ICANN77 | PF – GAC Discussion on DNS Abuse and Emerging Technologies
Wednesday, June 14 2023 – 10:45 to 12:15 DCA

JULIA CHARVOLEN: Hello and welcome to the ICANN77 GAC meeting on DNS Abuse discussions followed by discussions on Emerging Technologies. Please note that this session is being recorded and is governed by the ICANN expected standard of behavior. During this session, questions or comments submitted in the chat will be read aloud if put in the proper form. Remember to state your name and the language you will speak in case you will be speaking a language other than English. Speak clearly and at a reasonable pace to allow for accurate interpretation and please make sure to mute all other devices when you are speaking. You may access all available features for this session in the Zoom toolbar. With that, I will hand the floor over to the GAC Chair, Nicolás Caballero.

NICOLÁS CABALLERO: Thank you very much, Julia. Welcome everyone to the DNS abuse mitigation session. We will have Susan Chalmers from the US Department of Commerce, NTIA. We'll have Karel Douglas from the Telecom Authority of Trinidad and Tobago, also the Underserved Regions Working Group Co-Chair. We'll also have Lorraine Kapin from the US Federal Trade Commission, also Co-Chair of the GAC Public Safety Working Group, and Chris Lewis-Evans from the UK National Crime Agency, Co-Chair, by the way, of the GAC Public Safety Working Group. We'll also have as guest speakers Russ Weinstein, and I hope I'm

pronouncing the last name well, from ICANN Global Domains and Strategy, and Peter Jansen from EURid. So welcome everyone.

Next slide, please. We'll take a look at the agenda for today. So the first topic will be an overview of proposed DNS abuse contract amendments and the DNS security threats they are designed to address. Then we'll have the EURid talking about.eu and DNS abuse and so on and so forth. The third topic will be Day Zero GAC Capacity Development Workshop on DNS abuse, and for that I will most probably give the floor to Karel and the Underserved Regions Working Group team. And then finally we'll have a GAC discussion to determine next steps. So with that, welcome everyone again, and let me give the floor to Chris. Chris, please go ahead.

CHRIS LEWIS-EVANS: Thank you very much, Nico, and Chris Lewis-Evans for the record. So I'm actually going to pass over to Russ to give us a quick outline of the contract amendments and then after that I'll go over what that actually means from a public safety mechanism. So Russ, over to you. Thank you very much.

RUSSELL WEINSTEIN: Sure. Thank you, Chris, and thanks everyone for having me. My name is Russ Weinstein. I'm ICANN's Vice President of Accounts and Services within our Global Domains and Strategy team, and what that means is I manage all of our relationships and contract administration with our registries and registrars. I'm also responsible for coordinating ICANN's internal DNS security threat mitigation program, so this project related

to contract amendments for DNS abuse fits into both of those roles and pleased to be here and thanks for having us today.

So important to remember before we get into what the contract changes, what the changes are is where did this come from and what is the context behind it. So you all know that DNS abuse has been a topic of high interest and discussion for many years in the ICANN community, and there's been great progress along the way over the last several years, especially a lot of voluntary work and best practice work produced in the community, particularly in the contracted parties, but there was clearly a need for more.

And in the fall of this last year, the contracted parties got together and brought a proposal forward to ICANN and to the whole community that we can do some important changes to the contract, limiting those changes, focusing on creating an obligation to mitigate and disrupt DNS abuse, and then enable the ICANN community to have discussions about what further should be done when it comes to DNS abuse in an open policy development format, and doing that in a focused, productive way, but starting with the limited focused contract amendments. And so that's what we endeavored to do. To endeavor to create contract amendments that create a meaningful and enforceable obligation for all registries and registrars to mitigate or disrupt DNS abuse when it's evident in their zones. So we'll walk through what those contract amendments are. And the idea here is creating a floor, a new floor for registries and registrars having this obligation.

Next slide. So a high-level summary, and we've presented this at a couple places already, so hopefully you've either had a chance to check out the prep week session we did a couple weeks back, or the session we had yesterday, or if some of you were in our discussion on Monday, or on Sunday with some of the GAC members as well. But the changes in a nutshell are we've started with the existing obligations in the registry and registrar agreement, and there's nothing that's taken away from those existing obligations. We've only added on top to those. So in these amendments, we've clarified that the abuse contacts for each registry and registrar need to be readily available and accessible on the web pages, and we've improved some aspects with reporting of DNS abuse.

So we've added the ability for registries and registrars to utilize a web form to collect DNS abuse reports as opposed to email addresses, as we've known and learned over the years, publishing an email address on the web just becomes a source of spam and complicates and puts barriers to the good work that registries and registrars are doing trying to find the real abuse complaints and take action on those while they're dealing with filtering. We've also added the feature where registries and registrars now need to provide confirmation of receipt of an abuse report. And so this helps the complainant and the registrar and ICANN in situations where escalation is required or further follow-up is required. These amendments add a definition of DNS abuse for the purpose of these agreements, and we started, and we'll get into that in more depth. And then as we mentioned, it creates a new obligation to take action and mitigate, to stop or disrupt DNS abuse in each of the contracts.

And along with these changes in the contracts, the changes in the contracts are really only a couple of paragraphs to each of the contracts. But we've added a draft advisory that's also part of the supporting document with the public comment. And that advisory is about 15 pages long and goes in and explains what these requirements mean in more depth and clarity, what enforcement would look like and what implementation should look like in some cases. There's several examples in there that you can follow. I'd really, really encourage everyone who's interested in this topic to read that advisory. It's an easy read, but a really helpful complementary document.

Next. So I'm going to get into the two kind of key obligations here. So the first one starts with adding a definition of DNS abuse, and we've added this to both the registry and registrar agreements. And for the purpose of these agreements, DNS abuse means malware, botnets, phishing, farming, and spam when used as a vector to deliver other forms of DNS abuse. So these definitions come from work that's been done in the ICANN community for a while now. We've released several of these things back to SAC 115 as a source of good work coming out of the community. These are things that, looking across the community, there's been clear consensus that all of these are DNS abuse, and there's no dispute that -- there's little to no dispute that these things are DNS abuse. And so that's our starting foundation when we're talking about what these obligations are relative to.

So next slide. So knowing what DNS abuse is, the core obligations in the registrar agreement is when a registrar has actionable evidence that a registered name sponsored by a registrar is being used for DNS abuse, the registrar must promptly take the appropriate mitigation actions

that are reasonably necessary to stop or otherwise disrupt that name from being used for DNS abuse. And an important thing to remember with DNS abuse is not all -- it's highly contextual, and so not every case of DNS abuse has the same mitigation approach and the expected same outcome. But all of the mitigating actions that are required must be focused on trying to stop or disrupt that name from being used for DNS abuse. That's a big improvement to where we are today.

Next slide. Similarly, on the registry side, it's almost the same obligation, but it has some consideration for the role of the registry versus the role of the registrar. We think of the registrar as closest to the customer of the registered name and in often a different position in order to interact with that customer to solve issues of abuse. So the registry has, like I said, almost the same obligation, but they have at minimum that mitigating action should either be referral of the case along with any actionable evidence to the registrar, which would then kick in their obligation, the registrar's obligation that we just discussed, or to take that mitigating action on their own to either stop or disrupt the DNS abuse on their own and having the ability to do either of those things but require that they must do one of those things is a big deal again for registries. So those are the core obligations in the agreements. And I think I'm passing it back to Chris or is there more questions or are we breaking for questions?

