ICANN83 | PF – At-Large Plenary 2: Progressing DNS Abuse Mitigation Efforts Within ICANN
Thursday, June 12, 2025 – 10:45 to 12:15 CEST

BRENDA BREWER: Hello and welcome to the At-Large Plenary 2: Progressing DNS Abuse Mitigation Efforts Within ICANN. My name is Brenda Brewer, and I am the remote participation manager for this session. Please note this session is being recorded and is governed by the ICANN Expected Standards of Behavior and ICANN Community Anti-Harassment Policy.

During this session, questions or comments will only be read aloud if submitted within the Q&A pod. Interpretation for this session will include English, French, and Spanish. If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom. On-site participants will use a physical microphone to speak. Please state your name for the record, the language you will speak if speaking a language other than English, and speak at a reasonable pace. And I will now hand the floor over to Jonathan Zuck, ALAC Chair.

JONATHAN ZUCK: Thanks a lot, and thanks, everyone, for joining us for this cross-community plenary on DNS abuse mitigation brainstorming, if you will. I think it's important to always reiterate that this is an ongoing conversation and not be-all end-all session where we solve all

problems. Justine told me to say it's just the beginning, but I guess it might be it's just the middle as we talk about this topic. And I know that frustrations run high across the Board, the community on this, because everyone has a different perspective on it and different burdens associated with it as well.

And so, it can be a tense topic so let's all try to remember what Brenda just read to us about standards of behavior, and we'll keep it calm and hopefully cooperative, because I think in the end, we all want the same thing. And so, that's the upside of this topic. We asked folks to just come up with a couple of suggestions, so not to give exhaustive lists that are too difficult to react to, etc. So, let's just as we go through, we'll keep thinking about more, but let's keep it to a couple as we go through it.

I don't know what's happening with the agenda. As far as the At-Large is concerned, we don't have a particular expertise in this area. We're not the ones filing these abuse reports in most instances. One of the things that we are working on is some end-user education to do what is possible on the other end to get people to be more aware of what these attacks look like and be less susceptible to them. But here in the ICANN community we want to continue to beat the drum around preventing DNS abuse at the start or at the very least reacting to it as quickly as possible.

And so, the two things that come to our mind as being potentially priority areas for consideration, one is an exploration of the implications and correlations associated with bulk registrations.

And I'm aware that that's a term without specific definition, but if you look at the INFERMAL report and some of the other research that has made its way around the community, there does appear to be a correlation between getting high numbers of registrations at the same time and having them be abusive. And I know AI has complicated this. I know that APIs for creating multiple accounts has complicated this. But I think we continue to believe there's something that can be done on the front end when folks want to register a large number of domains.

The second is what has come to be known as the pivot. But that's, again, an idea that's been around a while, which is trying to figure out when once a malicious domain is identified, identifying other domains associated with that registrant that might be taken down at the same time and looking at how to make those determinations and how to bring about those shutdowns. So, those are a few areas that I think we are most interested in. And so, I don't think I need to take more time with that. I'm happy to pass the microphone to I think Mason Cole is next in our list. If we want to bring the agenda back up perhaps, then we'll keep track of the speakers but, Mason, take it away. Give us a couple from you.

MASON COLE Thank you, Jonathan. Good morning, everyone. My name is Mason Cole. Well, for another two weeks, I'm chair of the CSG. And, Jonathan, I think I had some slides. Are those available?

JONATHAN ZUCK Okay. Yeah, are there slides for Mason?

MASON COLE There we go. Thank you very much. So just by way of pretext, let me say that the CSG, I also chair the BC, both organizations have been very active on the abuse issue now for at least a couple of years. And starting in Istanbul last fall, the CSG began advancing some ideas about new tools for combating DNS abuse. And I'm pleased to say that there's overlap in the community with some of the ideas that we advanced and that were part of Graeme's NetBeacon white paper. Oh, yeah, I'm sorry. Thank you.

There's some overlap in terms of what's been proposed by the CSG and then some of the same ideas have come from other parts of the community. So, it's good to see that there's already some agreement on some tools that can be used to address the abuse problem. So, let me just provide some context. I'm sure some of this information is not new to those of you in the room, but DNS abuse is really a long-term issue. We don't expect it to be solved in ICANN's Next Round of identification of tools to combat abuse. Abuse, unfortunately, is going to be with the DNS for a long time. It's become endemic, meaning it exists internally and probably can't really be eradicated.

We've seen abuse since the first iteration of the Internet. I read an interview with Vint Cerf, who said he got his first spam message all

the way back in 1979. So, if Vint has been spammed for the last 45 years, then we know we have a problem. The global problem is real and it is expanding. So right now, in dollar figures, the cybercrime economy is now estimated at $9.5 trillion, which is now the world's third largest economy by gross domestic product, and those figures are from the World Economic Forum. And that number is expected to go up, obviously, in the coming years.

So, we know that the abuse problem is expanding and intensifying, and this is part of the reason the BC has been beating the drum so hard on abuse, because those that we represent are the ones who take the economic brunt of abuse activity.

And then we also wanted to point out that DNS abuse will never really be fully defined or even resolved, and we hearken back to the SSAC's advice to the Board in SAC115, where they said that the definitions that exist in the contracts, in ICANN's contracts, don't represent all the forms of DNS abuse that exist or are reported and are acted upon by service providers. New types of abuse are commonly created, and no particular list of abuse types ever will be comprehensive. So, we don't expect that, again, DNS abuse can ever really be fully defined, and fully resolved, or fully dealt with over time, but because ICANN is in a unique position to do something about abuse, that's what we're here to try to do.

Next slide, please. Okay, we were asked to put together-- Nope, that's not my slide. There we go. Next one in the slide series. Oh, I guess it was reformatted. So, okay, very good. So, I was asked to

provide a couple of topics in terms of where the CSG is interested in the abuse topic, give a problem statement rationale, and then potential policy questions.

So, the first issue is abuse occurring at scale, which Jonathan just alluded to. Abuse is staged across multiple domains, either under a single registrant or under one registrant's multiple registrar accounts. This is known as the pivot or associated domain check, whatever you want to call it, but we're all starting to coalesce around the idea that this is a real problem and that abuse can be taken out in a bigger swath at one time if you can act at the account level.

