ICANN76 | CF - GAC LAC Capacity Development Workshop (2 of 4)
Saturday, March 11 2023 – 13:15 to 14:30 CUN

JULIA CHARVOLEN: Hi, everyone, welcome back in the room, we're going to start off very soon. Thank you very much. So our next session will be the DNS abuse discussion. There will be three sessions following on. So we've got our GAC topic leads to lead these sessions. They have been working in these sessions for years, and also, our colleagues from the other organizations in other committees in ICANN. Without further ado, may I ask our speakers to introduce yourself, Gabrielle. Thank you so much.

GABRIEL ANDREWS: Hi. Okay, this works. Good. My name is Gabriel Andrews. I am here in my capacity as a member of the Public Safety Working Group advising the GAC as a type of lead on DNS abuse issues.

SAMANEH TAJALIZADEHKHOOB: Hi, I'm Samaneh Tajalizadehkhoob. I'm Director of Risk Security, Stability, and Resilience Research at ICANN office of CTO, and I'll be talking about the DNS abuse strengths today. Thank you.

CHRIS LEWIS EVANS: Thanks. Hi, everyone. Chris Lewis Evans, one of the co-chairs on the PSWG and one of the GAC lead. Sorry. So, Chris Lewis Evans, one of

the co-chairs for the PSWG, and one of the GAC subject matter experts on DNS abuse.

JEFF BEDSER: I am Jeff Bedser. I'm with the SSAC, and I'll be here speaking about SEC115, Inoperable Approach to DNS abuse mitigation.

NICK WENBAN-SMITH: And I'm Nick Wenban-Smith, and I am here in my capacity as chair of the ccNSO DNS Abuse Standing Committee. In my day job, I'm the General Counsel for the UK Registry, United Kingdom ccTLD. Thanks.

CHRIS LEWIS EVANS: Thanks, everyone. So as you'll see from the agenda, we've got a few speakers here, and the idea about this session is to give you an overview of DNS abuse and some of the different viewpoints on how different parts of the community see that and try and bring you up to speed with all the developments that go on and the impact it causes to people as well. So please feel free to ask questions at the end of each presentation, and we'll try and answer those as best we can. Gabe, over to you.

GABRIEL ANDREWS: And which one is live? Can we see the next slide? Great. All right. So as I mentioned, I am here in my capacity as a member of the Public Safety Working Group, and we are trying to give a very high level overview, an introduction to the topic of DNS abuse here with these

next few slides. This is not going to be new, it covers a lot of topics we've discussed here previously, it's not going to be complete, it is a very generalized discussion.

And finally, I'm trying to make this as neutral as possible. I hope it's not contentious as well. Next slide. So, it's very easy to talk about what the DNS is, that's the way that we translate the human readable domain names to the machine-readable IP addresses. It gets a lot harder to talk about what actually DNS abuse is, and there's kind of a reason for that. Next slide. You see here there is some various definitions that have come from different parts of the community about what they might consider to be DNS abuse.

And where they draw the line can depend a lot on who you're talking to at the time. And there might be a reason for that because, possibly depending on how you define DNS abuse, it might be perceived that you're also trying to assign responsibility for action, or perhaps trying to push responsibility away from yourself or your entity role.

Next slide. You might further find that when you're engaging your law enforcement agencies, your public safety professionals, cybersecurity practitioners outside of the ICANN space, that the phrase DNS abuse probably doesn't come up much at all. We tend, in public safety, to talk about fraud or crime, and we talk not about the number of domains that we're seeing being used so much, but rather tend to quantify the monetary loss associated with a certain scheme, or the number of victims that are impacted.

Next. You'll see here-- thank you. This is from the FBIs internet fraud, excuse me, internet crime report that was just released maybe three

days ago. We collect about 2000 complaints a day of various types of internet crime, and we try to publish reports on an annual basis that makes sense to the best as we can make sense of anything with what we're seeing. You'll note that within the categories that are described there, DNS abuse doesn't appear, but at the bottom, phishing does, and quite prominently. And it's phishing that actually enables a lot of other types and varieties of internet threat. We note that within the community in ICANN, phishing is one of those topics that is generally there's consensus that it is a piece of DNS abuse.

I see the slight change, so hold there for a moment, please. And so the loads -- oh, thank you. There's a picture of the blind men and the elephants. The metaphor I'm trying to explain here is that even though we don't necessarily use the same language all the time to discuss this, we are a lot of the time talking about the same animal. And your police officers are touching one part of the elephant and describing the trunk, and your folks in ICANN might be talking about the same creature, but touching a different place of it.

And if you want to be able to bring to ICANN matters that are important to you or your nation or your colleagues within your governments and have them be acted upon here, it's very important to be able to translate what you're hearing from them into ICANN discussions, and to know how to speak to it in a manner that you can obtain consensus on here. And now we can move to the next slide, thank you. And so to do that, I would suggest that it's very important that we look at the ICANN bylaws.

And I think I'm waiting for the next slide here. Thank you. I'm going to read a little bit of this, sorry for reading from a slide. But I think it's important that we recognize that ICANN is charged with, and I'm going to quote, "ensuring the stable and secure operation of the internet's unique identifier system." And reading a little bit further, we see that includes obligations that maintain the resilience, security, and stability of the DNS. At the same time, there are constraints that exist in these bylaws.

You'll see that there are constraints placed on whether or not ICANN policy can regulate website content, and whether that regulation is in scope of its mission. And these are very important things to consider when you're bringing topics to discuss here at ICANN and to build the consensus that's necessary to effect change. You'll commonly see these bylaws referred to in DNS abuse conversations about whether or not certain types of crime or abuse fall within its mission.

And even if they do not, there is still support behind the idea that while not all harmful or illegal activities will fall within ICANN's remit, the GAC remains an important venue for governments to be able to discuss DNS abuse and work towards solutions.

Next slide. Now, this is new since the last time I gave this at 75, but having spoken about phishing just a moment ago, I wanted to show why it's important to talk about not just the registrar and registry DNS level action, but the hosting level action as well, and explain within the phishing context where each of these components applies.

Imagine there's a bad guy, and he's trying to impersonate a fictitious bank, Rainbowbank.com. You can see there that he used a lookalike

domain name with an owl instead of the eye. Phishing as you probably already know is when a bad guy sends email messages pretending to be someone trusted and trying to get the fix to do something that's against their interest. It could be sent money, it could be click a dangerous link, it could be any number of things.

