ICANN76 | CF – GAC Discussion: DNS Abuse
Tuesday, March 14, 2023 – 10:30 to 12:00 CUN

JULIA CHARVOLEN: Hello and welcome to the ICANN76 GAC discussion on DNS abuse on Tuesday, 14 March at 10:30 local time. 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. If you wish to speak, please raise your hand via Zoom. 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. Please make sure to mute all your other devices when you are speaking. You may access all available features for this session in the Zoom toolbar.

And with that, I will hand over the floor to our GAC chairman. Manal Ismail, please.

MANAL ISMAIL: Thank you very much, Julia. Good morning, good afternoon, and good evening, everyone. Welcome back. This is the GAC discussion on DNS abuse mitigation, scheduled for an hour. During this session, we will continue GAC consideration of ICANN Org and ICANN community initiatives to prevent and mitigate DNS abuse.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

And we will also be briefed on relevant developments and continue discussing possible efforts by the GAC to engage with the broader ICANN community to support enhanced contract revisions and possible policy development processes to better mitigate DNS abuse.

So without any further ado, allow me to hand this over to our topic leads. We have with us Gabriel Andrews, US Federal Bureau of Investigation; Laureen Kapin, US Federal Trade Commission and co-chair of the GAC PSWG; and Chris Lewis-Evans, UK National Crime Agency and co-chair of the GAC PSWG. Over to you, Chris, please.

CHRIS LEWIS-EVANS: Thank you very much, Manal. Good morning, good afternoon, and good evening to everyone. Moving on to the next slide, please. We're going to do a session on DNS abuse and we've got an external presentation. I can see the Internet and Jurisdiction Policy Network Lead just in the corner, hopefully sorting out some slides with our GAC support.

So I'll do a quick introduction first, before that, and give us an idea of why tackling DNS abuse is important. We'll then have a presentation on cybercrime statistics and how they relate to DNS abuse. And then have a look at the other activities going on within the community. And then do a wrap-up and considerations for either communique advice or matters of importance for us. Go on to the next slide, please. Thank you.

I almost feel like I don't need to do this slide. We seem to talk about DNS abuse quite a lot. There's been some really good sessions already during this meeting. I'll do another shout-out for the capability-building workshop on Saturday. There was a good session for DNS abuse, which you can review on that.

On here, we have a number of links that you can go to. As always, you can do a search within the GAC website on DNS abuse and it will bring up items on the communique, which are support staff. Benedetta and the other support staff really keep that up-to-date. They do a really good job of having resources that we can search on there. So we have a number of items that we flag.

It's a very important part of the PSWG work as well. It's within our work plan, which we had ratified and endorsed this meeting, which was really good, for us to support the abilities of law enforcement and public safety officials to protect the public, which is really what they do on this.

As I said, there's a lot going on within the community so it's important for other stakeholders within the community. There's lots of discussions going on, Board consultations and correspondence. And the business community have sent quite a number around how it is important to them. There's also been review teams—so the CCT Review Team, RDS-WHOIS2, SSR2 to name a few—and also PDPs from the GNSO around Subsequent Procedures that touch on DNS abuse.

Then the other one, which we'll touch on later in the presentation, is the effort from the Contracted Parties. They sent a letter to the Board to open the contract negotiations to help tackle DNS abuse. That's a really good step. It just shows that everyone in the community wants to take action and it's really important to everyone, which is certainly why we've considered it for some time.

Then with that—and I'm going to just have a quick look at our support staff—are we close for the—

LAUREEN KAPIN: No.

CHRIS LEWIS-EVANS: No. Okay. So maybe, Gabe, a heads up here.

LAUREEN KAPIN: This is where we get to be flexible, and show that we're adaptable to current circumstances, and that we can pivot.

CHRIS LEWIS-EVANS: Yeah. Heads up, Gabe. You next. So we will go on to our presentation on cybercrime trends. So can we go on two slides, I think it is, in the pack? Thank you. Gabe, over to you. Thank you.

GABRIEL ANDREWS: Thank you. Hi. My name's Gabriel, speaking in my capacity here as a member of the Public Safety Working Group. What we hope to do here is something that we maybe are optimistic that we can do it on an annual basis later. But the reason for this is when it comes to understanding the scope and scale of DNS abuse, much like trying to understand the scope and scale of Internet crime, it's important to acknowledge that we don't have perfect facts. What we do have is a lot of different perspectives.

So like the blind man in this picture that you might recognize from the capacity building workshop—I used it there, too—we have a lot of folks who are all doing their best to observe what's in front of them, to talk about what they're perceiving, in the hopes that by collaborating, we can get a better idea of what's actually out there.

So here's where I recognize that there are a lot of great community efforts that are all aimed at providing data, metrics, measurements, observations on DNS abuse. And I'm thinking about things like the DNS Abuse Institute's Compass reporting that was started in fall of last year. Like ICANN's OCTO and their Domain Abuse Activity Reporting.

I hear that just in the conversation two days ago, maybe, with the executive staff, John Crain mentioned that in addition to what we're already expecting with registrar-level abuse reporting, he's got ideas about predictive analytics and machine learning that he wants to incorporate. I'm really excited to see what comes out of those efforts.

But to complement these community-driven efforts, we hope to provide additional perspectives that only law enforcement can bring to the table and that only come from public safety. I'm thinking in terms of the victim reporting that comes to us.

To be clear, we're not suggesting that all Internet crime is DNS abuse. Rather, it's our understanding that the scope and the scale of the victim harm that gets reported to us might be one of those perspectives that you might feel is important to consider in your deliberations, especially if we might be useful in some small way of helping to translate that reporting to how and where it does have connection to DNS abuse. And with that, I think, Chris, you have the first part of this.

CHRIS LEWIS-EVANS: Yes. Just very briefly, before we go on the next slide. Sorry. Can we go back one slide? Thank you. In our last PSWG meeting, we put a call out to all the members to provide us with some statistics that they have on cybercrime and how that may relate to DNS abuse.

At the moment, we haven't received any others than the US and the UK. So if you are engaged with your own law enforcement agencies or consumer protection agencies, then please feel free to give them a steer towards our direction. We'd be really keen to see what other countries are seeing and to be able to make this a little bit of a wider review on those statistics. And we look to do this for, probably on a once-a-year basis to give you an idea of the landscape.

Going on to the UK slides, in the UK we have a single reporting body called Action Fraud, who don't just do fraud. They do cybercrime as well. But the name was there first and then they've added on that remit.

Their top four collection statistics don't really track against DNS abuse. They have hacking, social media and e-mail. Viruses and malware, so the malware side, sort of, but viruses are in there as well so it doesn't really align with what we would understand as DNS abuse. And then hacking, whether that's personal or whether that's an extortion, which tends to be the more ransomware-focused material. So as you can see from this slide, data back from 2014 and a general trend upwards in the reporting of such crimes. Go on to the next slide, please.

