ICANN79 | CF – GAC Discussion on DNS Abuse Mitigation
Monday, March 4, 2024 – 4:15 to 5:30 SJU

GULTEN TEPE: Welcome to the GAC Discussion on DNS Abuse Mitigation Session on Monday, 4th of March at 20:15 UTC. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior. During this session, questions or comments submitted in the chat will be read aloud if put in the proper form. Please remember to state your name and the language you will speak in case you will be speaking a language other than English. Please 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 GAC Chair, Nicolas Caballero.

NICOLAS CABALLERO: Thank you very much, Gulten. Welcome everyone again. It's a pleasure to have such a team on stage today. A good friend of mine, Alan. We also have Martina Barbero, Susan Chalmers from the USA. We'll have Nobu Nishigata from Japan who will be joining us online. Laureen Kapin, of course, and my distinguished GAC Vice Chair, Mr. Nigel Hickson from the UK. And we'll also have Leticia Castillo from ICANN Contractual Compliance. I'm sorry, I need some coffee at this time. And as I mentioned before, Alan Woods from CleanDNS. The session will be running for 75 minutes. This is, as a matter of fact, our last session of the day before the welcoming reception hosted by .pr, which I hope you will be able to attend. So without further ado, welcome again. Let me give the floor to Mr. Nobu Nishigata from Japan. Nobu, the floor is yours.

NOBU NISHIGATA: Thank you very much, Chair and colleagues. This is Nobu Nishigata speaking for the record. And I hope you had a good coffee and a good morning from Tokyo to the distinguished delegates. And don't ask what time it is here. But I'm telling you that tonight or this morning to me, it has been very worthy spending the whole night up here. Let me thank everybody who helped make this happen. Notably, the guest speaker from the Contractive Party Houses and the panelists as well who organized the session from the GAC side. And also, we had a great session where we had a break. And I'd like to give a huge thanks to Leticia and Jamie for their presentation and their time.

So yesterday, as we discussed the GAC strategic plan, we shared that the DNS abuse is one of the priorities for us. And as it is written in the draft plan, we had to be mindful of that ever-growing nature of the DNS abuse. And it is very unfortunate, though, but it is getting really a threat to our public safety. So in this session, we will start by the presentation from the PSWG co-chair, Laureen. And she is going to provide the real evidence of what is taking place with respect to the online frauds in the United States. After that, we will invite the CleanDNS presentation by Alan on the measurement of the DNS abuse. Then, yes, we touched on some issue of the measurability during the previous session with the

Contracted Party Houses. And then I believe that the presentation will give us some hints on this matter.

So my colleague, Susan, will moderate that part of the session. And then we, the GAC, will discuss our action to the DNS abuse this year and in the future. So it is our turn to discuss what we can propose to the community or our actions or their actions to mitigate DNS abuse. So it has been a collective effort. And then my colleague, Martina, will moderate the part of the session. And we, the colleagues, really would like to hear what you think there. And so before the drink, please raise your issues. And then we are keen to hear what you think. So without further ado, then let me invite Laureen to please take the floor. Thank you.

LAUREEN KAPIN: Thank you so much, Nobu, especially at the probably very, very late or wee early hours of the morning. My name is Laureen Kapin, and I'm speaking in my capacity as one of the co-chairs of the Public Safety Working Group. And I am also proud to be wearing my agency hat today. I work for the Federal Trade Commission. I'm an Assistant Director for International Consumer Protection. And I'd like to tell you about our 2023 fraud statistics. Just briefly, the Federal Trade Commission is a civil law enforcement agency. We prosecute civilly unfair and deceptive practices. We go after all sorts of scams.

And we also have this wonderful database that collects complaints from all over the country from law enforcement, from private consumer protection organizations, and even some international data contributors. It's called our Consumer Sentinel Network. And every year we publish a summary. And that's what I wanted to share with you today. I want to make clear that this summary does not tell you about DNS abuse specifically. It talks about things that relate to DNS abuse in part. But it's more a big picture of what type of frauds we're seeing across the US. Some of which is facilitated by DNS abuse. So here on the slide, is our scammy snapshot of 2023. And you'll see we have 2.6 million of fraud reports. That's an all-time high in the United States. And the dollar amount lost also an all-time high, @10 billion.

For comparison in 2022, it was about a billion dollars less. And also, a million less reports. So that is quite a significant increase. Our top our top subject areas are imposter scams. And of course, an imposter scam can facilitate phishing. It can facilitate a business email compromise. And the imposters can be impersonating government agencies as well. And you'll see the other categories there on the top of the slide, including complaints about online shopping, prizes, sweepstakes and lotteries, investments. That's actually a category that's really surged in business and job opportunities. You'll see in that orange box that in 2023, folks lost $4.6 billion dollars to investment scams and a lot of those related to cryptocurrency investment scams. And that's because it's a hot area that people don't understand very well. So that has surged.

I also want to draw your attention to the business imposter scams because that has also really surged for 2023. 752 million dollars in losses and our own agency is subject to imposter scams. In fact, someone from my office is often impersonated and then he gets consumers calling him and then he has to report that as a complaint. So my point is it hits everyone and everyone can be ripped off. These people are really good at what they do. And if you think you are too smart for it, you are wrong. The people are very, very good at these scams. I also want to draw your attention to contact methods. Email has generated the highest number of reports for contact methods. And again, that relates to topics that that we handle in terms of DNS abuse, because emails can often be the communication device for a phishing attempt.

Next slide, please. So, again, what I just want to underscore is that this is a new high, that investment scams are surging, that imposter scams are surging, too. And look at these numbers again. Anything important is worth repeating. $10 billion, $4.6 billion to investment scams, $2.7 billion to imposter scams. And in terms of payment methods, how are people paying when they're victims? Bank transfers and cryptocurrency are the methods of choice. And why is that? Because once you transfer money that way, it is usually gone, gone, gone. And it can't be reversed or it's very challenging to reverse.