CHRIS LEWIS-EVANS: So Russ, I think if I could just do my two slides and then go for questions after that, if that's Nico. Brilliant, thank you. So Chris, let's set the record. So what I wanted to cover was actually how does some of that

language impact on what we're seeing from a public safety perspective and how does it enable us to take action? How does it enable the registries and the registrars to take action based upon the evidence that we might give them? And does it actually cover everything? Does it give us the tools that we need to be able to take appropriate action? And during the capability development workshop, we heard questions about, well, does it cover SMS phishing? Does it cover this? Does it cover that? And I've got two, three, four examples here of actually yes, it does.

So on the left-hand side is a screenshot of an SMS message saying that someone's account needs to be upgraded or needs to be suspended is normally the language that appears. And then it's got a link for someone to click that includes the domain name. This is phishing, DNS abuse every day. So this, along with a screenshot maybe of the site that it's linking to, to show that it's not the actual mobile provider site, would be actionable intelligence, would be able to provide some proof of harm if we have a complaint that this then steals passwords and takes over accounts. It enables us to say, here you go, this is a phishing, DNS abuse. And the language then says they must act promptly because they've got actionable evidence and take the appropriate action. So in this case if it is a maliciously registered domain, they would be able to suspend that domain and then that would take that. They may also recommend that we contact the host and remove the content, but that would be an appropriate mitigation step.

So yes, it is covered. If you receive the same thing by email, yes, it is covered. As long as it's got that domain name that you need to click on. We also heard about lookalike domains, so ones that rely on maybe a

slight typo error or ones that just add an extra word to still make you think it's legitimate. So the example on the right is one of those. And it pops up a service that probably a lot of people use. And it relies upon you doing that, whether that's one of the social media platforms or whether it's a package delivery that everyone gets from one of the retailers. Oh, I just need to log on. And then it will capture your passwords and everything and then utilize that for criminal activity. Is this covered? Yes, it is. So I think it's really good that there's some clarity in these amendments to identify some of those sort of phishing items that are covered. And the PSWG have said, certainly in ICANN's 67 -- sorry, 76, got the numbers the wrong way around.

A large proportion of the criminal activity seen is predicated by phishing attacks. So being able to have multiple types of phishing linked into this language is really important for us to be able to act against this. Go on to the next slide, please. Brilliant, thank you. So key thing for a lot of governments at the moment is ransomware. Is ransomware covered by this? It's not mentioned. But ransomware is a form of malware. So yes, it is. If there's a domain that is delivering malware that then encrypts someone's device or everything else, is this covered? Yes, it is. That's one of the key areas I know for a lot of governments at the moment around risk, both to commercial entities within their countries, but also to critical national infrastructure. So this is covered. Excellent. So spyware that gets put onto people's devices, is that covered? Yeah, it's another form of malware.

Some people also say Trojans. So something that you think is realistic, but then also steals your data. That's just another form of malware. So that would also be covered under legislation if that's linked to a domain

name. Adware, again, click on a domain, tells you to download something, you think it's real, that's malware, it's delivering malware. Is it covered? Yes, it is. So really, a lot of the threats that we see that deliver criminal or allow criminals to make an impact on victims, this is all sort of covered in the definition that has been used. So from our perspective, this is a really good step forward in what we have. It makes, for the registrars, it's a lot clearer upon what they should act upon or what they must act upon using the language. So I think it's a really good step forward and a good real raising of the floor. And with that, I'd like to open it to questions. Thank you.

NICOLÁS CABALLERO: Thank you. Thank you so much, Chris. So before I give the floor to Peter Janssen and we move on to the next topics, which is you read, is that the way to say it? Any question, any comment, any reaction in the room or online? Gulten?

GULTEN TEPE: Thank you, Nico. We have Ken-Ying Tsang from Chinese Taipei and then Kavouss Arasteh from Iran delegation.

NICOLÁS CABALLERO: Chinese Taipei, please go ahead.

KEN-YING TSENG: Thank you, Chair. For the record, my name is Ken-Ying. I'm from Taiwan Network Information Centre. I'm a GAC representative from Chinese

Taipei. With regard to the amendment to the agreements on DNS abuse, I believe that the language carefully drafted at a very delicate balance in the way that there are quite a few norms and deterrents for either party to have certain discretion to interpret in the future. This should be a nice way to return flexibility, which also shows the importance of the advisory, which I believe will be serving as a reference to all parties to future implement DNS abuse-related contract provisions.

But I have some questions on the interpretation of the language. First of all, I saw the words reasonably or reasonable showing the language so many times. I'm just wondering whether the interpretation of this reasonableness should be from the perspective from the registrar or registry or from ICANN, when ICANN conduct compliance audit. That's my first question. And my second question is about cross-border issues. I believe that for DNS abuse situation, oftentimes the abuser and the reporter and the registrar or registry, they probably would be in at least three different jurisdictions. I'm just wondering whether the obligations that we impose on registrars or registries, have we considered the cross-border nature of the incident, potential language or cultural barriers? Thank you.

NICOLÁS CABALLER: Chris, would you like to go ahead?

CHRIS LEWIS-EVANS: Maybe if Russ -- sorry, Chris. Maybe if Russ answers the first one, I can cover the second one.

RUSSELL WEINSTEIN: That sounds good. Thanks, Chris. This is Russ Weinstein from ICANN. Thank you for your question. So the first question was about reasonableness and I think who the arbiter of reasonableness is. So I think the way to interpret that is first the obligation to the contracted party is for them to behave reasonably. And then if that's put into question for ICANN to evaluate the reasonableness of those choices and make its own determination of was that reasonable or not, and we'll do that based on our experience, many years of experience in this field and also our experience with these contractual provisions. And so I think ICANN has the discretion we need to enforce these contracts is the key part.

CHRIS LEWIS-EVANS: Thank you, Russ. And to the second point around cross borders. So you're right, you will have probably three jurisdictions if you're lucky, maybe five or six I've seen, definitely in a number of cases. The language here doesn't allow law enforcement to just go in and say you must do this through an order. There is a process for that, a court system, MLAs, everything else. However, what it does do is allow cross border requests for registrars to look at the evidence that you're providing and then to take the appropriate action based on what is their determination of that evidence. And I know speaking to registrars and registries, they're always really appreciative of the good evidence that law enforcement are able to provide. We're quite used to providing evidence packets.

So when we provide that, that is generally well received and it starts that conversation about actually did you have something a little bit more and we'd be able to take this action. So the language definitely allows for cross border action. It's not a they will act on upon it. It will be a determination based off of the evidence. Thank you.

NICOLÁS CABALLERO: Thank you, Chris. Next, I have Iran. Please go ahead.

KAVOUSS ARASTEH: Thank you very much, Chris. Thank you, everybody. I think if you allow me, Chris, two cases exactly happened to me. Some months ago, I received a message from the Secretary General of ITU early morning, nine o'clock, please immediately come to my office. Then I prepared to go and then I check. I found that it doesn't come from the Secretary General of ITU, Mr. Zhao. What type of abuse is that?