One of the things they also do is put out surveys to businesses and charities to get an understanding of how they've been affected, what they're seeing, and how they're coping. This piece of analysis is around how many organizations have identified breaches or attacks on their systems. So fairly static, maybe a little bit of a downward trend on the business side. But very interestingly, on the charities, a definite rise.

Some of the thoughts behind this is charities, before GDPR, maybe weren't quite set up to look at their own networks and do analysis. Once you start looking for something, you tend to find it. So whether that's some of the reason for that increase, is that they're looking for it and they found it, or whether it's a rise in targeted attacks, it's very hard to say. It could be either so quite hard to tell. But just a little bit of trend there. And on to the next slide, please.

On this slide, obviously, of those that have suffered a breach, it was asked how they identify that breach and how the initial attack vector was. Across the years, the answer for that, 80-ish percent of the time, has been phishing. Phishing is definitely in the DNS abuse space. So you can see, from all that other crime that I had in the first lot, 80% or so is related to phishing, or the initial attack vector was phishing. So by reducing phishing, we can have a real impact on the harm being caused by the other crimes that we deal with on a day-to-day basis.

Then the second top one reads a little bit like phishing. But this is more focused on lookalike domains, and spoofed e-mails, and that side of things. That accounted for just under the rest of that. Obviously, some of those, there might be a bit of overlap as well. Next slide, please.

Same question to charities and a very similar answer. Again, 80% phishing. So really strong analysis there that if we can help DNS abuse and help tackle phishing, it'd have a really good impact on reducing the amount of crime that these businesses and charities are suffering. Next slide, please.

In the UK, we have a service called the Suspicious Email Reporting Service. It's not just ICANN that like acronyms. This was set up in 2020 and it's a service where individuals or companies can report suspicious e-mails into the government. There's the details there. They accept e-mail forwards and they also do SMSs because that's another big source of phishing reports. During 2022, we received 6.4 million reports into that service. So really large-scale. Lots of victims within the UK and people reporting those.

As I said, only launched in 2020, obviously as part of a response towards some of the activity that was going on during the pandemic. But since that launch, we've had 15.8 million reports into that service. And it is an upward trend but there's not really enough data at the minute to show that. So certainly, in the years to come, I'll probably be putting that on a nice little graph, no doubt.

Then, relating that to the government, what they can see from that reporting, obviously, is they're trying to pretend to be a governmental entity. So within those phishing attacks, they've had representations around our health service, our TV licensing, our revenues and customs, and then the gov.uk. So there's a site where we put out all our public information, whether that's advice what to do around COVID, travel advice. Everything is in there. And then the other one is the driver and vehicle licensing agency as well. So definitely a lot of governmental attacks and this service has been helpful to take some of those down. Next slide, please.

I touched on businesses. Now obviously, individuals and users of the Internet will also impacted by this and report crime into us. There was a telephone review of a number of the victims that reported into us to understand what was the impact on them from a financial perspective.

You can see here. It's a horrible graph. Sorry. This is what I was given. But you can see here a range between 20 and 250 pounds is probably the big thing of people losing. But when you think about that, that's not a lot of money. But then, we had 6.4 million, this year, people reported a crime. And if you say that each one of those lost even 20 pounds, 20 times 6.4 million is quite a good day's work or a good year's work.

So really large-scale when you look at that. It might seem a little bit. However, obviously, especially at the minute, with the cost of living crisis that we have in a number of countries, it's really impactful for people to lose this money. Next slide, please.

We talk a lot about money on cybercrime. And it's not just money that affects people, especially on individuals here. Businesses suffer data loss and it's impactful for them. But on an individual level, it can be really impactive and really upsetting to them.

I'm just going to go over a quick case study on this. We had some information received into our police system around a 17-year-old that reported a hacker was asking for more passwords and had access to a number of their social media accounts.

We were able to do some work off the back of that. We were able to identify the suspect, found that they had a history of hacking social media accounts of a number of individuals. So we obtained a warrant to visit his home address and found a number of active phones that he was using to commit some of these crimes. On those phones, there was evidence of mass phishing. Go on to the next slide, please.

This is an example of one of the communications. You'll see here that he represents to be someone that has found some information about an individual and says, "I found some images of you on a site. You might want to do something about it." The person comes back and says, "What's the link?" And then this individual posts a link for them to go to.

On reviewing the phones, we found hundreds of messages sent to young girls, generally, trying to get access to their accounts. So you see here, from one domain or one individual, he might have hundreds of victims. It's not an analogous thing, one domain, one victim. It could be one domain, hundreds of victims. And it all depends on the type of attack and the type of way it's being used on how that works. We also looked into that site, obviously, to see how this individual was using that to extort other people. Go on to the next slide, please.

This slide is going to be a bit busy, so I apologize in advance, and a bit small, but it's small for a reason. Top right of the screen is a phishing service hosted on the Internet that gives registered users the ability to buy phishing pages and to be able to have them on the Internet. So you click on one of those, whether it's Netflix, Facebook, Snapchat, or any of the other things. You can even select the language you want it in. So very small here but there's English, Spanish, French, and Russian, I think, all on there. So you can select the languages you want to appear on. You pay for that service.

And then, bottom left, there's an example of a Snapchat one. It will create a malicious domain that then you can attach to your message. That will then harvest the details for you. The bottom picture is an example of the dashboard that they create, that you can then go and see all your harvested credentials.

Obviously, once they harvest those credentials, that's where they start to do the extortion. They take the images that are stored on there, whether they're private, if it was a Google Drive, whether it's not even shared on social media. So this has real big impact on people.

We were able to take this site down with the support of the Registrars. So thank you for that. The individual involved is going up in front of court in the next month, but at the moment, is being remanded in custody because of the threat that he poses to the number of victims. On that, it's really important.

We obviously have tried to contact every single victim that we've been able to identify and been able to say to them we've secured their data, we've removed it, and to suggest that they update their passwords and everything else. It's really important to understand that impact to them. We've had so much, "Oh, thank you for doing that. I didn't know how to address it." And it's really key here on how do we address it and how do we remove some of this harm being caused.

Then, on to the next slide. I think I'm handing it over to Gabe.

LAUREEN KAPIN: I'm wondering where we are with respect to our colleague, Bertrand's, presentation. Are you ready to go? Would you prefer to go now or would you prefer to … What do you think?

CHRIS LEWIS-EVANS: I think we'll do Gabe's one because it follows on nicely. Then we'll stop back. Sorry. I do have one more slide. This is just a wrap-up of the business data and individual together. The most recent report was 2020 to 2021. Within the UK, they received 875,000 reports of fraud and cybercrime. Sorry. That should be both combined. That reports to 2.35 billion worth of losses in that report.

Then 80% of that fraud was cyber-enabled as well, whether that's from a phishing e-mail or otherwise. So a vast quantity of that loss is down to some form of cyber-enabled activity. And as we said before, phishing e-mails, 80% of that probably, so a really big enabler for criminals to use to initiate their cyberattacks. And that definitely is the last slide before I pass to Gabe.