Next slide, please. So in terms of the most common type of scam, again, it's imposter scams, followed by these other types of scams, which I've already described.

Next slide, please. Contact methods, we've already stated about email being the most common. And that is followed by phone calls and phone held the top spot for ages, followed by text messages. But if you're wondering of all those contact methods, what generates the highest losses? It's social media that generates the highest losses that as a contact method, perhaps because people may think they're dealing with someone they know. Look at imposter scams and then some online activities. Again, that brings us back to the topics that we're grappling with, online ads and pop ups and websites and apps. That's the third highest dollar loss.

Next slide, please. I wanted to zero in on phishing because that's a topic that is specifically defined as DNS abuse. Over the past year, our agency has received over a thousand reports and nearly a hundred in the last month. And in terms of the dollar losses, over 2.2 million in the last year. And in terms of the top product or service, business imposters, but government imposters are up there too in the in the top five categories. So we have some consumer education. That's the little box you see. And you yourself may be experiencing this. I know I am. A lot of text messages or emails about your FedEx package. There's something that's gone horribly wrong. Please respond and give them all your personal information. That is a very common scam these days.

Next slide, please. We also take in international information, not just information from folks in the US, but people from other countries who are complaining about US companies or complaints from the US where they are zeroing in on foreign companies. And that's through our eConsumer.gov portal. And you'll see that those top scams are similar to the same ones we have just seen as part of our regular data, although they're in a slightly different order.

Next slide, please. And then also just for folks who are curious, we have a whole bunch of publicly available data on our FTC.gov website for the consumer. If you are interested, for example, not in just contact methods or dollar losses, but if you are wondering what about the age of the victims, we have data on that too. So, for example, ages 30 through 39 and 60 through 69 are the people who report fraud the most. But in terms of who loses money, that is the 60 to 69 age group.

Next slide, which I think is our last slide. This is just some references for you. We have a lot of data on our website. We have this whole data book for 2023, and we also have a lot of information that you can look at in real time where you can compare this quarter to last quarter, contact methods, age groups, dollar amount loss. It's a very nimble system. It's in our data and spotlight section of our website. I'm happy to talk more with you about this one-on-one if you're interested and tell you more about our resources. Thank you.

GULTEN TEPE: Thank you, Laureen.

NICOLAS CABALLERO: Thank you so much, Laureen. Let me pause here and see if we have questions in the room or online. Any question for Laureen? Any comment? Any feedback? I don't see any hand up, which means that -- Sorry, sorry. Nobu, Japan. Go ahead, please.

NOBU NISHIGATA: Well, thank you very much, and thank you very much for the presentation, Laureen. This could be a silly question, but if possible, could you give us some imagination of how much the DNS abuse or DNS abuse technology, whatever you may call it, is going to facilitate or contribute to the damage that you count in your country? Thank you.

LAUREEN KAPIN: We don't measure our statistics in an exact match between the categories of DNS abuse and our complaints, but what I can say is that the FTC data tells us that many times complaints are facilitated by email and by websites. And of course, that has a direct relationship to DNS abuse, especially when it relates to phishing, but I can't say that there's an exact match because we don't measure our complaints in an exact parallel to, for example, phishing, farming, botnets command and control, the exact categories of DNS abuse. But that is why I presented a slide on our complaints that mentioned phishing, just to give you a flavor of the fact that phishing is definitely a topic that consumers are complaining to us about and are connected to some of the frauds that we see.

NICOLAS CABALLERO: Thank you, Japan. Thank you, Laureen. I have India. Please go ahead.

T. SANTHOSH: Thank you, Laureen, for the presentation. T. Santosh, for the record. So, I would like to know whether there is a trademark infringement of the domain names, which is happening in the US. Trademark infringement of domains.

LAUREEN KAPIN: I'm sure that that is happening. I couldn't give you statistics on that off the top of my head. And indeed, unless it relates to fraud, our agency wouldn't necessarily be the primary agency dealing with that, but it definitely occurs. And this, of course, relates to imposter scams, where an entity is pretending to be a legitimate business to try and grab your financial information or your personal information to steal your identity, et cetera. So there's definitely a link.

NICOLAS CABALLERO: Thank you, India. Thank you, Laureen. I have a question for you, Laureen. I like very much the way the information is presented, the graphics and everything. So I assume you have a fantastic data analytics team. How many people do you have there working for you, just out of curiosity?

LAUREEN KAPIN: Well, they don't work for me, but we do have a fantastic data analytics team. And I actually had a detail in the division that does all this. We have five to 10 people who work in our data analytics, and they are fabulous. They're data scientists, they slice and dice. But a different team does our graphics. We have a consumer education and outreach group that makes sure we can present all our data in a way that people find it easy to understand. So it takes a village and we are fortunate to have a great one at the Federal Trade Commission.

NICOLAS CABALLERO: Thank you so much for that, Laureen, and we'll have a conversation about that later on for sure. Any other question or comment in the room or online? I don't see any hand up. Rwanda, please go ahead.

CHARLES GAHUNGU: I just want to know, in the range you reported about the age of 60 to 69, what do you think is the main reason of that big number specifically in that range?

LAUREEN KAPIN: Sure, and this is speculation. But people who are older tend to have more money. So if they have more money, they're a more alluring victim, and you have the possibility of losing more money if you have more money. Younger people, our statistics show they may be a victim more often, but the dollar amounts are lower. We hear heartbreaking stories about people losing their life savings, their retirement savings, and the older people have more assets to try and steal, unfortunately.

NICOLAS CABALLERO: Thank you, Rwanda, for the question. Any other hand up? I don't see any online or in the room. So back to you, Susan.

SUSAN CHALMERS: Thanks, Nico. I'd just like to pass it over to Alan Woods from CleanDNS. Now we'll turn back to DNS abuse and have a presentation on measurement.