When we want to stop this phishing email from harming victims, theoretically, we could do so at the DNS level by addressing that domain name, and/or we could do so at the IP level, which is called the hosting provider, that's where the machines are that actually hosts the content. And you'll hear various members here espouse their preferences for action one way or the other. But I wanted to call out the reality that surrounds how the bad guys adapt to our action, because let's say that in this very simple case, if all of the bad stuff is hosted that particular IP, yes, we go there and we take it down, problem solved.

Next slide. The issue is that because domains are pointers, and as long as the bad guy controls the domain, they can point it anywhere they want. They can point it to any number of different places. And, in fact, the criminals are at least as smart as our law enforcement, they realize this and they do this, they learned that they can change the destination of that domain even after it's arrived in the inbox of the victims.

Next slide. They can even go one step further and employ networks of thousands of compromised machines, we call this botnets. That can each be one of those destination points. And in phishing cases, we see this a lot. It's called Fast Flux when it happens to denote how fast the

various IP addresses appear and disappear in the DNS record. And when this happens, the whole point of that is, the bad guys learn that yes, we want to take action at both the DNS level and the hosting level, but the better they are at hiding that true hosting IP address from us, the harder it is to take an action elsewhere.

And this is why sometimes that when we address cyber threats, we have to involve discussions of DNS. It's not always the case, this is one example. There are many types of crime, and there are many types of abuse. But I wanted to give a illustrative example of why sometimes action at the DNS level is actually necessary. Because if you're trying to stop that bad link in a victim's email inbox from harming people, sometimes the only way you can do that is to stop that domain from resolving. Now, next slide, and this is the last slide.

We wanted to provide some additional references and material for those that are interested in the topic of DNS abuse. I'm not going to go through each of them here, I just want to note that if you have access to the slides, there's a lot of interesting papers, tools that have been published, and I thought it would be useful for those that are interested to be able to go through and take a look at this material as well. And with that, I'm going to stop. We can handle some questions now. I don't know how we want to handle this.

Q&A now is fine for another few minutes. How am I tracking on time, by the way? Pretty good? Okay. So if you have questions about what I said, now is fine, it's also fine later, I think we're going to try to pause for some questions and answers after each of the speakers with a goal

of being about 15 minutes per speaker here with the Q&A included. I'm not seeing hands immediately though, which --

UNKNOWN SPEAKER: Questions from new GAC members, questions?

GABRIEL ANDREWS: You can ask so just attack us on our way off the stage too, if you're more comfortable doing that. We're fine talking after. But otherwise, I'm going to go ahead and hand over the mic to the next speaker.

CHRIS LEWIS EVANS: Jeff, over to you.

JEFF BEDSER: Thank you. So I'm Jeff Bitzer. I'm here representing the Security and Stability Advisory Committee for ICANN. The presentation I'm going to show you, I apologize up front that it actually has the name of the chair of SSAC on it, not me. I was the chair of the work party that drafted this report. Also, you'll note the date is from May of 2021. Apologies. Not much has changed in this presentation, and with the timing available, I didn't have a chance to update it, but I will go through this quickly and give you the contents and the basic premise of the report about basically the interoperable approach to addressing abuse handling and the DNS and the core takeaways, and also give you an update of what has happened since 2021 in regards to that.

So next slide, please. So we'll go over the scope and purpose of the report, we'll talk about how we define the problem, the framework for the approach we came up with, and we'll go over some findings and some recommendations we came up with. Next slide, please. And in interest of time, probably next slide after that as well. Purpose of the report slide which should be two slides up. And one more. Here we go.

So the overall goal is a goal I'm sure everyone in this room shares is to reduce victimization of internet users. In that regard, an inoperable reproach, gives you universal standards for DNS abuse handling that helps you achieve that, and the outcome, of course, is that we're hoping that SEC115 is a catalyst to channel ongoing efforts to establish a universal standard for taking these initiatives.

Next slide, please. And thank you. So we define the problem under technical abuse, as defined by the contracted parties at ICANN to be technical abuses of malware, botnets, phishing, farming and spam with the caveat on spam, it's when spam is being used to redirect to another type of technical abuse.

Next slide, please. What is happening today to deal with DNS abuse? Well, there's a lot of blocking and filtering, where people use block lists to ensure that traffic is not routed to domains associated with abuses, such as phishing and malware, you have a process of takedowns and notices between reporters, sometimes they are commercial, where there's a commercial entity that is looking for their customers or potential financial entities or banks to take down the domains that are associated with phishing their customers, and many

times it's a cybersecurity company looking for the spread of malware or another type of ransomware as such, and they're reporting it.

Our efforts going on, there are groups like the Anti-Phishing Working Group and others first, which is a group of certs as well as other policies in the DNS abuse institute for one and for example. And of course, there are a selection of notifier programs that currently exist to expedite reporting through trusted networks and connections.

Next slide, please. Next slide, please. Okay, so proposed framework really came down to the core on this slide, which is that each type of abuse has a primary point in the ecosystem that is best for it to be resolved. Sometimes it's the registry, sometimes it's the registrar, sometimes it's the hosting company, sometimes it's the content delivery network, but there's always a primary point where that abuse can get a result of the most quickly.

That gives you the next path, which is an escalation path, wherein if you report it to the appropriate party, and they do not take an action, refused to take an action, or away for the weekend, whatever reason they can act upon it, the escalation paths should shoot to the next point in that ecosystem, it is the next point where that can be escalated and can be resolved.

The next problem is, of course, in an industry where we've been dealing with abuse since the internet started, there really isn't a body of standards on what constitutes evidence on different types of abuse that everyone recognizes. One is a phish-a-phish, of course, is the pH spelling, when I will accept this standard to say that this is proof and

evidence that this phish has occurred so I can act against this phish, and potentially serve or hold the domain based on my policy.

We also talked about a framework for reasonable timeframes for action, wherein what is a reasonable timeframe from when an entity is notified about this abuse to when it can get resolved, passed along to the next party mitigated. And then, of course, the last point of all of this is, this entire chain of steps doesn't take place if you don't have quality contact information to know who at that infrastructure provider to go to to communicate this abuse.