GABRIEL ANDREWS: Can we see the next slide? Thank you. From the US perspective. And again, as Chris said, we really hope that there's other folks out there that can encourage your law enforcement agencies to share perspectives from around the globe.

The FBI just released, last week, its Internet Crime Report for the 2022 calendar year so this is hot off the presses. This is why, as well, that I think that being able to speak to this on an annual basis is a good thing because we like to be able to share this information when it comes out and while it's fresh.

This data is a summary of all the victim complaints that come into our Internet Crime Complaint Center. It's the centralized portal by which we receive and aggregate all of those figures. Then they turn around and then they publish reports based off of that. But to note, this is not a picture of all the Internet crime that exists. It's just that which is reported to us. Next slide, please.

Over the last five years, IC3—again, that's short for the Internet Crime Complaint Center—it's received an average of about 650,000 complaints a year. That averages out to just over 2,000 complaints a day so it's a fair number. But it still grossly under-represents the true amount of crime that's out there. We know that we don't get all of the complaints all the time.

One thing that's interesting to note here is that when you look at the number of actual complaints—those are the persons that reach out to us—it stayed relatively stable over the last three years, which is interesting. But the volume of the losses has steadily increased. I wish I had a good explanation for you as to why that is. We don't have a really great explanation of that at this time but it's definitely something that's interesting to note. It shows that the harm continues, even if the relative number of complaints stays stable. Please continue to the next slide.

As Chris mentioned within his categories of crime and how they aggregate it, we don't track DNS abuse as a category, either. But there are categories of DNS abuse which are tracked within our IC3 reports. And I note here in particular, at the bottom, phishing. When we look at the top five categories of Internet crime reported to us, we see that phishing is the top category.

What's more, because this shows over the last five years, you can see that for some reason or another, phishing has spiked tremendously from five years ago to where it is today, at least in terms of the complains that we receive. Next.

So this, again, is just showing all the categories of crime, not just the top five, and showing how phishing relates to them. Something to highlight here, as Chris has already mentioned, is that phishing, while it is tracked as its own category, it's often the initial method that the bad guys use to compromise the victims for a number of other categories of crime that exist here as well.

Just as an example, you might ask, "Is ransomware DNS abuse?" No. It's not. Ransomware is when a bad guy takes your data on your machine, and they encrypt it, and they don't let you get it unless you pay them a ransom. But if you ask the question, "Is ransomware spread by phishing?" the answer to that is yes.

There's a report that just came out last week on a new variant of ransomware called the Royal ransomware from CISA, one of my sister agencies. In this report, they estimated that 67% of Royal ransomware infections came from phishing. Again, we're tracking the initial category there but it has impact downstream.

Thus, just to belabor the point, when our friends, and collaborators, and colleagues in the ICANN community that exist at the registrar or registry level take responsible anti-abuse action to address maliciously-registered domains that are used in phishing , they are helping to address not only the most commonly-reported type of Internet crime that comes to us but also all of the other categories that are enabled by it. Next slide.

In addition to sharing those stats from the annual report, I did ask a number of my colleagues as well, “Hey, what’s the new hotness? What’s new, and upcoming, and trendsetting? What’s noteworthy in recent months?” What they came back to me with was something that they’re calling “malvertising.” For the benefit of the translators, this is a combination of malware and advertising combined together. It’s gotten a lot of attention, starting in about December of last year and well into the first few months of this year.

Like in phishing, the bad guy here obtains a lookalike domain name that’s registered for abusive purposes. Sometimes, they’re getting a domain name that might look like a software package, or some other trusted brand, or some service. But instead of using that in e-mail, rather, they go to the search engine providers and they buy ads.

In this case that you see on the screen here, this comes from Abuse CH. I took it from their Twitter feed. The bad guy in this case is pretending to have a site that is associated with the legitimate Thunderbird mail client. It’s a kind of software that a lot of people like. But obviously, they’re not just sharing it out of the goodness of their heart.

If you were to go to his advertising site there at the top, you would get that software plus malware on your machine—in this case, IcedID. It’s a form of banking Trojan. If it was installed on your machine, eventually it would capture when you logged into your bank, steal those login credentials, and then try to drain the accounts.

So this new trend, it's interesting because it still relies upon those maliciously-registered domains. Is it phishing, per se? Probably not because there's no e-mail connection there. But it still has the same end result. I call this out, one, because it's new; two, because it has direct nexus to DNS; but three, also because I think it's important to recognize that we have to be a little be agile and nimble in responding to the true world situations and be willing to incorporate these new trends into our ideas about what we can address.

But like before, the responsible registrars that take action against maliciously-registered domains are addressing this, too, and that's good. Next slide. And this will be my last slide.

I just want to really belabor the point. In English, we would say "beating a dead horse" here. But phishing is commonly-accepted amongst all of our community members here within ICANN as DNS abuse. It is also, as I just learned from our most recent reporting, currently the top-reported type of Internet crime. And phishing enables many other crimes.

Swift action against maliciously-registered domains and the incentivization that we can provide through our policies here for that, it matters. It affects what we see. That's my key takeaway and I appreciate your attention.

I think now that Bertrand is here to my side and ready, we can transition to him.

MANAL ISMAIL: Yes, please, Bertrand. Go ahead. And thank you very much to Internet and Jurisdiction for always reaching out to the GAC and keeping us posted of the work you do in relation to DNS abuse, which is obviously a topic of great interest to the GAC. Thank you.

BERTRAND DE LA CHAPELLE: Thank you so much, Manal. It's a pleasure to be back in the GAC because I used to be there as the French representative many years ago, including as the vice-chair of the GAC. I see a few familiar faces from those days. It's a pleasure to have the opportunity to present here.

I'm the Executive Director of the Internet and Jurisdiction Policy Network, which is an organization that I cofounded 10 years ago, now. And I'm very happy to come here and talk about this debate that has animated the ICANN community for several years and to indicate a little bit what we've been working on to help the debate go further and go toward solutions.

Internet and Jurisdiction Policy Network is … And Ajith Francis, who is in the back here, is the director of programs there. We're a multistakeholder initiative, bringing together governments, companies, technical operators, academia, civil society, and international organizations to deal with jurisdictional challenges on the Internet.

We have in particular—next slide, please—three programs that I will not belabor about the two first ones. But one of them is dedicated under the label domains and jurisdiction, to the question of precisely when is it appropriate to act at the level of the DNS to address abuses? And there is a contact group that has been working for more than five years now with about 40 people from the different communities.

I'm very happy to say that Manal has very kindly, and other people here, including Susan, have been participating actively in the work. I'm particularly grateful to her, given the high burden that she has, that she took the time to participate. It was important.

Basically—next slide, please—what is important is what we're talking about here, is how do we fight abuses that exist online? Those abuses are extremely diverse. The presentation just before me shows that the human ingenuity is absolutely without limit. Any way that we can misuse something will be misused. We all know that.