ALAN WOODS: Thank you very much, Susan. Alan Woods, for the record, and I am the General Counsel of CleanDNS, who is anti-online harms. I would like to say anti-DNS abuse, but we're trying to broaden that into an anti-online harms company. I will apologize in advance to the interpreters. I am

Irish, therefore I tend to race when I speak, so I'll try and slow down as much as I can. I'm very fortunate to have followed that presentation from Laureen, and thank you very much for that, because I think the important thing that the DNS abuse amendments specifically have dealt with over time is we are trying to move away from looking at absolute reporting and absolute measurements.

And we're trying to look at a little bit more of the qualitative assessment, the impact of the harm, not just the numbers that might or might not be causing harm. And I think that's a very important starting point when we're talking about the measurements of DNS abuse, especially after the following through of the contracted parties and ICANN in putting together these new DNS abuse amendments. I think what we need to be thinking about as well is that new term. Not only is it about stopping, it is also about disrupting and reducing the possibility and the time to live of abuse as it is occurring to prevent the victimization and the impact to victims, as Laureen has so very capably demonstrated with her presentation.

So we go to the next slide, please. Thank you. I have taken the basically what to me and to CleanDNS are three very crux points of the DNS abuse amendments and you've heard these terms. And these are very important as we look to measure DNS abuse and measure the impacts of the DNS abuse amendments. So the first one is that concept of actionable evidence. What is actionable evidence? What is the evidential threshold? There must be an evidence in order to take action. You can't take action on something that is not evidenced and I think that is the very important starting point for the approach of the contracted parties.

But the question we have now looking forward is how are we going to record, how are we going to verify and how are we going to ensure that that actionable evidence is available uniformly or indeed readily available, which is the words that you will find in the advisory from ICANN compliance.

The next question is that idea of prompt action. What is the prompt action? Because this is a very subjective viewpoint. How do you measure promptness when it comes to a response to DNS abuse? And from our point of view, the promptness should be very hand in hand with the concept of the impact to the victim, the impact of the abuse and making sure that where there is a very large impact that there is a more prompt response and it's probably a more appropriate response by somebody who is at the domain name level as opposed to looking at perhaps the hosting level or another level.

So again, the question that we are all faced with is how do we effectively measure promptness that is very subjective at scale? And then the final one, of course, is this stop and or -- sorry, stop or otherwise disrupt. So again, in this highly subjective viewpoint, how do you measure what is an appropriate action at a domain name level? Is it a suspension? Is it a server hold? Is it a client hold? Or is it disruption? Is it doing what you can at that point with the information that you have in order to prevent the harm from occurring? Even if that means that it doesn't actually remove the content at the end of the day, which we all know a registry cannot do or a registrar cannot do. So disruption is a very important word. And where can you give credit where credit is due? I'm being told I do need to speak slower. So, apologies.

So can I go to the next slide, please? So let me look at the state of play on a few of these things to give you an understanding of where we're at and why this is a new frontier for us in measuring. At the moment, the major metric that we see for dealing with DNS abuse is looking at reports, reports made. We look at block lists, we look at providers and they have hundreds of thousands of domains being listed as being reported for DNS abuse. But you must remember that a report does not mean that that abuse has actually occurred. There is some sort of quantitative and qualitative analysis that needs to be done on that report to make it into an actual evidenced report or as it says in the abuse amendments, an actionable report. It needs to be actionable.

So technically at the moment, what you see is lots of reports of domains, not why they were reported, not what evidence is allowed with those domains. And the percentage of those reports versus that of the actual top-level domain or the registrar zone is then created this ratio, this percentage of bad domains and tracks the health of the domain. But it's very difficult for a registry and a registrar to accept this because it doesn't tell the response. It doesn't show the mitigation actions. It doesn't say how has a registry, how has a registrar reacted to this report. It just says there was a report.

And I think that's an important thing to remember for these new amendments. We can't just measure the number of reports. We have to measure how also they were dealt with. So you'd see in the red at the side there, I think it's important that as a baseline expectation of how we're looking at the effectiveness of the DNS abuse amendments is that we need to look at the number of substantiated reports with evidence.

And this must be the expectation of the community, not just every report, the ones that are actionable.

If I can go to the next slide, please. I want to give a kind of an example of this that CleanDNS ourself has seen. And this is redacted to an extent, but I want to show from one particular source that is very often used within our industry. Over a six-month period, about a year ago, we measured specifically the amount of reports that were received. You will be able to look at this a bit more in depth in your own time. However, the main thing I want to point out is that of over 200,000 reports from one source in a six-month period, only about 9,000 of those reports were capable of being evidenced with an awful lot of work enrichment by CleanDNS.

So the amount of noise that we had to scrape through in order to pull out actual evidence of these reports was immense. So my point is, if you are measuring the health of a domain based on the number of reports and you're not taking into account how many of those reports are actually actionable at the end of the day, it's an unfair metric. So that's what we're trying to do is change that kind of that narrative and saying an actionable report must have evidence and only those actual reports should be the ones that the metrics focus on. So you'll be able to see this in your own time. Yeah, Nico.

NICOLAS CABALLERO: Let me stop you right there, Alan, and thank you so much for that. I have a question or a comment from Iran. Please go ahead. Iran, please go ahead. The floor is yours.

GULTEN TEPE: Kavouss, we cannot hear you.

KAVOUSS ARASTEH: Yes, thank you very much. Yes, Gulten, allow me just I have to put the microphone on. So I need some 10 seconds. Please kindly be patient. Thank you very much. You said about 200,000 only 9,000. What is the problem? Why this actionable evidence is not provided? What are the missing information? How we could inform the people to provide more actionable evidence? You said that continuing for 200,000 to reach 9,000 is a lot of work for you. I hope somebody does not tweet misinterpreted what I said. I'm not criticizing you at all. I'm criticizing ourselves. What is the problem? What is the missing information that they made a mistake and submit something without actionable evidence? What we can do that? Thank you.

ALAN WOODS: Thank you very much, Kavouss. And you're absolutely right. The what is missing there is we in this industry. We did not start with sources or expectations for really the domain name industry. We have used sources that were available that tended to support action by the domain name industry. So what we are trying to do and what the DNS abuse amendments, I believe, have tried to achieve is to look specifically at making better reporting, make better expectations on the domain name industry registries and registrars in order to provide us with that evidence from the beginning.