So, abuse reporting by individual domain name today is an inefficient way of handling abuse complaints. There's no outward visibility into the bad actor's real scale of abuse, and if you're a victim of abuse or you're reporting abusive activity, we need registrar level help for identification of other names or bad actors who are conducting abuse and then get help with mitigation. So, what policy questions does that raise?

Number one, how do you codify account level mitigation duties either in the contracts or in a best practice? And then how do you document resolution of that abuse back to the reporter of abuse? Sometimes you report DNS abuse, it goes to the registrar, action is either taken or not, but the reporter may or may not know what's eventually been done about abuse.

Second issue is on the issue of imposter domain names, and you may have seen this in the media last October when there was a US senator who wrote a letter to some registries and registrars to raise the issue of imposter domain names. He gave an example of fox-news.top. If you're unfamiliar, Fox News is a media outlet in the US and Senator Warner's concern was imposter domain names were being registered and used to dupe consumers into fake websites and as a way to advance fake news and influence the approaching US elections.

So, this isn't an issue of typosquatting. Sometimes these names are exact matches to known entities or known brands or known organizations. And the problem is that these are registered, put to use, and then taken offline so quickly that UDRP is not an effective tool to deal with those. UDRP is a process meant for trademark infringement, and it's too slow a process, too expensive, too cumbersome, and it deals with too few domain names at a time.

So, the policy questions here then are how do you create a mechanism there for registrars to help, and then importantly, how do you define a standard for acting against impersonation? This is a real problem, but it skates along the edge of content, and that's an area where registrars are loathe to tread, understandably so, and it's going to be important to be able to define a standard for how to move forward on an issue like imposter domain names.

Okay, next slide, please. Or that may be it for my slides. Much to the relief of everyone here in the room, Jonathan. Back to you. Thank you very much.

JONATHAN ZUCK

Oh, thank God. Yes, no, thank you. Thank you, Mason. That was very helpful. Gabriel, I think you're next.

GABRIEL ANDREWS

Hi. All right, I probably have a slide, too. Awesome. My name is Gabriel Andrews. I am a co-chair of the Public Safety Working Group. My day job involves working for a US law enforcement agency, FBI. We thought that it would be helpful to share the unique perspective that law enforcement might bring to these conversations. I think we don't often have the same perspective as other folks in the room.

And so, for awareness, when folks come to us to complain about being the victims of Internet crime, we have a portal that we direct them to go to, and that's ic3.gov. It is used to help us to compile the information about the bad guys that are victimizing these folks, and it really helps us to justify opening new investigations. But as a side effect, it also allows us to collect stats on the various types of crimes that are harming people. And even though this is pretty US-centric, we get reports from all around the world, and I believe that what we see and what we think are the top categories of crime are

probably very similar to what other law enforcement agencies around the world are also seeing.

So, the questions that we brought here and the perspectives and the potential policy questions we see as our top reported crime by the dollar loss is something that's called cryptocurrency investment fraud. It's also known as pig butchering, though that's not the preferred term from our perspective. But if you're not familiar with this, I'd really suggest that you should be, and you could take a moment later to go onto YouTube and look up John Oliver's Last Week Tonight. He did a whole episode on this scam. It is an incredible dive into it, but it can be helpful to protect yourself and your family.

The short of it is bad guys will try to convince people to invest in cryptocurrencies, and they'll take them for their life savings. As part of their schemes, we've seen them to engage in bulk malicious registrations of domain names, hundreds at a time, to promote their fake cryptocurrency exchanges. And so, Jonathan, the question that I have listed here I recognize is almost identical to the one that I think I saw in your ALAC, is how can policy here most effectively introduce friction into the malicious use of these bulk domain registration tools? And just to highlight that that actually would be helpful in addressing the largest category of crime that's currently being reported to us, amongst others.

The second question is that if you were to count just the number of complaints that we receive, so we're not organizing by loss of dollar

value here, but rather just what's most commonly reported to us, that would be the general category of phishing. My friend, Brian Cimbolic, over in the audience—hi, Brian—he rightfully asked me yesterday if we had the ability to only look at phishing that involves domains or emails. Unfortunately, I don't. I just think it's all in the same bucket. But we have to assume a fair amount of that is domain-based phishing.

And so, the question we have is when we know that so many of these phishing domains are malicious registers and homoglyphs, that is lookalike domains that target victims, my question is what possible policies can address the repeat malicious registrations of lookalike domains that impersonate real victim domains? And I wanted to float those for conversation.

JONATHAN ZUCK I thought we should turn the microphone on. Thanks, Gabriel, and thanks, folks, for getting this conversation started. And then we have basically a reaction round here from a variety of different perspectives, registry, registrar, and human rights. And so, I guess without further ado, I will hand the microphone to Dennis.

DENNIS TAN Thank you, Jonathan. This is Dennis Tan for the transcript. I work for Verisign but here I'm representing the Registry Stakeholder Group. So, I also co-chair with my colleague Reg on my left of the

CPH DNS Working Group. So reactions. So, the first one, I think there are commonalities. Let me take a step back.

So, on Monday, the CPH in the DNS Abuse Community Outreach, we presented four topics for potential work for the community to consider, including Policy Development Process. These four topics are the pivot idea, also known as the associated domain check, which is presented here. The second one, strengthening the obligations registered resellers in terms of use of API and other related DNS abuse mitigation requirements.

Third one, work on botnet DGAs. How can we registry operators, gTLD registry operators and potentially ccTLD operators alike, benefit of a framework in which we can have a uniform operational framework to ingest and distribute information about DGAs. And DGAs is domain generation algorithm. This is what the botnet operators use to create a list of hundreds, maybe thousands of domain names that potentially are batch register and use in time for operating those phishing attacks and whatnot. Individual registry operators today will have to go and look for that information, vet it, verify it and whatnot. So, what we're proposing is a cleaning house that does technical work up front and then gTLD registry operators can consume it and prevent DGAs from happening.

And the fourth one is one where it talks about how to report phishing to contracted parties. Time and time again we've encountered that the quality of reports, lack of evidence or are

misreported. So how can we use the ICANN community to elevate these quality standards in order to reach a critical mass to abuse reporters so that the reports that get to contracted parties are actionable so that we can reduce the mitigation times.