So the key challenge is that in most cases—and that's the second point—this is a transnational problem. It's particularly interesting to talk about this in the GAC because you are governmental representatives. I have been a governmental representative. And we all know that the reason why we have a problem addressing abuses online is because we do not have the cooperation tools between governments to act transnationally. We have an international architecture that is based on the separation of sovereignties and cooperation is extremely difficult.

One of the programs that we have is addressing cross-border access to electronic evidence. It is an extremely problematic issue and it takes years to organize due process between countries to conduct investigations using electronic evidence. So the problem we're confronted with is that not only is the network global, not only are the actors working freely across borders, but the tools we have to address this are not efficient and they're not here to facilitate intergovernmental cooperation.

The next thing is that in order to address those problems, there is a need to understand better how the Internet functions itself. When we're talking about the DNS system, there's a lack of understanding in many circles, that you're probably familiar with when you talk with colleagues, on how this architecture functions. If you want to understand how to reach out to a registrant, knowing how WHOIS functions, that you are going to find the registrar and so on. That's not something that is very easy.

The next thing, which is even more important, is that I was talking about the lack of tools but there is also a question of competences. The DNS operators are just basically making domain names available. They do not have any competence in examining, fundamentally, whether something is phishing, whether it is a malware thing, so they rely on notifiers. It's even worse—I'll come back to that later—when we're talking about content-related abuses. How do you manage to evaluate the legality of content of a patchwork of jurisdictions.

I'm mentioning resources because investigating any single cases—and it can be in the hundreds of thousands—takes time. This is a relatively slow and small-margin industry.

Bottom line is this is a problem that is a problem for everyone. It's a problem for governments because you are worried, legitimately, that abuses are not being tackled. It's a problem for businesses because they are also victims or they have a burden in addressing those things. And it's a problem for users.

So the next thing is we need to understand—next slide, please—something that is basic. You're all familiar with this but I want to share this that I share frequently with people outside of our own environment because they don't necessarily know exactly how the system functions. So the relationship between the registrant, the registrars, the registries, and the users; the queries that go from one to the other; and the roles that the different actors play in making the Internet that we know function the way we want it to function.

This is an architecture that I won't belabor on. The point I want to make is that there are only four actions that DNS operators can take regarding domain names.

The first one—next slide, please—is you can lock the domain. Basically, you cannot change the information that was provided by the registrant. You cannot have transfer, deletion, modification. And you cannot change either the server or the IP address that has been mentioned. Importantly, this action doesn't make the content inaccessible. Particularly, you can lock it. It's good for the investigation afterwards. But it doesn't change anything regarding the functioning.

The second element is you can hold. In that regard, you take the domain name, remove from the public TLD zone file, and the domain does not resolve. You cannot change the information, either, regarding the server. But here, again, the system still functions. If you use the IP address, you can still have access to the element.

The third element is redirect. This is often used for sinkholing a particular domain name when you want to conduct an investigation. It’s basically editing the zone file to redirect to another server to observe the behavior, identify the victims, and things like that.

The fourth element is transfer, when you put this to another registrar. This can happen when the registration has been done in a wrong manner at one particular registrar. But for whatever reason, there is an interest in putting it, for instance, to a registrar of last resort, which is something that Benedict Addis is very actively involved with.

The next slide is important because these are the four things. You can delete but I don’t belabor on delete because it’s not a recommended action for various reasons. The key question is, is acting at the level of the DNS, with only those four things, the right instrument to deal with the abuses?

The answer is yes, in certain cases, and no in others. It’s not the perfect panacea. It’s not basically what some people outside of our communities have a tendency to consider as a sort of big control panel. Like you have a problem on a domain name or attached to a domain name, you just flip the switch and the problem, it goes away. This is not the case but yet it is useful to have actions in certain cases.

So the key problems, or the key questions, are the following. First, it is an instrument that addresses not only the service of accessing a domain name site but also a lot of ancillary services. That can be e-mails, file transfer, and other things. So it’s a very blunt instrument.

Second thing is that it has a global impact. It's covering the whole world. You don't finesse. You don't geo-block the suspension of domain name. Here, it's interesting because you can see that as a feature or a bug. As a bug, it has a global impact so it is not granular. But when connected to what I was saying before, we lack the tools for international cooperation. Having something that has a global effect is beneficial in certain cases.

The next thing is, as I said, you can still access most of the services through the IP address. Next, you are in a situation where the DNS operators are part of a larger ecosystem. We need to take into account the overall architecture, including hosting providers, the ISPs, and other actors that can have also actions. Acting at the right level is the important one.

The next point is, currently, in the Registrar and Registry Accreditation Agreements with ICANN, there is an obligation to have points of abuse and to investigate, but there is a limited number of obligations that clarify what is really required and what is really necessary.

This leads to the situation that we have witnessed for a long period of time, which is there was and has been a protracted debate within ICANN, for many years, around particularly the very word "DNS abuse" and the definition of what it meant. People were having very different positions in that regard. So numerous sessions for several years around that. Criticism between the different constituencies on whether the definition is this one or that one. And even tensions within the different constituencies regarding how much action should be taken or not.

It's not to say that they are bad actors. We know there are bad actors. There are actors who are more responsible than others. But clearly, there was no way to move towards a consensus there. The result was this sense of frustration.

The bottom line is that if you ask the wrong question, you are unlikely to have the right answer, which requires to reframe the problem. Reframing, to the next slide, is that the real question is when is it appropriate to act at the DNS level to address abuses online? I think this is a formulation that can be agreed by everyone as a valid formulation that takes into account the different elements.

The next slide is … As part of this reframing, we've been working with the contact group that I mentioned earlier for a long period of time and narrowed down an understanding of DNS abuse, which we called at one point technical abuse. But with the help of some of the actors, we narrowed the notion that DNS abuse should be considered as those five things: malware circulation, botnets, phishing, pharming, and spam to the extent that it is used as a delivery mechanism for the above.

You can find more details about the definitions of those five things, first in the operational approaches that I&JPN produced in April 2019. That led to the incorporation of these definitions of DNS abuse in the Framework to Address Abuse that has been produced by a certain number of the actors within the community in December of 2019, and later on, the SSAC report 115 in 2021 that incorporated this definition of DNS abuse.

It may not be the perfect definition but it is a very important element to make a distinction between this, that we can call DNS abuse, that every actor is understanding has a reason to be investigated and is within the remit of the operators, from content-related abuse that I will address later.

It that context, we have produced—and I will not get into all the details—but a toolkit in 2021 that I encourage you to go and see online to help the DNS operators, the notifiers, and the legislators or the law enforcement to understand the different parameters and having guidance elements for convergence and working together.

The next slide mentions an important element which is there is workflow around four elements in dealing with any kind of abuse. The first one is basically identification of the abuse itself. It can be from notifiers or by the operators themselves. The second one is evaluation of this abuse. Is it indeed justifying an action at the DNS level?