The second one, I received another message called Christina and something. I thought it's one of those Christina that is working in ICANN working groups. I replied to that. He said, please acknowledge this email. Then I found that it is not the Christina that I know. It is Christina something. I don't know. What category of abuse is that and to whom should I have report or should I have not report to anything? However, I immediately, in two minutes, I changed my password immediately. Thank you.

LAUREEN KAPIN: Kavouss, those are actually great examples because it shows us the range of communications that along the spectrum can be irritating, annoying, all the way up to abuse, which may have real actionable harms in terms of economic consequences, et cetera, et cetera, even emotional consequences in the case of, for example, romance scams. But in terms of those, I don't think they would rise to the level of what we're calling DNS abuse because there wasn't really a harm, although there was irritation.

What I will point out to folks, just as we're all interested in protecting ourselves, is sometimes even these innocuous communications that you might get via text, something as simple as a hi could be the first step in something that becomes more dangerous, perhaps an imposter scam. So it's good to delete these emails and not go along the path to perhaps divulging sensitive information or allowing someone access to their computer because you think it's a -- they're going to help you with some technical issue. But for those specific situations, it wouldn't rise to the level of formal DNS abuse, although it is irritating.

NICOLÁS CABALLERO: Thank you very much, Laureen. I have Malaysia next. Mr. Mohamed Afiq. Go ahead, please.

MOHAMAD AFIQ: Yes, thank you, Nico, Afiq, for the report. First of all, I must say that this amendment is an excellent initiative and it's about time for us to better mitigate the DNS abuse within the DNS ecosystem. So in this regard, I had observed the amendments documents and I am not sure if there

are any other documents or provisions that cover the same. But I am wondering, in the case of discrepancy in the assessment of the registrar, the registry operator or maybe the contractual compliance unit, I want to ask, is there any determination to finalize or conclude the decision that would be taken on the domain name in dispute?

NICOLÁS CABALLERO: Thank you, Malaysia. Would you like to go ahead, Russ?

RUSSELL WEINSTEIN: Sure. This is Russ, for the record. I'm trying to parse the question a bit. Would you mind restating it?

MOHAMAD AFIQ: If there is any discrepancy in the assessment when the assessment has been made by the registrar or the registry operator, then they have contradictions in concluding whether the domain name is actually used for DNS abuse or not. So if there is any contradiction between the registrar and the registry operator or maybe the contractual compliance unit, is there any determination that we can take to conclude the decision that would be taken on the domain name itself?

RUSSELL WEINSTEIN: Great. Thank you. This is Russ again. So if you as a complainant submit your evidence to the registrar, you believe you have a valid case of phishing or one of the other forms of DNS abuse, and you get an answer that they don't think that was DNS abuse, you should bring that to our

contractual compliance department, and we will take that up with them. We'll do our evaluation of your complaint, ensure it's valid, that we have the evidence we need. We have the ability to validate if something is being used for DNS abuse as well, and if we find that, we'll take it to the registrar and work through that to get to rectification. So I think that addresses your concern.

MOHAMAD AFIQ: Thank you.

NICOLÁS CABALLERO: Go ahead, Mr. Afiq. Go ahead.

MOHAMAD AFIQ: So you are saying that the contractual compliance unit here will have the final say or maybe the one that determines whether there is a DNS abuse being conducted through that DNS, through that domain name?

RUSSELL WEINSTEIN: So ICANN compliance will have the ability to present our view to the contracted party with our determination. The contracted party will have the opportunity to present their view and work out whether we were right or they were right. There's also the possibility in this discussion that the action that the contracted party took may not match your expectation, but there may be that the contracted party took a reasonable actions, and if you go and read the advisory, there's several sections in there about the differences between types of DNS

abuse and particularly compromised domain names where suspending the domain name would not be always the appropriate action, and so they might take another path to resolve that, and that may be why you're feeling unsatisfied, and those cases would not necessarily result in a change of course by the contracted party. Hopefully that ties that up.

NICOLÁS CABALLERO: Thank you, Russ. Excuse me. Thank you, Malaysia. Next, I have Japan. Nobu, please go ahead.

NOBUHISA NISHIGATA: Thank you, Chair, and thank you all. Japan, first, let me say that we appreciate very much all the effort to reach to the draft amendment, and I have one clarification to ask. The question is, the current contract before the amendment, the current contract does not prohibit the contracted parties from taking voluntary actions against malicious or illegal activities if deemed to be necessary, involving the use of the domain names.

And then the question, the background is like just Russ said, sometimes the course of action from the victim of the bad malicious or illegal activities, but the reaction from the registry of risk may not always meet the expectation, just as you mentioned it, and then we see some frustration in Japanese industries. So having said that, we do appreciate that this amendment would help the contracted parties stop or disrupt the use of the gTLD domain names from DNS abuse. So thank you for asking. Let me ask one clarification. Thank you.

NICOLÁS CABALLERO: Thank you, Japan. Chris or Russ?

RUSSELL WEINSTEIN: Thank you. I apologize. I'm having trouble detecting what the question part was there.

NICOLÁS CABALLERO: Would you please repeat the question?

NOBUHISA NISHIGATA: So if you look at the draft amendment, and then we have some good text, like the contract parties must take some action, blah, blah, blah, but without that text in the current contract, but the contract parties can take necessary action if deemed necessary from them to do some actions from voluntary basis to the extent taking down the servers if necessary. Despite regardless of whether it is in DNS abuse or not, in defined in the SAC 115.

RUSSELL WEINSTEIN: So what this amendment does is codify what DNS abuse is as those five things, and what the requirements are to mitigate and stop or disrupt that DNS abuse. The existing contracts, you're right, use a little a abuse, and that will continue to be a provision in these agreements for a broader set of things, and the registrar has more discretion of how to address those. They still have to address those. They have to

investigate and respond, but it's respond appropriately and within their remit.

NOBUHISA NISHIGATA: And how about the registry side? We have the existing contract. We have the starting point that we can the victim can, or maybe like lawyers can send inquiry, then the registry is received the inquiry, then then the registry, if they think it's necessary or urgent, those kind of judgments, then they can take the voluntary action against these reported bad things.

RUSSELL WEINSTEIN: There's nothing in the contracts that prohibit registries and registrars from taking action on things they see fit.

NOBUHISA NISHIGATA: Thank you very much.

NICOLÁS CABALLERO: Thank you, Japan. Thank you, Russ. I have the Democratic Republic of Congo, Blaise. Go ahead, please.

BLAISE AZITEMINA FUNDJI: Thank you, Chair. First and foremost, I'd like to thank Chris for taking in consideration a matter that we were discussing on Sunday, if I remember well. And on the mobile environment that you brought, or is now considered clearly as a matter of DNS abuse, because that was of

concern for most of undeveloped or underserved region countries. Thank you very much for that. I think we're moving forward. But now I have a question, I think a comment. Most of the time with internet service providers, we have an issue, it's not really malicious, but I do not know if that falls under the general conditions, or it's an excuse for ISPs under the general conditions. They forcibly subscribe users to some services where users do not subscribe voluntarily.