Because as soon as we have that evidence, if we have to actually dig down for evidence, as opposed to getting evidence at the very beginning, it increases the time that this domain abuse, if it is occurring, from impacting the victim. So what we need to do is encourage better reporting, better measurement, and better evidence at the beginning. So I completely agree, Kavouss. We need to create a better expectation of evidence as well in the reporting, not just in the harvesting after a report.

KAVOUSS ARASTEH: Excuse me, may I have a follow-up question with the chair of the GAC?

NICOLAS CABALLERO: Absolutely, please go ahead.

KAVOUSS ARASTEH: Thank you very much. Could you provide some criteria, some advice, some guidelines, something that some people like me does not bother you, sending something without actionable evidence. I like these two words very much. I use them even in the ITU. That's saying any interference should be accompanied with actionable evidence, but not bothering the people that you distorted me without giving any actionable evidence. So what can we inform the community to provide a better report? It is not their mistake. It is their misunderstanding or unawareness or misinformation. I'm talking of myself. I don't think that somebody should tweet and reverse my intervention. Please kindly say that what you can do to better inform the people to provide you a more actionable thing. Thank you.

ALAN WOODS: And thank you, Kavouss, again. Now, the point in my presentation is not to be a platform for CleanDNS is wonderful, but what we are trying to do is make the reporting process far more user-friendly, far more easily achieved. And one of the things that we have helped out, and I believe I see [inaudible - 00:32:10] and Graeme Bunton in the back of the room from the DNS Abuse Institute. NetBeacon is something which CleanDNS provides the backend for, and it is intended to be an easy means by which we report. Not only is it an easy means to report, but it also takes you through what is necessary for the report that you are making. What is the evidence that should be attached? Not even who you should be sending it to, because that's what NetBeacon will do.

So there's that element. All our clients who use our ingestion feed for abuse management also takes through this, as I call this, choose your own adventure reporting, where it takes you through step by step what is necessary. And also, if you are making the report to the right provider, because sometimes, of course, people will just go to, I've typed into Google, this person is associated with this domain, but it might not be the correct place to report. So if it was a very large social media platform, if it was a platform that is being misused, the registry is probably only going to be able to pass that on, which is, of course, under the new amendments, point of disruption, pass on that report.

NICOLAS CABALLERO: Thank you, Graeme, for the question. Thank you, Alan, for the detailed and accurate answer. So why don't we let Alan finish his presentation and then right at the end, we take some more questions and comments. So please, go ahead.

ALAN WOODS: Thank you very much. I'll skip over maybe one or two slides, because I would ask you and encourage you to look at these slides. And we have a booth right outside, and I'm there. So just come and talk to us, and we're happy to fill in the gaps. So if you could perhaps move on to the Time to Live slide. Thank you very much. I want to do a shout out to SSAC 115. And for those of you who have not read SSAC 115, I would absolutely encourage you to read that. I was also an invitee on SSAC 115, so I don't want to be self aggrandizing in that. However, in SSAC 115, one of the important things, again, speaking slowly, one of the important things is ensuring that the time to live, that is the uptime of that measurement, is being properly measured.

So it needs to be considered that the faster the response to reports made, the less impact to people it will have. So I do worry that when we're thinking about how we will enforce compliance of these amendments, that we're looking at complaints made as being the point. When in reality, we need to be looking at systemic abuse, those domain name registries and those domain name registrars who are being absolutely non-responsive to potential high impact. We should not be seeking to only focus on reports made of the very large registries or the very large registrars who are actually being responsive.

We need to focus on rooting out those elements within our community who do not respond, who have a large time to live on DNS abuse and who are not responsive at all. That is the point of the DNS abuse amendments. So we do need to measure the qualitative, not just the quantitative. Look at the efforts that are being made in response. Look at the ways in which these things are being thought about by the registries and the registrars. How are they be proactive? How are they being reactive? What is their subjective objective? I know that's a lot, but how are they subjectively reacting to abuse as it occurs?

So if I go to the final slide, now this is an awful lot of text, so I will not explain this, but well I will explain it. That's the point. So to answer the questions that I posed at the beginning, actionable evidence. How will we measure actionable evidence? And to go to Kavouss's point, we need to create and agree minimum evidential thresholds and set evidencing standards. And that goes to absolutely everything such as the reporting standards. What are you looking for in the reports? Making it easy for reporters to understand, but also to take sources that give you that evidence. Let's not rely on sources that do not give evidence. Rely on better sources. Prompt action.

Again, I will ask you to look at SSAC 115. We're looking at basic contractual requirements. So prompt action already is spelled out in that as 96 hours. But again, the subjective aspect of that where the harm to the victim is higher, well then we suggest that, that number should be lower based on the subjective response. And there needs to be a way of measuring in that instance, why did you come to the decision to only respond within a certain amount of time? And that needs to be measured and it needs to be measured effectively. We're talking about good record keeping in response to DNS abuse simply.

And then finally, the stop and otherwise disrupt is can we seek clarification from contracted parties on a case-by-case basis or in an audit as to why they took an action in a particular way or indeed why they didn't take action in a particular way? That is also another important point. It is not always appropriate for the registrar to take action, but what did they do to disrupt? What did they do to help the victim at the end of the day?

Now, I don't want to take too much more time on this. I encourage you to come and talk to me, but there are a lot of questions that hopefully we can help answer. Hopefully we can help measure and please do look to us that we are going to be bringing out an awful lot of how we believe that this can be measured, how we believe it can be dealt with and how we can help the community in making these DNS abuse amendments exceptionally successful when it comes to reducing the impact to the victims of harm.

NICOLAS CABALLERO: Thank you so much for this, Alan. Now, let me open the floor for questions for CleanDNS. Any comment, any question in the room online? I see one hand up and that is Iran. Go ahead, please.