The third one is what is the action that should be taken among the four that I mentioned? And the fifth one is something we haven't discussed yet but it is part of the landscape, which is what are the avenues for the recourse when there is a decision that has been taken and that has to be changed, for whatever reason. Mistakes can happen.

Without belaboring too much, for each of those stages, we have produced a certain number of things, like defining more clearly the types of abuses. Mentioning elements regarding what notifiers should be doing, in terms of due diligence, to document those elements. It's not sufficient to just throw a notice without any sustainable evidence to it. What are the conditions for notifying the registrant, particularly when sites are being compromised?

On evaluation, there is a key question of what are the thresholds, criteria for action? When is it necessary to meet a threshold? And choice of action. There are different types of action, as I mentioned. And there is a document that precisely explains the drawings that I showed you before. Finally, on recourse, there's the question of the channels for recourse and elements regarding transparency.

This is a process. Everything that is linked to investigations of trying to remediate abuse goes through different stages that involve the cooperation between the different actors. If I go to the next slide, in that context, the contact group has produced a series of documents that I hope will be useful for you as a community but are useful in the general debate.

The first one is about what should notices contain? What are the components for notices that support evidence? The second one is what are the types of notifiers? Is it the same to be a notifier for child sexual abuse imagery or for commercial trademark infringement, for instance?

The next thing is, as I said, what is the due diligence that notifiers should be going through to ensure that the burden of validation is not entirely on the operators? What is the kind of arrangement that can be done between trusted notifiers? What are the trusted notifiers' arrangement?

I want to make a clarification here. Nobody can say, on their own, "I am a trusted notifier." At best, you can say, "I have expertise in that particular field that makes me an expert notifier." A trusted notifier relationship is a bilateral recognition. You can be a trusted notifier for one operator but not for others. It's an important distinction and we need to work more on the notion of the notifiers.

A dedicated document is addressing the question of botnets. I don't have time to get into the details. But there is a very important issue which is called algorithmically-generated domains. Finding a better cooperation between law enforcement, ICANN, and the DNS operators around algorithmically-generated domains is a very important element. I think this document has helped move the discussion a little bit forward.

Finally, regarding phishing and malware, we worked with the contact group to make a clear graphical workflow on what is the distribution of roles at the different stages between registries and registrars? What are the channels for information and so on?

I'm extremely happy to mention this here because Graeme Bunton is here in the corner and some of you have seen him beforehand. It has led to two great initiatives that I'm extremely happy were built on the foundation of the work conducted in I&JPN, the creation of the DNS Abuse Institute, thanks to the help of PIR, and the production within this context of something that we had discussed within the contact group, which is an interface for reporting abuse, called NetBeacon now.

CleanDNS has been … Jeff Bedser has been instrumental in making this happen. Brian Cimbolic is near him for PIR. Brian is actually the coordinator of the contact group that we have in I&J. This work is amazing for me because it is the result of five years of work leading to a very concrete element, something that is operational, that is not just discussion or paper. It's really something that is operational. Big tip of the hat to them who are carrying the torch forward.

This is important because in addition, this has led also to the discussions that are taking place here during this ICANN76 regarding the improvement of the Accreditation Agreement.

So I close this part and I have a very short one afterwards. This is about DNS abuse, understood as the five elements that we were talking about. Next slide, please. I think that, in summary, there is an agreement among the responsible actors that DNS abuse, understood in this way, is something that is indeed something that is generally justified to act at the DNS level when there is substantiated evidence unless the site has been compromised or there are other things. But generally speaking, we’re seeing the movement in a positive direction towards implementable cooperation.

The last part that I want to address, which is more in the making at the moment, is the question of content-related abuse, which is much more complex because here, the image is a little bit of a mirror image. Generally speaking, the DNS level is not the right place to address content-related abuse because of many reasons, including the fact that it's not granular enough. It is difficult to have something that is tailored with the illegalities in one region or the other.

The competence to evaluate whether there is abuse is much different. It’s not a technical thing that the operators know. And generally speaking, it is not an efficient tool because the content remains available in most cases.

But there are nonetheless a certain number of situations that are sufficiently exceptional to justify action at the DNS level when they are met. And in the operational approaches that we produced in 2019, before the global conference we organized in Berlin, there are four elements, very tentatively, that can be taken into account to guess or evaluate when it is appropriate to act at the DNS level for content-related abuse.

It's how globally-agreed is it that the content in question is illegal? Here, you have a full graduation between things that are—CSAM, for instance, at one extreme in a certain way and things that are extremely diverse in terms of the legislations around the world. Great variety on what is illegal and what is not. The proportion of the site that is dedicated to the infringing content. The intended purposed or bad faith of the registrant or the operator of the site. And also, whether the other levels have been exhausted in going to the site operator, the registrant, or the hosting provider.

I don't belabor on this but it is important to really make a distinction between those two categories of things. Both are important but they shouldn't be handled exactly in the same way. One of the big challenges is that we don't have a space to discuss this second problem. ICANN is the right place to discuss the question of DNS abuse the way we described it before. But it has been very clear that, according to the mandate—and the community is completely in line with this—it is not the place to discuss content-related abuse. There have been blog posts consistently regarding, "ICANN is not the content police," etc. And it's completely understandable.

The problem is, there is not much else where it can be discussed. This is the reason why, last May, in 2022, a significant portion of the people who participated in the contact group of I&J have asked us to basically be the place where the discussion on website content abuse could be explored for those exceptional circumstances, finding the thresholds, criteria, and mechanisms.

This is what we’ve embarked upon this year. It's preliminary. It’s only starting. But I think it is important for this community of the GAC to have the whole picture and understand that ICANN is really moving forward on the basis of the work that we collectively have done on the question of DNS abuse. It’s not perfect, and it has to be implemented, and it has to be strengthened. But it is really moving forward in that regard—better clarity, better mechanisms, and better cooperation.

On content-related abuse, although it is not within ICANN, we as I&JPN are continuing this activity around the following elements that are the next slide. One, the DNS layer for content-related abuse is either triggered because there is an absolute reason to go there directly or because it’s the last resort after having exhausted other levels in the stack. And the question of how do you contact the site operator, the registrant, the hosting provider? What is the escalation path is the first discussion.

Second element is how to formulate the threshold criteria. To give you an example, you can say, “The entirety of the site should be dedicated or is dedicated to the infringing content or activity.” Or you can say, “There is no other legitimate content on the site apart from this.” Or you can say, “The intent of the site operator is to do x, y, and z.” The formulations matter and we are facilitating those discussions.

Finally, the notion of reachability is an interesting one. The moment we say there is an escalation path, how do you send a notice and how do you contact the registrant, or the site operator, or the hosting provider for that matter? This is something that we are going to explore in more detail because there's not clear equivalent of the WHOIS for hosting providers. Finding where a particular site is actually hosted is a little bit more complicated than just finding who the registrar is.