So, with that backdrop, again, I think ALAC, you propose and let me, maybe at the risk of sounding repetitive, Jonathan, the first two ideas or the two ideas proposed here from the ALAC is the implication and correlation with the use of bulk registration as studied in INFERMAL. So, that talks about the unrestricted use of APIs in order to create registrant accounts or domain names in bulk, at scale. And the other idea is the pivot idea. So, those two overlap with the ones proposed by the CPH, so I think happy to continue working on that and develop those ideas. CSG's one is on, I think similar. The number one is on malicious registrations in bulk as well. Is that right? Oh, I'm sorry, associated domain check. So, I think there's an overlap there as well, so happy to work on that one.

On the second one, sorry, I didn't bring my reading glasses here and I'm struggling a little bit, so trying to adjust my eyesight here. Yeah, impossible. I think that's something that we need to continue working. I appreciate the idea put forward, and we at the CPH will want to have further conversations on that one. Oh, yeah, sorry. And Gabe's from the PSWG, I think also the friction on bulk registrations using API. Those tools also overlap with the one the

CPH has put forward, so happy to have further conversations in order to detail what we can work on.

On number two, I want to ask clarifying questions. The first one clarifying question is that qualifier repeat malicious registration. I would like to understand what do you mean by repeat malicious registration. And the second one would be more foundational. When you are talking about phishing report or phishing domain names for malicious purposes, what do you see in the policies and procedures today that are lacking that doesn't address the issue that you are proposing here?

GABRIEL ANDREWS

Thank you. This is Gabriel again. I think the first one's easier for me to answer than the second, but just to clarify what I mean here is bad guys, they might come to you, and they might register a number of domains under one name or one payment. They might try to change their name and do it again and so forth. And so, I suppose I'm really just expressing the hope that through conversation we can find out to what degree you're able to detect that. I don't know if you could have ideas on account level action as opposed to domain level action is one step.

Maybe even there might be ideas for when they might use multiple accounts, but still be able to track that. But the point is that if they keep coming back to the well to pull out poison over and over and over again, how can we try to make it harder for them to do that as

opposed to having to evidence in action each new domain that they register retroactively? Does that make more sense?

DENNIS TAN

I think so. And let me play it back and make sure I understand the use case here. We're not talking about domains that we're registering batch, maybe just changing one letter or whatnot, but they register one, didn't work. They come back, they register by changing just slightly a letter or two in the screen, and they come back using this pattern, if you will, just by changing by testing and maybe using different registrant accounts or other credentials and whatnot. Is that?

GABRIEL ANDREWS

For the most part, yes. And I think based off what I heard you say here and what I heard the Contracted Party House say earlier, I think that one of your proposals about addressing or pivoting off of information also might be applicable to this. And so, I think there's some degree of alignment there. And so, maybe if anything, what I'm saying is that if we're able to take or if we're able to come up with policies that support action at account level behavior or bad actor level behavior as opposed to just domain level behavior, then you're having the impact against the most commonly reported crime that we're seeing, if that makes sense.

JONATHAN ZUCK Thanks, Dennis. And Reg is next, I believe.

REG LEVY This is Reg Levy from the Registrar Stakeholder Group. I'm co-chair with Luc of the Registrar Stakeholder Group DNS Abuse Subgroup and co-chair with Dennis of the Contracted Party House DNS Abuse Subgroup. This is all really interesting and we are delighted that these proposals have been presented to us. And we're going to take all of this back to our respective stakeholder groups. As Dennis indicated, there's a lot of overlap. I think Gabe and Mason also indicated that there's a lot of overlap. And so, we're looking forward to continuing that conversation and the future work.

JONATHAN ZUCK Thanks, Reg. Do I have Graeme? I think Graeme was next. Go ahead.

GRAEME BUNTON Hi, everybody.

JONATHAN ZUCK Wake up.

GRAEME BUNTON I'm here. My name is Graeme Bunton. I'm the executive director of the NetBeacon Institute. NetBeacon Institute is a part of Public Interest Registry, but our jobs are to try and make the internet safer

for everybody, really focused on DNS abuse. And we put out a white paper on these sorts of topics about two weeks ago ahead of this meeting, and we did that for a couple reasons.

Primarily this is an issue we've been talking about as a community for a long time. It felt like there was really beginning to be a push to do something what's next, especially after the contractual amendments that changed abuse at registries and registrars last year, and how are we going to continue moving forward.

And we wanted to, frankly, help shape some of that conversation because a lot of it to us felt like it was missing the mark a bit, and so we went out and put a bunch of ideas on paper. And this is for community discussion. From my perspective, publishing that white paper has been a success. I think we've helped inform people. I think we've helped shape ideas. We would love it if the community took some of these ideas and continued moving forward, but that is about community engagement and discussion.

Next slide, please. Right, I just kind of covered that. That last bullet point is important. I think we all want to believe in the multistakeholder model. We want to see success within the ICANN community that we can take an issue and get something done on it, and boy, these are important issues. How do we get something done? And for us, we really wanted to see if we could provide examples of what narrow scope might look like so that we can all sort of familiarize ourselves. Whether these are the ideas or not, well, how do we scope these things in a way that we think as a

community we could try and tackle these issues and move forward? And so, that was really important for us as we were putting these ideas out there.

Next slide, please. I'm not going to go into depth here because I think we covered these already in previous presentations, associated domain check or a pivot. How do we find more abuse related to confirmed malicious registrations? There's a piece I will highlight here as we're thinking about what's the difference between reactive processes and proactive processes to reduce abuse.

Checking other domains in account is a reactive process, but it's also time-consuming, and so what we like about this sort of work at the Institute is that for a registrar that has to do this on the regular with accounts with large numbers of domains in them, is that that's time-consuming and expensive, and we think and hope that it will incentivize registrars to be thoughtful about who they let access the tools that enable them to register large volumes of domain names. So, there's, to this one, I think, and why it's an interesting idea for the community to consider is, A, it helps react to abuse at scale, and B, it helps potentially to prevent abuse at scale as well.