Next slide, please. There's probably a little bit too much detail here, I will share the deck through the group. Escalation paths as I mentioned, the evidence of both the abuse and the time of the report can be conveyed to the next party for the escalation. The temporal nature or when the abuse happened, is very important. In particular, when you're looking at whether the domain was registered for an abusive purpose, or whether the domain was compromised by another party to be used for an abuse.

In the case of a domain registered for an abusive purpose, the reality is, is there very little commercial harm to be very aggressive about taking that phishing domain down, that malware domain down, wherein if it's a compromised domain that may be involved in legitimate commercial or other freedom of speech issues, you don't want to be in a position of trying to take a domain down, that actually has other purposes, but there's a WordPress vulnerability, and it's been compromised and used for something else by a bad actor.

Next slide, please. So, when we're talking about standards referencing, it really comes down to four categories, and there's a lot of work to be done to take further types of online harms and other types of abuses into these categories, but you do, as I said, so you've got temporal relevance. When did it happen? How long did it happen after the domain was registered, for example? You've got visual, you've got something hosted at a record that shows you they're pretending to be the Rainbow Bank, as Gabe used as an example. And they are looking for a credential login for someone [00:20:24 - inaudible] customer for Rainbow bank.

But then, in the demonstrative component, it could be that that domain isn't spelled the same as Rainbow Bank, it's confusingly similar, but it's also hosted on a different IP address in a different country than where Rainbow Bank does business. But there's also behavioral things such as logs of activity of what's going on with the domain, where was it modified, was it doing one behavior at one point and moved on to another behavior at another point, thus demonstrating the change [00:20:53 - inaudible] compromise.

Next slide, please. So in reasonable timeframes, the report talks about the amount of time each party needs to give the next party the escalation path to react to this report of abuse. So in the report, we talked about a 24-hour window between reporters, which does count to a 96 hour block. However, in the report, we do talk very substantially about how that should be shorter, because again, the goal is reducing victimization. If you can reduce the uptime of the domain involved with the abuses, you are, of course, reducing

victimization is the number of people that can be victimized by whatever fraud or other type of abuse is going on there.

Next slide, please. And as I said before, this all happens or doesn't happen based on the adequate contact information to ensure you can reach that party who's doing that part of the infrastructure to best inform them in a timely manner of what the abuse is and what the suggested mitigation is. And as we suggest, in the report, with the right evidence package to demonstrate what is going on, so they can act upon their policy, which hopefully says they can act upon the domain if it is violating their policy.

Next slide, please. So, the findings are really simple here, is that we found that through a lack of coordination leads to an inconsistent approach to DNS abuse management and mitigation. When all different parties have different approaches to how they do it, they all have different evidence standards for what they accept to act upon the policy, it means that those that detect the abuse, the cybersecurity companies, law enforcement, whoever else, has a path to follow to find out who to report it to and how to report it to them based on their standards. And that's where the system breaks down for quick action to reduce victimization. So the opportunity really is to coalesce around that.

And we basically talked about an opportunity for a common abuse response facilitator. Since that time, the DNS Abuse Institute, which is part of the non for profit, Public Interest Registry, the runs. org. full disclosure, I'm the chairman of the board for .org and Public Interest Registry. They formed the data abuse Institute and started something

called NetBeacon, which is this common abuse response facilitator, where they will take in reports from anyone, and based on the type of report route that report once evidenced to the right party for mitigation.

They've been working to get adopted with the registrars and registries to accept those reports, and now they're working with governments, law enforcement and cybersecurity companies to get them to report the abuses to them so they can route them to the right parties, and setting up a evidence standard we can work with for each type.

Mostly, it works well for phishing, because of all the types of technical abuses we're talking about, that's the one that has the most confluence of agreement of what constitutes a phish. But there are other ones such as farming, which are technical abuse, but there really isn't a confluence of judgment of what demonstrates a phish so it can be evidenced, a lot of work needs to be done there.

Next slide, please. So finally, the recommendations. This, again, is a bit outdated being that is just sort of two years old. But the recommendation was for the ICANN community to work together to look for opportunities to do common abuse response facilitation, to set standards for evidencing, and to define the role and scope of these parties in a way that allows us to move this issue forward.

And I'll say from a personal basis, with the direction that's going on of many of the governments represented in the GAC, online harms are getting to be more and more to the forefront of the conversation. And as those online harms are defined as something that are going to be

legislated, we certainly want to be able to understand what is the standard for the evidence for that type of online harm.

So as there's a requirement to act upon those harms, we understand those standards and those evidentiary packages up front so that we can move forward to shut more of the things down that are hurting people. And I believe that's the last slide. And again, I offer tp hold my questions to the end or take any now.

CHRIS LEWIS EVANS: Thank you very much, Jeff. So any questions from any of the GAC members on the floor? Nigel, I see your hand in the back, I think, in between the lights.

NIGEL HICKSON: Yes, Nigel Hickson, UK GAC. Thanks so much for that presentation, and for the really influential report that you wrote, which I think is still referred to by many people in this regard. The question really was whether you think your recommendations have been taken up sufficiently, and whether there's any specific recommendations that you made where you think that ICANN specifically as opposed to the other elements in the equation needs to take further action? Thank you so much.

JEFF BEDSER: Thank you, Nigel, and that's a great question. I think the primary part of the report, that still allows for room, and I mentioned it briefly in the presentation, but it's basically setting the standards for evidence for

different types of harms as we move forward, coming to agreement on those standards, Alan Woods and I, Alan is on the Registry Stakeholder Group, and Alan was one of the co-authors, actually with Chris Lewis Evans as well on this report. He and I are doing a presentation during Tech Day tomorrow, or Monday, it's Tech Day session two, on standards and evidence, to start moving this agenda forward, because we believe there's quite a few other types of harms that can be more forward.

Quick example Nigel, would be smishing. It's when you get a phishing domain by text message, by SMS, what can be set as an evidentiary standard to allow a smishing domain to be recognized as a harm and mitigated so that all parties agree that this evidence package works, and there are many other examples much like that.

CHRIS LEWIS EVANS: Thanks, Jeff. Kavouss, I thought I saw your hand.

KAVOUSS ARASTEH: Thank you very much. Good afternoon to all. This is one of the, I would say, most interesting session of the GAC dealing with this issue of DNS abuse. As long as I remember, this has been on the table. We are not saying that nothing has been done, but the other party, the enemy is also clever. Whatever we do, they do the same thing or different things. What I would like to suggest that perhaps, either at this session or later on, we asking each GAC member whether they faced such evidence of DNS abuse, and in what sense?