Finally, I mentioned the notion of trusted notifier agreements. It is an extremely important point because especially for content-related abuse—even more than for phishing but for content-related abuse—there will be no solution for this without the cooperation between the three categories of actors—the law enforcement, the notifiers of various sorts that must ramp up their capacity and their credibility, and the DNS operators in existing agreements.

As a pun to those of you who remember the formulation of affirmation of commitments between NTIA and ICANN in the olden days, I believe that there is a framework concept which is mutual affirmation of commitments. We need to have mechanisms that bring together notifiers with competence and procedures of due process, law enforcement that facilitate cooperation, and operators to deal with the cases when it is appropriate to act at the level of the DNS.

I want to highlight that what we're talking about here is not dealing with the regulation of large platforms. It's not Facebook. It's not the Twitter of this world. You are not going to ask for taking down Facebook.com because there is some content in one of the subgroups that is there. But when somebody sets up a website behind a domain name to have a malicious intention, finding these people and basically stopping the whack-a-mole exercise of just stopping it here and then stopping it there, and moving towards catching the people who are actually doing this stuff is the important cooperation that is needed.

So my bottom line is this is a shared responsibility. This is something that requires the cooperation between the different actors. The motto of Internet and Jurisdiction is "enabling multistakeholder cooperation." We do it in facilitating the shaping of a certain number of agreements. We're very happy that it has led to progress within the ICANN environment. And it is the only way we can address those issues.

You have, in the slides, a series of … No, there should be a slide before. It disappeared. I will reintegrate it. There is a slide with all the connections and the links to the documents that I presented. On the last slide, here are my contact details and the contacts of Ajith Francis, if you want to talk to us about this afterwards. Thank you very much for the opportunity to present.

MANAL ISMAIL: Thank you very much, Bertrand, for a very thorough, well-structured, and informative presentation. Before handing this over to our GAC topic leads, I just want to recognize a very patient hand up in Zoom from Iran. You want to go first? Okay. Kavouss, just a second. Chris and then I'm going to give you the floor. Sorry.

CHRIS LEWIS-EVANS: Thank you, Manal. I was just going to suggest, actually. We've had quite a lot of input, quite a lot of us talking. Maybe, if you have any reflections or any questions for us on the last couple of presentations, that would be welcome now. Then we will cover ongoing activities within the

ICANN community and considerations for Cancun communique language. That will have questions as well. But maybe just on the last two presentations that we've done, some questions and reflections would be good now. Thank you.

MANAL ISMAIL: Thank you very much, Chris. Kavouss, anything on the first part of this session, either to topic leads or to Bertrand? Please go ahead.

KAVOUSS ARASTEH: Thank you very much, Manal. Let me express my sincere appreciations to persons on the podium. That was, in my view, one of the most interesting discussions that we've had on DNS abuse. While I don't want to make a comparison between the different, but the last portion, for me, was very interesting.

As I mentioned yesterday, we have problems. And we have resolved the problems. What I recommend, that first, distinguished chair, you and Nicol, the chair of the GAC for future, we need to put into the GAC agenda of the next meeting more time for this subject. It is not possible, superficially, to come something and don't go to the heart of the problem as we did today to see what we are. There are many things [to have]. I don't know. We don't have time right now that I explain. I have some suggestions. I don't know what you suggest to me. But there is a way forward.

But I think I want to only address one of the points. Distinguished friend on the righthand side of the podium mentioned intergovernmental cooperation. This was discussed many years. It is not an issue of ICANN because ICANN is not intergovernmental and GAC is not intergovernmental. GAC is Governmental Advisory Committee. Governments are intergovernmental. They are elsewhere but not here.

And I'm sorry. I am [very frank with] everybody. Many times, we wanted to address this issue, intergovernmental cooperation. Some governments opposed to that, saying that cybercrime is a national issue and should not be dealt with internationally. And they said that any intergovernmental cooperation could be useful if [entered] to a treaty. And it is not possible to have a treaty on that.

So let us go to the depth of the situation, not at this session because we are at the end of the meeting. Let us, distinguished chair of the GAC, if possible, we'll discuss issue a little bit further to see what we can do. Many good point has been raised. What, up to now, has been raised is mostly raising the problems. But still, solutions are not proposed. That is important. It is sometimes, I would say, not very easy but easy to raise the problem. But it's more difficult to suggest solutions. Where are the solutions?

We have to take most pragmatic approach, not to legislative part to see what we can do. Categorize them, on the degree of priority, what we can do. Intergovernmental cooperation, for the time being, is not so easy to address. But there are many other things to address and so on and so forth.

We have received reports from UK and from USA. We could ask all the GAC members, "Do you have the same experience? What is the report? Did you face …?" I have faced but I've never report. I personally, on my e-mail many times … I told yesterday. There was [another one] saying [they had a diplomatic car] with 10% of the price. I didn't open that because my son is very clever. Told me, "Daddy, don't open any of these things. Don't open. If you have an e-mail received, you don't know the sender, don't open that. I may be not good, not [inaudible]. But don't open that because you may be immediately …"

And then there are other approaches. Some of the e-mail providers, they have the double security, that if your password and so on and so forth are taken by someone, apart from your desktop or equipment, no one could use that because they ask them the second approach—the second security. So we have to provide some good advice to the people as a preliminary precaution. What are those things that at least they reduce amount of this? So this is something that we have to discuss.

There are many other things that I have but there is no time. So I'm sorry if I [inaudible] but that is everything. Thank you.

MANAL ISMAIL: Thank you very much, Iran. If you allow me, Chris, we have two other requests for the floor and maybe you can react a bit. We have only 20 minutes remaining and I have Democratic Republic of Congo and then US. Please go ahead. Democratic Republic of Congo, please.

BLAISE AZITEMINA FUNDJI: Thank you very much. Thanks to all the speakers on the floor. I'd really like to, a bit like Kavouss, to mention how very important is this presentation. On the government perspective, for most governments and mostly from Africa, I think the expectations of our government of having a delegate within the GAC is mainly to address this kind of abuses.

My question or comment will mainly be, of course, obviously, the title or the topic here is abuse. But I would really like to ask if there is any actions that can be done from governments to prevent. Of course, we're talking about healing, about curing. But as you know, in French, we say, "Il vaut mieux prévenir que guérir." Are there some actions where, as the ICANN can advise?

Of course, we're talking about cybersecurity issues where the sovereignty of nations is involved. But even in terms of advice, mainly for corporates and mostly for governments, what are the advices? How can we prevent this to happen?

We saw some presentations from the FBI and mostly also from the UK experience. I understand that there are some studies. There are some statistics which may help to understand why we have this kind of abuse. We know that, for end users' side, mainly it's phishing. It's e-mailing, password compromise. But for corporate and mostly governments, are there some actions that can be done to prevent than to wait for abuse to be healed or to be cured? Thank you.

MANAL ISMAIL: Thank you very much, Congo. I have US and France, please, very briefly. Then I'm going to hand it over to Chris. US, please go ahead.