Next slide, please. Gating APIs, I think we've covered this as well. These are the tools that enable people to register large volumes of domains at once. How do we put friction in place before people have access to these tools? And there's a point I'm going to make

here about this idea that I think is important, which is, from our perspective, we think that friction should be based on customer reputation, not on who that customer is, but on what activity they have done.

And I'll dig into that for just a brief moment. I think there's a lot of interest in registrant verification and data accuracy within this community. But boy, it's also a bit of a landmine, and so it's hard to get through that work in a timely and efficient manner. And it also, boy, in some circumstances, incentivizes things like identity theft.

When I was thinking about how to make this work, again, to like how can we constrain this and be productive, especially within the context of this community, I think it's important to focus here on friction based on registrant activity on a platform. And so, that could mean things like how many domains have they purchased, how many domains have they renewed, how long have they been a customer, have they had a domain get through the ad grace period without being reported for abuse, have they had a history of abuse of domains reported.

Those things can't really be faked, because they're attributes of activity on a registrar platform. And they don't have the same issues related to identity verification about privacy that I think we all get stuck in. And so, I would want to encourage us to try and look at that sort of approach as one that could be equally or more effective and a little bit less fraught.

Next slide, please. Subdomain Abuse Contacts. We see abuse happening at subdomains. This is an idea to give registrars a mechanism, a tool to speak with registrants who have services that offer subdomains to third parties to see if we can have-- basically copy those obligations from registrars to registrants operating services that provide subdomains to third parties. There's no enforcement here, to be clear. The enforcement from Compliance would be, do you have that language in your terms of service as a registry or registrar?

There's no enforcement to make registrars suspend domain names for activity at the third level in gTLDs, because that could have immense consequences that are extremely hard to enumerate. But what we do have is a tool. We have a tool for registrars to approach services that are generating a lot of abuse at subdomains and say, hey, your domain is at risk.

Next slide, please. Registrant Recourse Mechanisms. Boy, we need to be aware that if we are addressing abuse at scale, we need to ensure that registrants who've been inappropriately impacted by this, who have had benign domain suspended, have transparent and reasonable access to recourse. And so, we thought that was an important piece to put in place here.

Next slide, please. Botnets and DGA Coordination. Currently, this is a bit messy. When LEA or national certs need to address a botnet, they have to approach registries individually. And we contemplated that ICANN could offer a centralized function here to

make that more efficient. In conversations about it, this doesn't have to be a PDP. There are other ways that we could go about getting this done. And so, I'm happy to explore that, too. It just felt like a low-frequency but high-impact change that we could make.

Next slide, please. A couple key takeaways that I've been trying to reinforce this week as I've talked about this work is that I think all of us want to move forward on this issue. We all want to make progress. In order to do that, we need to all agree about scope. We need to all agree that we can constrain the work to make incremental progress on these issues. It means, very clearly, not everyone is going to get everything they want. But if we want to make progress, we need to focus. And small wins are better than no wins.

And then, overall, I think, and I've heard it from around this room already, some real clear themes. The amendments that were put in place created clear obligations for individual abuse reports. And that's great, and we've seen improvements across the ecosystem based on that. However, it's clear also to us, especially from the data we see going through our MAP service or our NetBeacon reporter service, that abuse happens at scale. We see large campaigns of abuse. And so, how do we, as a community, move forward on addressing safely, reasonably, responsibly, abuse at scale? So, that's me. Thank you.

JONATHAN ZUCK: Thanks, Graeme. I think you've started to tread a bit into Farzi's topic, I guess, talking about remediation and things like that, but let's go ahead, Farzi, with your thoughts.

FARZANEH BADIEI: Thank you. Thank you so much for the invitation. I'm Farzaneh Badiei. I'm a member of Non-Commercial Stakeholder Groups. The NCSG cares about freedom of speech, access to knowledge, and the non-commercial domain name registrants' rights, but as well as end users and Internet users' access to knowledge and access to the Internet and human rights in general.

So first of all, let me be very clear. We do care about mitigation of DNS abuse. We think that it is necessary and it should be done. However, we do not agree with the sense of urgency that is being portrayed all the time at ICANN. When we are presented with statistics, usually those statistics are not just a crime that has happened as a direct result of DNS abuse. It can be for a range of issues that can have nothing to do with ICANN.

But mitigation of DNS abuse is very important for us because as human rights advocates and activists, some of our members could be impacted because there are phishing attacks initiated by some state actors that want their data. So, it is very important. And DNS abuse mitigation can, if we do it right, can actually enable human rights. But putting up stats up there and saying that we are assuming DNS abuse and the Internet is dying I don't think is the right approach because then we will go to hasty decisions. But I

have not heard very drastic recommendations here, which I'm very grateful for.

Whatever recommendation or solution we want to come up with, it should be within the ICANN remit and mission. And it should consider the risk to human rights. How are we affecting domain name registrants and Internet users' human rights when we are mitigating abuse? And this can happen when we are-- Civil society has come up with a range of tools that you can use for human rights impact assessments. And human rights impact assessments should not happen after the fact. It should happen while we are mitigating the DNS abuse.

My colleague has an interesting saying that says, when we focus on access to remedy, she says "before they are dead or after they are dead". I'm exaggerating, but. So, what we need to do, and Graeme also said it, like for example, when we want to come up with solution, it should never lead to identification of domain name registrants. It is of utmost importance for NCSG, also enabling and protecting human rights, that domain name registrants can keep their anonymity online. It is important for the Internet user, and it is important for the domain name registrants. Privacy matters.

And it also can have an impact on freedom of speech. When we suspend malicious domains, or like sometimes hijack domains that are being used that are compromised, when we suspend them, we could be suspending access to information and knowledge, or like some kind of campaign that is going on. Also, Mason mentioned

imposter domains. That is not DNS abuse. It will go into the territories of contents, and we are at NCSG, we want to keep DNS abuse definition technical, and as it is in the contract. And domain like the example that you gave us, it is not fake news, is not DNS abuse. And we cannot bring ICANN to have a role in that, because then it is going to be a global regulator of speech.

Yeah. I have some remarks on Graeme's recommendations. I will be brief. Thank you, Graeme. We appreciate NetBeacon's efforts in this. We have to look at your recommendations more carefully, and we have to also discuss how this can have a-- like do some kind of like human rights impact assessments on how we can actually get these recommendations implemented without impacting human rights or reducing the risk to human rights.