If you need, for instance, you ask me, I can tell you what. I was sitting in my office in front of the computer, a secretary general of an organization sent me a message. My first name, Kavouss, can you please provide me this information? I need it very quickly. And to see my question, please click on this. I pick up the telephone and call that gentleman who is a good friend of mine. He says that my email has been hacked. I never asked any question like that.

And you were doing good things not to replying to that because coming from me of one of your close friends. So this is a simple example. But perhaps maybe there are some other people, colleagues, distinguished colleagues, whether any of them, they have been faced with similar things and gathering this information, which may also be helpful, how to tackle that, this is the first point. The second point, I would like to mention that many people, they're doing or following this DNS abuse, but perhaps it is time that we concentrate all of them in one single area.

Whether we create a task force, whether we create a central area, but not Christoph doing something on DNS abuse, ICANN doing something on DNS abuse, and many other people and so on so forth, but all of them, we should gather to see where we are. In my personal view, this is a top, top priority for the use of DNS. Instead of going to something like I would say SubPro, we have to resolve the problem that we're facing today.

So we have to give high priority to this issue, how to do that, from different angles, from different things, putting our thought together, and creating a unit or an area that all efforts be concentrated on that,

gathering information from the people that are facing abuses, and putting all other reports, as you mentioned, one from FBI, another, maybe Steve have some other things that he has every day, and so on so forth, to see what we can do about this.

I think we should pay absolute maximum attention to the DNS before going to something else. If we have a house, we have to maintain that house before making a new house, we can face the same problem, and more different problem at that and more, I would say, difficult than that one. So that is something that we have to know. At this stage, I limit myself to this preliminary and maybe you ask other people. Thank you very much giving opportunities to people to explain, to provide the information to you and make this session more interactive, rather than, let's say, just listening. Thank you.

CHRIS LEWIS EVANS: Thank you very much, Kavouss. And just flag obviously, there will be a GAC session on DNS abuse on Tuesday, and I'm sure we can probably address some of those things once the rest of the GAC have had a little bit more information from our other presenters as well. And sorry, I can't quite see who that is because of the lights.

ADERONKE ADENIYI: It's okay. Thank you. My name is Ronke from Nigeria. Thank you for your presentation. I'd like to seek further clarification regarding takedown of domain. You did say that you need to identify primary points in the ecosystem, be it the registry, registrar, hosting company, content developer. So my question is this, we've had a situation

where we had to work with Google to take down content. So, is this being addressed separately, or is this something that we can expatiate on?

What content would we bring down? There was an issue where we had elementary students practicing on principle things, and you know how it is, they have smart devices, it went viral, and it's something that was not for public interest. So as a government, we had to take it down. Is this something you're considering at a larger scale? Because considering the impact or proliferation of smart devices, especially to young users to keep putting up all manners of content, how do we address issues of content take down? Thank you.

JEFF BEDSER: So I'm probably not the best person to answer this specific question because the SSAC work on this was about what was within the bylaws for ICANN for us to handle which is the technical abuses, which specifically calls out content is not being covered. But I do know that most registries and registrar's and hosting companies have policies about when those types of abuses happen, that they are usually against their terms of service and can be acted upon. But they do differ across the industry, basically hosting companies which don't really have an entity like ICANN at the center of them.

So as a result, the policy is normally that as I've seen personally, would be they received the complaint, they validate the concerns and look to get it mitigated, particularly if it's content that is on a compromised domain, so someone else is running it. So for example, if the content is that reddit. co, and it's a subdomain of Reddit, well, you can't

suspend reddit.com because of one subdomain that has this content on it.

But in the case where that content is involved with a domain registered for an abusive purpose, so you can tell temporarily that that domain is very recently registered, and now it is doing something that for the visa, then it's more likely to be acted upon quickly because the commercial harms of making a mistake are much lower for breaking that contract with a registrant.

CHRIS LEWIS EVANS: Thank you, Jeff. And in the interest of time, I'll pass over to Nick next, please.

NICK WENBAN-SMITH: Thanks for Chris. Thanks very much. And we have some slides, I think, but I was going to say, now we are, to paraphrase Monty Python, something completely different. So there's three things that I want everybody here to take away from these slides. And this is just a summary of a fuller deck of slides, which is for a different session. But there's a specific one for you, folks. So there's three things. Firstly, these are ccTLDs, and there's therefore no role for ICANN in this, there's no contracts, no policy formation, so this is outside of the ICANN policy formation process. So that's the first thing.

Secondly, maybe because of that, controversial, the levels of abuse within the ccTLDs are incredibly low. Whether that's from the DNS abuse institute stats, or from the EU Commission report on this,

ccTLDs are extremely clean operators. And we will see that the vast majority of us report levels of abuse of registration less than 0. 05%, and less than that, so we're talking very small amounts. It's still an important topic for us, but the amounts are small, and we are very acutely aware of what we do.

And the third thing is in within the ccTLDs, there's an incredible amount of diversity. If you can look around the room, that reflects the diversity of the different nation states in the country and the diversity within this room. So those are the three key points. So I've just take you quickly through some of the slides, and we'll pick out some of the points here. So move on to the next slide. So the ccNSO Council formed a DNS review standing committee to look specifically at questions of DNS abuse since I was elected chair of that committee, but you'll see here that there's no policymaking remit to it.

This is more around sharing information and best practices, open and constructive dialogue, and actually giving members of the ccTLD community, whether or not they are members of the ccNSO, because not everybody is, some resources to help improve standards and raise the bar generally in tackling this globally. Okay, next slide. So specifically, we've started to benchmark ourselves and we undertook a survey in the fourth quarter of 2022. All ccTLDs are invited to respond, and we have here 57 unique responses from the ccTLDs.

Some ccTLD managers have numerous different ccTLDs because we have IDN variants. And some may know this is well known that the French have, I think, seven ccTLDs for various different French

territories. So these represent approximately 100 ccTLDs. And that, for comparison, is versus the 316 delegated ccTLDs globally.

We try to encourage engagement, so not everybody wishes to have their responses public, some people or about half are happy to have the responses made public, and we'll use some of those responses to tease out specific interest areas which were highlighted in this survey. But some people just wanted to do this on an anonymous basis, and we would respect that. Next slide, please. Okay, and moving forwards.