KAVOUSS ARASTEH: First of all, Nico, let me thank you very much for the agenda that you have set and for the invitation that you have made. That we are talking, I think, with the most urgent and I would say important constituencies and so on and so forth. This is the first point. I'm not complimenting you. I'm just giving what I think on the bottom of my heart. But now, I think we need to have a better communication with the government, government community in one way or the other. Perhaps you cannot describe all of them in the community, the meeting you have tonight or the other day. But perhaps we should think of some other tools.

One of the important tools for you, Nico, which always looking for some innovation for some innovation is that to craft a sort of the circular describing the important issues or government, the point that they have to pay attention, referencing them to the brief in the communiqué, but providing more information from what we have seen during these four or five days. So we need to have a better communication with the GAC community.

Some government, they know very well. Some other government, they may not be aware or may not have the time to go or they may not have sufficient awareness to understand what is going on. So I leave it to you perhaps to think it over. Maybe you find a way how better communicate with the government in order to increase their awareness. I'm not saying that teach them because we are not teaching anybody, but just increasing the awareness of the people. Thank you.

NICOLAS CABALLERO: Thank you so much. Number one, for the compliment. Number two, for the suggestions. Kavouss, do you have any specific question for CleanDNS or for Alan at this point?

KAVOUSS ARASTEH: I don't have. I just appreciate very much. I don't have, but I'm thinking that the issue is more, I would say, complex than what we thought and so on and so forth. So we should not have a unilateral understanding. We should understand each other mutually. Now we understand better the one side, but we as a government or the other side also understand what you have to do. And we need some information, some better, I would say, awareness and information to be sent to the people. May not be useful for some, but they're useful for many others. Thank you.

NICOLAS CABALLERO: Thank you so much again, Iran. Julie noted I have Japan and then the UK. Nobu, Japan, please go ahead.

NOBU NISHIGATA: Thank you very much, Alan. Thank you very much for the presentation. Very helpful. My question and my comment is that as a government people, one of them just an annotation, the Kavouss mission, like the ask the government people may incline to think about the prompt action or stop and then disrupt those kinds of things. But then just you gave me the good point about action or evidence. And then I have one question on this. And if there are any standards, just you, I'm looking at the slides, then is it developing the standard or is there already a standard that the government people can understand or that we should follow to make it more efficient, combat against the DNS abuse. Thanks.

ALAN WOODS: Thank you. Thank you very much for that question. So there are standards that are developed by people within the industry. And I think we need to look at the Registries Stakeholder Group have put out standards before they have worked on evidential standards and certain things. I will also point there was a PSWG collaboration with the contracted party specifically on botnets and what would be necessary for action and evidential standards and requirements and botnets. There are outputs from things such as the Internet and jurisdiction policy network group, but also the contracted parties are very much welcome, I believe, and I'm welcoming the challenge to work with people like CleanDNS in order to establish what are reasonable thresholds and evidential standards.

So our clients specifically have worked with us and they tell us what would be the point in which they believe they can intervene or they can escalate. And so we will continue to obviously create those standards. And we look forward to having those open dialogues, especially about standards as they apply to the community, but also having a realistic conversation about how those standards can be achieved and actions that can be achieved at the registry registrar and hopefully very soon at the hosting and other levels.

NICOLAS CABALLERO: Thank you, Japan, for the question. Thank you, Alan, for the answer.

NOBU NISHIGATA: Thank you.

NICOLAS CABALLERO: Japan, would you like to go ahead again?

NOBU NISHIGATA: No, I just say thank you for the answers.

NICOLAS CABALLERO: Fine. I have the UK.

NIGEL HICKSON: Yes, thank you very much, Mr. Chairman, and thank you so much, Alan, for the slides and the really interesting observations that you've made. And I think I'm not speaking for the whole GAC, but we need to see you more often, so to speak, and it's not just your Irish accent, but I think it really is informative what you have to share. The only question I had was on bulk registrations and whether you have any particular sort of observations there. It is something that the GAC has touched on before where bulk registrations are made and the veracity of those and whether they lead to more abuse than other types of registration, so to speak.

ALAN WOODS: Thank you very much. Again, Alan Woods for the record. I forgot to say that. Yes, I think bulk registrations, and also let's just put into the mix the concept of low-price registrations as being another thing to talk about. They can obviously have an impact on levels of DNS abuse, but to go back to my original point, that is the question of it's the response to that. So, if you are engaged in a pattern of you allow bulk registrations, but you have a strong response to abuse when it occurs, well, then that should balance it out, because abuse will happen.

A very interesting point that occurred recently enough that there was, we noticed an abuse trend on exceptionally high-priced domains, and they were both bulk and high priced, because whatever the output of the abuse campaign was, it was far in excess of what they were spending on the domains. But what I will say is there are good reasons for bulk registrations, because application-level uses of domain names also occur, and that is the best way of doing that is possibly bulk registrations. However, also, the impact is the final thing I'll make in that. If there are 100,000 domains being, and this is on one of my slides, but unfortunately, I have to go fast.

If there are 100,000 domains that are registered, but of that, none of them are actually evidenced as being used for DNS abuse or abuse at one time, versus there's one domain that has been up for five hours, and that has a fish of a US banking institution, where should the resource go in that to stop the one that's actively taking money from people or monitoring 100,000 domains that have done nothing yet? So I think we need to ensure that impact is an important aspect of how we monitor this. Those 100,000 domains may definitely show up. However, measuring that over the impact that, that one domain has is going to do a disservice to registries, registrars, and the entire community. So I will challenge us to think about the impact more than just absolute numbers.

NICOLAS CABALLERO: Man, we should have you more often around. I have Indonesia.

ASHWIN SASONGKO: Thank you, Nico. I don't know whether it is part of the internet problems, but what I want to know, because I'm very worried when I read about the statistics. People above 60 years old lost their whole life savings. I'm above 60 years old so I'm really worried. I don't want to lose my life-saving account.