Like for example, from the cursory review of the Recommendation 1, sub-domain association, it can have disproportionate effect on takedown or suspension of domain and sub-domain. I don't want to say more because we want to do some kind of analysis before we actually discuss this. Yeah, I am done.

JONATHAN ZUCK Thanks, Farzi, and thanks for bringing that perspective into this. It's all about trying to find balance and making the moves that accomplish the most for the effort required, and minimize the downstream consequences, if possible. So now that a lot of people

have spoken, does anybody on the panel want to respond to anything that anyone else said? Gabriel, go ahead.

GABRIEL ANDREWS

I took a couple of notes actually, Graeme, as you were speaking, and I just wanted to share them. So, again, Gabriel Andrews, Public Safety Working Group. And if I got my numbers right, I think your number five bullet was involving a contemplation of ICANN having a role to intake botnet DGAs, and to somehow share that with the right contracted parties, along maybe even with guidance as to how best to action them. And that's something we would, of course, be happy to explore with you, with contracted parties, with whomever. So, to the extent we can be helpful, absolutely.

And then on, I think, point number two, the topic of introducing friction on API access for malicious bulk registration, I just wanted to speak on my personal capacity now. Not GAC, not even PSWG, but absolutely my knee-jerk reaction when I read that INFERMAL report and saw the 400% increase in abuse with API access, my knee-jerk reaction does go to places like know your customer policies and so forth. But I think it's important for me to take a step back, pause, and recognize that really the key thing is preventing harm.

And if there are ideas that can get to that harm prevention end of the day, I don't care if you went down path A, path B, my path, whichever, as long as that harm prevention can occur. So, then it becomes more a matter of how can we come up with those ideas

that get there and then measure it to see that it's functional. And I'd be happy to collaborate. So, thank you for those ideas, both to you and to the other Contracted Party Houses who have shared similar.

EUNICE ALEJANDRA PEREZ COELLO: Thank you. I'll speak in Spanish. My name is Eunice for the record. I've got a question about the statistics that have been shown. Now, are you also taking into account the registrants who offer domain names for dynamic IPs? Are you monitoring this? Now, I'm talking specifically about this because I have one of these services and the registrants sometimes offer those domain names. You register, you give your domain name, and then you can connect different devices. For instance, devices related to the Internet of Things.

Now, my question is the following. Is there a monitoring mechanism which exists? Or is this perhaps not considered as a real register? Are we also taking into account as final users the fact that we don't always have the knowledge that we have to put in place safety or security measures using these types of services because they are generating vulnerabilities? That's my question. Thank you.

JONATHAN ZUCK: I don't know who would like to address that. Go ahead, Graeme.

GRAEME BUNTON

Thank you for the question. I think I can tackle a piece of that because I think the subdomain service provider is coming from our white paper. Part of the thinking behind that potential work was about addressing services that offer subdomains specifically, but for that sort of dynamic DNS piece. I wish I had a better example for this community, and Brian, feel free to correct me if I'm wrong here. Sorry, I say better because it comes from .org, who is our parent organization. I like to be a bit more neutral than that.

But I think it was something like 40% of the abuse in .org, and I'm looking to Brian, thank you, was from a single subdomain service provider. So, a single domain name on 11-point-something million was responsible for 40% of the abusive URLs that they saw. And that is not unique to .org. It's common across other TLDs where you have services offering subdomains that generate abuse. And so, how do we begin to ensure some responsibility there? And this was an attempt at that.

And I actually acknowledge there was a conversation with Michele Neylon, who I can see at the table, who was like and I'm paraphrasing Michele, and I can see a scowl, so feel free to correct me. But the sentiment was this, that if you're operating a service on the internet that is used by third parties, it's going to inevitably be abused in some fashion.

And so, like a basic requirement of offering a service that third parties use online is that you have and maintain an abuse contact and have abuse processes. It doesn't matter if it's subdomains. It

doesn't matter if it's URLs. It doesn't matter if it's a forum. People will abuse things if we make it available. And so, this was an attempt at providing some responsibility there to see if we can move that obligation in a reasonable way to people offering those services.

To your second piece about security and botnets and when you're using those services, does it provide a gate, like a punch through your network, might expose your IoT devices that haven't been patched to vulnerabilities. I think that's sort of outside the scope of our work here. It's certainly outside the scope of my thinking on this particular issue. Thank you.

EUNICE ALEJANDRA PEREZ COELLO: Thank you for your response. I have another question in Spanish, please.

ALAN WOODS: Thank you very much. My name is Alan Woods, ex-registries, but now I'm the chief legal officer of a company called CleanDNS. And I think as I'm listening to an awful lot of this conversation, it's probably good to have a point of view of a person who is kind of in between the registries and what people see from the outside. And we're looking at the effects and the measurements of what has happened, for instance, in the DNS abuse amendments, and how can we use what we've learned so far in order to apply that to the next steps in DNS abuse.

And I think, Farzi, you actually put it perfectly. There's been a lot of statistics. And when we look at this problem, we always look first to the statistics. And even this week alone, we've seen some very, very, very, very stark statistics being presented showing the scale of the issue. And when we lead with stark statistics showing scale of issue, we tend to jump to conclusions, and the community tends to put an awful lot of effort and emphasis on the role of the registry and the registrar in preventing that.

So, there was one presentation that showed a list of registrars who were used for bulk registration, specifically. And in that, they pointed out a registrar called the Registrar of Last Resort. That is a registrar which, by definition, any registration in there is mitigated. It is there for the purposes of monitoring, being sinkholed for DGAs. And yet, that was being used as saying 7,000 bulk registrations in this particular instance were used. Therefore, it's really bad. If you were to take down those domains, you're going to interrupt law enforcement actions. So, you need to be careful on that.

Another thing I would like to point out about is the sources that people are using. Again, as a company, we use over 60 sources for our registrants. There is a lot of noise, an awful lot of noise. And our basic premise when we're taking action for a lot of our registry and registrar clients is the proper action, the appropriate action by the appropriate party at the appropriate time where there is evidence. So, it is an evidence-based escalation.