So this is just a summary slide. I put it there for the record, just around the diversity and to show you that our survey was geographically diverse in terms of the participants, and not only geographically diverse, but the organization of each ccTLD is extremely diverse as well. And similarly, the registration models, most people in the ccTLD community follow our registry registrar agreement, but not everybody does that, and I think it's important to bear that in mind.

Okay, next slide. And this is just a little bit more around the size, you see that the majority of ccTLDs are quite substantial, more than a million domain names, and we have a high degree of expertise. We may not have a dedicated DNS abuse in offset, but we have many of us dozens and dozens of permanent staff and we have high levels of expertise in this area.

Okay, next slide. So, I think the key point on this slide, and this is an important one, it's one of the three points that I want everybody to remember when the session is finished, and we've flown home from Cancun, and it's on the right-hand side at the bottom. And this is the

recording, it is self-reported, but it is backed up by other studies which are done by independent bodies, that the amount of abuse in the ccTLDs is very low. So that's the one of the key points here.

Okay, next slide. And I think finally, when we look at it, and it's interesting listening to previous comments around the importance of the ICANN bylaws, and the difficulties of policies to tackle content abuse when it comes to the DNS, is that you will see that of course, nearly all of us recognize phishing and malware as orthodox examples of what anybody would define as abuse of the DNS.

However, a lot of us in the ccTLD community would certainly consider, obviously, child sexual abuse material, but also things like illegal drugs, counterterrorism, misinformation, bullying, a lot of the other things that I know we've talked about in the context of government concern about online harms, generally, a lot of ccTLDs will consider that part of the DNS abuse policies.

And this is a very interesting point, because it's quite a distinct point, I think, from the gTLD world where they are bound by the ICANN policies which specifically make content out with of the remit, and obviously, IP, there are fake goods on the internet shop. Next slide, please. Next slide. Just take you through quite quickly, I'm trying to try and make a bit of time.

Yes, this, essentially, is saying that there's a variety of different tools that we use, but in general, the ccTLDs take a very proactive and combative stance against abuse of their TLDs. You can talk about DNS abuse. From my perspective, it's not so much abuse of the DNS, it's actually running a good registry.

If you run a good registry, and that is from the registration policies, your cleansing of the data, your complaint processes, your active monitoring and custodianship, these are all going to result in low levels of abuse and a good registry. And I think it's the same thing for most of us, we wouldn't really say that abuse was a particular topic, it's something -- low levels of abuse happen because you run a good clean registry and have good policies.

Next topic. Next slide. Yes, so essentially, this is around trusted notifiers and trends.

Next slide. So here's just a list of some of the tools that we do. I think one of the topics as chair of the Standing Committee on DNS abuse, I think we are going to have more of a workshop to discuss within our community who finds which tools most cost effective, not just in terms of the cost of sourcing, but also the cost of operationalizing what you get from them. I think it's a well-known problem that there's a lot of false positives in any and all of these sorts of tools. And it makes it expensive operationally to deal with them when there's so many false positives.

Next slide. I think here. I will pass over these slides because if we just check through, there's more study on the geographic diversity and regional differences, but I don't think that's appropriate for this meeting.

Next slide. And more to come. So there's a full session on this on Wednesday, in block three, there's a proper 45 minute session for the whole of the ccTLD community. Obviously, outreach is very important to us, or anybody who is more specifically interested in this other than

the very quick overview I've given in the 15 minutes available is very welcome to come to that. And I will then pass that back to you, Chris. Thank you.

CHRIS LEWIS EVANS: Thank you very much, Nick. Chris Lewis Evans for the record. Yes, it's really important differentiations there, so really good to get an understanding of how the ccTLDs work set. Any questions? Tracy, I see you first. Thank you. And then.

TRACY HACKSHAW: Yes, thank you for the excellent presentation. Can you perhaps enlighten us as to why do you think the African region response rate was so low, it's only eight ccTLD respondent? And if so, is there a possibility that there may be some hidden issues that we may not understand, is there?

NICK WENBAN-SMITH: I think is a fair question, and we tried to be transparent about the data that we've collected. I think it is geographically representative. I think I talked before in our preparation session around the difficulty of drawing conclusions from different datasets where different registries are very different depending on the organization.

So we're looking more at a higher level of trends rather than a specific thing. I think engagement in the African region in the CCs is pretty strong, generally, but of course, it's a voluntary survey, we don't

mandate that people participate, we try to encourage, we have some excellent representation from the African region, so yes.

But I think there's more to do. I couldn't identify why there's a particular shortfall. One of the members of the committee actually is the Botswana registry, who has been very excellent and very active and has tried to gather support. So we are inclusive on that front, but yes, I think it's a challenge. I don't think it's just in this group, that it's a challenge.

CHRIS LEWIS EVANS: Thank you, Nick. Susan, USA.

SUSAN CHALMERS: Thank you kindly Nick. Susan Chalmers, the United States. Very much appreciated your presentation. You had made mention of trusted notifier programs, I was wondering if you wouldn't mind sharing a few words on the findings of the survey there. Thank you.

NICK WENBAN-SMITH: So one of the nice things about being a ccTLD is that your jurisdiction and law of operation is clear and unambiguous. And what I think comes through from the survey trends is that almost all of us have a very close relationship with our domestic law enforcement colleagues. Obviously, Chris is on the same platform. But I'd like to-- Chris, you have an opportunity to respond if he disagrees, but I'd like to say we have a very good relationship and have a very close cooperation.

I think it's independent in our case, sometimes ccTLD is a part of government and therefore that constrains how they can operate. But I think, from my perspective, as certainly as the UK registry, if there's good information, from my perspective, the work of our domestic law enforcement and certs from the cybersecurity centers and other intelligence agencies, they provide us with good information, which is helpful, and we'd be stupid to not take advantage of that and to use it.

And I think, across all the ccTLDs, there's nearly always a strong cooperation with both the government in terms of the legislative framework, but also with the law enforcement agencies. But also, we're not proud about knowing everything, and if there's a reputable source of information, who will give us something to action, then, of course, we will take that, because ultimately, they're helping us do our job of operating a good clean registry with low levels of abuse.

CHRIS LEWIS EVANS: Thanks, Nick. And sorry, I got a lot of colleagues in front who have not had the opportunity to meet yet.