But you just end up finding on your bill that you did subscribe, or you were cut, or you were billed for a certain amount of money for using service A or service B. Why you don't remember personally subscribing to these kind of services. But then when you get in touch with providers, they say that falls under the general conditions. Of course, they are not malicious to be considered as phishing or otherwise, but this is not done with the willing of the users. So how do you consider that? Thank you.

CHRIS LEWIS-EVANS: Yes, so Chris Lewis-Evans for the record. So that would probably fall under spam, but within the DNS abuse definition, as you say, it's not delivering any of the other malicious activities, so it wouldn't fall under DNS abuse. So it would be more of a data protection issue, from the sounds of what you're saying, relating to the ISPs, rather than a DNS abuse issue.

LAUREEN KAPIN: And just briefly, Blaise, that sounds like a consumer protection issue about unauthorized billing. So not necessarily something that falls into

DNS abuse, but certainly an issue that's important. People shouldn't be billed for things unknowingly.

NICOLÁS CABALLERO: Thank you, Laureen. And I'll give the floor to the European Commission, Gemma, and then we need to move on.

GEMMA CAROLILLO: Thank you very much.

NICOLÁS CABALLERO: Gemma, go ahead.

GEMMA CAROLILLO: Thank you. Thank you very much, Chair, and I will try to be very brief and build also on what some colleagues said, in particular, a colleague from Japan. So first and foremost, we are really happy to see this moving. This is a critical development. And the success of this initiative is going to be very important for the overall functioning of the ICANN model, if you want, for the way the whole community can come together and do something important. And for this reason, we also want to contribute constructively in this session. And we participated in the capacity building on Sunday, and we'll participate to the public comments, so do our best to contribute constructively. And just let me mention two, three things, which we also shared with the colleagues in the capacity building.

One is what Japan was referring to. So given the essence of speed in tackling DNS abuse, what is emphasized in the advisory so that the registries and the registrars can proactively monitor DNS abuse, for us is really of essence. We think there are a lot of good practices in the industry. We would rather see these embedded, if possible, in the contracts, but for consideration anyway. The second point is that we appreciate the advisory complementing the contracts very much. It's very helpful. But it would be important, either in the contracts or separately, to make sure that the provisions regarding enforcements are clear. Because this is important for ICANN compliance, and it's important for all interested parties that it's clear what are the consequences of non-compliance.

And last, there is an important part on transparency in the contracts, so registries and registrars giving accountability on reporting on DNS abuse action. And we also think it would be important to increase the level of transparency so that there is clarity on what are the policies on DNS abuse that the operators are taking, and reporting regarding the course of action. So you report about, this is the amount of abuse we have reacted in that way or the other way, because this also helps understanding how the contracts, which are, of course, at the high level, are implemented in practice. Thank you very much.

RUSSELL WEINSTEIN: Thank you very much, Gemma and Chris, this serves the record. So proactive monitoring is one of those things that is quite difficult to do. So I would suggest that maybe for the next stage of contracts, or whether there is voluntary frameworks around how the registrars and

registries can do that, would be a good comment to make for consideration next time. On the clarity about what compliance can do, I think that's probably a good comment for us to make as a GAC around how we can assure that the advisory reflects what Russ has said today, that compliance can take action to make sure that the community are aware of that. So on those two points, they're my reflection. Thank you.

CHRIS LEWIS-EVANS: Thank you for your comments. And just to add on to what Chris has said, hopefully it's clear in these amendments and through the advisory, but I'm hearing there might be some lack of clarity on it, that compliance has the discretion and the ability to go all the way to breach, to essentially terminate a registry or registrar agreement if we find violations of acting on these requirements. So that should be clear. That was part of the discussion all along with the contracting parties, that that's what we're trying to do. We're trying to raise the floor and ensure that everyone is doing this to protect the industry, to have a clean industry. And so there should be no misconception that this isn't an enforceable agreement that we have presented here for you.

NICOLÁS CABALLERO: Thank you very much, Chris. Thank you, Russ. Thank you, European Commission. And in the interest of time, I will take no more questions. And let's move on to the next topic. Peter Janssen, the floor is yours.

PETER JANSSEN: Thank you. Good morning, all. I see my slides are already up. My name is Peter Janssen. I'm the general manager of EURid. That is the Belgian-based not-for-profit organization that manages the.eu top-level domain, country code top-level domain. And for the record,.eu and its three different scripts, Latin, Greek, and Cyrillic, respectively, to support all the languages spoken within the European Union. T

his presentation today, I will try to give you an overview of the mitigation and prevention of DNS abuse that we as a registry have in place. And I already apologize up front. This is a subject that would take easily several hours to go into any kind of depth. I will try to be as brief as possible. Those that know me know I speak too much and speak too fast. So I apologize again up front also to the translation people that is really hard on them. So thank you for supporting me there.

So next slide, please. To give you a sense of what I'm going to talk about, I made a little overview of what I term the registration and delegation process. So there are different actors, as you might know, in this process of acquiring a domain name. On the top left, you have the registrant, the future holder of the domain name, who somehow, and that's the arrow with number one, gets into contact with a registrar that then uses some of the interfaces of the registry, and that's the arrow number two, to actually convey that request from the registrant for having a domain name registered.

Once the registry, in this case that is your ID, receives that request from the registrar, a number of checks and balances are done, which is arrow number three. For instance, for.eu, there are certain eligibility criteria

that need to be met. The registrant needs to have an address of residence within the European Union or any of the EEA states, or have citizenship in any of these member states or EEA states. So that is checked by the registry in a fully automatic fashion. Once all these checks and balances are okay then number four actually -- there is somebody else here. So then number four actually results in that domain name being registered and saved in the registration database. This is what we call the registration process.

Obviously, there is a lot more detail than this, but this is the high-level functionality of what registering a domain name actually entails. Once a domain name is registered, people can go to our website, can go to the UIS interface, and actually see that that domain name is registered, and it is no longer registrable by anybody else, obviously. But that doesn't mean that that domain name then actually functions on the internet, which is the second part of this process, which is the delegation process.

So towards the right, and now the arrows change into yellow and use letters instead of digits to make the distinction, there is what we call the domain name delegation process, which will extract all the DNS-related information from the registration database, which in technical terms is the domain name itself, the name service, and any kind of DNSSEC key material that is related to that domain name, and will insert it into what we technically call the zone file.

So again, we have .eu in Latin .eu in Greek, and.eu in Cyrillic, so we maintain three zone files that correspond to those three scripts. The domain name delegation process will inject that into that zone file, and

it's the task of the primary name server to actually make sure that everything on a technical level is fine, and will push out that information to the secondary name servers that sit around the world, which will actually make the domain name function, at least the part that the TLD is responsible for, which is the first part in the resolving process. I'll not go into any details there, because then we would be here still tomorrow, I think. So that is the registration versus the delegation process.

Next slide, please. If you look at that domain name delegation process in its simplest form, it will indeed extract that information from the registration database and feed it into the zone files that the primary name server will then, as you saw on the previous slide, propagate to the secondary name service, authoritative name service out there in the world. What we do is we actually add functionality to that domain name delegation process that once the domain name delegation process wants to actually delegate that domain name, it will ask what we call a decision engine.

NICOLÁS CABALLERO: Peter?

PETER JANSSEN: Yes.

NICOLÁS CABALLERO: Sorry to interrupt. You need to slow down a little bit. I'm sorry about this, but go ahead, go ahead. But slow down a little bit.