And I can say in one of the sources that is majorly used, we did a six-month review of, and I'm not going to name names, but please feel free to talk to me, over 220,000 reports came in from one reporter for three clients. And out of that, less than 1% of them had evidence that was enough to escalate, to justify even sending an email to say, hey, look at this. And so, to come to a point, the point is, as we're looking into the next steps, as we're looking into the next stages of dealing with these very specific and focused PDPs, absolutely. Let's focus on making sure that we are not using the alarmist, that we are looking at sources, that we are measuring the appropriate action by registries and registrars.

And I will leave with this, that there is one registry operator that has been in the news an awful lot for actions that have been taken because of the DNS abuse amendments. We need to be very careful that we're not just taking blacklists and taking them down en masse. There still needs to be a level of review, validation, and verification of those reports. Because just taking things down because they're on a blacklist is just as bad as not taking any action at all on this. We need to be calm, cool, and collected in how we approach. And I impress on people, this is not all on the heads and the shoulders of the registries and the registrars. It's on the entire ecosystem to work together, not just what we can agree here at the ICANN table. Thank you.

JONATHAN ZUCK All right. I think we have the name of our next session, DNS Abuse, Calm, Cool, and Collected. So, we'll keep that as an ongoing mantra. Farzi, I see your hand up.

FARZANEH BADIEI Yes, thank you. I just wanted to agree with everything that Alan said. So, the mere fact of existence of a phishing link doesn't mean that harm has already happened. And I think this is missing in our conversations. So, the number of reports and the number of phishing links, yes, of course, it's higher risk, but the terms that we use is important. Harm hasn't occurred yet if the phishing link has not been used by the internet user. And I think that when we are alarmist about things, then our solutions can be very blunt and not human rights respecting. So, I think your next session should be a rights-respecting DNS abuse mitigation.

JONATHAN ZUCK Well, we'll certainly take that into consideration. I mean, the flip side of this, I think, Gabriel might be able to shed some light, is that we do know that there's a lot of harm, too. We do know a lot of money is being lost by people, entire savings and things like that, and so there's something to be alarmed about. We shouldn't be, obviously, ham-fisted or too blunt in the way that we react to it, but I think we can't forget the real harms that are taking place. Michele, I see your hand, thank you.

MICHELE NEYLON

Thanks, Jonathan. Michele for the record. I think just picking up a little bit on what Farzi was just saying, and stuff that Alan was saying as well, the thing is that those of us who engage here at ICANN, I think, for the most part, most of us want a secure, stable, usable internet. We want one where there is a balance across the ecosystem so that you can have the good, and you can accept the fact that there is going to be a certain amount of bad as well.

I think the problem we've seen over the last couple of years is that the focus has become let's chase DNS abuse, let's chase more DNS abuse, and if the only tool you have is a hammer, everything is a nail. There needs to be a pivot and a switch in the approach and mentality of these discussions, because yes, bad stuff happens, yes, there's romance fraud, there's all sorts of different things out there that happen that impact my clients, my family, my friends, my enemies. There's lots of nasty stuff that happens out there.

We need to be looking at it in terms of how do we improve the overall experience rather than simply looking constantly for abuse. Because the problem is, if you are constantly looking for abuse and not looking at it from the perspective of how to improve the overall experience, then it's like everything becomes a jail cell, everything becomes a way of executing a criminal or something like that, rather than how do I make it so that they're sitting more comfortably, that they're having a better experience.

Now, I don't know if you understand exactly what I'm getting at, Jonathan, but the idea is just to pivot that around, because if users

move from using domains to platforms and apps, you've lost the room, it's gone. You've lost any control over that whatsoever. There's no way to track it, there's no way to see it, and we're done. We can just actually just throw in the towel. That's probably not what a lot of us would like, but I think many of us have seen how the internet has brought many wonderful things. I look at small businesses that are able to exist now because of the internet that couldn't have existed five years, couldn't have existed 10 years ago. But if all we're doing is constantly making it harder and harder for people to get online and to use the internet, then they're just going to stop using it that way. Thanks.

JONATHAN ZUCK

Thanks, Michele. I think that's a fair point. I think it'll be a question of what that really looks like, because obviously we're looking at trying to get to markets that haven't been opened yet, etc., and a large part of that. For example, the African delegation to ICANN, which is AFRALO and African representatives, they covered DNS abuse, and that's simultaneously a target market for growth for the continent of Africa at the same time, and it's also where some of the largest problems are in terms of trust in the internet infrastructure. And so, we have to make sure that we're not creating an environment conducive to people switching over and away from the domain name system, because they feel--

So, it sort of cuts both ways, and I don't know the best way to-- I think we're trying to have a balanced conversation about it. At the

same time, there are conversations that have gone on for a very, very long time that I think people feel like they need to keep bringing them up, because they don't seem to be going anywhere, I guess, if that makes sense. I think it's going to take more fluidity on both sides of this equation, I don't want to call them sides, in order for that utopia that you're describing to be the basis going forward. Because part of my enjoyment as an end user, there's registrants, but the majority of people we're talking about are people that are just trying to use the internet, and their enjoyment is suffering at the moment, yeah.

MICHELE NEYLON Just very briefly, Jonathan. Michele, again. I think this is the key thing. if you're looking at it from the user perspective, if getting online is really, really, really hard, which it can be.

JONATHAN ZUCK By getting online, you mean having a domain name?

MICHELE NEYLON No, I don't mean that, I didn't say that. No, getting online. Getting online, if that becomes really, really hard, which it can do in some places, and a lot of you, I'm sure, have traveled to some of these countries where to even get onto the Wi-Fi in a hotel or an airport, you have to give up a huge amount of personal information. If you make it harder, you get a lot of pushback. We hear this almost every single day. why are you asking me for this? Why do I have to give

you that? I already gave you this, now you're looking for something else. That's putting barriers in the way.

Now, that doesn't mean that it's a free-for-all. it's trying to find a reasonable balance. Balancing between protecting the users, because users are, much as we love them, they don't know what they're doing a lot of the time, and balancing that against making sure that they're not subject to criminal activity. But it's not a simple case of just focusing constantly on arresting people and looking for abuse on this and that. It's like it should be looking at getting that balance right. It's not easy. If it was easy, a lot of us would be out of a job, probably.