SARMAD HUSSAIN: Okay. My name is Hussain from Iran. First of all, I thank again for this interesting presentation. I have two quick questions. First, similar to what we have seen in the first presentation from FBI, is there any similar report in ccTLD level about how many reports we have seen, observed during recent years about this DNS abuse? And my second question, is there any like statistics or report showing the inter-governmental collaborations to face DNS abuse?

This is another question. Because when we talk about the ccTLD, sorry, I have difficulties using this word, I'm always in trouble, the government's normally they should have more interest because they are in charge or they are close to this domain registrar. So my question is how we can foster the collaboration in this regard. Thank you.

NICK WENBAN-SMITH: Sorry, in relation to the first question around surveys, there's a lot of data here. ICANN itself runs it's domain abuse activity reporting mechanism, and that includes some ccTLDs that gives direct comparisons, I mentioned the DNS abuse institute, which again, provides some independent and objective measurements on these sorts of things.

And I think it's a very comprehensive study was done by the European Commission, and a very lengthy report, including some interesting data and findings came out of that. So there's quite a lot of data now done. And actually, a lot of this data is current data, it's been done in the last couple of years, as this topic has become a high interest area across the community.

In terms of intergovernmental cooperation, I think, to foster that is the reason why we're here talking about this today. Tell me if I'm wrong, but it's not really for me to say, but from my perspective as standing outside of the government organizations, I think this is what this is about.

SARMAD HUSSAIN: Yes, just regarding my second question, is there any news you can share us just to encourage because this is not a new topic for ICANN, for GAC as well. Just I wonder, during recent years, have we seen any kind of collaboration between governments just as an information? Because sometimes, one authority, you see a DNS abuse, as we have seen in the first presentation, registrar or registry or hosting, they are outside the authority, so if they work together, they can avoid it.

NICK WENBAN-SMITH: Yes, so there are some really good collaborative projects put in place, so I think Emotet is a really well-known malware source responsible for a large amount of ransomware. Europol ran a project, I think there was 15 law enforcement nations somewhere, I forget now exactly, and they combined together to take down that malware platform, which included a large number of countries, some ccTLDs, very small percentage, [00:52:38 - inaudible] for you, thank you, and some other gTLDs as well, to disrupt that service. So there is, and it's a close collaboration, and the use of Europol and Interpol really helps that collaboration on a sort of inter-governmental level.

NICK WENBAN-SMITH: And then moving across to Samaneh for her presentation. Thank you.

SAMANEH TAJALIZADEHKHOOB: Thank you, Chris. Yes, thank you. So my presentation is mostly about how we perceive abuse within OCTO, Office of CTO, what kind of research we do in this domain of DNS abuse and what is our

focus will be also in the future. The first disclaimer I wanted to have is when we talk about abuse in this session in general, mostly within the ICANN community, we are talking about what is reported as abuse, what is listed online being abuse.

Most of the times, there is no extra evidence gathered that this materialized as abuse became an incident. So what is reported actually became an incident. This presentation also is only about what is reported and listed. For this specific research that I'm presenting today, we do not gather extra evidence so that to be sure that the report actually materialized.

Next slide, please. So, as many of you may know, we have a project within Office of CTO called domain abuse activity reporting, DAAR. It's one of the tools that we have in house, and it's developed many years ago when the topic was relatively new. The purpose of the system was, and still is, to just report on where abuse or security threat is concentrated, according to what is listed online on the so called reputation block lists. These lists are mostly gathered from third party sources, so it's not ICANN list, it's from all different providers.

And the DAAR system collects this data and just aggregates it to different levels for now gTLD and ccTLD levels. Within the community, we talked about the DAAR data a lot, so today's presentation won't be about DAAR. I just want to briefly touch upon the statistics that we have today from DAAR. So as of February 2023, we see in the DAAR system and only for gTLDs, we have 1145 gTLDs that the system covers for February, and we've seen around 216 million domains out of the gTLD zone files there. Out of these, 427 TLDs content domains that are

listed are security threat, and the sum of those listed domains were around 640,000.

Next slide, please. In the next few slides, I will be showing trends, these are trends again out of the DAAR data. The system goes back to October 2017, so we are plotting the data since then. This plot shows the total number of domains in zones of gTLDs that ICANN have access to since then, and you see that the zones are separated by two types, new and legacy gTLDs, and, as expected, the number of domains in zone grows over time. So that's what you see, the green line shows the changes in the new gTLD zone sizes, and the black line shows changes in the legacy gTLD sizes.

Next slide, please. In this slide, we show the changes in terms of abuse over time. Again, the colors are new and legacy gTLDs, and what you see is that since 2017, there has been a lot of fluctuations in numbers. The reason why in the beginning of this report, I emphasize the fact that we are looking at the domains that are listed as opposed to incident is that the fluctuations could be due to multiple reasons, one of them abuse actually changed.

So it's hard to conclude that if we see from this plot, an onward trend or downward trend, it's hard to conclude that this shows immediately that abuse is going up or down. The reason is because this data is fully dependent on the sources that its collected from. It could be that due to policies in place for those sources that provide data, it became harder to detect certain types of abuse, let's say, WHOIS, the GDPR was one of those policies, but there are multiple other things in place over multiple points in time.

So what we can conclude from the trends is that we see according to what is listed online, the trend is downward from 2017. This could be as much due to policies as the trend itself going down, namely abuse becoming less. This plot shows the total counts of domains that are listed online, that is the sum, the absolute sum. So here we are not taking any size of the gTLDs into account, this is just a rough sum of counts.

Next slide, please. This plot communicates the same information as the previous plots with only difference that here, the counts are normalized by the size of the zones. So if a certain gTLD has more domains, it should be accounted for when it comes to counting the abusive domains. This is what you see, when you normalize the accounts, then the trends change a bit.

So for instance, that was significant for legacy gTLDs where we see a lot of gTLDs that have very big zone sizes. Again, take a look at the timeframe of this plot, it's from 2017 to February 2023. The plot shows a downward trend from 2017 if we look up to now in terms of number of domains that has been listed as security threats. Next slide, please. Here you see a breakdown of the types for security threats.

Again, the numbers are normalized pair sizes of zone files, but you see four types of phishing, malware, spam, and command and control security threat types. If you look from 2017, specifically for most types except from phishing, you'll see that the relative numbers declined over time.