Now what I would like to know is, has ICANN unit that looks after the statistic and those phishing, ever talk about this with the banking organizations and see together whether the two organizations can make some sort of policy network that may reduce the problem. For example, just an example, perhaps to get more than $1,000, then you must use your, what's called it, this one, hand. No, or ice or whatever, those kinds of things. Biometrics, biometrics, exactly. Thank you.

Now, these kinds of things that might be possible and above that, for example, maybe then you have to talk directly with your CRM and above that, you must go directly to the bank and see the person personally. Perhaps if the bank office is not here, the bank can also ask another bank as their partners to be able to talk with the person who would like to draw a million dollars, for example. Just basically how to set up a policy network together between ICANN and banking institutions. Thank you.

NICOLAS CABALLERO: Was that question for Alan specifically or for…?

ASHWIN SASONGKO: First of all is actually to have you ever talk with banking institution and after that what kind of possibilities between IT regulations and banking regulations together to make sure that no more 60 years old and above people lost their life savings. Thank you.

ALAN WOODS: So if I may answer, Alan Woods for the record as well. So number one, I would just point out that the ICANN Octo team are absolutely wonderful, John and Samana. We are talking to them and they are developing and creating new statistics that really are going to be going to the crux of what we're looking at and things that also I look at the DNS Abuse Institute as well, the Compass, where they're not just looking at these absolute numbers, they're looking at the mitigation. So that's the first thing I would say. They're not at the table, but a shout out to them working and moving with the times. Yes is the answer.

CleanDNS specifically, we are talking with, we're not just relying on the same old sources such as the one that I pointed out there. A great source for its purpose, but not for our purposes. We are talking with banks, we are talking with government departments, we're talking with basically anybody who can give us a good evidenced based report so that we can get that to not only our clients, but to other registries and registrars outside of our client base in order to get that time to live as small as possible. Because the best possible sources are the people who are seeing the abuse impact to them as well.

So if we can get better reporting from the banks, we can get better reporting from telecommunications providers, from registries, from registrars with that evidence, then we can absolutely make an impact. So yes, we are definitely talking with them. And I'm putting the shout out there to any government here who has information and reports such as this, but they're not being made. Please come talk to CleanDNS for outside. We would love to have as many reports as possible so we can reduce that TTL for both clients and non-clients.

NICOLAS CABALLERO: Thank you for that, Indonesia. Thank you, Alan. And just in case, I don't mean to put you on the spot, John, but I spotted John Crane in the room. So just in case Indonesia, if you need to talk to him, he's right there. So having said that, let me give the floor to India.

T. SANTHOSH: Thank you, Chair. So as mentioned in the DNS abuse and also mentioned by Alan, that there are various standards. IETF comes with various standards like DNSSEC, IPsec, BGPsec. So what is the status of implementation? Can ICANN mandate this standards, which will protect the internet users from this abuse. Second question is, so this DNS abuse, which CleanDNS has made the presentation, it is about the domains which are made through Registry Registrar Network. What about domains created to DGAs or with Tor network? Is CleanDNS looking into that aspect as well? Thank you.

ALAN WOODS: You're not making it easy on me today. So the first question that I want to ask so the first question about DNSSEC, I am a lawyer, but at the end of the day, I think that's a very important conversation, specifically as we look to minimum standards within the ICANN community. We must remember that we were raising the floor. We were not looking at best practices.

So I'd ask you to think of two things. One is the raising of the floor. We do not need to pile on too much to meet that minimum standard, but have those conversations about benchmarking, have the conversations about perhaps generally accepted practices or best practices. And I think there is definitely a conversation there. I would look to the members of the SSAC and people with regards to DNSSEC because I know it's had a rocky few months, unfortunately.

So again, lawyer talking, so I'm not going to delve into that, but conversations need to be had. But in the right fora, I think is important in that one. The second one about DGAs. Yes, absolutely. I think one of the things and one of my team is actually working on it at this moment is being able to ensure that we are being very mindful to known DGAs and also being mindful to discuss and work closely with law enforcement. We know that law enforcement specifically have their fingers on the pulse of many DGAs as they occur, but maybe the means by which they are getting to providers such as the registries and the registrars are tied up in a lot of legalese and red tape.

Again, I would suggest look at the Registries Stakeholder Group paper that was done in conjunction with the PSWG and implement that across a much broader spectrum. And then please come to people such as

CleanDNS who are helping registries and registrars react to these and become reporters, have more law enforcement directly with us. Now a little plug and I'll stop, but we are also working on a specific law enforcement portal where we can give access to law enforcement to report directly to us again for our clients, but also that we can report that onwards. We can't guarantee any response to non-clients, but at the same time where it is our clients, we will bring it to them and we will have that conversation. So again, we are outside. Please do talk to us if you have such things. We want it because we want to make this faster, better, more evidenced.

NICOLAS CABALLERO: Thank you, India, for the question. Thank you, Alan, again for the detailed answer. We'll take one more question. That is Papua New Guinea. And then I just want to make sure we allocate enough time to Martina, to the European Commission and to the USA for their presentation. So please go ahead, Russell.

RUSSELL WORUBA: Thank you, Chair, and thank you, Alan, and distinguished colleagues. Just an observation and a comment. Our colleague from the US Trade Commission made it very clear that the issue now in cyber is more towards cyber safety as being an issue. And governments from our region are focusing a lot of attention into more so on cyber safety than cyber security as a subset, if I can put it that way. There is a growing capacity building movement under the global GFC, which they are doing. I'm just curious whether you have an engagement at that level where we make DNS work here mainstream as being a cyber safety effort. It's just a comment and a question. Thank you.

NICOLAS CABALLERO: Thank you, Russell. Please be brief and straight to the point, Alan.

ALAN WOODS: I will say yes. We are trying to engage in that. And I will give a shout out to a well-known name, Christopher Lewis Evans, who is now working as our Director of Government Engagement at CleanDNS. And you all know him and love him. So please call him, email him, text him, and we will be happy to be engaged more in that.