JONATHAN ZUCK: Thanks, Michele. I've got James Galvin next to the queue. Are you at the table, or do you need a room?

JAMES GALVIN: Thank you, Jonathan. Yes, James Galvin, SSAC's liaison to the ICANN Board. Building on what Michele just said, you called it, or seemed to suggest it, maybe that's a utopian kind of environment, a place to get to. But what occurred to me was what Michele's talking about could very well be an element of the safer cyber campaign that ALAC and SSAC are attempting to work on together that we're trying to develop. And I just wanted to put that out there as something to take forward for another discussion elsewhere. Thanks.

JONATHAN ZUCK Good reminder, James. Thank you. The other piece of this is the users, yeah. Who is it? Oh, Gabriel.

GABRIEL ANDREWS Hi. Gabriel, again. And I think I want to respond to Michele and Farzaneh both and say that without being at all alarmist, the point of view that we can bring here as public safety officials is just the view that we have, right?

And so, the numbers are the numbers, but if I can offer an olive branch, the message I'd really like to leave with is that some of the ideas that have been proposed here that seem like really potentially productive things we can work on together, the message I really would like to leave with is that those seem like they are directly addressing some of these harms that I'm really hoping that we can productively address and reduce the amount of harm that are being done to not just our customers, but our friends and family around the world.

So, I think that there is productive avenue for collaboration here. And I think that that is something to really take a moment and recognize. And that's all I wanted to say.

JONATHAN ZUCK Thanks, Gabriel. Eunice.

EUNICE ALEJANDRA PEREZ COELLO: Thank you. I will speak again in Spanish. Thank you. I think this session is really interesting. And the issue you've just mentioned about human rights, I think it involves a large part of education, education to the end-users. We are looking to find ways to resolve or mitigate these vulnerabilities or these attacks that we see. And we are not really thinking about a way to raise awareness in the end-users because in the end, they are using technologies that maybe they don't know that there are certain vulnerabilities that may appear there, may emerge there.

I think the fact that the SSAC group can work together with the ALAC to manage this awareness raising and training the end-users, this is one of the ways that can help us reduce these attacks or the statistics that we have about this. It is actually training the end-user that is a person that is actually using the resource. Thank you.

JONATHAN ZUCK: Yeah, and we're definitely trying to do that. So, it's a multi-faceted discussion. Claire. Oh, Reg. Sorry.

REG LEVY: Thank you, Eunice. And I think that you really raise an important issue because a lot of what we do here at ICANN is very high level and doesn't speak directly to the issues that an internet user has. The things that you're talking about with regard to the internet of things, accessing the internet and the vulnerabilities implicit in

situations where the device you have has an admin password and you connect it to your home Wi-Fi and now that is a direct way into your bank account and all these other things that you don't understand, right?

I've had to educate my husband about how we need to have three Wi-Fi networks at home. One is invisible and that's what we use, and one is for guests, and one is for all of our internet junk. And that took a long time. But unfortunately, that's not something that we can deal with necessarily here at ICANN. Here at ICANN, we have a very specific and as I said, specialized remit that operates at a level that the end user simply doesn't understand. They have no idea what it is that we do in this room. And I look forward to solutions to those problems but I don't know how we can help here today, unfortunately.

JONATHAN ZUCK: Thanks, Reg. Amrita? Oh, okay. Claire? We can't tell anymore who's first.

CLAIRE CRAIG: Okay, hi. Hi, I'm Claire Craig, one of the vice chairs of ALAC. Thanks for this conversation. This is more of a comment than a question. I really appreciate hearing the different perspectives from the different groups in the room. But what I wanted to say at this point is that one of the things that we in the At-Large community are really concerned about would be the interest of the end users. And

as a result of that, I think we need to have a more balanced approach when it comes to how our end users are affected when they access the internet and what are some of the things that occur, particularly in some of the underserved and developing regions.

Because while I hear the conversation about the registries and the registrars and how difficult it may be for some of them, I think I really liked the presentation by the Public Safety Group because they spoke to some of the real threats, as well as NetBeacon, some of the real threats that are out there concerning end users. So, I really think that that's the thing that we at ALAC and At-Large bring to the table are some of these threats. And one of the things that we try to do at the RALO level is really do some of the education that you're talking about. But we need to work with the other communities to ensure that our end users get the kind of support that they need. Thank you.

JONATHAN ZUCK Thanks Claire. Amrita.

AMRITA CHOUDHURY Thank you, Jonathan. Amrita for the record. Looking at the question, what do we agree on? We want the internet to be open, be used by all in a safe manner. We want to protect end users and we want to protect their rights as well as their rights when they are abused to get remedies. So, I think these are certain commonalities we agree upon. We also agree that innovation

should be allowed. So, these are certain broader things, but we also see abuse happening. So, what do we do?

Now many of the abuse which is happening on the domain is typically not domain name issues but content level issues. But if you go to the global the people outside this meeting, they would not understand. So, you have to clearly-- You can't say this is not my business but I give the business. So how do you simplify things? How do you differentiate and say this is my responsibility and I do this, this, this? So perhaps domain name abuse, whatever processes are being laid can be articulated, they can be improved.

No one is saying we do not want to improve. We want to be rights-respecting. We want to be privacy-respecting. Simultaneously, we also want to educate mass and improve even from registries and registrars what has to be done. I think those needs to be clearly articulated on what is being done so that even law enforcement, if they go and see it, they know this is what is being done. This is not being done or this is going to be done. As in we are not perfect, right? We should have certain things, just saying not happening or we will not, it doesn't work.

And obviously there are abusers whom I'm sure those who are tracking know that there are particular places from which or some domains from which the abuse normally happens. What is being done there? As in there are trends. I'm sure you know more than me about how the trends happen or who are the ones who are

abusing it. So, I think those are things which needs to be worked on.

And, Farzi, as you said, the rights of users need to be protected, even rights of people who are being abused because when we are looking into markets which are not that educated, and I come from that kind of a region wherein you have mass people coming into the internet, they don't know what to do. They really don't know whom they need to actually get in touch. And even if they reach out to their registrars for certain things, they don't get recourses. Then what? Are we not stopping them from enjoying the internet the way they do?