Next slide, please. One of the points that I want to emphasize in today's presentation is that this is what we see from the data we

collect in the DAAR system and that is limited to the third-party reputation blacklist sources we collect. This is one cut of the data from the perspective of this system. This is not holistic, this doesn't communicate information about the whole abuse landscape. There are other reports, there are other good practices, community works that are collecting other sorts of data, either similar or they complete these reports.

DAAR, it was specifically only reports on concentration of abuse, there are other reports, for instance, DNS AI compass reports that also looks at how registries and registrars react when abuse is reported. There are reports published by an anti-phishing working group every quarter that reports specifically on phishing focus, all of these provide different perspectives into the DNS landscape.

Important is that one cannot compare these together to say ICANN OCTO DAAR report says DNS abuse is going up, but artificial working group says it's because the specifications of these reports, the timeframe, the perspective, the data that is used, is defining the results of other outcomes. So, what we hear often in the community are these comparisons that are not even comparable. And here I want to show that the lens you took to look at DNS views really influenced the result, and this is what we see.

For instance, if we move to the next slide, please. I am showing the same data that is collected by the DAAR system in a different timeframe. I want to emphasize perspective matters, terminology matters. Here, we see an upward trend when we look at security trends or trends that are normalized. The reason is because I just

chose a different timeframe, and in this time frame I can say abuse is going up.

Now, again and again, I want to emphasize that the methods, you look at the data and you analyze the data, basically defines what results you get or for most part of it, and this is what our committee needs to also put emphasis on. Next slide, please. Just some other work that is done within the Office of CTO is apart from where abuses concentrated is also to make the methods that we look at abuse more reliable.

Identifying park domains was one of those things that we are doing and we are publishing on soon. The reason park domains is important when you look at abuse is because when we take zone files of gTLDs and look at domains that are not active, so do not serve active or are not active either, they are annexed domains or they are parked for different reasons, it's important because when you normalize by the size of the zone, you actually have to take these out because they are not distributing anything, by definition, they cannot be of any types that we are talking about. So the numbers are interesting.

When we look at the zones, we see around 10 to 20% in active domains right on the date that the zone file is published. So if we take the zone file of today and look at active domains, we see up to 20 persons are inactive, which is important when we talk about it abuse metrics. The second thing that is important, and we are doing research on and other groups also, we're outside of ICANN, is the amount of time that domains are up, which is often been interpreted the same as how domains are mitigated.

We are doing measures and we are very careful with not mixing these two terms, uptime is not equal to mitigation. The reason is because from the moment that the domain is listed on an RBL, it could be until that moment and before, that several things might have happens. If we look at the domains that are RBLs, and look at how many of them are already down, we see like, around 30% of the domains are down by the time they are listed on RBLs.

So if we start to take mitigation as the amount of time that the domain is up, from the moment it's listed on any reputation block list, then we are losing a big window of time where action has already happened and we haven't detected it. That's one thing. Another thing is that mitigation or measuring uptime cannot be done within one single method because each threat type use their own evasion technique.

Phishing, for instance, has a very sophisticated evasion technique by definition because of its attack. And from the most recent academic studies, we see that 30% of phishing cannot be detected in terms of the amount of times the domain is up because they use evasion techniques that are harder to detect. Command and control are the same. By definition, command control is set up in a way that the domains should be short and they rotate, and they have whitelisting techniques in place so that the uptime is minimal and makes it harder to detect.

So these are some of the other topics that within the Office of CTO, we are working on to make the basically the abuse metrics more precise when we report on stats of abuse going up and down. And we typically keep an eye on the state of the art of the research in the

community and within the academic area so that we are up to date and we are in contact with, and we are happy to have discussions with you guys, receive input, and have discussions about these topics, if any. Thank you, Chris.

CHRIS LEWIS EVANS: Thank you very much for that. So any questions, Kavouss around?

KAVOUSS ARASTEH: Yes, thank you very much, Madam, for the interesting presentation. I have a small, I would say, question, and that is the following. You said that combating or countering the difficulty depends on the size of the zone. Am I right? If that is the case, do you have different approach for different zone, and so on?

The second question, do you consider that we have been relatively successful in combating and countering this abuse? And the third is that, what do you expect from government, from GAC members to do in this regard? What action they have to take, what feedback they have to send, to whom they have to send, and how it should be sent? Thank you.

SAMANEH TAJALIZADEHKHOOB: Thank you for the questions, Kavouss. About the first question, that is not what I said. But it's a good question because it's an important distinction. Whether combating DNS abuse depends on the size of the zone is a matter that I didn't talk about because it relates to the policies or the facilities to-- it relates to gTLDs and

registries. I cannot absorb that from the data I have or the reputation data that is available publicly.

What I did say was interpreting where abusing is concentrated should be taken into account size of the zone, because the more domains that a gTLD has, the more attack surface is there, so there is more to mitigate. So the size should be taken into account when we report on abuse. About your second question, which I --

KAVOUSS ARASTEH: How far you have been successful with combating?

SAMANEH TAJALIZADEHKHOOB: It is very hard to answer that question. The reason for that is because there is no single holistic data that can talk about that. So, if anybody ever-- so, I want to make a statement about that. I can say that there are policies in place that helped proactive anti-abuse measures became effective rather than reactive. For instance, bulk detection of registration, et cetera. But whether as a whole that has been successful, I have no information to talk about that.

KAVOUSS ARASTEH: The third question was that what do you expect from us? How we should act, how we should send the feedback? So, I think we have to also do something, I don't know, each of us. So, what is the recommendation, what is the advice, what is the requirement that just listening that they had been abused, you do this, you do that, what we have to do? Thank you.

SAMANEH TAJALIZADEHKHOOB: As a leader of a research group, the only comment I can make on that is to-- so one of the goals of the DAAR project was to facilitate and educate our community members to be able to do their own abuse research and abuse reporting and monitoring. That is what we are happy to help the GAC members to do and to provide expertise and trainings if necessary, so that every government can or registry registrars community members can do their own abuse monitoring.

KAVOUSS ARASTEH: I have a question if you allow me. Do you believe that it may be useful that some sort of question or inquiry be said that have you ever encountered any DNS abuse? Which area you have encountered? What you have done in that aspects? And whether if you have reported, the problem has been resolved or problem reappeared in different form and different case, would it be possible that at least these sorts of communication back and forth would be in order to help the researcher to have some feedback? Thank you.

SAMANEH TAJALIZADEHKHOOB: What you just said is kind of a survey method and it's a qualitative method to gather information. Yes, can be done.