SUSAN CHALMERS: Thank you kindly, Manal. I'm actually happy to cede the floor so our colleague's question can be answered. Thank you.

MANAL ISMAIL: Thank you very much, US. I have France and then I'm handing it over to you. Is that okay, Chris? France, please go ahead.

JONAS ROULE: First of all, let me thank all the panelists for their presentations. I'm honored to be here replacing my previous colleague. I just wanted to intervene, just to contribute to the discussions. I'm new in the GAC and I am under the impression that before starting to work, I should learn more about certain topics.

First, as a newcomer, I would like to explore some aids to see if I can do something to prevent external attacks. I feel that the advantageous price proposed by some actors leads to some abuse in DNS. So I would like to know how we could work to see the rate of renewal of domain names. Perhaps this could help the community in doing something about that.

We know which actors are not playing legally. So perhaps we can uncover some mechanisms they use. But some of the difficulties that we observe need to be proven with evidence. I think that is something that we need. Thank you for your attention.

MANAL ISMAIL: Thank you very much, France. I see Rwanda's hand up. So can you please make it very brief because we're running out of time.

VINCENT MUSEMINALI: Thank you very much. I just want to thank the presenters, the panelists who made the presentation on the US report and the UK report on cybercrime. Just to get some clarification [inaudible] cryptocurrencies. Most people are now facing some challenges that are related domains that are using cybercrimes that are [linked] to cryptocurrencies. And those domains are sometimes closed and the people [inaudible] lose their money and investment. And they [now have] to make the follow-up of that investment. I would like just to know how they cooperate with INTERPOL. Thank you.

MANAL ISMAIL: Thank you very much, Rwanda. Back to you, Chris. Sorry to squeeze you on time but it's good to hear from GAC colleagues. Please go ahead.

CHRIS LEWIS-EVANS: Thank you, Manal. It definitely is and thank you very much for your input. I will try and summarize some of my input quite quickly. On the advice side, which we heard from both Congo and France, we're not going to cover that here, now. There's lots of advice. There's lots of things you can do. Maybe that might be something for a capability building workshop in a future ICANN. So maybe one for the GAC to consider because it would need to be a slightly longer session. So that might be something that we could consider.

Then, on Iran's point around the proactive, "What can we do?" I think Bertrand covered a couple of those. NetBeacon, certainly mentioned as a reporting tool, is a way of action and a way to combat some of this.

That leads nicely on to ongoing activities, if we can flip to those slides. We'll cover some of the action that has been going on in the community that is supporting some of that DNS abuse.

On the cryptocurrency side as well, I think that comes to Bertrand's point a little bit as well. That can either be delivered from a phishing e-mail, where it would fall into the DNS abuse, or it might be a content-related issue, where it would fall into mechanisms there.

Then, going on to community activities. There's lots of work going on. Registries are working on voluntary sharing of statistics. As we've seen from the law enforcement point, we think that's quite important. It gives us an overall picture. Likewise for the registries that would support that.

Just to mention the next one, which is acidtool.com. Bertrand said there's no tool to identify hosting and e-mail providers. Actually, the Registrars have created this tool to help people identify the right and correct point to go into, to take effective action. We heard from the I&J presentation, taking effective action is really important. And identifying that right point, whether it's a reseller, a registrar, a registry, or a hosting provider is really important.

Another call-out to NetBeacon, again, within here, as a method of taking action. This is very in-line with the recommendations within SSAC115. We had a good presentation from SSAC on that, and again, mentioned in the I&J report. These are all activities that are helping to mitigate that [advice] that's going on at the moment. Also, DNS Abuse Institute is sharing its analysis work from the data it's collected and seen as part of that DNS abuse reporting. Next slide, please.

I'm probably speaking too fast for the interpreters so I will apologize now and slow down a little bit. The GNSO Small Team on DNS Abuse have also been very active. I just want to flag here that their findings mirror some of our issues of importance within The Hague Communique that any future PDP work on DNS abuse should be narrowly-tailored to produce some timely and workable outcomes. So very much to Iran's point, any work that we do in the community needs to be targeted to enable it to happen and happen quickly. I know there's frustrations sometimes about things not happening quickly enough. Then, next slide, please.

Also within the ICANN remit, they have the OCTO Team, have the DAAR system. That, we also heard about on Saturday, I believe it was, around them analyzing data of 1,145 gTLDs, which surprised how many there were on that. Also there's, I think, 21 ccTLDs. Again, it's just a better picture to give a bigger understanding of what's going on to able to take effective action. Next slide, please.

This one is just a reminder about that pathway and who to contact. It's a complicated space. This is an ICANN diagram so thank you very much. I can't draw anywhere near like that at all. We hear about going to the right person to be able to take the right action at the appropriate time. Certainly, from my perspective, we see where we're able to do that, that also reduces the harm. So being able to understand where to go and where to go quickly is really important. So tools like NetBeacon, ACID Tool are really helpful.

The picture is actually slightly more complicated than this as well. On the righthand side, you have the registrant and then a reseller. There's not always a reseller or sometimes there's more than one reseller. So understanding that is really important to be able to find that right place to go into. Next slide, please.

Just to flag on that reseller front, during the Phase 1 work on the EPDP, it recommended that registrars should generate a reseller data element for the reseller with a relationship with the registrant. That's important where there's multiple. So within the WHOIS response at the moment, there is a reseller field but not necessarily collecting all of those. And as I said, it's really important for us to be able to go directly to the person that can take the most effective response. That was also reflected in the CCT Review as well. Next slide, please.

And hand it over to Laureen. I apologize for going fast but I wanted to get to our second set of questions if we could.

MANAL ISMAIL: Laureen, we already have a request for the floor. Would you like us to take it first? Okay. I see UK's hand up. Nigel, please go ahead.

NIGEL HICKSON: Thank you very much, madam chair. I would be happy for Laureen to go first and then we'll come in later, perhaps. Go ahead, Laureen, please.

LAUREEN KAPIN: Thank you, Nigel. I'm speaking in my capacity as one of the co-chairs of the Public Safety Working Group and one of the subject matter experts on this very important topic. Can we go to the next slide?

I'm glad the session has been interactive, even before this moment. But there's been a lot of discussion, and perspectives, and information about what the GAC would like to … Let me rephrase it. There's been a lot of information and perspectives shared. Now we're at the point where we can discuss what the GAC would like to highlight in the communique, so potential issues.

First of all—and this falls into the "if it's worth saying, it's worth saying many times" category—we have the ongoing contract negotiations between Registries, and Registrars, and ICANN. Again, the whole aim of this process is to raise the floor, so improve contract obligations with regard to taking action against DNS abuse. So obligations, not voluntary efforts. These obligations, the aim would be to reflect an obligation that's going to cover everyone. That would hopefully include bad actors and also give ICANN even more tools than it has already to deal with those scenarios regarding DNS abuse.

Again, this is just step one and there could be future steps. But this could be an important time for the GAC to acknowledge and applaud that this effort is ongoing and that it was done at the contracting parties' initiative. This is a proactive step and that's always to be welcomed.