So, there are other issues. It's a huge issue. I don't think we would be able to solve it. It's something like world peace. But at least we need to be open to this discussion and see if we are doing something, how do we make it easy for others even in the ICANN ecosystem to know, yes, this has happened or this is being done, so that that feeling is not there that nothing is being done. And yes, sometimes issues are magnified. If there are 10, it is made 100, but even that 10, a 1 out of 10 may have a huge impact. So, we need to look at impacts, not the numbers, that how is it hitting someone or what is the impact. So, it's not the numbers which count, it is the impact of that abuse or whatever you term it. Thank you.

JONATHAN ZUCK Thanks, Amrita. And I've been asked to remind everyone to speak slowly for interpreters as well. Not naming any names, Amrita.

Okay. And really, it's Gabriel I'm focused on. Gabriel, try to keep your pace down so that the interpreters can-- You're the next in the queue. That's why I'm picking on you.

GABRIEL ANDREWS I think if I was next in the queue, it was an old hand, so I'm taking it easy on them.

JONATHAN ZUCK Okay. Then Tijani is next.

TIJANI BEN JEMAA Thank you very much. First of all, a big thank you to NetBeacon for the work they are doing. I really appreciate it. I think the key word here is the balance. Yes, abusers need DNS abuse mitigation because this protects their rights as users, as Farzi stressed, but not every and any DNS abuse notification should lead to an action. The verification of this notification is, I think, the main node in the DNS abuse mitigation chain. We need to know, not to know, but we need to make this node very efficient. We don't want to see an abuse of the DNS abuse mitigation. So, the balance is the main, I think, the key word here that we have to take into account. Thank you.

JONATHAN ZUCK I think on that we agree. Farzi.

FARZANEH BADIEI

Yes, there are many agreements, but I think that it's more of an alignment than balance. Privacy, freedom of expression, security, they also can create safe environment for the end user to operate and have access. And yes, there is, and as I said, mitigation of DNS abuse is very important for us. And I think that it's not just the end user's safety that is at stake. As I said, it's also the end user's human rights that is at stake when we do DNS abuse mitigation that can hamper their access to a website that they want to have access to knowledge and information about something.

So, these are the things that when we talk about end users, and as I said, NCSG cares deeply about end users. We are not only talking about the domain name registrants here. All of this I said to say that DNS abuse is just not at a level that makes accessing the internet impossible. I'm not saying anybody argued that, but our policies and what we come up with could have an impact on making maintaining domain names so difficult that everybody's going to move to platforms. And then, on the other hand, there are people that say, oh, why is there social media concentration? And why is there big tech? Well, why? Because we made it so difficult for people to have their websites and run it on their own.

JONATHAN ZUCK

Thanks, Farzi. I guess, again, I don't get the impression that we're moving too quickly on this area. The contract amendments that we recently had enacted were first suggested by the head of Contract

Compliance 16 years ago. I don't know that we're so massively, as a community, overreacting to the statistics or numbers. We do talk about it a lot, and maybe that gets to be annoying over time, but it's hard for me to imagine that we've, among our ICANN community, created an environment that's tipped the balance too far in the wrong direction, at least at this point.

So, I guess I push back on that a little bit, just because things don't move so quickly here in ICANN that there's so much danger of a complete overcorrection. I could be wrong, but that hasn't been my impression. Hadia? Hadia. And then I also wanted to say, there's a roving mic, so if there's people in the audience that want to make a statement or ask a question, we can come to you with a microphone. But, Hadia, now you're up next.

HADIA ELMINIAWI: Thank you. This is Hadia, for the record. So, I hope we all agree or I think we all agree that end users, safety, security, and privacy are all equally important. If we actually agree on that, then what we need, and I take from your words, Farzi, what we need is an aligned approach and an aligned approach that considers all those three factors. Thank you.

JONATHAN ZUCK: Greg Shatan

GREG SHATAN

Thank you. Greg Shatan for the record. I think we have to obviously avoid being alarmist on both sides of the issue. We don't want an internet where it's impossible to get on, but we also don't want an internet that's impossibly unsafe once you get there. We want a neighborhood that's both safe and easy to operate in. I'm hopeful that's not an impossible balance, but that really is the balance I think we need to achieve. Ease of use without necessarily, the same kind of ease of abuse is a goal. If we make one thing too paramount, other things, other prongs will suffer.

I think we need to watch out for the idea that, I guess the latest bugbear, or maybe it's not a very new one, is everyone's going to go to platforms. I think that there's always going to be reasons to be on the internet, but one reason not to be on it is if your risk of getting scammed, or spammed, or hijacked is not vanishingly small. Hopefully we will continue to work for balance, thank you.

JONATHAN ZUCK

Is there anybody else in the room? Okay. Well, it's not like we need to press into lunch or anything like that. This has been a very dynamic and fruitful conversation, and mostly cool, calm, and collected as Gabriel preached, so I appreciate that. Say that again? Oh Justine, did you want to say something at the end? Sorry.

JUSTINE CHEW

Well, since we have time. This is Justine for direct. So, if you see the agenda, I'm supposed to give a five-minute summation. I have

to confess that because the discussion has been so rich, I've just stopped taking notes. So, I can regurgitate a few things that I heard. There needs to be balance, definitely. Perhaps also communication. I think a bit of what the contracted parties may already be doing is not necessarily well known, so I think communication would help.

And from the perspective of end users, or at least At-Large in the ALAC, we are all always not pressing things to the point of being unreasonable. I mean that's why we are all here at this table, and this is a multistakeholder conversation. And from the perspective of DNS abuse policy, we are always talking about seeing what the good registries and registrars are doing, and whether those things can be transferred into policy so they become mandatory for everyone in the ecosystem. It's not just the good people doing the good things, and the bad people are still doing all the bad things.

So, I think we are all coming to that conclusion. Just some of us are like, because we do what we do, and you know. Anyway. So, I think it's all good, it's all good. Thanks for the suggestions on the next session's name and the topic, we'll take that into consideration. Yeah, we always end up with long names. But I'd just like to thank personally the panelists who have agreed to come and speak to us, and also all of you who have been contributing to this very rich discussion. Thank you.

JONATHAN ZUCK Enjoy your lunch.

[END OF TRANSCRIPTION]