PETER JANSSEN: Yes, expected. I again apologize. So I will try to be slower. It will function for 10 seconds, probably. So the domain name delegation process normally extracts the information from the registration database, inserts it into the zone file, and its task is done. What we have done is we add functionality to that domain name delegation process. And actually, at the moment of delegation, it will ask the decision engine, as we term it, should I really delegate this domain name? And that decision engine will actually determine based on the attributes of a domain name, and I will come back to that in a slide, if that domain name potentially has been registered with potential malicious intent.

So it will try to predict this domain name, is this a malicious domain name registration, yes or no? I will give a bit more details in the next slides about that. If the decision engine decides, yes, this is a potential malicious registration, it will delay the delegation. What does that mean? It will not insert it into the zone file. So technically, the domain name is registered, so nobody else can register it. But it doesn't function on the internet, so no DNS abuse can actually happen with that domain name.

Secondly, we start what we call a validation process, where we will request the registrant to actually validate the registrant data. Obviously, as you can imagine, if this is a malicious entity that wants to register a domain name with malicious intent, that validation will not happen for the very simple reason that that person or that entity doesn't want to be found out. And at that moment in time, with lack of that successful validation by the registrant, we basically suspend and

withdraw the domain name after a while. If the decision engine says, no, everything is fine, it doesn't look fishy, no pun intended there, then obviously the domain name will get delegated as such.

Next slide, please. So that decision engine, you might have heard, some of you, of the acronym APEWS. And we do love our acronyms. All two, three, and four letters are taken, so we went to the five letters acronym. APEWS stands for Abuse Prediction and Early Warning System, and its goal is really to, at the time of registration of a domain name, predict if that domain name is registered with malicious or abusive intent. It does that by building a number or training a number of machine learning models that base themselves on the attributes of a domain name. What are the practical attributes that we take into account? Obviously, the registrant's data, the name, the address, the email, the phone number, and so on.

The registrar in question that actually registered a domain name. Something that we term the domain name randomness. We as humans, we very easily detect a Q7499P7-3 looks rather random to us, so that might be weird. So that's one of the things that plays in as well. And then, obviously, the DNS info, the name servers are taken into account as well.

So next slide, please. So how does this work? That predictive model, on the one hand, takes a list of known abusive domain names by third party security feeds, names that have been used in the wild to send spam, do phishing attacks, and that kind of thing. On the other hand, the domain name registration data corresponding to those names, but also a whole lot of names that are genuine bona fide domain names that

are not abusive. That information is fed into a daily automatic training process that ultimately delivers a predictor, a machine learning predictor. That predictor will, at the time of delegation, take the information about the new registration and come up with a prediction if that domain name is potentially registered with malicious intent, yes or no. So you might wonder, it's fine. We're trying to predict if a domain name is with bad intentions, yes or no. How good or how bad is this?

Next slide. What you see here is a graph where on the x-axis, so the horizontal axis, you see the beginning of 2018. And on the right side, you see January a bit further, 2023, so quite recent. And on the y-axis, so the vertical axis, you see the number of domain names that are registered on a monthly basis, at least a percentage that are being flagged by our APU system as being potentially malicious. So the 0.02 that you see there means 2%. There are a number of things that you could conclude from this graph. One, the overwhelming vast majority of all domain names is flagged as bona fide, genuine, no issues, no nothing whatsoever. So the domain name gets delegated as usual, and there is no harm done. There is no problem whatsoever.

Secondly, if you look at 2018 to 2019, you see a rather big drop of the number of domain names that actually get flagged as malicious or potentially malicious. That could mean a number of things. It could mean that the bad guys are getting better in evading our radar. Or, and that's what we proved, is that no, our system actually discouraged a number of bad actors to actually do the way of a number of registrations that they were doing in the past. So our system actually shows that by putting this in place, and it's a fully automatic system, a number of abusive registrations has disappeared over time.

Over time, you see a number of peaks. We have investigated those things, and some of these are actually attempts by bad actors to circumvent our mechanisms, and it's a sort of chicken and, no, not chicken and eggs, cat and mouse game where we will always adapt our systems to avoid the bad actors from evading our systems and so on. Next slide, please. So the prediction model, as typical with machine learning, needs to be tuned, and there are two terms that are interesting to talk about here. There are a lot more, but I will concentrate only on two. One is called recall, which is essentially meaning how many of the stuff that you're looking to find did you actually find? And the other one is precision.

Of those that you were finding, how many were actually correct? So in our terms, that means the domain name got tagged as a malicious registration. Was it indeed a malicious registration? Yes or no? How can we know? We did this by running the system in the beginning without acting on the decisions. So we had the system running in real time, and when the system predicted a malicious domain name registration, we didn't stop the delegation. We just let it go through, and we actually checked later on if that domain name indeed was used for malicious purposes. Yes or no? And as you can see there, both recall and precision, in our experience, was above 80%.

What does that mean, a precision of 80%? That in four of five cases when a domain name gets flagged as malicious, it indeed later on appeared on security feeds that it was indeed used for a phishing attempt or any of the DNS abuses that were mentioned in the previous presentation. The typical bane of machine learning is you can't have it all. You can't have perfect recall and perfect precision. It's a choice, and

that is what we are tuning our model for. And here we're trying to be as safe as possible, in the sense that if we flag a domain name as malicious, we want to be reasonably sure that indeed it was a malicious registration. So we optimize for precision, even to the level where some of the malicious registrations are not found.

But if we flag a domain name as malicious, but it's really registered by a normal internet user for normal purposes, what's the bad things that happen extra here? This is what we call a false positive. So it's predicted as malicious, but it's really benign. In that case, as you saw on the previous slide, the registrant is invited to validate the registrant data. We have a number of mechanisms based on EID, bank payments, and that kind of thing that allow the registrant to very easily verify the registrant data. So even in the case of false positives, it is not the worst thing that happens to the registrant. It's a very simple process than to go through the motions and prove that you are who you said you were.

Next slide, please. So where can you use this thing? We have it in what we call a post-registration pre-delegation setup. The system kicks in after the domain name is registered, but before the domain name is potentially deployed into the zone file, which means if we don't delegate, the domain name can't be used. So the abuse is actually not possible at all, which is the good thing. Another possibility would actually be to do with pre-registration. So not allow the registration if the prediction is that the domain name registration would be a malicious registration.

First of all, your system would have to be fast enough to actually be able to do that. But secondly, there is a risk that if you have a false positive

where you're saying this domain name registration would be malicious, so you do not allow the registration, you're basically impeding the first come, first serve principle, hence the reason why we decided to let the registration go through. But before the domain name goes live, so pre-delegation to actually do those checks.

Another possibility is post-registration, post-delegation. So for all the normal domain names that are in the registration database, you could use this system to actually detect if any of those domain names that potentially have been registered 10, 20 years ago, if they are malicious, yes or no. But at that moment in time, there is a vast amount of other information that is available that makes this far easier to see if a domain name is malicious, yes or no. Content of the websites is obviously an example there. And lastly, a very interesting project that we are currently looking into is Cross TLDs. We see similar abusive patterns within different extensions. So we are talking here today about .eu and its three scripts, but that's all still with the same registry.