CHRIS LEWIS EVANS: Perfect, thank you. Sorry.

ASHWIN RANGAN: Yes, thank you. My name is Ashwin from Indonesia for the record. Maybe just following Kavouss' questions. I would like to say the possibility of ICANN to support "the socialization of this type of problem you see for us, for the country." In Indonesia for examples, we have the NIC is looked after by the Australian, the APAC, the Asia Pacific NIC, but ICANN also have offices in Singapore that can support us for example, to carry out, what do you call it, socialization or whatever, trading or whatever in DNS abuse.

Now it can be also related to the standard regulation that are already in the country. For example, as a member of ISO and IEC, the government request many operators to use ISO/IEC 27001 as security management. Now how can then you include this kind of DNS abuse problem when you do the certification of ISO/IEC 27,000 for the DNS operators, that kind of things, that's one of the possible topics for discussion, for further discussion of [01:14:47 - inaudible], there'll be more and more topics that I cannot discuss here.

But the 27001 is widely used because we are a member of ISO and IEC, not only Indonesia, of course, but almost all countries, and how it can be connected to DNS abuse in this process of certification, this kind of things that can be discussed and then socialize further. Thank you.

CHRIS LEWIS EVANS: Yes, thank you Ashwin. And I think it's really important just to summarize that we understand everyone's viewpoint here and have the quantitative data along with the quality of data to make a proper assessment of the impact of DNS abuse and what we can do to address it, and to Kavouss' point earlier is to really focus down on

areas where we can support that within ICANN as a multi stakeholder model.

We're now at the end of the session. So I would just like to thank you all for your questions and interaction, and thank you all to the panelists as well. And no doubt, see you in another session soon. Thank you very much.

TRACY HACKSHAW: Thank you very much, Chris, PSWG team, ccNSO DNS Abuse Steering Committee, SSAC, as well as ICANN Org. Before you go, though, and I think this is something I wanted to make sure before we finish, we wanted to put a regional perspective on this topic. This is one of the things that the capacity building workshop was supposed to achieve, and I noticed that time is running out. But if there are some -- Gulten, the slides, we have some questions on the regional perspective, if you can just put that up.

So as you can see those questions there. They're not really for you, they're for the audience, but I want to understand if there's any thoughts in the five minutes because time has run out on this for the LAC region. Do you see any specific issues that we need to address for the LAC region given that this is where we are with discussing today? And what issues do you think that kind of like what Kavouss was asking a little bit, but now for the LAC region?

Is there anything that you could tell the governments to do specifically in this region to help with this issue, if at all? So I'm going to toss to

you first and ask maybe one question from the audience before we go to break. Just anybody from the panel.

CHRIS LEWIS EVANS: So for the government's, number one, does the DNS abuse impact Latin America? Yes, definitely does, impacts everywhere, all the joint work we've done together in law enforcement, it's multinational, everywhere. What can the government's do, and I'm going to sort of look at Nick a little bit here, it encourage the ccTLDs that you work with to engage with the surveys.

I think it's really important to understand how this impacts your countries, and how it impacts on your own ccTLD. A lot of the individuals that are impacted trust their ccTLDs. So it's really important to get that right and get that level right. And the ccTLDs do some really good work, so engaging with that community, I think is a really big step. And that's probably one I would recommend it for that region.

TRACY HACKSHAW: Thank you, Chris. So just quickly to the audience from the LAC region. Anyone from the LAC region would like to respond to any of these questions before we go to break? And if you don't know, we call upon you that we have colleagues from the Caribbean, colleagues from Latin America. Anyone would like to speak to this? May I ask Nicolás if he wants to see anything on this.

NICOLÁS CABALLERO: Not really, other than thinking this fantastic team? Not really, I don't really have a question unless any of my distinguished colleague.

TRACY HACKSHAW: I just saw a hand go up. Yes, thanks Nicolás.

GABRIELLA SZLAK: Hello. Good afternoon. My name is Gabriella from Argentina. It's not really question, it's just a comment. We are going through negotiations with the United Nations on cybersecurity, cybercrime, and also the Budapest Convention also, the second protocol. So I don't think you have to respond right now because we are finishing, but I would like to know, which is the involvement in a DNS abuse on these negotiations going on. Thank you very much.

TRACY HACKSHAW: Sorry, I think she asked about the UN cybercrime discussions that are going on.

CHRIS LEWIS EVANS: I think I missed one word. Was that what's the ICANN involvement in those processes?

TRACY HACKSHAW: Yes.

CHRIS LEWIS EVANS: Sorry. Thank you. So from a law enforcement perspective, which is the only one I can talk to directly without passing over to some of my other colleagues here, we are engaged, we do utilize functions within the Budapest, and obviously the UN one is still going through at the minute. So they provide us with important tools to be able to address DNS abuse or address cybercrime.

So those sorts of multi nation bilateral agreements are really important for the fight. And making sure they are written in a way that has a good understanding of ICANN policies is really important to work together. So I think that's the main thing for me. Thank you.

NICK WENBAN-SMITH: Okay, so speaking in the capacity of someone who is involved in law enforcement as his day job, there are relatively few mechanisms to obtain data across international borders. The most commonly employed is the mutual legal assistance treaty. It's quite burdensome in terms of the amount of work that has to be done to engage on that. And it's not necessarily appropriate to something that is as foundational to an investigation as obtaining registration data.

And so I think that just speaking as someone that's involved in this kind of work, it's encouraging to see discussions such as those that occur at the second additional protocol for the Budapest amendment to address these issues that still are very important, but might not be best served by unlap processes. And so, it's very encouraging to see nations that collaborate to enable such.

TRACY HACKSHAW: All right, thank you very much, PSWG, and I'm going to toss back to my colleague, Pua, for the final wrap up. Thanks.

PUA HUNTER: Thank you, Tracy. And thank you so much, Gabrielle, Dr. Samaneh, Chris, Jeffrey, and Nick for making the time. I know it's last minutes to come in addressed the GAC colleagues today this afternoon. Thank you so much for your time, and GAC colleagues, they'll be around this week, so feel free to go up, you can see them, their face now, feel free to go and see them if you have further questions that you have later on in the weekend.

We'll be back here for our coffee break. And thank you, Tracy, for the regional perspective, for leading that small part of the session, and thank you so much, everyone. A round of applause please for our presenters.

[END OF TRANSCRIPTION]