This is the first of many steps so future policy work is envisioned. I want to echo one of the comments from my colleague from Iran that it's so important to prioritize here and focus because that's the way things get done. And we can apply these two guiding principles to any PDPs, which haven't necessarily been known for their quick and focused action but they could be and they should be in this context. Also, there may be opportunities for more negotiations between the Contracted Parties and ICANN.

To flag, there will be an upcoming opportunity for public comments once the Contracted Parties release the fruits of their labors, which we're eagerly awaiting. Then there will be opportunities for the GAC to decide what sort of input it would like to broadcast. Next slide, please.

This issue of resellers has also been identified. The reason that connects to DNS abuse is because it's so important, as our colleague from the Internet and Jurisdiction Society, Bertrand, has noted. It's so important to be able to go to the right entity when you're dealing with DNS abuse. This topic has been the subject of GAC input in many different forms, related to the CCT final report, and also more recently, the Phase 1 domain registration data recommendations. Next slide, please.

Now I'm turning it back to my GAC colleagues for their input as to thoughts and ideas about what could go in the GAC communique. I also note, I know because time is short, that we have communique drafting sessions. But this would be a great time to get a preview of what folks are thinking.

MANAL ISMAIL: Thank you very much, Laureen. We have UK, Iran, and European Commission. And we have three minutes so I hope … Please keep it brief. UK, please go ahead.

NIGEL HICKSON: Yes. Thank you very much, Manal. Thank you very much for the folks on the top table for presenting to us. It was an exceptionally useful session, as other GAC members have noted. Just four very quick points, if I may.

One is that to reiterate our position on the contract negotiations going ahead. I'm incredibly positive. The session yesterday we had with the representatives from Registrars and Registries, I thought was excellent. We certainly look forward to the public consultation. No intent to interfere in those negotiations at all. Look forward to updates, of course. And as was said yesterday by the representatives, this is a first step. There might well be other initiatives—mini PDPs or whatever—to look at on DNS abuse.

Secondly, in terms of the communique, we'll no doubt be discussing these issues. I think it's only right for us to be very clear in the communique how we welcome these initiatives but also to itemize those recommendations—the GAC advice on the CCT Review Recommendation 17 and other issues in terms of the resellers that's been talked about that we ought to be flagging so the whole community understands that there's certain actions in place that need to be taken before the next SubPro process. I'll leave it there. Thank you very much.

MANAL ISMAIL: Thank you very much, UK. I have Iran next and I'm closing the queue after Japan, please. Iran, go ahead.

KAVOUSS ARASTEH: Thank you very much, Manal. I have discussed with some distinguished colleagues, including yourself, that the issue of DNS abuse is the core issue of the current and the near future and long-term of ICANN. That is something important. But everybody—Board, ICANN Org, membership, and everybody—is studying the matter. There is no need to have any GAC advice on that. Let the people breathe, think it over, digest the matter, and not push more than what we need to do. They know what is a problem.

On the other hand, in the issues important for GAC, the first thing we need to mention that recognizing the negotiations being carried out within ICANN Board or ICANN and the Contracted Parties, Registries and Registrars, that is a good step—saying that. And then we should mention that we need a progress report on that at our next ICANN meeting, ICANN77 at Washington, DC—a progress report what is going on.

And we expect that the final report will be either 78, or 79, or 80 but with sufficient measures also, in order to advise government or GAC people how to combat, how to fight, as my colleague mentioned, or how to counter this situation, and to see many other elements that was indicated in the report of Chris, and Laureen, and Gabriel—putting into it issues important for GAC.

And try to emphasize on the importance of the thing. Work on the text to be more clear, to be more precise and concise as well, and try to [put the dots] and make a follow-up action. But I suggest that we do not include anything on DNS abuse in the GAC advice at this stage. Thank you.

MANAL ISMAIL: Thank you very much, Iran. I have European Commission, then Japan. And a friendly reminder to please keep it brief. European Commission, please. Gemma, go ahead.

GEMMA CAROLILLO: Thank you very much, Manal. I have commended the presentations in the chat so I won't do it again in the interest of time. Regarding very briefly on the points and the considerations for the communique, as asked kindly by Laureen, surely we agree that this is a great move. The negotiations, we have been calling for this for a long time inside the GAC. So this is something, for sure, where we should support.

In terms of the additional substance, we might want to add to the DNS abuse section under the issues of importance. They will take it, but of course, for further discussion. First of all, the importance of a preventive measure. We are a bit concerned that what we have heard so far, it's mostly about reactive measures. But the prevention for the DNS abuse is really key from our perspective. I heard it previously, also, from one or two colleagues. Then, possibly explore the issue of incentives, which has been raised in the very good advice from the colleagues from the PSWG, etc. locations.

And last but not least, linking to what Nigel said regarding the next round of gTLDs, in general, we would like to make sure that previous work is not forgotten—in particular, in relation to reasonable measures to prevent DNS abuse. But the GAC has been quite strong in linking data accuracy, domain name registration accuracy, and DNS abuse in Communique 71, 72, 73, and I'm sure there are more. So it's not about listing that but just to make the point that we would like the work done regarding registration data accuracy and the importance for preventing DNS abuse not to be lost. Thank you very much.

MANAL ISMAIL: Thank you very much, European Commission. And last but not least, of course, I have Japan.

NOBU NISHIGATA: Thank you very much, Manal, and the co-chairs of the PSWG. Good night, actually. It's already night in Japan. So good morning, good afternoon to everybody from Tokyo. Thank you very much for the organization that did this wonderful session today.

Just responding to Laureen's presentation about the consideration for the communique. Japan would like to express the support for the contract negotiation ongoing, which is very much welcome—the current progress so far.

But on the other hand, Japan would like to raise one question and issue among the Registrar Accreditation Agreement, the Article 3.18.1, which is about the registrar's required action to report on illegal activities. The Japanese government [has reported] and are aware that some registrars do not take any action or even do not respond to the illegal activities report from Japanese parties. So this is why the Japanese government continue to ask for the improvement of this contract text or terms.

There was some evidence from Japanese government. But still, there are a bunch of other evidence similar to this—ICANN's audit report or the recent report from ICANN, the GNSO, the Parties. So this is the point, just saying that Japan is looking forward to seeing the draft report coming. Of course, they're happy to discuss intersessionally, if we've got some progress.

And of course, in the end, I have to express my great appreciation for the previous session which gave us the update on the contract negotiation. So we are willing to continue the discussion—happy to have a discussion with you. Thank you very much.

MANAL ISMAIL: Thank you very much, Japan. And thank you very much, Bertrand, from Internet and Jurisdiction, Gabe, Chris, and Laureen, the GAC topic leads. And thank you, everyone. We will reconvene here at 15:00 Cancun time, 20:00 UTC, for our bilateral with the Board. So please be prompt. Thank you.

[END OF TRANSCRIPTION]