But what we do see is that the same bad actors actually also register malicious registrations within other extensions. So it would be interesting to see what kind of intel, what kind of information, and what kind of gain can be found by actually joining that information. And that is exactly what we're doing at this moment in time. We are working with other ccTLDs within Europe to actually come up with a joint system where the registration information of those different registries are fed into one central system to be able to pick up better on those abusive patterns. Obviously, at that moment in time, one aspect that comes around the corner is GDPR, data privacy, because at that moment in

time, you're actually feeding one system with registration data of different jurisdictions and different registries.

And that is something that we solved by anonymizing the registrar data. And I give you an example there. My name, Peter Janssen, is mapped into a technique called MD5 hash. Doesn't mean anything to humans. What is important to note here, it's one way. From Peter Janssen to that random looking string is easy. Going back is next to impossible. And actually, what is interesting is, contrary to humans, machine learning models don't care if it is Peter Janssen or if it's C103CE and so on and so on. It only wants to see certain patterns. And I'm coming to the end for those that are pushing me to shut up now. I think we're on the last slide anyway.

So what we're doing here is seeing if we can make this even better in recognizing abusive patterns by going across different TLDs without going to special hoops in privacy-related information. Because basically, the information that we feed into the system is random as far as human beings are concerned.

Next slide, please. I think I was at the end of the slide. So thank you for your attention. If there are any questions, I'm happy to try to answer them.

NICOLÁS CABALLERO: Thank you very much, Peter. This is fascinating indeed. Sorry to interrupt you, but for the sake of time, I think we'll be able to take only two or three questions at the most, and we've got to make sure we allocate sufficient time for the Hamburg meeting. Sorry about this,

Peter. Thank you so much for that detailed explanation. Do we have any quick questions or comment in the room or in the chat room? And I see none. So with that, back actually to you. Is it Susan or Karel? Karel, I'm sorry. I'm sorry. Karel, go ahead, please.

KAREL DOUGLAS: Thank you, Nico. This is Karel Douglas, Trinidad and Tobago GAC. And thank you so much for your invitation here. I know we have a couple of minutes left, so I'm going to be very brief. I did have some notes, but I think it'd be easier for me just to speak off the top of my head. So just going back, and the slide or the picture in front of you would give you an idea of what we had on the 11th of June, which was our capacity building day. The reason why we have this capacity building day is really to allow persons who are new to the GAC, and maybe those who are not so new, to know what the issues are and to be able to understand the issues and contribute to those issues, and really to have as many people as possible contribute.

So for this day in particular, we focused on the DNS abuse issues. So two issues I want to say. The DNS abuse is one, and also the public comment process. So the public comment process, of course, is the consultation process that is employed when we consider issues. So it was important for us to ensure that GAC members understood the public comment process and the steps that are taken in that regard. And also, the issue of the DNS abuse. And we had fantastic presentations from the community. And I must say, we had fantastic presentations on the process. And to marry those two issues, those

critical issues, we decided to have breakout sessions where participants were broken out into different groups by language.

So we had five groups, and it was French, Spanish, Arabic, Chinese, and English. That's important. And the idea was that persons would now have an opportunity to discuss amongst themselves in the language groups issues that are pertinent to them. So coming out of that, and I know we're tight for time, we had volunteers. Critical deliverable was the fact that we now have five persons who are volunteering to assist in the public comment process concerning DNS abuse. And we, of course, in those breakout groups, a couple of things that were discussed were the process itself and also the issues of DNS abuse. So those same two issues. And I might just segue to one of the questions that were asked as to the definitions.

And that was a topic that we spent some time on because the issue of reasonableness and prompt and somewhat vague, but we did understand or explore the issue and know that those issues tend to be defined in the particular circumstance. So obviously, when it is a life or death scenario, reasonable or reasonable time or prompt may be amount of seconds, whereas when it's not life or death, it may be amount of weeks as the case may be. So this would explain why in some cases the definitions are broadly construed so that it will apply according to the case as the case may be.

This picture before you, my last point, is actually the breakout session. We have Nigel, I see there, in the English group. This is basically what we had a couple of days ago and having those conversations. And

hopefully this will transcend to a document and our contributions on the DNS abuse issue on the contract.

Future, and I'll just end with this, the capacity building workshop is held by, under the underserved regions working group. I'm one of the co-chairs along with Paul Hunter and we have support from Tracy Hackshaw and others. In this case, certainly, US government, Susan Chalmers. So we certainly want to have others in the future, not just on DNS abuse, but others. And it's really to bring everybody into the fold so you feel comfortable making your contributions. So thank you very much and I'm sorry if I ran through that.

NICOLÁS CABALLERO: Thank you very much, Karel. Unfortunately, we won't be able to take any questions at this point, so I'll give the floor to Susan Chalmers from the US. Susan, please go ahead.

SUSAN CHALMERS: Thanks kindly, Chair. So I will be brief. ICANN has opened a public comment process on the proposed contract amendments and comments are due on July 13th. This date is fast upon us and we have an ambitious timeline, as you can see here, to prepare the GAC's input. So the process should go something like this. First and immediately, beginning today, we're going to solicit input from GAC members and observers on a Google Doc that will contain guiding questions, which we had sought to get to today, but unfortunately, I believe we've run out of time for that.

The small group, the volunteers that Karel had mentioned, and thank you to those volunteers, will develop a first draft based upon this input and then quite simply, the draft will be circulated to the GAC. The small group will review and adjudicate the input and the red lines and circulate a document for consensus in time for July 13th. So in sum, we welcome the participation of all GAC representatives. Please do join us in contributing to the GAC's contribution to the community's important work on this issue.

NICOLÁS CABALLERO: Thank you very much, United States. Laureen, would you like to add anything?

LAUREEN KAPIN: Sure. Microphone. Yes, if we can just go to the next slide. We are out of time, but Nico has kindly granted a short, small five-minute window just so we could all say, plant seeds. We won't get all of the sprouts and blossoms now, but we will have time during the GAC communique drafting to also discuss this further. So these are the seeds I want to plant for you to think about. Considerations for the public comment process. What in your view are the positive aspects of these amendments? I think there's been really some good discussion on that already. The question of enforceability. It's great to have language, but the rubber hits the road where it's enforceable, so consider this language and its enforceability.

Thoughts on the proposed definition of DNS abuse, and this is like the three bears, Goldilocks and the three bears. Too broad, too narrow,

sufficiently flexible, just right. Thoughts on the role of the ICANN advisory on the amendment, because that provides some really good guidance information that might be viewed as a document that will evolve as compliance gains more experience with these scenarios and considers what might be useful in terms of guidance, and is it sufficiently informative as to some of these terms that have already been discussed, like reasonable, like prompt, like actionable, and escalation paths. Who is responsible for doing what? What makes sense in the particular circumstances?

Next slide, and I'm sorry if I'm speaking too fast for the interpreters. I hope I'm not. And then, because this has been signaled as the first of many steps on this complicated and evolving topic, the issue is also important to think about what comes next, and an idea that has been discussed and I think endorsed also by many folks within the ICANN community is the idea of very targeted, specific policy development processes on very particular issues.