NICOLAS CABALLERO: Thank you for that. And with that, let me give the floor to the European Commission. Martina, please. Sorry to keep you waiting. The floor is yours.

MARTINA BARBERO: Thank you very much, Nico. I think this was a very, very good discussion and warned us up for what's coming next. If we can go back to the main presentation and slides on possible future developments. Here we go. Thank you. I think we have heard two excellent presentations, well, three actually with compliance and Alan and Laureen today. And this feeds into our reflection as a GAC on what could be possible future developments. What you see on the slides is actually some bullet points that were extracted from the comments that the GAC submitted to the public consultation on contract amendments last July.

So these were areas that the GAC highlighted in its response to the public consultation as areas of importance in which the community needed to, to which the community needed to pay attention and notably in terms of proactive monitoring and enhanced transparency, inevitable evolution of DNS abuse, recognizing the need to address DNS abuse inside and outside ICANN. And then specifically, there were a few ideas for possible policy development processes regarding guidance on key terms, due process considerations, setting threshold to trigger policy response and then training as well.

So those were some of the thoughts that the GAC had at the time. I think they're still quite relevant given the time we just spent discussing what is actionable evidence and prompt response. So these are some still a hot topic, I believe. And those were areas that we could we mentioned at the time as area for possible community work and for reflection. So in fact, what we wanted to do, and we're going to go to the next slides very quickly, is to have a brief discussion, which I think we already initiated with Alan and with the input from Laureen, to respond to these two questions. So by when should the GAC expect to be briefed by compliance on the progress made under the DNS abuse amendments?

And then we would like to hear from you. And here we are in listening mode, acknowledging we are the last thing or almost between you and the reception. So we will try to pick your brain before leaving, letting you go to the reception. But if you can share your thoughts on any prospective policy development process building upon the foundation created by the contract obligations. And I think what Alan highlighted as well is that the contract amendments about the threshold, like raising the bar. And then there's also this work about best practices and benchmarking that we can consider. So with this, I finished my presentation and just wanted to hear if any GAC representative has anything to share at this stage. I think you already shared quite a lot, but it would be interesting to respond to this question if possible.

NICOLAS CABALLERO: Thank you so much for that European commission. As a matter of fact, I think it was kind of short after listening to Alan, now I'm joking, I'm joking. So let me open the floor again for questions or comments in the room or online, any hand up, any feedback, any comment you would like to give at this point? I don't see any hand up online or in the room, which -- I'm sorry, I have Switzerland, go ahead, please.

JORGE CANCIO: I think the mic didn't want me to take the floor. Jorge Cancio, Switzerland for the record and just to break the ice, I was just reflecting on the first question. If I understood it correctly, the amendments into force in April. So it would make sense to wait perhaps six months to have a first reporting and it would of course be very valuable if the reporting would be also iterative, well, that it could be evolving through time with the inputs from the community where we need more data points. So more feedback, but that's my first answer.

And on the second question, perhaps we need also more, still more discussion also with colleagues from the community. There's an opportunity, of course, in the bilateral we have with the GNSO Council to see how they are thinking about this, where they stand by now. Thank you.

NICOLAS CABALLERO: Thank you very much, Switzerland. Before I give the floor to Susan Chalmers, to the USA, any other reaction? Sorry, that's Susan precisely. I'm sorry. Go ahead, USA.

SUSAN CHALMERS: I just raised my hand in the interest of time, though I really sincerely would encourage further input from any other GAC representatives on the two questions on the screen. Well, I think what we heard, I'm just keeping in mind the presentation that we heard from compliance earlier, which had said that they will provide reporting on a monthly basis, if I'm not mistaken. And so I think we're going to have to rely on that. And I think six months, as Jorge mentioned, is a reasonable timeframe to be able to see any reflection of progress under the amendments. I just wanted to bring that up.

I also think that earlier today, since I'm trying to create a thread through all the discussions on this topic that we've had today, we heard from Chris Despain during the contracted parties, how it's bilateral, that there does need to be time in their opinion for a measurement to take place under the new amendment. To be able to have a discussion on future work. So the future work needs to depend on the results of the work that we've just established under the contract amendments, I believe is the message.

NICOLAS CABALLERO: Thank you for that, US. The floor is still open for questions, comments, any feedback you might want to give at this point. I see the UK, please go ahead.

NIGEL HICKSON: Yes, thank you, Mr. Chairman. And just very briefly, it's been enormously useful. And I think our distinguished colleague from the US is absolutely right in that a thread has been drawn through a lot of our discussions. I suppose I just want to not put a contrary view so much as to just say that we do need, I think in light of what we've been hearing about, especially from Laureen and in terms of the statistics in the US and I'm sure in many of our countries as well, if we looked at the statistics of abusive registrations and what is happening on the ground, then it doesn't mean to a great picture.

And I suppose we just have to have in mind that although of course we need to assess the evidence from the steps that are already been taken, we also need to consider that we might need to do something in terms of policy development on botnets or phishing or other issues in due course and perhaps start at least thinking about what elements would be suitable to do further work on. Thank you.

NICOLAS CABALLERO: Thank you for that UK. Any reactions to that? Laureen, Martina, are we okay to move on? Perfect. I have next, I have Michele Neylon from

Blackknight, and then I have Iran and the European Commission. Michele, please go ahead.

MICHELE NEYLON: Thank you, Michele Neylon for the record. I think there's a couple of things that I think it's interesting that you're looking at the future, which makes a lot of sense. But I'm not sure if six months is going to be sufficient. And part of that is the reason for that is that these contractual amendments are specifically related to registrars and registries. They do not have any impact. Do not touch on ISPs, hosting providers and other parts of the ecosystem.

What that means in practical terms is when you see some form of online harm, a bad thing on the internet that involves a domain name. If the registrar is not hosting the website, the email service, the thing that's causing issues, the only option they have is to either take action, which is to take the domain off the internet completely, which will kill all other services associated with it or not take action. You don't have a scalpel, you have a sledgehammer.

