws, court orders, law enforcement, like my esteemed colleague here from Spain, trying to figure out, how do we handle abuse at the domain level? And again, as this is changing, it can create a lack of clarity for the operators themselves specifically because quite a few operate across jurisdictions.

And all of that comes together in this kind of mix to lead to registrants' rights often remaining an afterthought. And I want to highlight here a couple of folks have already mentioned transparency reporting and that's one thing that we also really wanted to highlight as part of this report, that transparency around mitigation decisions is a really powerful tool, and that can allow registrants to at least understand why something isn't accessible.

As someone without a technical background, if I couldn't access my website, I might not know necessarily, without doing a deeper dive, I'm not as brilliant as Rod, for example, happy birthday again, in

terms of being able to determine the cause of why my website isn't available. And that was one of the findings of the report as well.

And I'll leave you with, I didn't actually think I would have enough time to go into the recommendations of the report, but I'd like to leave you with the thought that as we go through, both for governments working on national and international legislation and for the ICANN folks in the room, that as we go into DNS abuse mitigation discussions, as we further those discussions, we want to make sure that we find that balance between addressing very real safety and security concerns with freedom of expression. So, I'll leave you there on that. Thank you.

NICOLAS CABALLERO Thank you so much, Michaela. Thank you, everyone. As a matter of fact, we're about to wrap up. Thank you so much, Alan Wood, Steinar, Rod, Reg, Dennis. I know, I know. If you please allow me to finish thanking our guests and then I'll give you the floor for the considerations for the GAC Communiqué.

I was thanking Reg, Dennis, Vivek, Michaela again, and Graeme Bunton and of course, Diego Alejandro, and Karen Rose. Thank you so much. Thank you for your time, patience, and energy today for sharing all these very interesting insights and findings with us. And now, I will kindly give the floor to the European Commission for some considerations for our GAC Communiqué. Over to you, Martina.

MARTINA BARBERO

Thank you, Nico. Sorry, we thought that the pressure to get lunch would you know. As you've mentioned, wrap up, I saw people already looking at the food in their eyes and I thought, no, no, no, you need to stay in the room until we discuss the communiqué considerations.

So, yes, so as you know, DNS abuse is an important topic, so we suggest to have issues of importance, part of the communiqué dedicated to it reflecting our discussions of today, so basically the progress on the PDP, possible future efforts, and anything else that you would want to mention in the next, I think, six minutes, Nico, if there is any, yeah? So, back to this room in case there is any suggestion or any thought.

NICOLAS CABALLERO

Thank you so much, European Commission. That was quick, as a matter of fact. Thank you so very much. So, as you can see, you know, the idea is to include this under issues of importance, you know, and the three things you see there on the screen. Let's see. We actually have five minutes for very quick and very, as I always try to say, narrowly scoped questions. So, the floor is open. I see a hand from Switzerland. Please, go ahead.

JORGE CANCIO

Thank you, Nico. Jorge Cancio, Switzerland, for the record. So, it's more a comment in the sense of commending really our topic leads

and everybody that participated in this session because I think they managed to transform a GAC session into a cross-community session, which was exactly our request from the GAC leadership to, not talk separately, but to talk with each other. So, thank you very much and kudos for that.

NICOLAS CABALLERO: And by the way, they actually deserve a big round of applause. Thank you so very much. Okay, so the floor is still open. We still have four minutes. And on a different note, let me tell you that for the ones who would like to stay in the room for the memorial service to our good friend, Alan Barrett, you might stay in the room. We will start with the memorial service at 13:15, I stand to be corrected. Julia, Gulten, is that correct, 13:15? So, for the ones interested in, I don't know, sharing whatever you would like to share, you know, as regarding the early departure of our good friend, Alan Barrett, more than welcome to stay in the room.

So, other than that, Susan, is there anything I forgot to mention, Martina? And thank you again to our panelists for today. Susan?

SUSAN CHALMERS: Just on the Communiqué text, I think there's really the issues of importance, that's what the GAC topic leads have recommended. I think we can try and keep it short and sweet, and no advice for ICANN86 on this topic. Thank you.

NICOLAS CABALLERO: Thank you very much, and thank you again to each one of you for your energy and patience. So, let me call at this point, let me call, is it Chris, is it CK that's going to be running the memorial service? Let me call Tripti Sinha, Chair of the Board, and any other board member who would like to join the head table for the memorial service for Alan Barrett. Please approach the head table. Thank you.

[END OF TRANSCRIPTION]