For example, you could have a PDP on what is the best way to deal with phishing, for example. What should be appropriate responses? This is by way of an example. So you can consider what might the subject matter of future policy work be on the topic of DNS abuse, and also not just what it should be, but when should it be? Should it take place before the next round of new gTLDs, or not necessarily?

The role of public interest and registry voluntary commitments, we just heard about that in the discussion with the board. The important issue of how you deal with recidivist bad actors, registrants, registrars, registries that are havens for illicit activities. For registrants, of course,

it could be the actors who are engaging in illicit activities, and what would be the ideal timing for these issues? This is not a complete list. Again, it seeds to plant in your minds, ideas for further discussion for the potential GAC public comment. So I leave it to you to do some hard thinking about this, and I know everyone will join in making sure that the GAC contribution here is as strong and thoughtful as it can be.

NICOLÁS CABALLERO: Thank you so very much, Laureen, and thank you to Susan, Carol, Chris, who's not here anymore, and Russ and Peter. That's certainly food for thought for the GAC, but we need to close the session. Any quick question or reaction? And we need to be really quick. If not, then the session is closed. Thank you so much. We'll adjourn. And actually, we'll need to stop for about five minutes in order to reschedule. Rob, correct me if I'm wrong. Please go ahead.

GULTEN TEPE: We are ready to continue, Nico.

NICOLÁS CABALLERO: So our next session is on emerging technologies. The session goals are basically to create a list of technology topics the GAC, the committee, would like to learn more about and suggest priorities and preferences. That's the first one. The second one being to identify and discuss options for informational frameworks the GAC could best use to share information or content in the future. And thank you again. Thank you again, Karel, Susan, Laureen.

So the basic idea was to create a list of technology topics. The background is that in planning discussions for the ICANN77 public meeting, GAC members expressed a desire to identify and discuss topics involving new technologies that will or would influence or impact the DNS and the internet in the future. So the initial topic suggestions we have so far are three, alternative DNS route, blockchains, and artificial intelligence. And again, the idea here is to identify and discuss any other additional topics. I understand we have some suggestions from Chinese Taipei. Ken-Ying, I don't know if you would like to go ahead now. You have a presentation or is just an oral briefing to the GAC? How would you like to proceed?

KEN-YING TSENG: Thank you, Chair. I can briefly present my thoughts and the reason why I proposed this topic. First of all, I think everybody in this room should already notice that emerging technologies have become the hottest topic in recent years. Maybe for the past two years, Web3 and blockchain has been very popular. And starting from the end of 2022, chat GPT has become very popular and artificial intelligence has been dominating all of the technology discussion around the world. So that's why I'm proposing that for GAC and ICANN to consider whether this emerging technology would in any aspect affect the DNS system and whether we should look into any of the issues.

For example, for artificial intelligence, I think Peter's presentation shows a very good example because it seems that ICANN or other related parties have already adopted artificial intelligence in combating DNS abuse. So I think we could think more in that regard, whether

artificial intelligence would either influence our cybersecurity threats or it could also be the other way around. It could help us to prevent cybersecurity issues or DNS abuse activities. That's my original thoughts. Thank you.

NICOLÁS CABALLERO: Thank you very much, Ken-Ying. Do we have any questions? Any comments? Any reactions to Ken Ying's briefing? If not, let me give the floor to -- Please move on to the next slide, Gulten. And I understand this is for Alisa. Julia, go ahead.

JULIA CHARVOLEN: I'm sorry. Yes, we do have a hand raised from Kavouss Arasteh from Iran delegation.

NICOLÁS CABALLERO: Iran, go ahead. But please, please be brief and to the point. Go ahead, Iran. Iran, the floor is yours. Iran, the floor is yours. Could you please go ahead?

JULIA CHARVOLEN: Now we have Ana Neves from Portugal delegation on the line.

KAVOUSS ARASTEH: Excuse me. Do you hear me now?

JULIA CHARVOLEN: Yes, we can hear you now, Kavouss.

KAVOUSS ARASTEH: Thank you very much. I'm sorry. I asked that what do you mean by alternative DNS? Thank you.

NICOLÁS CABALLERO: Ken-Ying, would you like to take that question? He asked what do you exactly mean by -- what you meant by alternative DNS, right? That was the question.

KEN-YING TSENG: Thank you, Chair. I believe that alternative DNS means the other type of web identifier that is not the normal identifier that we are used to, that is through the ICANN system. I think for Blockchain or Web3, they have their own web identifier, which is similar to our own, our current system with layers, but they do not go through our registrar and the registries. That's my understanding, but perhaps the other GAC representative or any other participant here would have broader knowledge than I have.

NICOLÁS CABALLERO: Thank you very much, Chinese Taipei. Netherlands, please go ahead, Alisa.

ALISA HEAVER: Thank you. On alternate DNS route or alternate naming systems, I kind of prepared three questions and -- sorry, am I going?

NICOLÁS CABALLERO: No, no, go ahead, because I had Portugal. I'm sorry, Portugal, I didn't see your hand, but we'll go ahead with the Netherlands and then I'll give you the floor. Sorry about that, I didn't see it. Sorry, go ahead, Alisa.

ALISA HEAVER: So to Kavouss's question, maybe we should go to -- I believe there's a question prepared in a poll. So I hope all the GAC members are in the Zoom room and they can answer the question in the poll, and that was kind of going towards Kavouss's question. What alternate DNS route or alternate naming systems are? And thanks. There is the poll.

NICOLÁS CABALLERO: Thank you very much, Netherlands. Portugal, I'm so sorry. Go ahead.

ANA NEVES: No problem. Just be prepared to hear me in Portuguese, of course. I'm going to speak in Portuguese. I'd like to mention -- well, I'm waiting for the others to use headphones for the interpretation. I'd like to support, entirely support, Taiwan's intervention as well as the Netherlands' intervention. It's fundamental to have any kind of capacity building to understand the impact of emerging technologies on the DNS. It will be very interesting here, this in the GAC, and to be able or have the possibility of perceive what this impact is about. These emerging

technologies are important. We need to understand the impact in the future, and it would be necessary to have this discussion here in the context of the GAC sessions.

NICOLÁS CABALLERO: Next I have Nigel Hickson from the UK, and then I have the WIPO. Go ahead, Nigel.

NIGEL HICKSON: Yes, thank you, Mr. Chairman. Well, I will defer just for a second back to the Netherlands in case there's more for Alisa to impart, having done the poll.

ALISA HEAVER: Sure, happy to continue, but I don't want to step on Brian's intervention here.

NICOLÁS CABALLERO: No, no, you're good to go, Netherlands.

ALISA HEAVER: Do we have the results of the first question? And I'm hoping that people filled it in just before having heard of Kavouss's question. So we have 53%, I believe I'm reading, that have heard of it and 47% no. And well, if this is mostly answers of GAC members, well, basically half of the GAC has never heard of this. The second question we could go towards. As you're seeing, I'm trying to build up to something.

NICOLÁS CABALLERO: Which is perfectly okay. That's the idea of the whole session. So go ahead, Netherlands.

ALISA HEAVER: Do we have the second question coming up?

JULIA CHARVOLEN: This is Julia from the GAC support team. We do have the second question up.

ALISA HEAVER: Thanks, Julia. Maybe in the meantime, while people are answering the question, we could either go to Nigel's intervention or Brian.