So the thing that people need to understand is that yes, with these amendments, registrars and registries, as Alan articulated very well, ones that were not doing anything up until now will be obliged to do certain things. But this is not, as we say, this is not a silver bullet. This will not fix all online harms. And many of them are issues that are completely out of scope. Now, there are many things that governments can look at doing. There are many things that other providers within the ecosystem could look at doing, but not all internet issues can be solved by registries and registrars. Thank you.

NICOLAS CABALLERO: Thank you so much for that. Blackknight, Michele. I have, and thank you for the reference to Sledgehammer, one of my favorite songs, by the way, from -- Anyways, I have Iran and then the European Commission. Iran, please go ahead.

KAVOUSS ARASTEH: Thank you very much. My understanding of the time for the briefing is progressive briefing. It's not definitive. I think six months would be a reasonable period, and then you would receive something, and that would be complemented afterwards, so on and so forth. So the reason I've asked question, I have to raise my hand is not this one. The reason was that, do we have a list of the countries or entities they have reported abuse? I would like to know that among the 206 or 208 countries and territories, how many they have already reported? One or two or three countries would not be taken representative. We should see a full image of the situation.

And then we should look, if those countries who have not reported anything, does it mean that there is no abuse, or they don't know how to do it, or they have some obstacle, or so on and so forth? It would be good, if possible, to have a list of those countries, or at least regional ones, saying that in region X, Y, Z, whatever way is possible. I don't want to point myself to particular country or countries, but I would like to know the percentage of those community countries, entities that have reported that abuse. I know many countries that can tell them that they have not reported. Doesn't mean that there is no abuse. Not reporting does not mean absence of abuse. I would like to know at least where we are. Thank you.

NICOLAS CABALLERO: Thank you for your comments, Iran. Well noted. I have the European, unless you want to react to that. Laureen, please go ahead.

LAUREEN KAPIN: Just very quickly, I think Kavouss raises a really important point about, do people know who to report abuse to? Whether it's to ICANN compliance, whether it's to the registrar, or the hosting provider, or some other entity who has primary responsibility. And I think all education efforts and outreach that the community can do on that is really important, because I think we get a very partial perspective, whether it's at ICANN or even from my own agency, we get a partial perspective because we know these things are vastly under-reported. It's a tip of the iceberg. So any education and outreach efforts we can do to let people know where they should report these issues to, I think is crucial.

NICOLAS CABALLERO: Thank you for that, Laureen. European Commission, please go ahead.

GEMMA CAROLILLO: Thank you, Nico. This is Gemma Carolillo from the European Commission for the Records. First of all, in solidarity with Nobu also here, it's late evening, I would say, nighttime, but I will not take the competition with Japan for sure. Greetings to everybody from Brussels. So I wanted to congratulate for the organization of the sessions, because I think we have had a very high quality conversation and the very informative presentations, including from ICANN compliance. So where I think we got part of the answers to the questions for the discussion.

So it is also my understanding that the reporting will be done regularly and perhaps even earlier than the six months expected. I understood that this is monthly reporting. And then of course, I think as the time goes by, there will be more evidence collected. So the reports will be progressively more informative. The other element I wanted to underline is that I think from the presentation that we got from CleanDNS, there are references to several of the elements that the GAC has highlighted as topics for work. So this is the second question.

So first of all, key information from Alan, so that the harm suffered is very often more important than the numbers. So it's not about necessarily the number of reports. It's important seeing what's been the harm suffered. And in this case, one very big phishing campaign can produce significant harm. So this is not only about the number of reports in terms of metrics. And second, the fact that we are navigating for the tools that are at hand and also for the history about what sources have been used to track down a DNS abuse. I have heard a highly subjective environment. So since the objective, it's preventing harm from occurring because in the end, it is important to disrupt abuse and it's important to prevent to the extent possible harm from occurring.

I think we got inspiration about the need to have conversations about minimum standards, about benchmarkings, so that there is a clear information about what it is that is actionable evidence. How is it possible to obtain actionable evidence? How is it possible that this actionable evidence allows to prevent harm from occurring? This was one of the points from the GAC submission to the public comments. And also to the fact that the numbers, so the number of reports would not necessarily express the health of status of a domain, of a TLD, and hence that the quality of the reporting can be improved if there is clear information about how reporting should be done. And this is also a topic which is linked with transparency.

I am not perhaps saying anything new. What I'm saying is that I kind of found comfort that from the presentations we heard today, we found lots of references to the topics that the GAAC had proposed as issues for further work. And I also echo what some colleagues have said that the importance of the issues as also shown by the excellent presentation from Laureen is such that we should continue this conversation and see how these relevant conversations about minimum standards can be achieved pretty soon. Thank you very much.

NICOLAS CABALLERO: Thank you so much, European Commission. We're at the top of the hour. We need to wrap up the session. I'll close the queue right now. Regarding the first question, as a matter of fact, I just wanted to give my personal opinion. I really think that we should be briefed on a quarterly basis. This is my personal opinion. That would be four times a year because in times of big data, things tend to happen very fast and at a big scale, so to say. So anyways, this is just my two cents on the point.

Two important things. Tomorrow, we'll be having at nine o'clock the open microphone session. Sorry for the housekeeping details. But so be prepared because we will hear directly from the community. As a matter of fact, any kind of question. So be prepared. That's one thing. The other thing is that I heard some rumors about some good Puerto Rican beer tonight for the welcome reception, as well as some salsa lessons for GAC members. I don't know. We need to see how it goes.

So thank you so much, Alan. Thank you, Martina. Thank you, Laureen. And obviously my distinguished GAC vice chairs. Fantastic session. I'm kind of jealous about your data analytics team, Laureen. We need to talk about that because I would like something like that for the GAC, as a matter of fact. So maybe we should start negotiations and see how it goes. So again, enjoy your salsa lessons tonight and your food and enjoy Puerto Rico. Thank you so much. The session is closed.

**[END OF TRANSCRIPTION]**