NICOLÁS CABALLERO: Thank you, Netherlands. Brian, please, the floor is yours.

BRIAN BECKHAM: Thank you, Chair. Good afternoon, colleagues. Brian Beckham from WIPO. In relation to this topic, I wanted to mention a couple of things I think which would be of interest. This fall, this September, we have our eighth WIPO conversation on IP and frontier technologies. We have a frontier technologies division which is looking at the intersection of AI and IP and discusses some of the topics that are being discussed here. We have on our website an archived version of the seventh

conversation, which was specifically focused on blockchain and NFTs and IoT and metaverse. I can share links to those on the GAC list. In April of this year, INTA, the International Trademark Association, produced a white paper on NFTs, which included Web3 domains.

Again, I can share the link to that on the GAC list. I'd like to read one of the recommendations from this INTA paper. It says trust by consumers is required for Web3 domain names to gain mass adoption by consumers and brand owners. INTA, in collaboration with WIPO, could consider developing a global trademark dispute resolution policy akin to the UDRP that can be adopted for the emerging digital ecosystems of NFTs and the metaverse. Just to recall for colleagues, WIPO was requested by its member states in 1998 to produce a recommendation to the problem of the intersection of domain names and trademarks, often called cybersquatting.

The result of that process was the UDRP, which was ICANN's first consensus policy, and we've been managing that process ever since. Of course, you may recall that there is a planned policy review by ICANN of the UDRP, and we've provided briefings to colleagues on that previously. And concretely, I wanted to mention that yesterday at the IPC meeting, we announced that Namebase, which is one of the operators of these alternate root domains on the Handshake protocol, is voluntarily adopting the UDRP for trademark disputes in that particular alternate root. So we think that's a very positive development for brand owners, and hopefully that is useful to start further conversations in that regard. Thank you.

NICOLÁS CABALLERO: Thank you, Brian. Thank you very much. I have the United Kingdom and then China. Go ahead, please, Nigel.

NIGEL HICKSON: Yes, thank you very much, Nigel Hickson from UK GAC. Just really to emphasize, I think, the importance of this session. Obviously, we're not going to cover all the ground this morning because it's nearly lunch. But I think this really does, taking up the points that Taiwan and the Netherlands have made, point towards the need for a longer session in our next meeting in Hamburg. And I'm sure that we have the responsibility as vice chairs and the chair and others, of course, to schedule this if the wider GAT thinks this is appropriate.

I think, in particular, this area of alternative DNS root and blockchains is very important. Obviously, artificial intelligence is important as well. But I think the first two items are more, perhaps, more germane to us at the moment, given their significance. And what Brian Beckham said and others, I think, has to be taken into account as well. So thank you.

NICOLÁS CABALLERO: Thank you, United Kingdom. I have China, and then we'll go back to the Netherlands. And then, if we have any more time, we'll -- I'm sorry about that, Ola, but it's just the way it is. China, please go ahead.

GUO FENG: Thank you, Chair. Guo Feng from China, for the record. So this session, I find this session is interesting. But with regard to the organization of this kind of session, if we are going to have additional the same session in the future, perhaps in Hamburg, I suggest that perhaps we may want to invite some of the IT experts or technology people to our session to explain the technology with regard to those topics. Because we, as a GAG, most of us, I think, are policy people. So perhaps this is my suggestion at this moment. Thank you.

NICOLÁS CABALLERO: Thank you very much, China. Well noted. But the idea at the beginning was to identify possible topics, develop a reasonable agenda, and then see if the GAG actually wants to move on with this or not, because it's up to us in the end. Now, if we agree on that, then we can develop something a little bit more structured. And sorry about the lack of time at this point. We only have five more minutes. Netherlands, go ahead, please.

ALISA HEAVER: Thank you. Well, already perfect. The results are up. I'm seeing a lot of low, so some medium, and a few high. So most people say they don't know that much about it. And we could go to the next slide. Yes. Well, I'm definitely not going to read everything on this slide, but it really basically says what alternative route DNS is. And I would just like to point my colleagues to an Okta report from April 2022. I thought it was a really good report, and that kind of sparked my interest in this topic.

And so I prepared actually a third question. Do you want to have capacity building on this topic? But it seems kind of already answered by all the interventions, and so feel free to answer it. But my suggestion was, well, to, with this, briefly introduce the topic and let everyone read about it. And hopefully, most of my colleagues will have read this report before the session, and we can dive deep into the matter. And I'll leave it with that here.

NICOLÁS CABALLERO: Thank you very much, Netherlands. Again, I have Switzerland. Jorge Cancio, please be brief and to the point, we're running out of time. Go ahead, Switzerland.

JORGE CANCIO: Yes, Nico. Jorge Cancio, for the record, very brief. Just in case the GAC is interested about artificial intelligence, what the Council of Europe and other countries are doing, your predecessor, Thomas Schneider, is chairing the corresponding committee at the Council of Europe. He would be interested or happy to come over to the GAC at some point of the future, if you have interest. Thank you.

NICOLÁS CABALLERO: Certainly. That would be awesome. That would be certainly good. So with that, anything else to add, Netherlands?

ALISA HEAVER: Well, maybe one last thing is that I yesterday briefly spoke to John Crane, the CTO, and he would be more than happy to help us with the capacity building workshop. So I think that's really good news. And I hope everybody will attend it. Thanks.

NICOLÁS CABALLERO: Thank you, Netherlands. And finally, I have my distinguished Vice Chair, Ola Bergström from Sweden. Floor is yours. Ola, go ahead.

OLA BERGSTRÖM: Thanks, Nico. So I think we covered the first part now on the topics. I think there's a lot of interesting topics we need to dig into. You can have the next slide. I think now going into the how, which is also a very complex issue, of course. I think we have a lot of options on different approaches, different tools, different how often should we do this, and also what we already have and on our kind of options.

I think that we need to have a discussion on what would fit. I don't think we would need to find a solution that would fit all. So I think we need a flexible approach to have different kind of tools and approaches to fit the entire GAC community. And we are definitely interested in your input, but we don't have the time to dig into that issue in detail at the moment. But we'll come back on this.

NICOLÁS CABALLERO: Absolutely. Thank you so much, Ola. Any final question? Any final comments? Any reactions in the room or online? Gulten? Julia? No? Anything none?

GULTEN TEPE: We have a call from Chinese delegation.

NICOLÁS CABALLERO: China, China, go ahead.

GUO FENG: Thank you, Chair. Actually, I want to chime back a little on the topics we perhaps initially identified with regard to this session. I believe the second topic is about blockchain, but perhaps I want to perhaps add the element of NFT. Perhaps some of you know that. It's non-fungible token. I think it is based on the blockchain and it is a particular perhaps identifier because DNS is an identifier system. I think NFT is particular the case perhaps we want to look at. Thank you.

NICOLÁS CABALLERO: Thank you so much, China. And NFT will definitely be added. Non-functional tokens will be added to the list. Any other reaction, we're two minutes away from lunch. But any final comment? Any other feedback? If not, let's -- Julia, are we okay? Everything all right? All right. Thank you so much. Merci beaucoup, obrigado, muchas gracias. Enjoy your lunch. We'll reconvene here at 1:45. Goodbye. Thank you.

[END OF TRANSCRIPTION]